COMUNE DI GENOVA

DIREZIONE GENERALE

DETERMINAZIONE DIRIGENZIALE

ATTO N. DD 5734

ADOTTATO IL 09/10/2024

ESECUTIVO DAL 09/10/2024

OGGETTO: Adozione Modello organizzativo e data breach

IL DIRETTORE GENERALE

Premesso che:

- la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale sancito a Livello europeo dalla Carta dei diritti fondamentali dell'Unione Europea e trattato sul funzionamento dell'Unione Europea ("TFUE")

- il Comune di Genova, in quanto Titolare del trattamento, è tenuto a mantenere sicuri i dati personali trattati nell'ambito delle proprie attività istituzionali e ad agire senza ingiustificato ritardo in caso di violazione dei dati stessi (*data breach*), incluse eventuali notifiche all'Autorità di controllo competente ed eventuali comunicazioni agli interessati;

Visto:
- il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati di seguito "Regolamento");
- il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali, così come modificato dal decreto legislativo 10 agosto 2018, n. 101, recante «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE» (di seguito "Codice");
- il decreto legislativo 18 maggio 2018, n. 51, recante Attuazione della direttiva (UE) 2016/680 del

Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (di seguito "d.lgs. n. 51/2018");

- le Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679 (WP250);
- *la Opinion 5/2019 on the interplay between the ePrivacy Directive and the RGPD, in particular regarding the competence, tasks and powers of data protection authorities*, adottata ai sensi dell'art. 64 del Regolamento, dal Comitato europeo per la protezione dei dati in data 12 marzo 2019;
- il Provvedimento del Garante sulla notifica delle violazioni dei dati personali (*data breach*) - 30 luglio 2019 [doc-web n. 9126951]

Rilevato che le norme introdotte dal GDPR si traducono in obblighi organizzativi, documentali e tecnici che tutti i Titolari del trattamento dei dati personali devono considerare e tenere presenti per consentire la piena e consapevole applicazione del nuovo quadro normativo;

Considerato pertanto opportuno adottare un "Modello organizzativo e di gestione" per la protezione dei dati personali, che comprenda il complesso di attività organizzative, ruoli, azioni e sistemi dell'Ente, disciplinandoli e organizzandoli al fine della migliore applicazione della normativa sul trattamento di dati personali.

Considerato altresì che per gestire le eventuali violazioni dei dati personali, che comportano obblighi comunicazione in capo al titolare del trattamento, è opportuno predisporre una procedura organizzativa interna che riguardi tutte le violazioni concrete, potenziali o sospette di dati personali, adempiendo agli obblighi di legge ed evitando rischi per i diritti dell'interessato e danni economici per l'Ente;

Visti inoltre:

- la procedura di segnalazione suggerita dal Responsabile della protezione dei dati del Comune di Genova con comunicazione n. 6, prot. 257199 del 24/07/2018;

- la comunicazione integrativa del Responsabile della protezione dei dati del Comune di Genova con comunicazione n. 19, prot. 0367452 del 22/10/2019;

- il provvedimento del Sindaco numero ORD-2023-239 in data 06/06/2023 con il quale è stato designato l'avv. Massimo Ramello quale Responsabile della Protezione dei Dati Personali (DPO), nel rispetto della vigente normativa;

DISPONE

1) di approvare l'allegato A, Modello Organizzativo, contenente le disposizioni a carattere organizzativo necessarie ed opportune a consentire la corretta applicazione della normativa, comunitaria e nazionale, in tema di protezione delle persone fisiche con riguardo al trattamento dei

dati personali.

2) di approvare altresì l'allegato B, Procedura nel caso di violazione dei dati personali (*data breach)* in sostituzione delle precedenti in uso presso il Comune di Genova;

3) di dare mandato agli Uffici della Direzione Generale di assicurare la massima diffusione presso tutto il personale operante presso il Comune e presso tutti i soggetti esterni alla struttura organizzativa comunale, qualificabili come Contitolari o Responsabili del trattamento.

La presente determinazione è pubblicata sulla pagina amministrazione trasparente del Comune di Genova, sezione Atti Generali.

Il Direttore Generale

Dott.ssa Concetta Orlando

COMUNE DI GENOVA

PIANO DI PROTEZIONE E MODELLO ORGANIZZATIVO A TUTELA DEI DATI PERSONALI

Sommario

PREMESSA

Il 25 maggio 2018 è divenuto ufficialmente operativo il nuovo Regolamento generale in materia di Protezione dei Dati personali. Il GDPR, acronimo (in lingua inglese) di "*General Data Protection Regulation*" (in italiano, RGPD) va ad abrogare, dopo oltre un ventennio, la cosiddetta direttiva madre n. 95/46/C, che, fino ad oggi, costituiva il quadro normativo di riferimento a livello europeo. Il nuovo Regolamento costituisce, insieme alla Direttiva (UE) n. 2016/680, il "Pacchetto di protezione dei dati" elaborato ed approvato dall'Unione Europea. Il Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 fa riferimento a dati concernenti persone identificate o identificabili in possesso di vari soggetti e quindi anche della Pubblica amministrazione utilizzabili per le proprie finalità istituzionali. Dati che devono essere trattati nei limiti delle funzioni e servizi del Comune di Genova, il quale avrà anche l'obbligo di proteggerli con nuovi strumenti.

Il trattamento dei dati personali avviene secondo le norme contenute nel **RGPD** nonché nel Decreto Legislativo 30 giugno 2003 (di seguito, per brevità "**Codice privacy**"), così come modificato dal D.Lgs. 10 agosto 2018, n. 101 recante "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*"

Il nuovo apparato normativo si regge su di un nuovo principio di fondamentale importanza: la responsabilizzazione, ovvero il principio di accountability (nell'accezione inglese).

Tale concetto rappresenta un'assoluta novità nel campo della protezione dei dati personali, in quanto il titolare del trattamento, oltre ad avere l'esclusiva competenza per il rispetto dei principi e delle regole previste dal RGPD, deve anche essere in grado di comprovarne il corretto adempimento.

Ai titolari, altresì, viene affidato il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri indicati dal regolamento.

Come specifica chiaramente l'art. 25 del RGPD, uno di quei criteri è sicuramente rappresentato dall'espressione anglofona "*data protection by default and by design*" ossia dalla necessità di configurare il trattamento prevedendo dall'inizio, ovvero fin dalla fase di progettazione, le garanzie indispensabili "*al fine di soddisfare i requisiti*" del regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

Spetta dunque al titolare mettere in atto una serie di misure tecniche ed organizzative adeguate, per garantire che siano trattati, per impostazione predefinita, solo i dati personali strettamente necessari per ogni specifica finalità del trattamento.

Tra le nuove attività previste dal RGPD, riguardo agli obblighi dei titolari, saranno fondamentali quelle relative alla valutazione del rischio inerente il trattamento. Quest'ultimo è da intendersi come rischio da impatti negativi sulle libertà e sui diritti degli interessati; tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione, tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per diminuirne l'impatto.

Una lettura organica e sistematica del Regolamento europeo consente di affermare che, data l'importanza della normativa e di ciò che essa mira a proteggere, la migliore risposta in termini di cambiamento organizzativo sia quella di realizzare un complessivo "Modello organizzativo e di gestione" per la protezione dei dati personali, considerando come tale un complesso di attività organizzativa, di ruoli, di azioni e di sistemi, mirato al fine dell'applicazione "ordinata" e completa, nell'azione amministrativa del Comune, della normativa sui trattamenti di dati personali. Tale logica di costruzione di un modello ad hoc è, peraltro, simile a quella risultante, in materia di prevenzione della corruzione.

L'adeguamento al Regolamento UE 2016/679 impone al Titolare di trattamento pubblico di prestare grande attenzione al fattore organizzativo. Per questo, l'approvando Modello organizzativo individua le politiche, gli obiettivi strategici e gli standard di sicurezza per garantire la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati personali, definendo il quadro delle misure di sicurezza informatiche, logiche, logistiche, fisiche, organizzative e procedurali da adottare e da applicare per attenuare e, ove possibile, eliminare il rischio di violazione dei dati derivante dal trattamento.

Al fine di garantire la migliore e più puntuale attuazione del principio di accountability, il presente Modello contiene disposizioni organizzative minime, la cui concreta attuazione è demandata alla struttura organizzativa operante all'interno del Comune, nelle sue articolazioni gerarchiche.

E' ammesso ed anzi incoraggiato l'utilizzo di modulistica differente rispetto a quella allegata al presente Modello, a condizione che essa ne rispetti i criteri e le regole generali.

Il presente Modello organizzativo sarà sottoposto a revisione ogni qualvolta si renderà necessario e, comunque, a cadenza almeno annuale.

PARTE I - NORME E PRINCIPI GENERALI

Il Comune di Genova assicura che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale ed al diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o della loro residenza. In attuazione del suddetto principio il Comune assicura che, nello svolgimento dei compiti e funzioni istituzionali, i dati personali siano trattati nel rispetto della legislazione vigente oltre che dei seguenti principi:
a) «*liceità, correttezza e trasparenza*»: i dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
b) «*limitazione delle finalità*»: i dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'art. 89, paragrafo 1 del RGDP, considerato incompatibile con le finalità iniziali;
c) «*minimizzazione dei dati*»: i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
d) «*necessità*»: è ridotta al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità possano essere perseguite mediante dati anonimi o con l'uso di opportune modalità che permettono di identificare l'interessato solo un caso di necessità;
e) «*esattezza*»: i dati personali sono esatti e, se necessario, aggiornati; sono adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
f) «*limitazione della conservazione*»: i dati personali sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'art. 89, paragrafo 1 del RGPD, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste a tutela dei diritti e delle libertà dell'interessato;
g) «*integrità e riservatezza*»: i dati personali sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;
h) «*responsabilizzazione*»: il titolare del trattamento è competente per il rispetto dei principi di cui al comma 1 dell'articolo 5 del RGPD e deve essere in grado di comprovarlo.

La presente disciplina si applica a tutti i dipendenti e collaboratori del Comune, individuati quali soggetti designati ed autorizzati ai sensi dell'articolo 2-quaterdecies del Codice privacy, nonché ai responsabili del trattamento ai sensi dell'articolo 28 del RGPD.

Il rispetto delle presenti disposizioni è obbligatorio per tutti i soggetti sopra richiamati e la mancata conformità alle regole di comportamento previste dallo stesso potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero l'applicazione di sanzioni o penali nei confronti delle terze parti inadempienti, secondo le normative vigenti in materia.

Il presente Modello organizzativo è sottoposto a costante monitoraggio da parte del RPD e revisione annuale a cura della Direzione Generale, anche su proposta del RPD, allo scopo di intervenire rapidamente con aggiornamenti specifici nel caso di modifiche normative od a seguito dell'evoluzione tecnologica o dell'opportunità di introdurre nuove e più efficaci politiche di gestione dei dati personali.

Il Comune di Genova si impegna ad inserire, all'interno degli strumenti di programmazione e pianificazione previsti dalla legge, l'indicazione specifica delle specifiche misure ed iniziative volte ad attuare i principi di protezione dei dati personali.

I.1. SENSIBILIZZAZIONE E FORMAZIONE

Dall'esame della materia emerge come sia, oramai, imprescindibile un cambiamento di mentalità che porti alla piena tutela della privacy, da considerare non solo come un oneroso rispetto di adempimenti burocratici, ma, soprattutto, come garanzia, per il cittadino che si rivolge alle pubbliche amministrazioni, di una riservatezza totale dal punto di vista reale e sostanziale.

Ai fini della corretta e puntuale applicazione della disciplina relativa ai principi, alla liceità del trattamento, al consenso, all'informativa e, più in generale, alla protezione dei dati personali, il Comune di Genova sostiene e promuove, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione che possa consolidare la consapevolezza del valore della protezione dei dati, e migliorare la qualità del servizio.

A tale riguardo, il Comune di Genova riconosce che uno degli strumenti essenziali di sensibilizzazione sia rappresentato dall'attività formativa del personale.

Per garantire la conoscenza capillare delle disposizioni normative vigenti, al momento dell'ingresso in servizio, è data ad ogni dipendente o collaboratore una specifica comunicazione, con apposita clausola inserita nel contratto di lavoro, contenente il richiamo ai principi ed alle norme di cui al presente Modello organizzativo, oltre che alle vigenti disposizioni nazionali e comunitarie.

Il Comune di Genova organizza, nell'ambito della formazione continua e obbligatoria del personale, specifici interventi di formazione e di aggiornamento in materia di protezione dei dati personali, finalizzati alla conoscenza delle norme, alla prevenzione di fenomeni di abuso e illegalità nell'attuazione della normativa, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza delle misure di sicurezza per il trattamento e la conservazione dei dati, dei rischi individuati e dei modi per prevenire danni agli interessati.

La formazione in materia di prevenzione dei rischi di violazione dei dati personali viene integrata e coordinata con la formazione in materia di trasparenza e di accesso, con particolare riguardo ai rapporti tra protezione dei dati personali, trasparenza, accesso ai documenti amministrativi e accesso civico, semplice e generalizzato, nei diversi ambiti in cui opera il Comune.

I.2. TRATTAMENTO DEI DATI PERSONALI

Il Comune di Genova tratta i dati personali necessari per lo svolgimento delle proprie finalità istituzionali e per l'erogazione dei servizi di propria competenza, quali identificati da disposizioni di legge, statutarie e regolamentari e nel rispetto dei limiti imposti dalla vigente normativa in materia di protezione dei dati personali e dai provvedimenti delle Autorità di controllo.

Le operazioni di trattamento possono avvenire esclusivamente ad opera dei soggetti all'uopo individuati, designati ed autorizzati secondo quanto previsto infra nel presente documento. Non è consentito il trattamento da parte di persone non puntualmente autorizzate ed istruite in tal senso.

Al fine di garantire la correttezza delle operazioni di trattamento il Comune provvede alla ricognizione di tutti i trattamenti di dati personali effettuati nell'ambito dei processi e procedimenti svolti, finalizzata alla compilazione ed aggiornamento del Registro delle attività di trattamento di cui all'articolo 30 del RGPD.

I.2.1. Tipologie di dati trattati

Nell'ambito delle operazioni di trattamento conseguenti all'esercizio delle proprie funzioni istituzionali il Comune, tratta in modo anche automatizzato, totalmente o parzialmente, le seguenti tipologie di dati:

- dati personali, quali definiti all'articolo 4, paragrafo 1 del RGPD;
- categorie particolari di dati personali di cui all'articolo 9, paragrafo 1 del RGPD (c.d. dati sensibili);
- categorie particolari di dati personali di cui all'articolo 2-septies del D.Lgs. 196/2003 (c.d. dati super-sensibili);
- dati personali relativi a condanne penali e reati di cui all'articolo 10 del RGPD (c.d. dati giudiziari)

I.2.2. Finalità del trattamento

Il Comune di Genova effettua periodicamente una ricognizione delle finalità che impongono o consentono il trattamento dei dati personali, anche sensibili (e super-sensibili) e giudiziari.

Il Comune rende disponibile attraverso il proprio sito web istituzionale una pagina contenente le informazioni sul trattamento dei dati personali ad opera dei propri uffici e servizi, conformemente a quanto previsto dagli articoli 13 e 14 del RGPD.

I.2.3. Liceità del trattamento

Il Comune di Genova garantisce che il trattamento dei dati personali avvenga nel rispetto delle condizioni di liceità previsti dalle seguenti disposizioni:

1) articolo 6 del RGPD e 2-ter del Codice privacy;
2) articolo 9 del RGPD, 2-sexies e 2-septies del Codice privacy, in relazione al trattamento delle categorie particolari di dati personali (c.d. dati sensibili e super-sensibili);
3) articolo 10 del RGPD e 2-octies del Codice privacy, in relazione al trattamento dei dati personali relativi a condanne penali e reati

Nel rendere all'interessato le informazioni di cui agli articoli 13 e 14 del RGPD, il Comune presta particolare attenzione all'individuazione ed alla illustrazione delle condizioni che legittimano il trattamento.

I.3. CIRCOLAZIONE DEI DATI PERSONALI

Fatto salvo il rispetto di specifiche e puntuali disposizioni normative che lo vietino, Il Comune favorisce la circolazione all'interno dei propri uffici dei dati personali degli interessati il cui trattamento sia necessario ai sensi degli articoli 6, 9 e 10 del RGPD.

La circolazione, ove possibile, è assicurata mediante l'accessibilità diretta delle banche dati informative detenute da ciascun ufficio, previa creazione di appositi profili di utenza che tengano conto dei profili di autorizzazione conferiti.

Forme similari di accessibilità sono garantite in favore di contitolari e responsabili del trattamento, limitatamente ai dati personali diversi da quelli contemplati dagli articoli 9 e 10 del RGPD.

I.4. COORDINAMENTO DI NORME

Il Comune di Genova intende perseguire l'obiettivo di assicurare le forme più estese di accessibilità e trasparenza sul proprio operato, ad opera dei cittadini, nelle varie forme in cui è prevista la pubblicazione di atti, documenti ed informazioni ed è riconosciuto il diritto di accesso, quali (a titolo esemplificativo) quella prevista dal TUEL (D.Lgs. 267/2000) negli articoli 10 e 43, quella prevista dalla Legge 241/90 e quella prevista dal D.Lgs. 33/2013.

A tale proposito - fermo restando che i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso ai documenti amministrativi e del diritto di accesso civico, semplice e generalizzato e la relativa tutela giurisdizionale, così come gli obblighi di pubblicità e pubblicazione restano disciplinati dalla normativa di settore – gli Uffici dovranno interpretare la vigente normativa in materia di trasparenza ed accesso in modo da garantire la più rigorosa tutela dei dati personali degli interessati, anche tenendo in considerazione le motivazioni addotte dal soggetto (eventualmente, in caso di accesso) controinteressato.

In attuazione dei principi contenuti nella normativa nazionale e comunitaria vigente, l'Ufficio, nel dare riscontro alle richieste di accesso ovvero nel pubblicare i provvedimenti, dovrebbe in linea generale scegliere le modalità meno pregiudizievoli per i diritti dell'interessato, privilegiando l'ostensione di documenti con l'omissione dei «dati personali» in esso presenti, laddove l'esigenza informativa, alla base dell'accesso o della trasparenza e pubblicazione, possa essere raggiunta senza implicare il trattamento dei dati personali.

PARTE II - PROFILO ORGANIZZATIVO

PROFILO STRUTTURALE

La prima risposta all'esigenza di protezione dei dati personali è l'individuazione di una struttura organizzativa per la protezione dei dati personali, che, ovviamente, si sovrapponga, in gran parte, all'attuale struttura amministrativa comunale, integrandosi con essa. La creazione di tale struttura comporta tre azioni principali:

- il disegno di struttura (organigramma) per la Privacy;
- la definizione dei ruoli;
- l'individuazione dei soggetti "abilitati" dal Comune a trattare i dati personali.

Successivamente alla costruzione sarà, quindi, necessario adeguare le competenze mediante la formazione e l'informazione dei soggetti, abilitando concretamente i soggetti stessi.

II.1. TITOLARE DEL TRATTAMENTO

Articolo 4, n. 7 del RGPD:

"*«titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;*"

Un puntuale approfondimento dei concetti di Titolare, Contitolare e Responsabile del trattamento si rinviene all'interno delle "*Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR - Versione 2.0*" adottate il 7 luglio 2021 dal Comitato Europeo per la Protezione dei Dati Personali (EDPB), consultabili al seguente indirizzo web:
https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_it.pdf

Il concetto di Titolare del trattamento serve a determinare, in primissimo luogo, chi risponde dell'osservanza delle norme relative alla protezione dei dati.

Competenze e responsabilità

Le competenze e le responsabilità che il RGPD assegna al Titolare del trattamento possono così essere riassunte:

a) determinare le finalità ed i mezzi del trattamento dei dati personali: in considerazione del carattere pubblico che contraddistingue questa Amministrazione, le finalità sono determinate e circoscritte in quelle necessarie a garantire il corretto svolgimento delle funzioni istituzionali e dei compiti di interesse pubblico (art. 4);
b) mettere in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al RGPD (c.d. accountability) (art. 24);
c) garantire che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali non tratti tali dati se non è adeguatamente istruito in tal senso (artt. 29 e 32);
d) individuare i responsabili del trattamento, controllarne e garantirne l'operato (art. 28);

e) individuare i contitolari del trattamento e, ove necessario, determinare in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal RGPD, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14 (art. 26);
e) agevolare l'esercizio dei diritti dell'interessato (art. 12) e fornire agli interessati le informazioni previste dal RGPD (art. 13);
f) designare il Responsabile della protezione dei dati (art. 37) ponendolo in grado di svolgere adeguatamente l'attività (art. 38);
g) istituire e tenere aggiornato un registro delle attività di trattamento svolte in qualità di titolare o di responsabile (art. 30);
h) effettuare, prima di procedere al trattamento, una valutazione dell'impatto sulla protezione dei dati personali (art. 35);
i) comunicare all'autorità di controllo (art. 33) ed all'interessato (art. 34) eventuali violazioni dei dati;
l) ricevere ed osservare provvedimenti, notifiche e ingiunzioni dell'autorità di controllo (art. 58);
m) rispondere per il danno cagionato dal trattamento che violi il RGPD (art. 82);
o) rispondere delle violazioni amministrative ai sensi del RGPD (art. 83)

Alla luce del testo normativo e delle interpretazioni correnti, **si ritiene che titolare del trattamento sia il Comune nel suo complesso in quanto la legislazione nazionale e regionale gli ha affidato il compito di raccogliere e trattare certi dati personali**. Tuttavia, in concreto, esso manifesta la propria volontà attraverso coloro a cui è attribuito il potere di decidere per esso, nell'ambito delle suddivisioni di ruolo nascenti dal diritto amministrativo.

E' fatto salvo quanto previsto da specifiche disposizioni normative che attribuiscano la titolarità del trattamento dei dati personali a figure specifiche (vedasi, ad esempio, l'articolo 3 del DPCM 10 novembre 2014, n. 194, il quale attribuisce al Sindaco, nell'esercizio delle attribuzioni di cui all'articolo 54 del D.Lgs. 18 agosto 2000, n. 267, la titolarità del trattamento dei dati di propria competenza, limitatamente alla registrazione dei dati stessi all'interno dell'ANPR).

Le competenze e le responsabilità quali delineate dal RGPD e dalla normativa nazionale in tema di protezione dei dati personali sono attribuite agli organi ed al personale del Comune in relazione alle funzioni agli stessi assegnati dal D.Lgs. 18 agosto 2000, n. 267 e dallo Statuto e, in generale, previste dalla legge. Tale ripartizione è così intesa da questa Amministrazione:

A. al **Consiglio** sono assegnate eventuali competenze di tipo regolatorio o programmatorio generale in materia di riservatezza dei dati. Ai sensi dell'articolo 43 del TUEL, i consiglieri comunali hanno diritto di ottenere dagli uffici del comune, nonché dalle loro aziende ed enti dipendenti, tutte le notizie e le informazioni in loro possesso, utili all'espletamento del proprio mandato. Essi sono tenuti al segreto nei casi specificamente determinati dalla legge;
B. alla **Giunta** sono assegnate tutte le competenze a carattere non gestionale e non rientranti nella competenza del Consiglio, con particolare riferimento agli atti e attività a contenuto organizzativo e di indirizzo e le competenze politiche ed esecutive;
C. al **Sindaco** competono le nomine e le designazioni rilevanti in materia di protezione dei dati personali, con riferimento in particolare al Responsabile della protezione dei dati, ai Titolari di incarichi dirigenziali amministrativi di vertice ed ai titolari di incarichi dirigenziali (dirigenti non generali), al Segretario generale, fatto salvo l'esercizio del potere di delega in favore del Direttore generale;

D. Il Comune di Genova si articola in nove **Municipi** come particolare e più accentuata forma di decentramento di funzioni e di autonomia organizzativa e funzionale. Essi sono responsabili della funzione politica relativa al rispettivo territorio, nonché organismi di democrazia, partecipazione, consultazione e gestione di servizi di base e di esercizio di ulteriori funzioni delegate dal Comune nei limiti dello Statuto, dei Regolamenti comunali e delle disposizioni di legge.
Sono organi dei Municipi il Consiglio, il Presidente e la Giunta. La competenza di ciascun organo è stabilita dallo Statuto comunale.
E. ai **Dirigenti (generali e non)**, secondo l'ambito di competenza, spettano i seguenti compiti (con elencazione meramente esemplificativa):
a) verificare la legittimità dei trattamenti di dati personali effettuati dal Comune;
b) disporre, in conseguenza alla verifica di cui alla lett. a) le modifiche necessarie al trattamento perché lo stesso sia conforme alla normativa vigente ovvero disporre la cessazione di qualsiasi trattamento effettuato in violazione alla stessa;
c) adottare soluzioni di privacy by design e by default;
d) contribuire al costante aggiornamento del registro delle attività di trattamento;
e) garantire la corretta informazione e l'esercizio dei diritti degli interessati;
f) individuare i soggetti autorizzati a compiere operazioni di trattamento (di seguito anche "autorizzati") fornendo agli stessi adeguate istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite;
g) disporre l'adozione dei provvedimenti imposti dal Garante;
h) collaborare con il Responsabile della protezione dei dati personali al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
i) individuare, negli atti di costituzione di gruppi di lavoro comportanti il trattamento di dati personali, i soggetti che effettuano tali trattamenti quali incaricati, specificando, nello stesso atto di costituzione, anche le relative istruzioni;
l) adottare misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 del RGPD e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 del RGPD;
m) garantire al Responsabile della protezione dei dati personali i necessari permessi di accesso ai dati ed ai sistemi per l'effettuazione delle verifiche di sicurezza, anche a seguito di incidenti di sicurezza;
n) la preventiva valutazione d'impatto ai sensi dell'art. 35 del Regolamento, nei casi in cui un trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
o) consultare il Garante privacy nei casi in cui la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 del RGPD indichi che il trattamento presenta un rischio residuale elevato;
p) gestire la procedura in relazione alle violazioni di dati personali, curando la notifica all'Autorità di controllo e l'eventuale comunicazione agli interessati;
q) individuare i responsabili ed i contitolari del trattamento adottando gli atti (accordo sul trattamento dei dati personali ed accordo di contitolarità) e svolgendo le attività, anche di verifica, necessarie.

II.2. PERSONALE AUTORIZZATO AL TRATTAMENTO

Articolo 4, del RGPD
Definizioni
«terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le **persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare** o del responsabile

Articolo 29, del RGPD
Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento
Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Articolo 32, del RGPD
Sicurezza del trattamento
4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri

Articolo 2-quaterdecies, del Codice privacy
Attribuzione di funzioni e compiti a soggetti designati
2. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.

L'articolo 29 del RGPD (confermato dal paragrafo 4 dell'articolo 32), in particolare, preso atto dell'eventualità che sotto l'autorità del titolare del trattamento si possano trovare ad operare una o più persone, aventi accesso ai dati personali, si limita a stabilire che le medesime non possano trattare tali dati se non previamente autorizzate ed istruite dal titolare medesimo.

Contrariamente a quanto avveniva nel passato, ad opera dell'articolo 30 del D.Lgs. 30 giugno 2003, n. 196 (nel testo antecedente la modifica apportata dal D.Lgs. 10 agosto 2018, n. 101, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679), il **RGPD** non prevede espressamente la figura degli "incaricati" e, tuttavia, tale figura può essere implicitamente desunta dall'**articolo 29**, rubricato "*Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento*". Analoga previsione è contenuta al paragrafo 4 dell'articolo 32 del RGPD ed è desumibile altresì dalla definizione di "terzo" contenuta nell'articolo 4, n. 10 del RGPD.

In attuazione di ciò, l'articolo 2-quaterdecies del Codice privacy, al comma 2, lascia ampia libertà di forma al titolare per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.

Il RGPD e la normativa nazionale di adeguamento consentono dunque di mantenere le funzioni ed i compiti assegnati a figure interne alla struttura organizzativa comunale che, ai sensi del

Codice nel testo previgente all'adeguamento al RGPD, ma non anche ai sensi del RGPD, potevano essere definiti come "incaricati".

Il personale operante (a qualunque titolo ed a qualunque livello) all'interno del Comune è autorizzato al compimento delle sole operazioni di trattamento di dati personali, necessarie allo svolgimento delle mansioni e funzioni assegnate, sotto l'osservanza delle istruzioni contenute nell'ALLEGATO 1 al presente Modello organizzativo, ovvero di quelle impartite dal Dirigente competente.

In fase di prima attuazione del presente Modello Organizzativo ciascun Dirigente, competente in ragione del servizio o settore coinvolto, invia al personale da esso dipendente una comunicazione nella quale si prescrive l'osservanza del presente Modello organizzativo e della procedura di gestione delle violazioni di dati personali (c.d. Data breach policy) e, in particolare, l'osservanza delle istruzioni previste nell'ALLEGATO 1.

Nelle ipotesi in cui il trattamento di dati personali consegua all'esercizio di una specifica delega da parte del Sindaco (ad es., in relazione ad Anagrafe e Stato civile), le istruzioni sono contenute nel medesimo od atto successivo.

In caso di nuove assunzioni si stabilisce che il contratto debba riportare una clausola del seguente tenore (o similare):
"*L'Amministrazione comunale si è dotata di un modello organizzativo che, in applicazione del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito solo GDPR), individua gli attori, i ruoli e le responsabilità del sistema organizzativo preordinato a garantire la protezione dei dati personali.*
In attuazione di quanto ivi previsto, è conferita formale ed espressa autorizzazione al trattamento dei soli dati personali necessari allo svolgimento delle funzioni assegnate, con invito al più scrupoloso rispetto della normativa, comunitaria e nazionale, di protezione dei dati personali, oltre alle specifiche istruzioni ed indicazioni operative contenute nel predetto modello organizzativo, applicabili in ragione della posizione ricoperta.
E' stato nominato il Responsabile della protezione dei dati personali i cui riferimenti e dati di contatto sono disponibili sul sito web istituzionale dell'Ente."

II.3. DIRIGENTE - DESIGNATO AL TRATTAMENTO

Articolo 2-quaterdecies, del Codice privacy
Attribuzione di funzioni e compiti a soggetti designati
1. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.

All'interno della struttura organizzativa del Titolare, una fattispecie alquanto peculiare (prevista solo a livello nazionale e non comunitario e sulla quale, in dottrina sussistono non poche perplessità) è quella prevista dal comma 1 dell'articolo 2-quaterdecies del Codice privacy, ove viene prevista la possibilità per il titolare del trattamento di individuare e designare talune persone fisiche alle quali assegnare specifici compiti e funzioni connessi al trattamento di dati personali.

Con specifico riferimento al settore degli Enti Locali, **l'articolo 107 del D.Lgs. 18 agosto 2000, n. 267**, già stabilisce "*Funzioni e responsabilità della dirigenza*", in attuazione del principio per cui i poteri di indirizzo e di controllo politico-amministrativo spettano agli organi di governo, mentre la gestione amministrativa, finanziaria e tecnica è attribuita ai dirigenti mediante autonomi poteri di spesa, di organizzazione delle risorse umane, strumentali e di controllo.

Deve pertanto ritenersi che le decisioni in ordine alle finalità ed ai mezzi del trattamento, con particolare riferimento alle attività di tipo gestorio, già rientrino nella competenza dei dirigenti, in relazione al settore di competenza.

Il presente Modello organizzativo intende perseguire l'obiettivo di sintetizzare i principali adempimenti previsti dalla normativa di protezione, offrendo un indirizzo per il riparto delle relative competenze.

Il Comune di Genova stabilisce che ciascun Dirigente, competente in ragione del servizio o settore coinvolto, debba essere autorizzato al compimento delle operazioni di trattamento dei dati necessarie allo svolgimento delle mansioni e funzioni assegnate, sotto l'osservanza delle istruzioni contenute nell'ALLEGATO 1 al presente Modello organizzativo.

Considerato che al Dirigente spettano l'adozione degli atti e provvedimenti amministrativi, compresi tutti gli atti che impegnano l'amministrazione verso l'esterno, nonché la gestione finanziaria, tecnica ed amministrativa mediante autonomi poteri di spesa, di organizzazione delle risorse umane, strumentali e di controllo e che egli è responsabile, in via esclusiva, dell'attività amministrativa, della gestione e dei risultati della struttura organizzativa a cui è preposto, appare **opportuno attribuirgli altresì specifici compiti e funzioni spettanti al Titolare, quali individuati nell'ALLEGATO 2**, ferma restando il generale principio di responsabilità del titolare del trattamento previsto dall'articolo 24 del RGPD.

II.4. AMMINISTRATORE DI SISTEMA

La figura dell'amministratore di sistema, sebbene non specificamente prevista dal RGPD, svolge un ruolo fondamentale nel garantire il rispetto dei principi di protezione dei dati personali, contribuendo all'attuazione dei principi di "privacy by design" e "privacy by default" (art. 25 del RGPD), di accountability (articolo 5 del RGPD) ed all'adozione di misure di sicurezza adeguate (artt. 24 e 32 del RGPD). I compiti tradizionalmente affidati a tale figura consistono in:
- installazione e configurazione dei sistemi operativi: l'amministratore di sistema è responsabile dell'installazione e della configurazione dei sistemi operativi sui server e sulle workstation. Deve assicurarsi che i sistemi siano correttamente configurati ed ottimizzati per le esigenze del titolare.
- gestione delle reti: l'amministratore di sistema si occupa della gestione e della configurazione delle reti aziendali, compresi i router, gli switch e i firewall. Deve garantire la sicurezza e la stabilità delle reti, nonché l'accesso corretto alle risorse condivise;
- amministrazione dei server: l'amministratore di sistema è responsabile della gestione dei server aziendali, inclusi i server di posta elettronica, i server web, i server di database ed altri server specifici per le esigenze del titolare. Deve assicurarsi che i server siano sempre disponibili, sicuri e performanti;
- gestione degli account utente: l'amministratore di sistema si occupa della gestione degli account utente all'interno delle reti e dei sistemi informativi. Deve creare, modificare e disabilitare gli account utente in base alle esigenze del titolare, garantendo al contempo la sicurezza e l'accesso corretto alle risorse aziendali;
- backup e ripristino dei dati: l'amministratore di sistema deve pianificare e gestire i backup dei dati aziendali, assicurandosi che i dati siano protetti da perdite o danni. In caso di incidenti o guasti, deve essere in grado di ripristinare i dati in modo tempestivo.

Tale figura è stata oggetto di due importanti provvedimenti rilasciati dal Garante per la protezione dei dati personali, rispettivamente del 27 novembre 2008 (Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema) e del 25 giugno 2009 (Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento).

Nei provvedimenti del Garante, che continuano ad applicarsi anche a seguito delle modifiche introdotte al Codice privacy dal D.lgs. 101/2018, l'amministratore di sistema è la figura dedicata alla gestione ed alla manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali, compresi sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali.

La funzione di amministratore è quella di garantire il regolare funzionamento dell'infrastruttura tecnologica aziendale ed il corretto utilizzo della stessa da parte degli utenti interni ed esterni all'organizzazione. Quindi, in virtù di queste sue funzioni, l'amministratore svolge attività che comportano un'effettiva capacità di azione sul dato, anche quando l'amministratore non consulti in chiaro il dato stesso.

Inoltre, lo svolgimento delle mansioni di amministratore di sistema comporta, di regola, la concreta capacità, per atto intenzionale, ma anche per caso fortuito, di accedere in modo

privilegiato a risorse del sistema informativo ed a dati personali cui non si è legittimati ad accedere ad altro titolo.

Per tale motivo, l'individuazione dei soggetti idonei a svolgere le mansioni di amministratore di sistema riveste una notevole importanza, costituendo una delle scelte fondamentali che, unitamente a quelle relative alle tecnologie, contribuiscono ad incrementare la complessiva sicurezza dei trattamenti svolti, e va perciò curata in modo particolare evitando incauti affidamenti.

L'obiettivo è quello di adottare idonee cautele volte a prevenire e ad accertare eventuali accessi non consentiti ai dati personali, in specie quelli realizzati con abuso della qualità di amministratore di sistema.

Sulla scorta delle indicazioni fornite dal Garante, si ritiene indispensabile porre la massima attenzione a che:

- l'attribuzione delle funzioni di amministratore di sistema avvenga previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di protezione dei dati personali, ivi compresi i profili relativi alla sicurezza;
- la designazione ad amministratore di sistema sia individuale e rechi l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
- sia mantenuto un elenco recante i nominativi degli amministratori e delle relative funzioni ad essi attribuite (di sistemi, reti, software).
- siano adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione ed agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi;
- l'operato degli amministratori sia oggetto di verifica periodica, almeno annuale da parte dell'Area Technology Office (Sistemi informativi) od altra equivalente, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti;
- nel caso in cui l'attività dell'amministratore di sistema riguardi procedure che determinano il trattamento di dati personali di lavoratori dipendenti, sia resa conoscibile l'identità degli amministratori di sistema nel contesto organizzativo di riferimento;

E' demandata alla competenza del Direttore dell'Area Technology Office (Sistemi informativi) la gestione delle figure di amministratore di sistema affidate al personale appartenente alla struttura organizzativa comunale, nel rispetto dei principi sopra indicati.

Nel caso in cui le attribuzioni di Amministratore di sistema conseguano all'affidamento di servizi tecnologici a soggetti esterni al Comune, disposti dal Dirigente di altra struttura organizzativa, spetta a quest'ultimo di coinvolgere il Direttore dell'Area Technology Office per il coordinamento della relativa gestione.

II.5. CONTITOLARE DEL TRATTAMENTO

Articolo 26, par. 1, del RGPD:
"*Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un* ***accordo interno****, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'****esercizio dei diritti dell'interessato****, e le rispettive funzioni di comunicazione delle* ***informazioni di cui agli articoli 13 e 14****, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un* ***punto di contatto per gli interessati***".

Un puntuale approfondimento dei concetti di Titolare, Contitolare e Responsabile del trattamento si rinviene all'interno delle "*Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR - Versione 2.0*" adottate il 7 luglio 2021 dal Comitato Europeo per la Protezione dei Dati Personali (EDPB), consultabili al seguente indirizzo web:
https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_it.pdf

La contitolarità di trattamento può configurarsi laddove più di un soggetto sia coinvolto nel trattamento. In termini generali, sussiste una contitolarità del trattamento, in relazione a una specifica attività di trattamento, quando soggetti diversi determinano congiuntamente la finalità e i mezzi di tale attività di trattamento.

La valutazione della contitolarità del trattamento dovrebbe essere fondarsi su di un'analisi fattuale, piuttosto che formale, dell'influenza effettivamente esercitata sulle finalità e sui mezzi del trattamento.

È altresì importante sottolineare che un soggetto sarà considerato contitolare del trattamento insieme ad altri solo per quelle operazioni rispetto alle quali determina, insieme agli altri, i mezzi e le finalità di quello stesso trattamento dei dati. Se uno dei soggetti in questione decide isolatamente le finalità e i mezzi delle operazioni precedenti o successive nelle varie fasi del trattamento, tale soggetto deve essere considerato l'unico titolare di tale operazione di trattamento precedente o successiva.

Il fatto che più soggetti siano coinvolti nello stesso trattamento non significa che essi agiscano necessariamente in qualità di contitolari del trattamento.

La qualifica di contitolari del trattamento avrà principalmente conseguenze in termini di ripartizione degli obblighi di rispetto delle norme in materia di protezione dei dati e, in particolare, per quanto concerne i diritti delle persone fisiche. **L'esistenza di una responsabilità congiunta non implica, necessariamente, pari responsabilità**.

Spetta al Dirigente, competente in ragione del servizio o settore coinvolto, anche valendosi della collaborazione del RPD, di identificare gli eventuali contitolari di riferimento, e sottoscrivere gli accordi interni per il trattamento dei dati - sulla base delle indicazioni contenute nell'ALLEGATO 3 al presente Modello organizzativo - avendo cura di tenere costantemente aggiornata la relativa documentazione.

A seconda delle circostanze, potrà valutarsi l'adozione delle seguenti misure:

a) ciascuno dei Contitolari identifica un referente interno alla propria struttura, con il compito di relazionarsi con analogo soggetto designato dall'altra parte, a presidio del corretto adempimento di quanto previsto dall'accordo. In questo caso, il nominativo ed i dati di contatto del referente interno andranno tempestivamente comunicati all'altra parte;
b) i Contitolari designano congiuntamente un referente unitario quale punto di contatto per gli interessati. Le richieste di esercizio dei diritti presentate dagli interessati saranno gestite, in via esclusiva, dal referente unico, contattabile ai recapiti che saranno resi noti unitamente al suo nominativo, restando in ogni caso inteso che gli interessati potranno esercitare i propri diritti nei confronti di ciascun Contitolare;
c) I Contitolari si obbligano, in solido tra loro, a predisporre, attuare e mantenere aggiornati tutti gli adempimenti previsti in materia di protezione dei dati personali. E' tuttavia ammessa una diversa ripartizione "Interna" del profilo di responsabilità, da valutarsi caso per caso;

Si ricorda che, a norma dell'articolo 26, par. 2 del RGPD, **il contenuto essenziale dell'accordo di Contitolarità è messo a disposizione degli interessati**. Inoltre, è opportuno richiamare il rapporto di contitolarità all'interno delle informative

II.6. RESPONSABILE DEL TRATTAMENTO

Articolo 4, n. 8, del RGPD:
"*«responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che* ***tratta dati personali per conto del titolare del trattamento***"

Articolo 28 del RGPD:
"*1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo* ***ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti*** *per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.*
2. Il responsabile del trattamento ***non ricorre a un altro responsabile senza previa autorizzazione*** *scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.*
3. ***I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico*** *a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.*
(…)
9. Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico.
10. Fatti salvi gli articoli 82, 83 e 84, se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione."

Un puntuale approfondimento dei concetti di Titolare, Contitolare e Responsabile del trattamento si rinviene all'interno delle "*Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR - Versione 2.0*" adottate il 7 luglio 2021 dal Comitato Europeo per la Protezione dei Dati Personali (EDPB), consultabili al seguente indirizzo web:
https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_it.pdf

Il concetto di "Responsabile del trattamento" riveste un ruolo importante nel contesto della riservatezza e sicurezza dei trattamenti poiché serve ad individuare le responsabilità di coloro che si occupano più da vicino dell'elaborazione dei dati personali, sotto l'autorità diretta del Titolare del trattamento o per suo conto.

Per poter agire come Responsabile del trattamento occorrono quindi due requisiti:
a) essere un soggetto distinto rispetto al Titolare;
b) trattare i dati personali per conto di quest'ultimo.

Essere "*Un soggetto distinto significa che il titolare del trattamento decide di delegare tutte o parte delle attività di trattamento a un soggetto esterno*". L'esistenza di un Responsabile del trattamento dipende, quindi, da una decisione presa dal Titolare. Quest'ultimo può decidere di trattare i dati all'interno della propria organizzazione – ad esempio attraverso collaboratori autorizzati a trattare i dati sotto la sua diretta autorità - o di delegare tutte o una parte delle attività di trattamento a un'organizzazione esterna, pubblica o privata.

"*Il trattamento di dati personali per conto del titolare comporta innanzitutto che il soggetto distinto tratti i dati personali a beneficio del titolare del trattamento*". Il trattamento deve essere effettuato per conto del titolare, ma non agendo sotto la sua autorità o controllo diretti. Agire «per conto di» significa servire gli interessi di terzi e richiama la nozione giuridica di «delega». Nel caso della normativa in materia di protezione dei dati, il responsabile del trattamento è chiamato a seguire le istruzioni impartite dal titolare, almeno per quanto concerne la finalità del trattamento e gli elementi essenziali che ne costituiscono i mezzi. La liceità del trattamento, ai sensi dell'articolo 6 e, se pertinente, dell'articolo 9 del RGPD, deriva dall'attività del titolare del trattamento: il responsabile del trattamento non deve trattare i dati in modo diverso da quanto indicato nelle istruzioni del suddetto titolare. Agire «per conto di» significa, inoltre, che il responsabile del trattamento non può effettuare trattamenti per finalità proprie.

Non tutti i fornitori di servizi che trattano dati personali nel corso della prestazione di detti servizi sono «responsabili del trattamento». In pratica, se il servizio prestato non è destinato specificamente al trattamento di dati personali o se non prevede tale trattamento come un elemento essenziale, il prestatore del servizio può essere in grado di determinare in modo indipendente le finalità e i mezzi di tale trattamento necessario ai fini della prestazione. In siffatta situazione, il prestatore di servizi va considerato come un autonomo titolare del trattamento e non come responsabile dello stesso.

E', pertanto, **necessaria un'analisi caso per caso per stabilire il grado di influenza esercitata da ciascun soggetto nella determinazione delle finalità e dei mezzi del trattamento**.

Spetta al Dirigente, competente in ragione del servizio o settore coinvolto, anche valendosi della collaborazione del RPD, di identificare gli eventuali responsabili del trattamento, valutare l'adeguatezza delle garanzie prestate e sottoscrivere gli accordi sul trattamento dei dati, avendo cura di tenere costantemente aggiornata la relativa documentazione.

II.6.1. Scelta del responsabile del trattamento

Il titolare del trattamento ha il dovere di impiegare "*unicamente responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate*", in modo tale che il trattamento soddisfi i requisiti del RGPD, anche in merito alla sicurezza dello stesso, e garantisca la tutela dei diritti degli interessati.

Il **Dirigente, competente in ragione del servizio o settore coinvolto, è pertanto responsabile della valutazione dell'adeguatezza delle garanzie presentate dal responsabile del trattamento e dovrà essere in grado di dimostrare di aver preso in seria considerazione tutti gli elementi di cui all'articolo 28 del RGPD**.

Le garanzie presentate dal responsabile del trattamento sono quelle che il responsabile del trattamento è in grado di dimostrare in modo soddisfacente al titolare del trattamento, essendo queste le uniche che possono essere effettivamente prese in considerazione da detto

titolare nel valutare l'adempimento dei suoi obblighi. Spesso ciò richiederà uno scambio di documentazione pertinente (ad esempio, politica in materia di privacy, condizioni di erogazione del servizio, registro delle attività di trattamento, meccanismi di gestione dei log, politica in materia di sicurezza delle informazioni, relazioni di audit esterni sulla protezione dei dati e certificazioni internazionali riconosciute, come la serie ISO 27000).

La valutazione della sufficienza delle garanzie da parte del Dirigente è una forma di valutazione del rischio che dipenderà in larga misura dal tipo di trattamento affidato al responsabile e va effettuata caso per caso, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento nonché dei rischi per i diritti e le libertà delle persone fisiche. **Non esiste un elenco esaustivo e predefinito dei documenti o delle attività che il responsabile del trattamento è tenuto a presentare o a dimostrare in un dato caso, in quanto ciò dipende in larga misura dalle circostanze specifiche del trattamento**.

Il Dirigente dovrebbe tenere conto, almeno, dei seguenti elementi, al fine di valutare l'adeguatezza delle garanzie: le conoscenze specialistiche (ad esempio, le competenze tecniche in materia di misure di sicurezza e di violazione dei dati), l'affidabilità e le risorse del responsabile del trattamento. Anche la reputazione del responsabile del trattamento sul mercato può essere un fattore pertinente di cui si può tenere conto.

Inoltre, l'adesione a un codice di condotta o a un meccanismo di certificazione approvato può essere utilizzata come elemento in grado di dimostrare garanzie sufficienti.

L'obbligo di impiegare solo responsabili del trattamento «che presentano garanzie sufficienti», ai sensi dell'articolo 28, paragrafo 1, del RGPD è un obbligo permanente. Ad intervalli adeguati, il Dirigente dovrebbe verificare le garanzie offerte dal responsabile del trattamento, anche, se del caso, mediante attività di revisione e ispezioni.

II.6.2. Forma dell'accordo

Qualsivoglia trattamento di dati personali per conto del Comune dev'essere disciplinato da un contratto od altro atto giuridico, concluso tra il titolare e il responsabile del trattamento.

Non è prescritta una specifica forma contrattuale o convenzionale: essa dipenderà dal singolo caso. Ad esempio, potrebbe trattarsi di una convenzione tra enti pubblici o di un contratto nel caso di fornitori privati.

L'accordo sul trattamento deve essere stipulato per iscritto, anche in formato elettronico. Inoltre, il contratto o l'altro atto giuridico deve vincolare il responsabile del trattamento nei confronti del titolare del trattamento, ovverosia deve definire obblighi vincolanti in capo al responsabile del trattamento.

Sebbene l'accordo possa essere integrato in un contratto o convenzione più ampi, l'EDPB raccomanda che gli elementi del contratto volti a dare attuazione all'articolo 28 del RGPD siano chiaramente identificati come tali in un unico punto.

Sia il titolare che il responsabile del trattamento hanno la responsabilità di garantire l'esistenza di un contratto o di un altro atto giuridico che disciplini il trattamento. Fatte salve le disposizioni di cui all'articolo 83 del RGPD, l'autorità di controllo competente potrà infliggere una sanzione amministrativa pecuniaria sia al titolare sia al responsabile del trattamento, tenendo conto delle circostanze di ogni singolo caso.

Valendosi della possibilità prevista dal paragrafo 6 dell'articolo 28 la Commissione Europea, con la decisione di esecuzione 2021/915 del 4 giugno 2021, ha approvato uno **schema di** "**Clausole contrattuali tipo**", consultabili al seguente indirizzo:
https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX%3A32021D0915

II.6.3. Contenuto dell'accordo

Quanto al contenuto obbligatorio dell'accordo sul trattamento dei dati, la Commissione interpreta l'articolo 28, paragrafo 3, in modo tale per cui deve esservi stabilito:

- l'oggetto del trattamento (ad esempio, registrazioni di videosorveglianza di persone che entrano o escono da una struttura ad alta sicurezza). Sebbene sia un concetto ampio, esso deve essere formulato con specifiche sufficienti affinché l'oggetto principale del trattamento sia chiaro;
- la durata del trattamento: occorre specificare il periodo di tempo esatto o i criteri utilizzati per determinarlo; ad esempio, si potrebbe fare riferimento alla durata dell'accordo relativo al trattamento;
- la natura del trattamento: il tipo di operazioni eseguite nell'ambito del trattamento (ad esempio: «ripresa», «registrazione», «archiviazione di immagini» ecc.) e la finalità del trattamento (ad esempio: la rilevazione degli ingressi illegittimi). Tale descrizione dovrebbe essere la più completa possibile, a seconda dell'attività di trattamento specifica, in modo da consentire a soggetti esterni (ad esempio le autorità di controllo) di comprendere il contenuto e i rischi del trattamento affidato al relativo responsabile;
- la tipologia di dati personali: questo elemento dovrebbe essere specificato nel modo più dettagliato possibile (ad esempio: le immagini video delle persone che entrano ed escono dalla struttura). Non sarebbe sufficiente limitarsi a specificare che si tratta di «dati personali, ai sensi dell'articolo 4, paragrafo 1, del RGP» o «di categorie particolari di dati personali, ai sensi dell'articolo 9». Nel caso di categorie particolari di dati, il contratto o l'atto giuridico dovrebbero specificare almeno i tipi di dati in questione, ad esempio «informazioni relative alle cartelle cliniche» o «informazioni sull'appartenenza dell'interessato a un sindacato»;
- le categorie di interessati: anche questo aspetto dovrebbe essere indicato in modo piuttosto specifico (ad esempio: «visitatori», «dipendenti», servizi di consegna ecc.);
- gli obblighi ed i diritti del titolare del trattamento: (ad esempio, per quanto riguarda il diritto del titolare del trattamento di effettuare ispezioni e attività di revisione). Quanto agli obblighi del titolare del trattamento, tra gli esempi figurano quello di fornire al responsabile del trattamento i dati di cui al contratto, di fornire e documentare qualsivoglia istruzione relativa al trattamento dei dati da parte del responsabile del trattamento, di garantire, prima e durante l'intero corso del trattamento, l'adempimento degli obblighi di cui al RGPD posti in capo al responsabile, di controllare detto trattamento anche mediante attività di revisione e ispezioni unitamente al suddetto responsabile;
- l'obbligo del responsabile del trattamento di trattare i dati solo su istruzione documentata del titolare del trattamento;
- l'obbligo del responsabile del trattamento di garantire che le persone autorizzate a trattare i dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- l'obbligo del responsabile del trattamento di adottare tutte le misure richieste a norma dell'articolo 32 del RGPD;

- l'obbligo del responsabile del trattamento di rispettare le condizioni di cui all'articolo 28, paragrafo 2, e all'articolo 28, paragrafo 4, per ricorrere a un altro responsabile del trattamento;
- l'obbligo del responsabile del trattamento di assistere il titolare del trattamento nell'adempimento dell'obbligo di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
- l'obbligo del responsabile del trattamento di assistere il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del RGPD;
- l'obbligo del responsabile del trattamento, al termine della relativa attività, di cancellare o restituire, su scelta del titolare del trattamento, tutti i dati personali al titolare del trattamento e cancellare le copie esistenti;
- l'obbligo del responsabile del trattamento di mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'articolo 28 e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal titolare del trattamento o da un altro soggetto da questi incaricato;

Al fine di garantire un sufficiente livello di omogeneità all'interno della struttura organizzativa comunale, si suggerisce al Dirigente, competente in ragione del servizio o settore coinvolto, l'utilizzo della bozza di accordo contenuta nell'ALLEGATO 4, da personalizzare con riferimento al caso di specie.

Il Dirigente, competente in ragione del servizio o settore coinvolto, in relazione ai compiti e/o ai servizi affidati ha il dovere di **verificare che il soggetto esterno osservi le predette prescrizioni**. La periodicità delle verifiche dovrà essere determinata in funzione della natura dei dati, della probabile gravità dei rischi, dei mezzi da utilizzare per il trattamento e della durata dell'affidamento. Le verifiche e i risultati delle stesse dovranno registrate in appositi distinti verbali, sottoscritti, in duplice originale, dal Responsabile del trattamento e dal soggetto che svolge ciascuna verifica.

II.7. RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI

Articolo 38 del RGPD:

*"1. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia **tempestivamente e adeguatamente coinvolto** in tutte le questioni riguardanti la protezione dei dati personali.*

2. Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

*3. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. **Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento** o del responsabile del trattamento.*

*4. **Gli interessati possono contattare il responsabile della protezione dei dati** per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.*

*5. Il responsabile della protezione dei dati **è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti,** in conformità del diritto dell'Unione o degli Stati membri.*

6. Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi."

Articolo 39 del RGPD:

*"1. Il responsabile della protezione dei dati è incaricato almeno dei **seguenti compiti**:*

*a) **informare e fornire consulenza** al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;*

*b**) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento** o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;*

*c) fornire, se richiesto, un **parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento** ai sensi dell'articolo 35;*

*d) **cooperare con l'autorità di controllo**; e*

*e) **fungere da punto di contatto per l'autorità di controllo** per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.*

2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo."

Il Comune di Genova ha individuato e designato un Responsabile della protezione dei dati (RPD), in possesso di qualità professionali idonee, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di competenza.

I dati identificativi e di contatto del RPD, pubblicati nel sito web istituzionale del Comune, sono comunicati all'Autorità di controllo, ai componenti degli organi di governo, a tutti i dipendenti del Comune ed ai componenti degli organi di controllo interni.

I medesimi dati sono inclusi nel contesto delle informazioni rese agli interessati ai sensi degli articoli 13 e 14 del RGPD e delle comunicazioni effettuate ai sensi degli articoli da 15 a 22 e 34 del RGPD.

Al fine di evitare una eccessiva frammentazione degli indirizzi e pareri forniti, nello svolgimento dei suoi compiti, il RPD si rapporta con i Dirigenti (generali e non), ferma restando la facoltà per gli stessi di delegare talune attività a favore di personale specificamente individuato.

E' istituita un'apposita sezione all'interno della "intranet" comunale ove il RDP riporta e mantiene aggiornati:

a) **gli indirizzi e le risposte fornite nella propria attività di informazione e consulenza**;
b) **la modulistica in bozza e le procedure suggerite agli uffici per l'adempimento degli obblighi imposti dal RGPD**.

PARTE III - ADEMPIMENTI E PROCEDURE

III.1. MISURE PER LA SICUREZZA DEI DATI PERSONALI

Articolo 5 del RGPD:
"1. *I dati personali sono:*
(…)
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).
2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»)."

Articolo 24, par. 1, del RGPD:
"*Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario*"

Articolo 32, par. 1, del RGPD:
"*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio (…)*"

Il **Dirigente, competente in ragione del servizio o settore coinvolto,** provvede all'adozione ed alla dimostrazione di aver adottato le misure tecniche ed organizzative adeguate per garantire un livello di sicurezza correlato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi con cui sono trattati i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

In relazione alle misure di sicurezza informatiche e, in genere, tecnologiche, il Dirigente, competente in ragione del servizio o settore coinvolto, si coordina con l'Area Technology Office (Sistemi Informativi).

III.2. REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

Articolo 30, par. 1 del RGPD:
"*Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. (…)*"

Articolo 30, par. 2 del RGPD:
"*Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento (…)*"

la medesima norma individua il contenuto minimo di tale registro, specificando poi che esso è tenuto in forma scritta, anche in formato elettronico e dev'essere messo a disposizione dell'autorità di controllo.

La tenuta di siffatto registro si configura pertanto come base necessaria al fine di dimostrare la conformità dei trattamenti ai principi enucleati dal RGPD e non soltanto come strumento operativo di mappatura dei trattamenti effettuati.

Una grande differenza rispetto a quanto previsto sotto il regime del previgente Codice privacy è la modalità di mantenimento di tale documento. **Non c'è più una scadenza di revisione annuale, ma viene richiesto che il documento sia sempre aggiornato**.

Il Comune di Genova adotta un sistema informatico che meglio possa consentire l'aggiornamento e l'accesso alle informazioni. Il sistema informatico dovrà rispettare il contenuto prescritto dal RGPD e dovrà tener conto delle prescrizioni impartite dal Gruppo ex art. 29 (Ora Comitato europeo per la protezione dei dati) nonché dal Garante per la protezione dei dati personali.

Spetta al Dirigente, competente in ragione del servizio o settore coinvolto, di:

- effettuare la ricognizione integrale di tutti i trattamenti di dati personali svolti nella struttura organizzativa di competenza, al fine di procedere alla tenuta ed all'aggiornamento del registro;
- effettuare l'aggiornamento periodico, almeno semestrale e, comunque, in occasione di modifiche normative, organizzative, gestionali che impattano sui trattamenti, della ricognizione dei trattamenti al fine di garantirne la costante rispondenza alle attività effettivamente svolte dalla struttura organizzativa;
- effettuare l'analisi del rischio dei trattamenti e la determinazione preliminare dei trattamenti che possono presentare un rischio elevato per i diritti e le libertà degli Interessati, da sottoporre alla Valutazione d'impatto sulla protezione dei dati personali (DPIA);

Una importante funzione di controllo in ordine alla regolare tenuta nonché aggiornamento del registro delle attività di trattamento è demandata alla figura del DPO.

Ai sensi dell'art. 39 del RGPD che disciplina infatti le prerogative del Responsabile della protezione dei dati personali si evince che tra le altre è tenuto a "*sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la*

sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo".

All'attribuzione di controllo che gli viene assegnato direttamente dalla legge si aggiunge il principio di accountability che impone in tal caso al DPO di verificare che l'organizzazione per la quale compie attività di verifica sia conforme alla disciplina del Regolamento non solo in termini di adempimento, ma anche di capacità di dimostrazione della compliance normativa.

Al RPD compete di prestare assistenza al Dirigente nell'individuazione di:

a) finalità del trattamento;
b) soggetti esterni rispetto ai quali il Comune di trovi in una fattispecie di trattamento di dati personali "per conto di" (Responsabile);
c) categorie di destinatari;
d) trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale (e relativa adeguatezza);
e) misure di sicurezza;

III.3. VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

Articolo 35 del RGPD:
"*1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua,* ***prima di procedere al trattamento****, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.*
2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si ***consulta con il responsabile della protezione dei dati****, qualora ne sia designato uno.*
(…)
11. Se necessario, il titolare del trattamento ***procede a un riesame*** *per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento*"

Articolo 36, par. 1, del RGPD:
"*Il titolare del trattamento,* ***prima di procedere al trattamento, consulta l'autorità di controllo*** *qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio*"

La Valutazione d'impatto sulla protezione dei dati (DPIA) rappresenta una delle principali novità introdotte dalla recente normativa in materia di protezione dei dati personali, in quanto correlata al principio generale di responsabilizzazione del Titolare del trattamento (accountability).

La redazione del documento di valutazione consiste in una procedura finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali (attraverso la valutazione di tali rischi e la definizione delle misure idonee ad affrontarli). Più nello specifico il documento illustra le considerazioni logiche che hanno accompagnato le fasi di identificazione, valutazione e risposta a tutti i rischi rilevati all'interno del trattamento oggetto di analisi.

Qualora l'esito della DPIA escluda la sussistenza di un rischio elevato, il Titolare può ritenersi legittimato ad eseguire il trattamento, in caso contrario, non potrà attivare il trattamento senza prima aver adottato le misure idonee a garantire un livello di sicurezza adeguato ai rischi per attenuarli o eliminarli.

Nell'ipotesi residuale in cui il Titolare non sia in grado di individuare dette misure tecniche od organizzative dovrà allora consultare l'Autorità di controllo, ai sensi dell'**articolo 36 del RGPD**, dando luogo alla c.d. consultazione preventiva.

Il mancato svolgimento della DPIA quando il trattamento è soggetto a tale valutazione (**articolo 35, paragrafi 1, 3 e 4 del RGPD**), lo svolgimento non corretto di una DPIA (**articolo 35, paragrafi 2, 7 e 9 del RGPD**) o la mancata consultazione dell'autorità di controllo competente ove ciò sia necessario (**articolo 36, paragrafo 3, lettera e) del RGPD** possono comportare l'irrogazione di una sanzione amministrativa pecuniaria fino a un massimo di 10 milioni di Euro.

III.3.1. Casi di obbligo ed eccezioni

La corretta interpretazione dell'obbligo generale di effettuazione della DPIA è chiarita dalle "**Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 - WP248rev.01**" adottate dal Gruppo di Lavoro articolo 29 per la protezione dei dati (ora EDPB) il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017, il cui testo è raggiungibile al seguente indirizzo web:

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

Alla luce delle indicate Linee-guida, si ritiene che una valutazione d'impatto sulla protezione dei dati **non sia richiesta nei seguenti casi**:

- quando il trattamento non è tale da "presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35, paragrafo 1);

- quando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata svolta una valutazione d'impatto sulla protezione dei dati. In tali casi, si possono utilizzare i risultati della valutazione d'impatto sulla protezione dei dati per un trattamento analogo (articolo 35, paragrafo 119);

- quando le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate (cfr. Linee-guida, III.C);

- qualora un trattamento, effettuato a norma dell'articolo 6, paragrafo 1, lettere c) o e), trovi una base giuridica nel diritto dell'Unione o nel diritto dello Stato membro, tale diritto disciplini il trattamento specifico o sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nel contesto dell'adozione di tale base giuridica (articolo 35, paragrafo 10), a meno che uno Stato membro non abbia dichiarato che è necessario effettuare tale valutazione prima di procedere alle attività di trattamento;

- qualora il trattamento sia incluso nell'elenco facoltativo (stabilito dall'autorità di controllo) delle tipologie di trattamento per le quali non è richiesta alcuna valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 5). Tale elenco può contenere attività di trattamento conformi alle condizioni specificate da detta autorità, in particolare attraverso linee guida, decisioni o autorizzazioni specifiche, norme di conformità, ecc. (ad esempio in Francia, autorizzazioni, esenzioni, norme semplificate, pacchetti di conformità, ecc.). In tali casi e a condizione che venga eseguita una nuova valutazione da parte dell'autorità di controllo competente, non è richiesta una valutazione d'impatto sulla protezione dei dati, ma soltanto se il trattamento rientra a tutti gli effetti nel campo di applicazione della procedura pertinente menzionata nell'elenco e continua a rispettare pienamente tutti i requisiti pertinenti del regolamento generale sulla protezione dei dati.

Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dall'Autorità di controllo ai sensi dell'art. 35, paragrafi 4-6, del RGPD.

In particolare, si segnala che **il Garante per la Protezione dei Dati Personali, in data 11 ottobre 2018, ha adottato un "Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679"** [doc. web n. 9058979], raggiungibile al seguente indirizzo web:
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9058979

Con particolare riferimento ai trattamenti già esistenti alla data di entrata in vigore del RGPD, le richiamate Linee-guida del Gruppo di Lavoro ex articolo 29 (pag. 15), chiariscono che:

"L'obbligo di svolgere una valutazione d'impatto sulla protezione dei dati si applica alle operazioni di trattamento esistenti che possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche e per le quali vi è stata una variazione dei rischi, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento.

Non è necessaria una valutazione d'impatto sulla protezione dei dati per i trattamenti che sono stati verificati da un'autorità di controllo o dal responsabile della protezione dei dati, a norma dell'articolo 20 della direttiva 95/46/CE e che vengono eseguiti in maniera tale da fare sì che non si sia registrata alcuna variazione rispetto alla verifica precedente. In effetti, "[l]e decisioni della Commissione e le autorizzazioni delle autorità di controllo basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite o abrogate" (considerando 171).

Al contrario, ciò significa che qualsiasi trattamento di dati le cui condizioni di attuazione (ambito di applicazione, finalità, dati personali raccolti, identità dei titolari del trattamento o dei destinatari, periodo di conservazione dei dati, misure tecniche e organizzative, ecc.) sono mutate rispetto alla prima verifica effettuata dall'autorità di controllo o dal responsabile della protezione dei dati e che possono presentare un rischio elevato devono essere soggette a una valutazione d'impatto sulla protezione dei dati."

III.3.2. Metodologia

I contenuti minimi della DPIA sono specificati come segue dall'**articolo 35, paragrafo 7 del RGPD**:
a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati;
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Al fine di valutare i rischi e le modalità concretamente operative per la corretta protezione dei dati di terze parti, definiti 'interessati', si dovrà procedere alla valutazione dell'effettivo tipo di dati raccolti e trattati, del modo in cui detti dati vengono raccolti e trattati, dei metodi di conservazione custodia e protezione dei medesimi allo stato della valutazione, il tutto al fine di predisporre idoneo piano di iniziative finalizzate all'adempimento degli obblighi dettati dal RGPD. Lo schema suggerito è il seguente:
· la descrizione sistematica del trattamento e delle finalità;
· la descrizione della natura, dell'ambito, del contesto e degli scopi del trattamento;
· i dati personali trattati, i destinatari e il periodo per il quale sono conservati;
· una descrizione funzionale dell'operazione di trattamento;
· la descrizione dell'asset model su cui si basano i dati personali (es. Siti, hardware, software, reti, organizzazione, ecc.);
· la valutazione della necessità e la proporzionalità del trattamento;
· la descrizione delle misure previste per conformarsi al regolamento;
· la descrizione del modo in cui sono gestiti i rischi per i diritti e le libertà degli interessati;
· la descrizione dell'origine, della natura, della particolarità e della gravità dei rischi;
· la determinazione delle misure previste per il trattamento di tali rischi;
· la descrizione del modo in cui sono coinvolte le parti interessate;
· il parere del Responsabile della Protezione dei Dati Personali (RPD);
· le opinioni eventualmente raccolte dagli interessati o dei loro rappresentanti

Un processo di DPIA può riguardare una singola operazione di trattamento dei dati. Tuttavia, si potrebbe ricorrere a un singolo DPIA anche nel caso di trattamenti multipli simili tra loro in termini di natura, ambito di applicazione, contesto, finalità e rischi. Ciò potrebbe essere il caso in cui si utilizzi una tecnologia simile per raccogliere la stessa tipologia di dati per le medesime finalità. Oppure, un singolo processo di DPIA potrebbe essere applicabile anche a trattamenti simili attuati da diversi titolari del trattamento dei dati. In questi casi, è necessario condividere o rendere pubblicamente accessibile un DPIA di riferimento, attuare le misure descritte nello stesso, e fornire una giustificazione per la realizzazione di un unico DPIA.

La DPIA deve essere effettuata dal **Dirigente, competente in ragione del servizio o settore coinvolto**, **prima di procedere al trattamento, già dalla fase di progettazione del trattamento** stesso anche se alcune delle operazioni di trattamento non sono ancora note, in coerenza con i principi di privacy by design e by default per determinare se il trattamento deve prevedere misure

opportune in grado di mitigare i rischi. L'aggiornamento della valutazione d'impatto sulla protezione dei dati nel corso dell'intero ciclo di vita del progetto garantirà che la protezione dei dati e della vita privata sia presa in considerazione e favorisca la creazione di soluzioni che promuovono la conformità.

Il Dirigente garantisce l'effettuazione della DPIA, salvo che ne affidi l'esecuzione ad altro soggetto, anche esterno al Comune, ed è responsabile della stessa.

In relazione alle misure di sicurezza informatiche e, in genere, tecnologiche, il Dirigente, competente in ragione del servizio o settore coinvolto, si coordina con l'Area Technology Office (Sistemi Informativi), la quale fornisce ogni informazione necessaria quanto agli strumenti utilizzati ed alle misure di sicurezza adottate.

Il Dirigente **deve consultarsi con il Responsabile della protezione dei dati personali anche per assumere la decisione di effettuare o meno la DPIA**; tale consultazione e le conseguenti decisioni assunte dal Dirigente devono essere documentate.

Il Dirigente, competente in ragione del servizio o settore coinvolto, conduce, quindi, una prima fase **di valutazione preliminare, il cui scopo è quello di raccogliere tutte le informazioni necessarie a valutare prima di tutto se il trattamento sia conforme al RGPD** e, in seconda battura, comprendere se quel trattamento debba essere sottoposto ad una valutazione DPIA. L'attività quindi si compone di **3 sottofasi**:
a. descrizione del trattamento (le categorie di soggetti interessati dal trattamento, le finalità del trattamento, le categorie di dati oggetto del trattamento, le modalità di trattamento, il luogo di conservazione dei dati trattati, …) sulla scorta delle risultanze contenute nell'apposito registro;
b. valutazione della conformità (analisi della necessità e della proporzionalità del trattamento rispetto alle finalità; rispetto dei principi applicabili al trattamento di cui al capo II del RGPD; rispetto dei diritti degli interessati di cui al capo III del RGPD);
c. valutazione della obbligatorietà di condurre una DPIA;

Una volta determinata la necessità di procedere ad una attività di DPIA (vedasi il successivo paragrafo III.3.2.) si rende necessario **procedere alla raccolta delle informazioni necessarie allo sviluppo successivo delle attività di analisi dei rischi e produzione del piano dei trattamenti**. L'attività si compone in **ulteriori 4 sotto-fasi**:
a. raccolta delle informazioni per l'analisi dei rischi (informazioni presenti all'interno dei trattamenti, procedimenti coinvolti dal trattamento, finalità dei dati raccolti, flussi informativi, autorizzati all'accesso alle informazioni, asset model a sostegno dei trattamenti (applicativi, hardware, reti, ecc.). Le valutazioni che dovranno essere fatte durante la fase di analisi dei rischi devono tenere in considerazione due aspetti fondamentali: sia i rischi derivanti dai contenuti intrinseci del trattamento stesso comprendenti soprattutto modalità e finalità sia i rischi derivanti da possibili violazioni di sicurezza della protezione del dato)
b. valutazione dei rischi, di norma sviluppata nel classico concetto di valutazione degli impatti e probabilità afferenti ad una serie di minacce in grado di compromette un asset (informativo) (alcuni esempi sono gli impatti derivanti da una violazione della sicurezza fisica; da una violazione dei dati di identificazione o attinenti l'identità personale; perdite finanziarie o al patrimonio, perdite dovute a frodi; turbamento per la diffusione di una notizia riservata, compromissione di uno stato di salute,

evento lesivo dei diritti umani inviolabili o dell'integrità della persona; conseguenze di tipo discriminatorio, perdite di autonomia);
c. valorizzazione delle contromisure e rischio residuo. L'associazione di minacce e contromisure esistenti consente a questo punto di determinare il rischio effettivo che sarà confrontato con un valore di rischio accettabile;
d. piano di trattamento dei rischi;

La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:
a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);
b) valutazione della necessità e proporzionalità dei trattamenti, sulla base:

1) delle finalità specifiche, esplicite e legittime;
2) della liceità del trattamento;
3) dei dati adeguati, pertinenti e limitati a quanto necessario;
4) del periodo limitato di conservazione;
5) delle informazioni fornite agli interessati;
6) del diritto di accesso e portabilità dei dati;
7) del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
8) dei rapporti con i responsabili del trattamento;
9) delle garanzie per i trasferimenti internazionali di dati;
10) consultazione preventiva del Garante privacy;

c) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;
d) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il RGPD, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione;
e) l'acquisizione del parere del Responsabile della protezione dei dati personali

Assume quindi fondamentale importanza l'attività di **formalizzazione dei risultati** la quale consiste nel valutare se le misure individuate sono idonee a mitigare i rischi ad un livello accettabile, stimando in tal senso un rischio residuo, nonché documentare i risultati di tutte le attività svolte durante la DPIA ed i razionali che determinano la scelta se procedere o meno alla Consultazione Preventiva.

Tutti i documenti prodotti all'interno del processo di DPIA, partendo dal censimento e descrizione del trattamento, passando dalle valutazioni preliminari per arrivare, quando necessario, al calcolo di analisi dei rischi e relativo piano di trattamento, devono concorrere alla realizzazione di un documento finale in grado di dimostrare, oltre ovviamente ai risultati ottenuti, la corretta esecuzione formale del processo e la sua aderenza ai requisiti richiesti dal RGPD. Il documento deve inoltre esplicitare la frequenza di aggiornamento del DPIA, tanto maggiore quanto più si utilizzino tecnologie in evoluzione o si prevedono potenziali variazioni nei processi di trattamento.

Il Dirigente può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.

Il Dirigente deve consultare l'Autorità di controllo prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato (tale obbligo è previsto se si ritiene che il trattamento sottoposto a DPIA violi il RGPD, in particolare qualora l'Ufficio non abbia identificato o attenuato sufficientemente il rischio). L'Ufficio consulta l'Autorità di controllo anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

Quando è stata richiesta una valutazione preventiva all'Autorità di Controllo il trattamento non può essere iniziato almeno fino a che in procedimento di consultazione preventiva si è concluso con successo.

Salvo diversa disposizione dell'Autorità di controllo è bene che la comunicazione di richiesta di consultazione avvenga con modalità che consentano di dimostrare la data certa della stessa comunicazione (es. PEC, Raccomandata, ecc.) visto che i tempi stabiliti per lo sviluppo del processo di consultazione preventiva decorreranno da tal data.

L'attività include il recepimento dell'eventuale risposta e l'attuazione degli eventuali interventi necessari per aderire al parere fornito dall'Autorità.

Il processo DPIA deve sempre prevedere un monitoraggio dei risultati raggiunti ed un conseguente e costante riesame al fine di garantire nel tempo la mitigazione dei rischi e la conformità al RGPD, anche a fronte di fisiologici cambiamenti a cui sono soggetti tutti i trattamenti (contesto interno ed esterno, finalità del trattamento, strumenti utilizzati, organizzazione comunale, presenza di nuove minacce, ecc.).

Il Responsabile della protezione dei dati personali (RPD) monitora lo svolgimento della DPIA. **Può inoltre proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale**.

Eventuali Responsabili del trattamento collaborano e assistono il Dirigente oltre che il Responsabile della protezione dei dati nella conduzione della DPIA fornendo ogni informazione necessaria.

In relazione ai trattamenti per i quali, pur rientranti nell'ambito di applicazione della normativa richiamata, non sia stata effettuata la prescritta valutazione (DPIA), il Dirigente vi provvede senza ritardo e, comunque, entro 12 mesi dall'adozione del presente Modello organizzativo.

La DPIA deve essere effettuata - con eventuale riesame delle valutazioni condotte - anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

III.4. VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

Il Comune di Genova adotta una idonea procedura organizzativa interna per la gestione di eventuali violazioni concrete, potenziali o sospette di dati personali, per adempiere agli obblighi imposti dalla normativa europea ed evitare rischi per i diritti e le libertà degli interessati, nonché danni economici per il Comune (**data breach policy**).

I dati oggetto di riferimento saranno i dati personali trattati "da "e "per conto" del Titolare, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo.

L'obiettivo di tale documento è, pertanto:

• sensibilizzare il personale in ordine alle responsabilità in materia di protezione dei dati personali ed all'importanza della collaborazione nella tempestiva segnalazione e risoluzione degli incidenti sulla sicurezza (inclusi i data breach);

• definire processi per identificare, tracciare e reagire ad un incidente sulla sicurezza e ad un data breach, per valutarne il rischio, contenere gli effetti negativi e porvi rimedio nonché stabilire se, in caso di data breach, si renda necessario procedere alla (i) notifica al Garante e (ii) comunicazione agli Interessati;

• definire ruoli e responsabilità per la risposta agli incidenti sulla sicurezza ed i data breach;

• assicurare un adeguato flusso comunicativo all'interno della struttura del Titolare tra le parti interessate.

PARTE IV - DIRITTI DELL'INTERESSATO

Articolo 12, par. 2 del RGPD:

"1. Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

*2. Il **titolare del trattamento agevola l'esercizio dei diritti dell'interessato** ai sensi degli articoli da 15 a 22. Nei casi di cui all'articolo 11, paragrafo 2, il titolare del trattamento non può rifiutare di soddisfare la richiesta dell'interessato al fine di esercitare i suoi diritti ai sensi degli articoli da 15 a 22, salvo che il titolare del trattamento dimostri che non è in grado di identificare l'interessato.*

*3. Il titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 15 a 22 **senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa**. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il titolare del trattamento informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato.*

*4. Se non ottempera alla richiesta dell'interessato, il titolare del trattamento informa l'interessato **senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta**, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.*

*5. **Le informazioni fornite ai sensi degli articoli 13 e 14 ed eventuali comunicazioni e azioni intraprese ai sensi degli articoli da 15 a 22 e dell'articolo 34 sono gratuite**. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può:*

a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure

b) rifiutare di soddisfare la richiesta.

Incombe al titolare del trattamento l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

*6. Fatto salvo l'articolo 11, qualora il titolare del trattamento nutra ragionevoli **dubbi circa l'identità della persona fisica che presenta la richiesta** di cui agli articoli da 15 a 21, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato."*

IV.1. Oggetto ed ambito di applicazione

La presente sezione costituisce adempimento dell'obbligo di agevolare l'esercizio dei diritti previsti dagli articoli da 15 a 22 del RGPD e definisce le attività, i ruoli e le responsabilità che il Comune di Genova, in qualità di Titolare del trattamento dei dati personali, individua per la gestione delle richieste ricevute da parte dei soggetti interessati per l'esercizio dei propri diritti.

In particolare, rientrano nell'ambito di applicazione della presente disciplina le richieste di esercizio dei diritti riconosciuti dagli articoli da 15 a 22 del GDPR, quali di seguito riassunti:

a) diritto di accesso dell'interessato (articolo 15)
b) diritto di rettifica e cancellazione (articolo 16)
c) diritto alla cancellazione («diritto all'oblio») (articolo 17)
d) diritto di limitazione di trattamento (articolo 18)
e) diritto alla portabilità dei dati (articolo 20)
f) diritto di opposizione (articolo 21)
g) diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato (articolo 22);

I diritti di cui agli articoli da 15 a 22 del RGPD sono riconosciuti ricorrendo i presupposti previsti nei medesimi articoli ed in applicazione delle deroghe previste dal combinato disposto di cui all'articolo 23 del RGPD ed al Codice privacy, articolo 2-undecies.

Il Comune di Genova gestirà direttamente tutte le richieste di esercizio dei diritti che pervengano da interessati in relazione a trattamenti rispetto ai quali il Comune assume la qualifica di titolare o contitolare del trattamento, anche se ricevute da soggetti terzi individuati ed operanti in qualità di responsabili del trattamento ai sensi dell'articolo 28 del RGPD.

Resta escluso dall'ambito di applicazione della presente disciplina l'esercizio dei diritti che, pur riguardando dati personali, siano disciplinati da specifiche discipline di settore quali, a titolo meramente esemplificativo:
a) Legge 24 agosto 1990, n. 241 (c.d. diritto di accesso documentale);
b) Decreto legislativo 14 marzo 2013, n. 33, articolo 5 (c.d. diritto di accesso civico "semplice");
c) Decreto legislativo 14 marzo 2013, n. 33, articolo 5-bis (c.d. diritto di accesso civico "generalizzato" o "Foia");
d) Decreto Legislativo 19 agosto 2005, n. 195 (c.d. diritto di accesso "ambientale");
e) Decreto del Presidente della Repubblica 30 maggio 1989, n. 223 (Regolamento anagrafico della Popolazione Residente)
f) Decreto del Presidente della Repubblica, 3 Novembre 2000 n. 396 (Ordinamento dello Stato civile);
g) Decreto del Presidente della Repubblica 20 marzo 1967, n. 223, articolo 51 c.d. accesso alle liste elettorali).
Resta, inoltre, escluso dall'ambito di applicazione della presente disciplina, l'esercizio del diritto di reclamo, quale previsto dall'articolo 77 del RGPD e dagli articoli da 140-bis a 143 del Codice privacy.

La segnalazione di fattispecie costituenti violazione di dati personali ai sensi degli articoli 33 e 34 del RGPD va effettuata e viene gestita secondo le norme contenute nella Data Breach policy approvata dal Comune.

IV.2. Informazioni sui diritti riconosciuti all'interessato

Le informazioni di cui agli articoli 13 e 14 del RGPD sono fornite dal Dirigente, competente in ragione del servizio o settore coinvolto, mediante predisposizione di idonea pagina web sul sito istituzionale del Comune. Essa contiene tutte le informazioni necessarie a consentire all'interessato di conoscere termini e modalità di esercizio dei propri diritti (c.d. Informativa privacy). In relazione

a specifiche esigenze il Dirigente, competente in ragione del servizio o settore coinvolto, rende disponibili le informazioni in argomento su supporto cartaceo.

Il RDP sovraintende la predisposizione delle informative e fornisce un modello che garantisca uniformità a tutti gli Uffici e Servizi comunali. Parimenti, spetta al RPD verificare la conformità delle informazioni rese.

Al fine di semplificare la modulistica in uso agli uffici per la raccolta dei dati personali di quanti abbiano relazioni con il Comune, si stabilisce che la medesima possa contenere una formulazione riassuntiva delle informazioni previste dal RGPD (**c.d. informativa sintetica o di primo livello**), accompagnata da un rimando espresso alla pagina informativa presente sul sito web istituzionale (**c.d. informativa completa o di secondo livello**).
L'informativa sintetica può essere, altresì, fornita:

- in avvisi agevolmente visibili dal pubblico, posti nei locali di accesso delle strutture del Comune, nelle sale d'attesa ed in altri locali in cui ha accesso l'utenza o diffusi nell'ambito di pubblicazioni istituzionali e mediante il sito internet del titolare;
- in apposita avvertenza inserita nei contratti ovvero nelle lettere di affidamento di incarichi del personale dipendente, dei soggetti con i quali vengono instaurati rapporti di collaborazione o libero-professionali, dei tirocinanti, dei volontari, degli stagisti ed altri soggetti che entrano in rapporto con il Comune;
- in apposita avvertenza inserita nelle segnalazioni di disservizio e, in genere, in tutti i modelli di comunicazioni predisposti dall'Amministrazione e ad essa dirette;
- in sede di pubblicazione dei bandi, avvisi, lettere d'invito, ecc..

Qualora l'interessato richieda che le informazioni prescritte dagli articoli 13 e 14 del RGPD sia fornite oralmente il Dirigente, competente in ragione del servizio o settore coinvolto, procede all'identificazione del richiedente, acquisendo gli estremi del documento di identità in corso di validità ed annota la circostanza in apposito verbale da conservare nel rispetto delle norme in materia di documentazione amministrativa.

In attuazione del principio di accountability il Dirigente, competente in ragione del servizio o settore coinvolto, conserva tutte le versioni delle informative in uno specifico archivio interno cartaceo o telematico e tiene traccia di tutte le modifiche al testo (connesse alle modifiche organizzative, tecniche e normative) al fine di consentire al Comune una maggiore tutela in sede amministrativa e/o giudiziaria nel caso di reclami o procedimenti giudiziari per risarcimento di danni conseguenti a trattamenti illeciti di dati.

Qualora il trattamento dei dati personali avvenga ad opera di un responsabile del trattamento e questi raccolga direttamente dati personali presso l'interessato o presso terzi, è tenuto ad informare l'interessato circa la propria condizione di responsabile richiamando, quanto alle informazioni previste dagli articoli 13 e 14, la pagina web sul sito istituzionale del Comune.

IV.3. Organizzazione degli uffici

Spetta al Dirigente, competente in ragione del servizio o settore coinvolto, esaminare e dare seguito alle richieste di esercizio dei diritti, garantendo:
a) l'acquisizione delle richieste in data certa;
b) l'identificazione dell'interessato e del richiedente;
c) la non ricusabilità delle richieste;
d) il tracciamento dei tempi di risposta da parte del Comune;
e) la verifica del destinatario della comunicazione e della documentazione prodotta in adempimento alle richieste;

Del ricevimento delle richieste di esercizio dei diritti e degli esiti delle medesime è dato tempestivo avviso al Responsabile della Protezione dei Dati Personali (DPO), il quale fornisce il proprio supporto nella valutazione circa la sussistenza dei presupposti di ammissibilità e nella scelta dei termini e delle procedure di riscontro all'interessato.

Nel caso la richiesta riguardi una o più attività di trattamento svolte da più servizi o settori del Comune, il coordinamento dei Dirigenti avviene a cura del Dirigente, competente in ragione del servizio o settore maggiormente coinvolto. In casi di incertezza o contrasto, spetta al RPD individuare la figura del coordinatore. Resta inteso che, l'utilizzo nel presente documento, della terminologia "Dirigente, competente in ragione del servizio o settore coinvolto" sta ad indicare altresì la figura del coordinatore di cui sopra.

Nel caso in cui si tratti di una richiesta che riguardi uno o più trattamenti informatizzati, il Dirigente competente in ragione del servizio o settore coinvolto dovrà coinvolgere in tutta la procedura indicata nel presente documento anche l'Area Technology Office (Sistemi Informativi) od altra struttura organizzativa equivalente.

E' istituito un Registro informatico delle richieste di esercizio dei diritti, da tenersi a cura del Dirigente, competente in ragione del servizio o settore coinvolto, al fine di esaminare e dare seguito alle richieste di esercizio dei diritti, contenente le seguenti informazioni:
a) identificativo univoco della richiesta;
b) dati identificativi e recapiti dell'interessato e dell'eventuale richiedente, se diverso;
c) descrizione sintetica dell'oggetto della richiesta;
d) data di accettazione della richiesta;
e) esito della richiesta;
f) data di comunicazione all'interessato circa l'esito della sua richiesta;
g) note e segnalazioni.

Il registro è tenuto anche allo scopo di valutare eventuali criticità delle procedure di informazione e trattamento dei dati personali nonché al fine di attivare, a seguito dell'apposita valutazione del rischio, le procedure periodiche di audit e verifica dell'adeguatezza delle misure tecniche ed organizzative adottate per il singolo trattamento dei dati ai sensi dell'articolo 32 del GDPR.

Il Dirigente, competente in ragione del servizio o settore coinvolto, fornisce **periodica informativa al RPD delle registrazioni effettuate nel Registro delle richieste di esercizio dei diritti**.

La formazione, la gestione e la conservazione della documentazione inerente il procedimento di esercizio dei diritti riconosciuti dall'interessato dal RGPD avviene nel rispetto di quanto previsto dal D.Lgs. 7 marzo 2005, n. 82 (CAD) e relative Linee Guida AgID, dal D.P.R. 28 dicembre 2000 n. 445 (TUDA) e dal D.Lgs. 22 gennaio 2004, n. 42 (Codice dei beni culturali e del paesaggio).

La misura del contributo spese previsto dall'articolo 12, paragrafo 5 e dall'articolo 15, paragrafo 3 del RGPD è commisurata a quanto stabilito in materia di accesso ai documenti amministrativi, ai sensi dell'art. 22 della Legge 24 agosto 1990, n. 241.

IV.4. Procedura

IV.4.1. Presentazione della richiesta

Requisito soggettivo per l'esercizio dei diritti di cui trattasi è che la richiesta si riferisca ad informazioni relative a persona fisica, detenute dal Comune o che si presume lo siano.

La richiesta dev'essere in forma scritta e va presentata mediante invio agli indirizzi indicati nelle informative di cui al precedente paragrafo IV.2. Essa deve precisare il più possibile l'informazione o le attività di trattamento cui la richiesta si riferisce. **Al fine di agevolare la presentazione della richiesta, dovrà essere reso disponibile sul sito web istituzionale del Comune il fac-simile predisposto dall'Autorità Garante della Protezione dei Dati Personali** (https://www.garanteprivacy.it/documents/10160/10704/MODELLO+esercizio+diritti+in+materia+di+protezione+dei+dati+personali.docx/a356cedc-77b9-4f69-b24b-dadf877bb940?version=1.9).

Richieste di informazione e chiarimento verbali, rivolte agli uffici, sono accoglibili esclusivamente quando comportino il rilascio di informazioni generiche sulle modalità di trattamento dei dati personali adottati dal Comune e sulle modalità di esercizio dei diritti dell'Interessato, escludendo tassativamente la comunicazione di ogni altra tipologia di informazione, personale o meno.

La **presentazione della richiesta ad un ufficio incompetente** comporta l'onere per il ricevente di trasmetterla, senza ritardo, all'ufficio competente.

La **presentazione della richiesta ad un responsabile del trattamento** comporta l'onere, per il ricevente, di trasmetterla senza ritardo e, comunque, entro 7 giorni, all'ufficio comunale competente. Contestualmente, il responsabile del trattamento dovrà fornire all'ufficio i dati, le informazioni e tutta la collaborazione necessaria affinché lo stesso possa assolvere al dovere di risposta nei confronti dell'interessato.

Nel caso in cui l'accordo stipulato ai sensi dell'articolo 28 del RGPD preveda la gestione delle richieste dell'interessato come adempimento a carico del responsabile, spetta a quest'ultimo di fornire al competente ufficio tempestiva e documentata notizia circa il ricevimento e l'evasione della stessa.

In caso di presentazione della richiesta al Responsabile della Protezione dei Dati Personali, in quanto punto di contatto ai sensi dell'articolo 38, paragrafo 4, del RGPD, la medesima dovrà essere tempestivamente inoltrata al competente ufficio, dando avviso all'interessato dell'inoltro e dei dati di contatto dell'ufficio competente.

IV.4.2. Identificazione dell'interessato

Il Dirigente, competente in ragione del servizio o settore coinvolto, accerta che la richiesta provenga dal soggetto interessato o da altro soggetto da questi delegato, anche raccogliendo informazioni ulteriori rispetto a quelle contenute nella richiesta, ai sensi e per gli effetti di cui agli articoli 11, paragrafo 2 e 12, paragrafo 6, del RGPD. In particolare:
a) qualora la richiesta provenga direttamente dall'interessato, si procederà alla sua identificazione;
b) qualora la richiesta provenga da parte di un soggetto diverso dall'interessato, incluso un familiare, dovrà essere identificato il richiedente, il quale dovrà produrre apposito atto di delega sottoscritto dall'interessato. La delega non è necessaria nel caso in cui il richiedente eserciti il diritto per conto di soggetto privo della capacità di agire. In tale caso dovrà essere fornita adeguata documentazione a supporto della richiesta;
c) qualora la richiesta, riguardi una persona deceduta e provenga da chi abbia un interesse proprio o agisca a tutela dell'interessato, in qualità di suo mandatario o per ragioni familiari meritevoli di protezione, ai sensi di quanto previsto dall'articolo 2-terdecies del Codice privacy, dovrà essere identificato il richiedente ed acquisita adeguata documentazione a supporto della richiesta.
In relazione alle istanze e dichiarazioni presentate per via telematica, si applica il disposto di cui all'articolo 65 del D.Lgs. 7 marzo 2005, n. 82.

La mancata produzione della documentazione richiesta determina l'improcedibilità della richiesta, qualora il richiedente non ottemperi, entro il termine di 10 giorni, all'invito rivoltogli dal Dirigente con apposita comunicazione. La comunicazione di improcedibilità è inviata entro i 7 giorni successivi e, comunque, nel rispetto del termine previsto dall'articolo 12, paragrafi 3 e 4, del RGPD.

IV.4.3. Esame della richiesta

Ricevuta la richiesta ed effettuata l'identificazione dell'interessato e/o del richiedente Il Dirigente, competente in ragione del servizio o settore coinvolto, individua il trattamento cui la medesima si riferisce e procede alla relativa istruttoria nell'osservanza dei **criteri** di seguito indicati:
a) verifica circa la presenza dei dati personali negli archivi del Comune;
b) individuazione del trattamento oggetto della richiesta;
c) individuazione delle condizioni di liceità del trattamento ai sensi degli articoli 6, 9 e 10 del RGPD;
d) individuazione di altri uffici e servizi, interni al Comune, coinvolti nel trattamento;
e) individuazione di soggetti esterni al Comune, coinvolti nel trattamento (Responsabili e/o Contitolari);
f) valutazione dell'eventuale carattere di manifesta infondatezza o eccessività della domanda;
g) verifica circa l'esistenza di eventuali criticità nel trattamento o violazioni di dati personali (data breach);

Il Dirigente acquisisce ogni informazione utile all'istruzione del procedimento, ivi compreso il profilo della competenza ad istruire e decidere, sia rivolgendosi all'interessato che ad altri uffici e servizi del Comune.

IV.4.4. Disposizioni relative a specifici diritti

Ove l'interessato presenti una istanza di **accesso ai sensi dell'articolo 15 del RGPD** e questa attenga ad una notevole quantità d'informazioni riguardanti l'interessato Il Dirigente, competente in ragione del servizio o settore coinvolto, lo invita a precisare, prima che siano fornite le informazioni richieste, a quali dati o attività di trattamento si riferisca l'istanza. In ogni caso, l'esercizio di tale diritto, può riguardare esclusivamente i dati personali e non i documenti che li contengono.

Il diritto d'accesso ai sensi dell'articolo 15 del RGPD può essere esercitato anche più volte e con una cadenza periodica, purché ad intervalli ragionevoli e senza carattere vessatorio.

Ove l'interessato abbia esercitato il **diritto all'integrazione di cui all'articolo 16 del RGPD**, il Dirigente verifica, anzitutto, la necessità di procedere all'integrazione richiesta nonché la completezza e, ove possibile, la veridicità della dichiarazione integrativa fornita.

Il diritto di rettifica di cui all'articolo 16 del RGPD non può essere esercitato in riferimento ad informazioni di tipo valutativo, relativi a giudizi, opinioni o ad altri apprezzamenti di tipo soggettivo.

Nell'ipotesi di esercizio del **diritto di opposizione ai sensi dell'articolo 21 del RGPD**, il Dirigente verifica che l'interessato abbia indicato nell'istanza i motivi connessi alla sua situazione particolare che ne legittimano l'esercizio. La mancata indicazione e documentazione dei motivi determina la non accoglibilità della richiesta, qualora il richiedente non ottemperi, entro il termine di 15 giorni, all'invito rivoltogli dall'Ufficio con apposita comunicazione. La comunicazione di non accoglibilità è inviata entro i 7 giorni successivi.

Ciascun Dirigente, competente in ragione del servizio o settore coinvolto, anche avvalendosi dei soggetti di cui all'articolo 28 del RGPD, adotta misure appropriate per consentire di contrassegnare i dati personali presenti nei propri sistemi ICT come "limitati", a seguito di presentazione dell'istanza ai sensi dell'articolo 18 del GDPR.

IV.4.5. Trattamento di dati effettuato in qualità di responsabile o contitolare

In caso di ricevimento di una richiesta di esercizio dei diritti relativa ad un trattamento di dati personali effettuato dal Comune nella qualità di responsabile del trattamento il Dirigente, competente in ragione del servizio o settore coinvolto:

a) avvia una istruttoria preliminare, al fine di rilevare gli elementi informativi da rendere al titolare, trasmettendogli tempestivamente la richiesta;

b) invia al titolare gli esiti della istruttoria preliminare effettuata, garantendogli tutto il supporto possibile nell'evasione della richiesta;

c) informa l'interessato di aver inoltrato la sua richiesta al titolare del trattamento, il quale sarà competente ad istruire il relativo procedimento ed assumere la necessaria decisione.

Nel caso un soggetto titolare del trattamento abbia ricevuto una istanza di esercizio dei diritti riconosciuti dal RGPD e l'abbia inoltrata al Comune quale responsabile del trattamento il Dirigente, competente in relazione del servizio o settore coinvolto, fornisce al titolare stesso, mediante comunicazione a mezzo PEC e senza ingiustificato ritardo, le informazioni utili o necessarie per consentire il corretto adempimento degli obblighi previsti dagli art. 12-21 del RGPD.

La medesima procedura di cui ai precedenti paragrafi è adottata nel caso in cui il Comune sia contitolare del trattamento cui inerisce la richiesta di esercizio dei diritti ma l'accordo interno

sottoscritto ai sensi dell'articolo 26 del RGPD preveda in capo ad altro contitolare la competenza alla gestione delle istanze formulate dall'interessato.

Nel caso in cui il Comune sia contitolare del trattamento cui inerisce la richiesta di esercizio dei diritti e l'accordo interno sottoscritto ai sensi dell'articolo 26 del RGPD preveda in capo ad esso la competenza alla gestione delle istanze formulate dall'interessato, si osservano le istruzioni previste per l'ipotesi in cui il Comune sia (unico) titolare del trattamento, ferma restando la necessità di fornire adeguata informazioni anche agli altri contitolari.

IV.4.6. Riscontro all'interessato

Il riscontro all'interessato deve avvenire in forma scritta, anche attraverso strumenti elettronici che ne favoriscano l'accessibilità. La risposta fornita all'interessato deve essere intelligibile, concisa, trasparente, facilmente accessibile, utilizzare un linguaggio semplice e chiaro.

In caso di esercizio del diritto di accesso di cui all'articolo 15, paragrafo 3 del RGPD, il Dirigente, competente in ragione del servizio o settore coinvolto, fornisce una copia dei dati personali oggetto di trattamento utilizzando modalità che ne garantiscano adeguata sicurezza. In particolare, il riscontro:
a) deve contenere una copia integrale e completa delle sole informazioni richieste, in formato di tipo aperto;
b) non deve recare danno ai diritti ed alle libertà altrui;
c) in caso di trattamento che non prevede l'uso di strumenti elettronici, deve avvenire in busta chiusa, indirizzata all'interessato, anche se la consegna avviene per il tramite di soggetto delegato;
d) in caso di trattamento che prevede l'uso di strumenti elettronici, deve avvenire utilizzando preferibilmente la posta elettronica certificata (PEC), il download diretto dal sito istituzionale del Comune od altro strumento di condivisione che presenti adeguate garanzie di sicurezza o supporti non riscrivibili e proteggendo i documenti con password o sottoponendoli a procedure crittografiche. L'uso della crittografia è obbligatorio nel caso di dati personali appartenenti alle categorie particolari di cui agli articoli 9 e 10 del RGPD.

In caso di esercizio del diritto di portabilità di cui all'articolo 20 del RGPD il Dirigente, competente in ragione del servizio o settore coinvolto, provvede alla comunicazione dei dati per i quali sussista la condizione di portabilità, in formato aperto, esclusivamente in favore del richiedente, escluso il trasferimento diretto ad altro titolare del trattamento. La trasmissione avviene nel rispetto di quanto previsto al precedente paragrafo.

Qualora, a seguito del suo esame, la richiesta appaia manifestamente infondata o eccessiva, ai sensi dell'articolo 12, paragrafo 5 del RGPD il Dirigente, competente in ragione del servizio o settore coinvolto, espone adeguata motivazione nella comunicazione all'interessato, informandolo che l'accoglimento della richiesta è subordinato al pagamento di un contributo spese, determinato ai sensi del precedente paragrafo IV.3.

In caso di diniego opposto alla propria richiesta, l'interessato è sempre informato della possibilità di proporre:
• reclamo all'Autorità Garante per la protezione dei dati personali;
• ricorso giurisdizionale avanti il Tribunale il tribunale del luogo in cui il titolare del trattamento risiede o ha sede ovvero il tribunale del luogo di residenza dell'interessato.

IV.4.7. Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento

La comunicazione di cui all'articolo 19 del RGPD è effettuata, tempestivamente, a mezzo di posta elettronica certificata.

IV.4.8. Istanza di riesame al Responsabile della protezione dei dati personali

All'interessato che non ritenga soddisfatto l'esercizio dei diritti, come formulato nella propria istanza ed eventualmente integrato a seguito delle richieste del Dirigente, è assicurata la possibilità di ottenere un riesame ad opera del Responsabile della Protezione dei Dati Personali (RPD).

La comunicazione di riscontro inviata all'interessato ai sensi del precedente paragrafo IV.4.6. contiene, altresì, l'indicazione della facoltà di cui al paragrafo precedente nonché i dati di contatto del Responsabile della Protezione dei Dati Personali.

L'eventuale istanza di riesame indirizzata al Responsabile della Protezione dei Dati Personali è acquisita al protocollo del Comune a seguito della sua trasmissione all'Ufficio competente.

Al procedimento di riesame si applica la previsione contenuta al paragrafo 3 dell'articolo 12 del RGPD.

Il Responsabile della Protezione dei Dati Personali che, in occasione della procedura di riesame, riscontri delle non conformità nel trattamento od una immotivata inottemperanza delle richieste di esercizio dei diritti, comunica al Dirigente competente le azioni correttive o migliorative da adottare (e la relativa tempistica) per assicurare la tutela dei diritti dell'Interessato.

IV.4.9. Informazioni sul trattamento dei dati personali

Il Comune, in qualità di titolare del trattamento, tratta i dati personali raccolti in occasione e nel contesto delle procedure per l'esercizio dei diritti, di cui alla presente disciplina, con modalità prevalentemente informatiche e telematiche, per le finalità previste dal GDPR, in particolare per l'esecuzione degli obblighi previsti dalla normativa di protezione dei dati personali, ivi incluse le finalità di trattazione delle istanze pervenute, di archiviazione, di ricerca storica e di analisi per scopi statistici.

Il conferimento dei dati è obbligatorio e la loro mancata indicazione non consente di effettuare l'esame delle istanze. I dati acquisiti nell'ambito della procedura di esame delle istanze saranno conservati in conformità alle norme sulla conservazione della documentazione amministrativa.

I dati saranno trattati esclusivamente dal personale e da collaboratori del Comune o delle imprese espressamente nominate come responsabili del trattamento. Al di fuori di queste ipotesi, i dati non saranno diffusi, né saranno comunicati a terzi, fatti salvi i casi in cui si renda necessario comunicarli ad altri soggetti coinvolti nell'attività istruttoria e nei casi specificamente previsti dal diritto nazionale o dell'Unione europea.

Anche in relazione alle procedure instaurate a seguito della presentazione dell'istanza di esercizio dei diritti riconosciuti dal RGPD, gli interessati hanno il diritto di ottenere dal Comune, nei casi previsti, l'accesso ai propri dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt. 15 e ss. del Regolamento). L'apposita istanza è presentata nelle forme previste dalla presente disciplina.

ALLEGATI

ALLEGATI 1 – “Elenco degli specifici compiti e funzioni attribuiti e connessi al trattamento dei dati personali e specifiche istruzioni ai soggetti designati”

ALLEGATO 2 – “Elenco degli specifici compiti e funzioni attribuiti e connessi al trattamento dei dati personali e specifiche istruzioni al dirigente”

ALLEGATO 3 – “Bozza di accordo di contitolarità”

ALLEGATO 4 – “Bozza di accordo sul trattamento de dati personali”

ALLEGATO 1 - ELENCO DEGLI SPECIFICI COMPITI E FUNZIONI ATTRIBUITI E CONNESSI AL TRATTAMENTO DEI DATI PERSONALI E SPECIFICHE ISTRUZIONI AI SOGGETTI DESIGNATI

Il Comune di Genova, in forza del principio di «responsabilizzazione», impartisce alla persona fisica individuata ed autorizzata al trattamento, le istruzioni a cui è obbligata ad attenersi, sotto la comminatoria delle sanzioni di legge e di contratto.

In particolare, nella gestione dei processi/procedimenti dell'Ufficio a cui la persona fisica designata al trattamento è preposta e, più in generale, nello svolgimento dell'attività lavorativa presso detto Ufficio, l'autorizzazione ad effettuare le operazioni di trattamento dei dati personali nell'ambito della suddetta attività viene rilasciata a condizione che si rispettino le seguenti istruzioni:

- in attuazione del principio di «liceità, correttezza e trasparenza»,
    - le operazioni di raccolta, registrazione, elaborazione di dati ed in generale, le operazioni di trattamento tutte, avvengono agli esclusivi fini dell'inserimento o arricchimento degli archivi/banche dati presenti nell'Ufficio di appartenenza, nell'osservanza delle tecniche e metodologie in atto;
    - autorizzazione a comunicare od eventualmente diffondere o trasferire all'esterno i dati personali esclusivamente ai soggetti autorizzati a riceverli legittimamente, per le finalità per le quali gli stessi sono stati raccolti e comunque nel rispetto delle istruzioni ricevute dal Dirigente competente in ragione del servizio o settore coinvolto;
- in attuazione del principio di «minimizzazione dei dati», obbligo di trattamento dei soli ed esclusivi dati personali che si rivelino necessari rispetto alle finalità per le quali sono trattati nell'attività a cui la persona fisica designata al trattamento è preposta;
- in attuazione del principio di «limitazione della finalità» il trattamento dev'essere conforme alle finalità istituzionali del Titolare e limitato esclusivamente a dette finalità;
- in attuazione del principio di «esattezza», obbligo di assicurare l'esattezza, la disponibilità, l'integrità, nonché il tempestivo aggiornamento dei dati personali, e obbligo di verificare la pertinenza, completezza e non eccedenza rispetto alle finalità per le quali i dati sono stati raccolti, e successivamente trattati;
- in attuazione del principio di «limitazione della conservazione»
    - evitare di creare banche dati nuove senza espressa autorizzazione del Dirigente competente in ragione del servizio o settore coinvolto;
    - conservare i dati in una forma che consenta l'identificazione dell'Interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati e obbligo di esercitare la dovuta diligenza affinché non vengano conservati, nell'Ufficio di competenza, dati personali non necessari o divenuti ormai superflui, fatte salve le norme in materia di archiviazione amministrativa. Alla conclusione del trattamento, obbligo di assicurarsi che i documenti contenenti i dati di cui agli articoli 9 e 10 del RGPD vengano conservati in contenitori/armadi muniti di serratura od in ambienti ad accesso selezionato e vigilato;
- in attuazione del principio di «integrità e riservatezza» obbligo di garantire un'adeguata sicurezza dei dati personali, compresa la protezione, dando diligente ed integrale attuazione alle misure logistiche, tecniche informatiche, organizzative, procedurali definite dal Dirigente competente in ragione del servizio o settore coinvolto, trattando i dati stessi con

la massima riservatezza ai fini di impedire trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali. In particolare:

- riporre in archivio, al termine del periodo di trattamento, i supporti ed i documenti, ancorché non definitivi, contenenti i dati personali;
- non fornire dati personali per telefono, qualora non si abbia certezza assoluta sull'identità del destinatario;
- evitare di inviare, per fax, documenti in chiaro contenenti dati personali: si suggerisce, in tal caso, di inviare la documentazione, senza alcun esplicito riferimento all'Interessato (ad esempio, contrassegnando i documenti semplicemente con un codice). In alternativa, si suggerisce di avvisare preventivamente il destinatario della comunicazione fax in modo che possa curarne la diretta ricezione;

- In attuazione del principio di «trasparenza»:
  - accertarsi dell'identità dell'Interessato, prima di fornire informazioni circa i dati personali od il trattamento effettuato;
  - fornire all'Interessato tutte le informazioni di cui agli articoli 13 e 14 del RGPD e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 del RGPD, relative al trattamento attenendosi alle istruzioni ed utilizzando la modulistica all'uopo predisposti dal Dirigente competente in ragione del servizio o settore coinvolto;
  - ove si renda necessario, segnalare al Dirigente competente in ragione del servizio o settore coinvolto la necessità di adeguamento, correzione ed integrazione della modulistica in uso all'Ufficio;
  - agevolare l'esercizio dei diritti dell'Interessato ai sensi degli articoli da 15 a 22 del RGPD. In particolare, qualora riceva richieste provenienti dagli interessati, finalizzate all'esercizio dei propri diritti, dovrà:
    - darne tempestiva comunicazione al Dirigente competente in ragione del servizio o settore coinvolto, allegando copia delle richieste ricevute;
    - coordinarsi, ove necessario e per quanto di propria competenza, con il Dirigente competente in ragione del servizio o settore coinvolto per gestire le relazioni con gli Interessati;

- seguire i seminari d'informazione e formazione in materia di protezione dei dati personali, obbligatori alla luce delle nuove disposizioni del RGPD ed a sostenere i relativi test finali finalizzati alla verifica dell'apprendimento;
- segnalare al Dirigente competente in ragione del servizio o settore coinvolto, con tempestività, eventuali anomalie, incidenti, furti, perdite accidentali di dati connessi con una ricaduta sul trattamento dei dati personali, al fine di attivare le procedure di comunicazione delle violazioni di dati all'Autorità di controllo ed ai soggetti autorizzati (istituto del c.d. data breach o violazione di dati personali);
- assistere il Dirigente competente in ragione del servizio o settore coinvolto nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del RGPD, tenendo conto della natura del trattamento e delle informazioni a propria disposizione ed in particolare a collaborare nelle comunicazioni di violazioni di dati personali, negli adempimenti della valutazione di impatto e consultazione preventive;
- assistere il Dirigente competente in ragione del servizio o settore coinvolto nella tenuta del registro delle attività di trattamento istituito ai sensi dell'articolo 30 del RGPD, tenendo conto della natura del trattamento e delle informazioni a propria disposizione;
- segnalare al Dirigente competente in ragione del servizio o settore coinvolto, con tempestività, eventuali circostanze che rendano necessario od opportuno l'aggiornamento

delle misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

- effettuare la comunicazione dei dati esclusivamente ai soggetti indicati dal Dirigente competente in ragione del servizio o settore coinvolto e secondo le modalità stabilite dal medesimo;
- mantenere, salvo quanto precisato al punto precedente, la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento dell'incarico, per tutta la durata del medesimo ed anche successivamente al termine di esso;
- fornire al Dirigente competente in ragione del servizio o settore coinvolto, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentirgli di svolgere efficacemente la propria attività di controllo;
- in generale, prestare la più ampia e completa collaborazione al Titolare del trattamento, nel suo complesso ed articolazioni, al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente;
- nel caso di presenza di utenti, ospiti o personale di servizio, all'interno dell'Ufficio, sarà necessario:
    - che la persona non sia visibile dall'esterno;
    - non ammettere in ufficio altre persone se non espressamente richiesto e in accordo con l'utente con cui stiamo parlando;
    - apporre fuori dalla porta una targhetta o altro equivalente che indichi che è in corso un colloquio;
    - fare attendere in luoghi in cui non sono presenti informazioni riservate o dati personali;
    - evitare che l'utente esponga le proprie questioni personali prima di accedere all'ufficio (se necessario, spiegare alla persona la motivazione);
    - è importante che sulla scrivania vi siano solo informazioni neutre ed impersonali e, comunque, appartenenti alle categorie di cui agli articoli 9 e 10 del RGPD;
    - evitare di allontanarsi dalla scrivania o riporre i documenti ed attivare il salvaschermo del PC;
    - durante il colloquio non devono essere ricevute telefonate; se necessario, rispondere e rinviare a più tardi la conversazione telefonica. Se nell'ufficio è inserita una segreteria telefonica assicurarsi sempre che, in presenza di persone, il volume sia al minimo e che i messaggi eventualmente lasciati non possano essere sentiti;
    - assicurarsi che schedari e armadi che contengono dati personali siano chiusi a chiave quando siamo assenti dall'ufficio, salvo che sia possibile chiudere l'ufficio stesso;
    - bloccare l'accesso ad estranei dell'ufficio.

Le stesse istruzioni e prescrizioni cogenti sono obbligatorie anche per il trattamento di dati personali realizzato, interamente o parzialmente, con strumenti elettronici, contenuti in archivi/banche dati o destinati a figurarvi.
In particolare, per tali trattamenti la persona fisica designata e delegata al trattamento ha l'obbligo di utilizzo e gestione attenendosi alle seguenti istruzioni:

A) Strumenti elettronici in generale

1) i personal computer fissi e portatili ed i programmi per elaboratore su di essi installati

sono uno strumento di lavoro e contengono dati riservati e informazioni personali di terzi ai sensi della normativa sulla protezione dei dati personali: vanno, pertanto, utilizzati e conservati, insieme ai relativi documenti esplicativi, con diligenza e cura, attenendosi alle prescrizioni fornite dal Dirigente competente in ragione del servizio o settore coinvolto;
2) in generale tutti i dispositivi elettronici sono forniti al dipendente per lo svolgimento della sua attività lavorativa, nell'ambito delle mansioni a questo affidate. L'uso per fini personali è da considerare pertanto eccezionale e limitato a comunicazioni occasionali e di breve durata, ad esclusione dei dispositivi per i quali è esplicitamente regolamentato l'uso per fini personali;
3) le impostazioni dei personal computer e dei relativi programmi per elaboratore installati sono predisposte dagli addetti informatici incaricati sulla base di criteri e profili decisi dal Titolare, in funzione della qualifica del dipendente, delle mansioni cui questo è adibito, nonché delle decisioni e della politica di utilizzo di tali strumenti stabilita dall'Amministrazione stessa. Il dipendente non può modificarle autonomamente; può ottenere cambiamenti nelle impostazioni solo previa autorizzazione da parte del Dirigente competente in ragione del servizio o settore coinvolto.
4) assicurarsi, in caso di sostituzione del computer utilizzato, che siano effettuate le necessarie operazioni di formattazione o distruzione dei supporti di memorizzazione dei dati;
5) rivolgersi tempestivamente, per difficoltà o questione inerente la sicurezza, al Dirigente competente in ragione del servizio o settore coinvolto;
6) per finalità di assistenza, manutenzione ed aggiornamento e previo consenso esplicito del dipendente stesso, soggetti appositamente incaricati allo svolgimento di tale attività potranno accedere da remoto al personal computer del dipendente attraverso un apposito programma software;
7) il dipendente è tenuto ad osservare le medesime precauzioni e cautele, ove queste siano applicabili e pertinenti rispetto allo specifico strumento utilizzato, in relazione a tutti i dispositivi elettronici di cui fa uso, tra cui ad esempio fax, fotocopiatrici, scanner, masterizzatori, telefoni fissi, cellulari, pen-drive e supporti di memoria.

B) **Password e username (credenziali di autenticazione informatica)**

1) per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali altrui ed astenendosi dall'accedere a servizi telematici non consentiti. Le credenziali di autenticazione informatica sono individuali. Non possono essere condivise con altri incaricati del trattamento;
2) è vietato comunicare a terzi gli esiti delle proprie interrogazioni delle banche dati;
3) i codici identificativi, le password e le smart card dei dipendenti saranno disattivate nel caso in cui i dipendenti cessino il loro rapporto di lavoro, oltre che nei casi espressamente e tassativamente previsti dalla normativa. In tali casi il dipendente è tenuto a restituire la propria smart card agli uffici a ciò preposti.
4) la password che il dipendente imposta, con il supposto e l'assistenza, in caso di difficoltà, dell'Amministratore di sistema:

- deve essere sufficientemente lunga e complessa e deve contemplare l'utilizzo di caratteri maiuscoli e speciali e numeri;
- non deve essere riconducibile alla persona del dipendente;
- deve essere cambiata periodicamente, in conformità alle policies adottate dal Comune;
- non dev'essere rivelata o fatta digitare al personale di assistenza tecnica;

- non dev'essere rivelata o comunicata al telefono, via fax od altra modalità elettronica. Nessuno è autorizzato a chiederla;

C) Assenza od impossibilità temporanea o protratta nel tempo

1) nell'ipotesi di assenza o impossibilità, temporanea o protratta nel tempo, del dipendente, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività del Titolare sia necessario accedere ad informazioni o documenti di lavoro presenti sul personal computer del dipendente, inclusi i messaggi di posta elettronica in entrata ed in uscita, il dipendente può delegare a un altro dipendente a sua scelta ("fiduciario") il compito di verificare il contenuto di messaggi e inoltrare al responsabile dell'area in cui lavora quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività deve essere redatto apposito verbale e informato il dipendente interessato alla prima occasione utile.

2) in caso di assenza o impossibilità, temporanea o protratta nel tempo, del dipendente, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività dell'ufficio sia necessario accedere a informazioni o documenti di lavoro presenti sul personal computer del dipendente, inclusi i messaggi di posta elettronica in entrata ed in uscita, ed il dipendente non abbia delegato un suo fiduciario, secondo quanto sopra specificato, il Dirigente competente in ragione del servizio o settore coinvolto può richiedere con apposita e motivata richiesta rivolta all'Amministratore di sistema od aziende competenti di accedere alla postazione e/o alla casella di posta elettronica del dipendente assente, in modo che si possa prendere visione delle informazioni e dei documenti necessari. Contestualmente, il Dirigente competente in ragione del servizio o settore coinvolto deve informare il dipendente dell'avvenuto accesso appena possibile, fornendo adeguata spiegazione e redigendo apposito verbale.

D) Log-out

In caso di allontanamento anche temporaneo dalla postazione di lavoro (personal computer fisso o portatile), il dipendente non deve lasciare il sistema operativo aperto con la propria password e/o smart card inserita. Al fine di evitare che persone estranee effettuino accessi non consentiti, il dipendente deve attivare il salvaschermo con password o deve bloccare il computer (ad es. utilizzando i tasti CTRL+ALT+CANC) e togliere la smart card dall'apposito alloggiamento.

E) **Utilizzo della rete internet e relativi servizi - Cloud storage**

1) non è consentito navigare in siti web non attinenti allo svolgimento delle mansioni assegnate, soprattutto in quelli che possono rivelare le opinioni politiche, religiose o sindacali del dipendente;

2) è da evitare la registrazione a servizi online, a titolo o di interesse personale;

3) non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi direttamente autorizzati dal Dirigente competente in ragione del servizio o settore coinvolto e con il rispetto delle normali procedure di acquisto;

4) non è permessa la partecipazione, per motivi non professionali, a servizi di forum, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nicknames);

5) il dipendente, si impegna a circoscrivere gli ambiti di circolazione e di trattamento dei dati personali (es. memorizzazione, archiviazione e conservazione dei dati in cloud) ai Paesi

facenti parte dell'Unione Europea, con espresso divieto di trasferirli in paesi extra UE che non garantiscano (o in assenza di) un livello adeguato di tutela, ovvero, in assenza di strumenti di tutela previsti dal Regolamento UE 2016/679 (Paese terzo giudicato adeguato dalla Commissione Europea, BCR di gruppo, clausole contrattuali standard, consenso degli interessati, etc.).

F) Posta elettronica

1) la casella di posta elettronica è uno strumento finalizzato allo scambio di informazioni nell'ambito dell'attività lavorativa;
2) si invitano i dipendenti a non utilizzare gli indirizzi di posta elettronica assegnati dal Titolare per le comunicazioni personali;
3) al fine di garantire la continuità all'accesso dei messaggi da parte dei soggetti adibiti ad attività lavorative che richiedono la condivisione di una serie di documenti si consiglia e si incoraggia l'utilizzo abituale di caselle di posta elettronica condivise tra più lavoratori o delle caselle di posta istituzionali del Comune, eventualmente affiancandoli a quelli individuali;
3) le comunicazioni via posta elettronica devono avere un contenuto espresso in maniera professionale e corretta nel rispetto della normativa vigente.
4) non è consentito inviare o memorizzare messaggi di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
5) la posta elettronica diretta all'esterno della rete comunale può essere intercettata da estranei e, dunque, non deve essere usata per inviare documenti contenenti dati personali di cui agli articoli 9 e 10 del RGPD;
6) non è consentito l'utilizzo dell'indirizzo di posta elettronica istituzionale del Comune per la partecipazione a dibattiti, Forum o mail-list, salvo diversa ed esplicita autorizzazione;
7) qualora si verifichino anomalie nell'invio e ricezione dei messaggi di posta elettronica sarà cura del dipendente informare prontamente il Dirigente competente in ragione del servizio o settore coinvolto.

G) Software, applicazioni e servizi esterni

1) onde evitare pericolo di introdurre virus informatici nonché di alterare la stabilità delle applicazioni dell'elaboratore, è consentito installare programmi provenienti dall'esterno solo se espressamente autorizzati dal Dirigente competente in ragione del servizio o settore coinvolto o dall'Amministratore di sistema
2) non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
3) non è consentito modificare le configurazioni impostate sul proprio PC;
4) non è consentito configurare gli strumenti per la gestione della posta elettronica per la gestione di account privati. Non è inoltre consentito utilizzare detti strumenti per la ricezione, visualizzazione ed invio di messaggi a titolo personale;
6) il Titolare si riserva la facoltà di procedere alla rimozione di ogni file od applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti od installati in violazione delle presenti istruzioni;
7) tutti i software caricati sul sistema operativo ed in particolare i software necessari per la protezione dello stesso o della rete internet (quali antivirus o firewall) non possono essere disinstallati o in nessun modo manomessi dai dipendenti, (salvo quando questo sia richiesto per compiere attività di manutenzione o aggiornamento).

H) **Reti di comunicazione**

1) nel caso di trattamento di dati personali effettuato mediante elaboratori non accessibili da altri elaboratori (cioè, mediante computer stand alone) è necessario utilizzare la parola chiave (password) fornita per l'accesso al singolo PC;

2) nel caso di trattamento di dati personali effettuato mediante elaboratori accessibili da altri elaboratori, solo in rete locale, o mediante una rete di telecomunicazioni disponibili al pubblico, è necessario: utilizzare la parola chiave (password) fornita per l'accesso ai dati, oltre a servirsi del codice identificativo personale per l'utilizzazione dell'elaboratore;

3) le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono, in alcun modo, essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità;

4) al fine di garantire la disponibilità dei documenti di lavoro assicurandone il backup periodico, il dipendente dovrà procedere al loro salvataggio nell'apposita area di rete individuale o di gruppo a ciò dedicata e disponibile sui sistemi server del Titolare;

5) è proibito tentare di acquisire i privilegi di amministratore di sistema;

6) non collegare dispositivi che consentano un accesso, non controllabile, ad apparati della rete del Titolare.

7) non condividere file, cartelle, hard disk o porzioni di questi del proprio computer, per accedere a servizi non autorizzati di peer to peer al fine condividere materiale elettronico tutelato dalle normative sul diritto d'autore (software, file audio, film, etc.).

I) Supporti esterni di memorizzazione

La persona fisica designata e delegata al trattamento, ha l'obbligo di:

- utilizzare i supporti di memorizzazione solamente qualora i dati in essi precedentemente contenuti non siano in alcun modo recuperabili, altrimenti etichettarli e riporli negli appositi contenitori;
- proteggere i dati personali archiviati su supporti esterni con le stesse misure di sicurezza previste per i supporti cartacei;
- verificare che i contenitori degli archivi/banche dati (armadi, cassettiere, computer, etc.) vengano chiusi a chiave e/o protetti da password in tutti i casi di allontanamento dalla postazione di lavoro;
- evitare che i dati estratti dagli archivi/banche dati possano divenire oggetto di trattamento illecito;
- copie di dati personali su supporti amovibili sono permesse solo se parte del trattamento; copie di dati contemplati dagli articoli 9 e 10 del RGPD devono essere espressamente autorizzate dal Dirigente competente in ragione del servizio o settore coinvolto. In ogni caso tali supporti devono avere un'etichetta che li identifichi e non devono mai essere lasciati incustoditi;
- evitare di asportare supporti informatici o cartacei contenenti dati personali di terzi, senza la previa autorizzazione del Dirigente competente in ragione del servizio o settore coinvolto;
- procedere alla cancellazione dei supporti esterni contenenti dati personali, prima che i medesimi siano riutilizzati. Se ciò non è possibile, essi devono esser distrutti;
- verificare l'assenza di virus nei supporti utilizzati;

ALLEGATO 2 - ELENCO DEGLI SPECIFICI COMPITI E FUNZIONI ATTRIBUITI E CONNESSI AL TRATTAMENTO DEI DATI PERSONALI E SPECIFICHE ISTRUZIONI AL DIRIGENTE

Ferma restando la necessaria osservanza dei compiti e funzioni di cui al precedente **ALLEGATO 1**, spetta al Dirigente competente in ragione del servizio o settore coinvolto:

SOTTO IL PROFILO ORGANIZZATIVO E FUNZIONALE:

- collaborare con la Direzione generale e gli altri Dirigenti nell'elaborazione degli obiettivi strategici ed operativi del sistema di sicurezza e di protezione dei dati personali da sottoporre all'approvazione del Titolare;
- collaborare con la Direzione generale e gli altri Dirigenti nell'elaborazione e nell'aggiornamento delle procedure necessarie al sistema di sicurezza e, in particolare per la procedura da utilizzare in caso di violazione dei dati personali (c.d. data breach);
- coordinare la ricognizione integrale di tutti i trattamenti di dati personali svolti nella struttura organizzativa di competenza;
- annotare e mantenere aggiornate le attività di trattamento rilevate, all'interno del registro previsto dall'articolo 30 del RGPD;
- identificare contitolari, responsabili e sub responsabili di riferimento della struttura organizzativa di competenza e sottoscrivere gli accordi interni e gli accordi sul trattamento dei dati, avendo cura di tenere costantemente aggiornati i documenti relativi ai contitolari ed ai responsabili;
- acquisire dai contitolari e dai responsabili una dichiarazione dalla quale risulti che le persone fisiche che, presso gli stessi contitolari e responsabili abbiano accesso ai dati personali, siano state autorizzate al trattamento dei dati e siano state istruite in tal senso;
- individuare, per iscritto ed in numero sufficiente a garantire la corretta gestione del trattamento dei dati inerenti la struttura organizzativa di competenza, le persone fisiche della struttura organizzativa medesima, che operano sotto la propria diretta autorità, impartendo a tale fine analitiche istruzioni, eventualmente integrative di quelle stabilite nel presente Modello organizzativo e controllando costantemente che le persone fisiche individuate al trattamento dei dati effettuino le operazioni di trattamento:
  - in attuazione del principio di «liceità, correttezza e trasparenza»;
  - in attuazione del principio di «minimizzazione dei dati»;
  - in attuazione del principio di «limitazione della finalità»;
  - in attuazione del principio di «esattezza»;
  - in attuazione del principio di «limitazione della conservazione»;
  - in attuazione del principio di «integrità e riservatezza»;
  - in attuazione del principio di «liceità, correttezza e trasparenza».
- effettuare l'aggiornamento periodico, almeno annuale e, comunque, in occasione di modifiche normative, organizzative, gestionali che impattano sui trattamenti, della ricognizione dei trattamenti al fine di garantirne la costante rispondenza alle attività effettivamente svolte dalla struttura organizzativa, con obbligo di sottoporre l'aggiornamento all'approvazione del Titolare;
- effettuare l'analisi del rischio dei trattamenti e la determinazione preliminare dei trattamenti che possono presentare un rischio elevato per i diritti e le libertà degli Interessati;

- effettuare, prima di procedere al trattamento, quando questo può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, una valutazione dell'impatto del trattamento sulla protezione dei dati personali (DPIA);
- prima di procedere al trattamento, consultare l'Autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuare il rischio;
- adottare le misure tecniche ed organizzative adeguate e funzionali a garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
  a) la pseudonimizzazione e la cifratura dei dati personali;
  b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
  c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
  d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
- adottare le misure tecniche ed organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento, fermo restando che:
  a) tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità;
  b) dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica;
- documentare e tracciare, per iscritto, ed essere in grado di provare, in caso di richiesta dell'Autorità di controllo, l'attuazione del sistema di sicurezza finalizzato alla protezione dei dati personali;
- cooperare, su richiesta, con il RPD e con l'Autorità di controllo nell'esecuzione dei rispettivi compiti;
- osservare le prescrizioni ed adempiere ai compiti previsti nella procedura di gestione delle violazioni di dati personali (data breach policy) adottata dal Comune;
- osservare le prescrizioni ed adempiere ai compiti previsti nella Parte IV del presente Modello organizzativo, relativamente ai diritti riconosciuti dal RGPD agli interessati;
- assicurarsi che il RPD sia tempestivamente ed adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali;
- sostenere il RPD nell'esecuzione dei compiti assegnati, fornendogli le risorse necessarie per assolvere tali compiti e per accedere ai dati personali ed ai trattamenti;
- documentare tutte le attività e gli adempimenti delegati e, in ogni caso, tracciare documentalmente l'intero processo di gestione dei rischi e del sistema di sicurezza e protezione;
- controllare e monitorare la conformità dell'analisi, della valutazione dei rischi e della valutazione di impatto nonché controllare e monitorare la conformità del trattamento dei rischi al contesto normativo, regolamentare, gestionale, operativo e procedurale, con obbligo di tempestiva revisione in caso di rilevazioni di non conformità o di scostamenti;
- tracciare documentalmente le attività di controllo e monitoraggio mediante periodici report/resoconti/referti da sottoporre al RPD;

- conformare il trattamento ai pareri ed indicazioni del RPD e dell'Autorità di controllo nonché alle linee guida ed ai provvedimenti dell'Autorità di controllo;
- formulare proposte, in occasione dell'approvazione/aggiornamento annuale degli strumenti di pianificazione e programmazione, volte ad implementare il sistema di sicurezza e ad elevare il livello di protezione degli interessati;
- programmare e partecipare alla formazione in tema di diritti e libertà degli interessati, di rischi di violazione dei dati, di informatica giuridica, e di diritto alla protezione dei dati personali;
- promuovere la cultura della prevenzione del rischio di violazione dei dati e la cultura della protezione come valore da integrare in ogni processo/procedimento;
- effettuare ogni ulteriore attività, anche se non espressamente indicata in precedenza e necessaria per la integrale attuazione del RGPD e della normativa di riferimento.

ALLEGATO 3 - BOZZA DI ACCORDO DI CONTITOLARITA'

ACCORDO DI CONTITOLARITA'

AI SENSI DELL'ART. 26 DEL REGOLAMENTO (EU) 2016/679

_____ (C.F.: _____ - P. IVA: _____) con sede in _____, PEC: _____, all'uopo rappresentato da _____

E

_____ (C.F.: _____ - P. IVA: _____) con sede in _____, PEC: _____, all'uopo rappresentato da _____ (d'ora innanzi, entrambe le parti saranno identificate, congiuntamente, quali "Contitolari" o "Parti")

PREMESSO CHE

1) è in essere tra le Parti un progetto comune consistente in _____, il quale comporta la necessità di determinare congiuntamente le finalità e le modalità del trattamento dei dati personali coinvolti nella realizzazione del medesimo progetto comune;
2) che in data 25 maggio 2018 è divenuto pienamente operativo il REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (d'ora innanzi, più semplicemente, "RGPD");
3) l'articolo 4, paragrafo 1, n. 7) del RGPD definisce quale titolare del trattamento "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali*";
4) a norma dell'articolo 26, paragrafo 1 del RGPD "*Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati*";
5) a norma dell'articolo 26, paragrafo 2 del RGPD "*L'accordo di cui al paragrafo 1 riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato*";
6) è intenzione delle Parti contraenti regolamentare in modo trasparente i diritti e gli obblighi reciproci quali conseguono alla puntuale osservanza delle norme e dei principi contenuti nel RGPD, con particolare riguardo all'esercizio dei diritti dell'interessato, nonché i rispettivi ruoli nella comunicazione delle informazioni agli interessati, addivenendo alla sottoscrizione della presente accordo;

SI CONVIENE E SI STIPULA QUANTO SEGUE

Articolo 1 – Pattuizioni preliminari

1. Nell'ambito delle rispettive responsabilità come determinate dal presente Accordo, i Contitolari dovranno in ogni momento adempiere ai propri obblighi conformemente ad esso e in modo tale da trattare i dati senza violare le disposizioni di legge vigenti e nel pieno rispetto delle linee guida e dei codici di condotta applicabili, di volta in volta approvati dall'Autorità di controllo.
2. Resta inteso tra le Parti che, ai sensi dell'art. 26, comma 3, del Regolamento (EU) 2016/679, indipendentemente dalle disposizioni del presente Accordo, l'interessato potrà esercitare i propri diritti nei confronti di e contro ciascun Contitolare del trattamento.
3. In coerenza con la propria missione e i propri valori, i Contitolari si impegnano reciprocamente a proteggere i dati personali di ogni persona fisica che si trovasse ad avere contatto o ad operare con i medesimi ("Interessato"), nel rispetto dell'identità, della dignità di ogni essere umano e delle libertà fondamentali costituzionalmente garantite nel rispetto del RGPD relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione degli stessi.
4. Il presente accordo non determina l'insorgere di alcun diritto alla revisione di prezzi od altre forme di impegno, anche economico, già definiti tra le Parti, trattandosi di obblighi ed adempimenti derivanti da norme di legge già conosciute.
5. Il presente accordo annulla e/o sostituisce qualsivoglia regolazione pattizia esistente tra le Parti in relazione al medesimo oggetto, di talché, a far data dalla sua stipulazione, i loro rapporti saranno regolati esclusivamente dal presente accordo.
6. Qualsiasi modifica od integrazione del presente accordo potrà farsi soltanto per iscritto a pena di nullità.
7. Il contenuto essenziale di questo accordo di Contitolarità è messo a disposizione dell'Interessato nella sezione Trasparenza del Portale di ciascuno dei Contitolari.

Articolo 2 - Oggetto del trattamento

1. I Contitolari dichiarano, in merito al trattamento dei Dati Personali, di condividere le decisioni relative alle finalità e modalità del trattamento di dati e, in particolare:
- le seguenti banche dati; dipendenti e collaboratori, _____;
- le finalità del trattamento di dati personali, ciascuna con le proprie specificità legate alle attività concretamente svolte;
- i mezzi del trattamento e le modalità del trattamento di dati personali;
- la politica di conservazione dei dati;
- lo stile e le modalità di comunicazione delle informative art. 13 del RGPD;
- la procedura di gestione dei consensi (ove necessari);
- la designazione e la formazione dei soggetti autorizzati;
- istruzioni sull'uso degli strumenti informatici per il personale;
- la gestione delle comunicazioni e nomine dei responsabili ai sensi dell'art. 28 del RGPD;
- la tenuta dei registri del trattamento ai sensi dell'art. 30 del RGPD;
- le procedure nel caso di trasferimento dei dati fuori UE;
- gli strumenti ed i mezzi utilizzati per l'attuazione delle decisioni e in parte anche per l'operatività dei Contitolari soprattutto in relazione alle misure di sicurezza fisiche, organizzative e tecniche;
- l'approccio basato sul rischio;
- i profili e la politica di sicurezza dei dati personali, la procedura del Data Breach e la procedura di valutazione di impatto sulla protezione dei dati personali (DPIA);
- la gestione della procedura di esercizio dei diritti dell'Interessato;

- una raccolta congiunta delle procedure sulla protezione dei dati personali attraverso la tenuta comune e gestione di un modello organizzativo.
2. La contitolarità è riferita al trattamento dei dati personali ed ha ad oggetto il trattamento di tutti i dati già presenti, in tutti gli archivi sia cartacei che informatizzati, e di tutti quelli che si acquisiranno in futuro. Il flusso dei dati personali sarà così strutturato: _____.
3. Con il presente accordo i Contitolari convengono che i dati personali presenti negli archivi tanto cartacei quanto informatizzati, nonché quelli futuri, verranno trattati per le seguenti finalità: _____.
4. Le attività alla base del presente accordo comportano il trattamento delle seguenti categorie di dati personali: _____.
5. Le categorie di Interessati sono: _____

Articolo 3 – Durata ed effetti conseguenti allo scioglimento del Contratto
1. Il presente accordo diviene efficace tra le parti immediatamente all'atto della sua sottoscrizione e sarà valido ed efficace sino alla scadenza, originale o prorogata del rapporto convenzionale che lega i Contitolari, ovvero alla sua cessazione di validità ed efficacia a qualsiasi causa dovuta.
2. Il Trattamento dei dati personali in regime di contitolarità, pertanto, deve avere una durata non superiore a quella necessaria agli scopi per i quali i dati personali sono stati raccolti e tali dati devono essere conservati nei sistemi e nelle banche dati dei Contitolari in una forma che consenta l'identificazione degli Interessati per un periodo di tempo non superiore a quello in precedenza indicato, fatto salvo che il trattamento e la conservazione dei dati medesimi ad opera di ciascuno dei Contitolari sia imposta dalla normativa vigente.
3. A seguito della cessazione del trattamento, nonché a seguito della cessazione del rapporto convenzionale sottostante, qualunque ne sia la causa, i Contitolari saranno tenuti a provvedere alla integrale distruzione dei dati personali trattati, salvi solo i casi in cui la conservazione dei dati sia richiesta da norme di legge e/o altre finalità od il caso in cui si verifichino circostanze autonome e ulteriori che giustifichino la continuazione del trattamento dei dati da parte dei singoli Contitolari, con modalità limitate e per il periodo di tempo a ciò strettamente necessario.
4. Ciascun Contitolare provvede a rilasciare apposita dichiarazione scritta contenente l'attestazione che, presso di sè, non esiste alcuna copia dei dati personali e delle informazioni trattate nell'ambito del progetto comune. Sul contenuto di tale dichiarazione l'altro Contitolare si riserva il diritto di effettuare controlli e verifiche volte ad accertarne la veridicità.

Articolo 4 – Obblighi tra le parti
1. La tutela dei dati personali è fondata sull'osservanza dei principi illustrati nel presente documento che i Contitolari si impegnano a diffondere, rispettare e far rispettare ai propri amministratori, ai propri dipendenti e collaboratori ed ai soggetti terzi con cui collaborano nello svolgimento della propria attività istituzionale. In particolare, i Contitolari sono impegnati affinché la politica della protezione dati personali, e quanto ne consegue, sia compresa, attuata e sostenuta da tutti i soggetti, interni ed esterni, coinvolti nelle attività dei Contitolari, tenuto conto della loro realtà concreta, delle loro possibilità anche economiche e dei loro valori.
2. I Contitolari si impegnano a mantenere e garantire la riservatezza e la protezione dei dati personali raccolti, trattati e utilizzati in virtù del rapporto di contitolarità. In particolare, essi, anche disgiuntamente tra loro, si impegnano a:
a) comunicare e diffondere la propria politica in merito alla protezione dei dati personali;
b) prestare ascolto e attenzione a tutte le parti interessate proprie – a mero titolo esemplificativo, amministratori, personale dipendente e collaboratore, cittadini, utenti e beneficiari di prestazioni

anche di natura assistenziale, fornitori, consulenti – e tenendo in debito conto le loro istanze in materia di trattamento di dati personali e dando pronto riscontro;
c) trattare i dati personali in modo lecito, corretto e trasparente in linea con i principi costituzionali e con la normativa vigente in materia, in particolare il RGPD, e solo per il tempo strettamente necessario alle finalità previste, comprese quelle per ottemperare agli obblighi di legge;
d) raccogliere i dati personali limitandosi a quelli indispensabili per effettuare le attività costituenti il progetto comune (dati personali pertinenti e limitati);
e) trattare i dati personali secondo i principi di trasparenza per le sole finalità specifiche ed espresse nelle proprie informative;
f) adottare processi di aggiornamento e di rettifica dei dati personali trattati per assicurarsi che i dati personali siano, per quanto possibile, corretti e aggiornati;
g) conservare e tutelare i dati personali di cui è in possesso con le migliori tecniche di preservazione disponibili;
h) garantire il continuo aggiornamento delle misure di protezione dei dati personali. Tale impegno sarà costantemente seguito nell'ambito del principio di responsabilizzazione mettendo in atto, con costanza, misure tecniche e organizzative adeguate e politiche idonee, per garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al RGPD tenuto conto dello stato dell'arte, della natura dei dati personali custoditi e dei rischi ai quali sono esposti. Ciascun Contitolare eseguirà un monitoraggio periodico sul livello di sicurezza raggiunto, al fine di renderlo sempre adeguato al rischio;
i) garantire il tempestivo recupero della disponibilità dei dati personali in caso di incidente fisico o tecnico
l) rendere chiare, trasparenti e pertinenti le modalità di trattamento dei dati personali e la loro conservazione in maniera da garantirne un'adeguata sicurezza;
m) favorire lo sviluppo del senso di responsabilizzazione e la consapevolezza dell'intera organizzazione verso i dati personali, visti come dati di proprietà dei singoli interessati;
n) assicurare il rispetto delle disposizioni legislative e regolamentari applicabili alla tutela dei dati personali aggiornando eventualmente la gestione della protezione dei dati personali;
o) prevenire e minimizzare, compatibilmente con le risorse disponibili, l'impatto di potenziali violazioni o trattamenti illeciti e/o dannosi dei dati personali;
p) promuovere l'inserimento della protezione dati personali nel piano di miglioramento continuo che il Contitolare persegue con i propri sistemi di gestione.
3. I Contitolari si impegnano con particolare riguardo all'esercizio dei diritti dell'Interessato e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, ad uniformare le modalità, lo stile i modelli e soprattutto le procedure per la protezione dei dati personali a favore dell'Interessato.
4. La comunicazione dei dati personali necessari a garantire il perseguimento del progetto comune avverrà curandone l'esattezza, la veridicità, l'aggiornamento, la pertinenza e la non eccedenza rispetto alle finalità per le quali sono stati raccolti e saranno successivamente trattati.

Articolo 5 - Incaricati e persone autorizzate
1. Ciascuno dei Contitolari dovrà identificare e designare le persone autorizzate ad effettuare operazioni di trattamento sui dati trattati nel perseguimento del progetto comune, identificando l'ambito autorizzativo consentito ai sensi dell'art. 29 del RGPD e provvedendo alla relativa formazione, anche in merito ai principi di liceità e correttezza a cui deve conformarsi la presente politica per la protezione dei dati personali e il trattamento dei dati personali nonché al rispetto delle misure di salvaguardia adottate.

2. Ciascuno dei Contitolari garantisce che i propri dipendenti e collaboratori sono affidabili ed hanno piena conoscenza della normativa primaria e secondaria in materia di protezione dei dati personali.
3. Ciascuno dei Contitolari identifica un referente interno alla propria struttura, con il compito di relazionarsi con analogo soggetto designato dall'altra parte, a presidio del corretto adempimento di quanto previsto dal presente accordo. Il nominativo ed i dati di contatto del referente interno sono tempestivamente comunicati all'altra parte.

Articolo 6 - Responsabili del trattamento

1. Ciascuno dei Contitolari il quale ravvisasse la necessità di avvalersi di un responsabile del trattamento per l'esecuzione di specifiche attività richieste nell'ambito del progetto comune, è tenuto a comunicarlo all'altra parte con congruo preavviso.
2. Su tale responsabile del trattamento sono imposti, mediante un contratto od un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, specifici obblighi in materia di protezione dei dati, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti della legge vigente.
3. I rapporti tra i Contitolari e gli eventuali responsabili del trattamento restano disciplinati dall'articolo 28 del RGPD.

Articolo 7 – Valutazione d'impatto e Violazioni di dati personali

1. Nei casi previsti dall'art. 35 del RGPD, la valutazione d'impatto sulla protezione dei dati personali ed il suo eventuale riesame, così come la consultazione preventiva di cui all'art. 36 del RGPD, sono a carico di _____, il quale informa tempestivamente l'altro Contitolare della relativa necessità e dell'attività compiuta.
2. In eventuali casi di violazione della sicurezza dei dati personali che comporti, accidentalmente od in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati e tali da mettere a rischio i diritti e le libertà degli individui i cui dati personali sono trattati nel contesto del progetto comune, l'attività di coordinamento ai fini dell'adempimento degli obblighi di cui agli articoli 33 e 34 del RGPD è affidata a _____ il quale curerà la predisposizione di un apposito documento (data breach policy), ove non già esistente ed adottato.
3. Al verificarsi di una violazione di dati personali, il Contitolare non assegnatario dell'attività di coordinamento provvederà:
a) ad informare l'altro Contitolare tempestivamente ed in ogni caso entro e non oltre 24 ore dalla scoperta dell'evento, tramite PEC, di essere venuto a conoscenza di una violazione fornendogli tutti i dettagli della violazione subita, in particolare una descrizione della natura della violazione dei dati personali, le categorie e il numero approssimativo di interessati coinvolti, nonché le categorie e il numero approssimativo di registrazioni dei dati in questione, l'impatto della violazione dei dati personali sugli Interessati coinvolti e le misure adottate per mitigare i rischi;
b) fornire assistenza per far fronte alla violazione ed alle sue conseguenze soprattutto in capo agli Interessati coinvolti. Esso si inoltre attiverà per mitigare gli effetti delle violazioni, proponendo tempestive azioni correttive ed attuando tutte le azioni correttive approvate e/o richieste dal Contitolare assegnatario dell'attività di coordinamento. Tali misure sono richieste al fine di garantire un livello di sicurezza adeguato al rischio correlato al Trattamento eseguito.
4. Ciascun Contitolare si impegna a predisporre e tenere aggiornato un registro interno delle violazioni di dati personali nonché a raccogliere e conservare tutti i documenti relativi ad ogni

violazione, compresi quelli inerenti alle circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Articolo 8 - Decisioni in merito ai trasferimenti internazionali di dati personali

1. Il presente accordo prevede che i dati personali saranno trattati all'interno del territorio dell'Unione Europea.
2. Nell'ipotesi in cui per questioni di natura tecnica e/o operativa si rendesse necessario avvalersi di soggetti ubicati al di fuori dell'Unione Europea, il trasferimento dei dati personali, limitatamente allo svolgimento di specifiche attività di Trattamento, sarà regolato in conformità a quanto previsto dal capo V del RGPD. Saranno quindi adottate tutte le cautele necessarie al fine di garantire la più totale protezione dei dati personali basando tale trasferimento: (i) su decisioni di adeguatezza dei paesi terzi destinatari espresse dalla Commissione Europea; (ii) su garanzie adeguate espresse dal soggetto terzo destinatario ai sensi dell'articolo 46 del RGPD; (iii) sull'adozione di norme vincolanti d'impresa.

Articolo 9 - Condivisione della procedura per l'esercizio dei diritti dell'Interessato

1. I Contitolari designano congiuntamente un referente unitario quale punto di contatto per gli interessati. Le richieste di esercizio dei diritti e gli eventuali reclami presentati dagli interessati saranno gestiti in via esclusiva dal referente unico, contattabile ai recapiti che saranno resi noti unitamente al suo nominativo, restando in ogni caso inteso che gli interessati potranno esercitare i propri diritti nei confronti di ciascun Contitolare.
2. In particolare, qualora il referente unitario riceva richieste provenienti dall'Interessato, finalizzate all'esercizio dei propri diritti, esso dovrà:
- darne tempestiva comunicazione scritta a ciascun Contitolare via posta elettronica certificata, allegando copia delle richieste ricevute;
- coordinarsi, ove necessario e per quanto di propria competenza, con le funzioni interne designate da ciascun Contitolare per gestire le relazioni con l'Interessato;
- verificare la sussistenza dei presupposti e consentirne, differirne o rifiutarne l'esercizio, dandone tempestiva comunicazione scritta a ciascun Contitolare via posta elettronica certificata.
3. Il referente unitario fornisce altresì assistenza a ciascuno dei Contitolari nell'ambito dei procedimenti amministrativi e giudiziari instaurati dall'Interessato o dall'Autorità di controllo in conseguenza dell'attività di cui al presente articolo.

Articolo 10 - Verifiche circa il rispetto delle regole di protezione dei dati personali

1. Ciascuno dei Contitolari riconosce all'altro il diritto di effettuare controlli (audit) relativamente alle operazioni aventi ad oggetto il trattamento dei dati personali nell'ambito del progetto comune. A tal fine, Ciascuno dei Contitolari ha il diritto di disporre – a propria cura e spese – verifiche a campione o specifiche attività di audit o di rendicontazione in ambito protezione dei dati personali e sicurezza, avvalendosi di personale espressamente incaricato a tale scopo, presso le sedi dell'altro.
2. Ciascuno dei Contitolari rende disponibile tutta la documentazione necessaria per dimostrare la conformità a tutti i suoi obblighi e per consentire la conduzione di audit, comprese le ispezioni, e per contribuire a tali verifiche.
3. Ciascuno dei Contitolari deve informare e coinvolgere tempestivamente l'altra parte in tutte le questioni riguardanti il trattamento dei dati personali ed in particolare nel caso di richieste di informazioni, controlli, ispezioni ed accessi da parte dell'Autorità di controllo;

Articolo 11 - Responsabilità per violazione delle disposizioni

I Contitolari si obbligano, in solido tra loro, a predisporre, attuare e mantenere aggiornati tutti gli adempimenti previsti in materia di protezione dei dati personali.

Articolo 12 - Responsabile della Protezione dei dati personali

1. Ciascuno dei Contitolari rende noto di aver provveduto alla nomina del Responsabile della Protezione dei Dati personali (RPD o DPO) in conformità alla previsione contenuta nell'art. 37, par. 1, lett a) del RGPD, individuando quale soggetto idoneo:

_____

Detto nominativo è stato altresì comunicato all'Autorità Garante per la Protezione dei dati personali con procedura telematica.

Articolo 13 – Clausole nulle o inefficaci

Qualora una o più clausole del presente accordo fossero o divenissero contrarie a norme imperative o di ordine pubblico, esse saranno considerate come non apposte e non incideranno sulla validità dello stesso, fatto salvo il diritto di ciascuna parte di chiedere una modifica dell'accordo ove la pura e semplice eliminazione della clausola nulla menomasse gravemente i suoi diritti.

Articolo 14 – Comunicazioni

Qualsiasi comunicazione relativa al presente accordo dovrà essere data per iscritto ed a mezzo di posta elettronica certificata, con ricevuta di accettazione e conferma di consegna, purché inviati o consegnati all'indirizzo indicato in testa all'accordo. Tale indirizzo potrà essere modificato da ciascuna delle Parti, dandone comunicazione all'altra ai sensi del presente articolo.

Articolo 15 – Disposizioni finali

Per quanto non espressamente indicato nella presente Appendice, i rinviano al RGPD, alle disposizioni di legge vigenti, nonché ai provvedimenti dell'Autorità di controllo.

ALLEGATO 4 - BOZZA DI ACCORDO SUL TRATTAMENTO DE DATI PERSONALI

ACCORDO SUL TRATTAMENTO DEI DATI PERSONALI TRA IL TITOLARE E IL RESPONSABILE SECONDO LA DECISIONE DI ESECUZIONE (UE) 2021/915 DELLA COMMISSIONE del 4 giugno 2021 relativa alle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento a norma dell'articolo 28, paragrafo 7, del regolamento (UE) 2016/679 del Parlamento europeo.

SEZIONE I

Clausola 1 - Scopo e ambito di applicazione

a) scopo delle presenti clausole contrattuali tipo (di seguito «clausole») è garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
b) i titolari del trattamento e i responsabili del trattamento di cui all'allegato I hanno accettato le presenti clausole al fine di garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679.
c) le presenti clausole si applicano al trattamento dei dati personali specificato all'allegato II.
d) gli allegati da I a IV costituiscono parte integrante delle clausole.
e) le presenti clausole lasciano impregiudicati gli obblighi cui è soggetto il titolare del trattamento a norma del regolamento (UE) 2016/679.
f) le presenti clausole non garantiscono, di per sé, il rispetto degli obblighi connessi ai trasferimenti internazionali conformemente al capo V del regolamento (UE) 2016/679.

Clausola 2 - Invariabilità delle clausole

a) le parti si impegnano a non modificare le clausole se non per aggiungere o aggiornare informazioni negli allegati.
b) ciò non impedisce alle parti di includere le clausole contrattuali tipo stabilite nelle presenti clausole in un contratto più ampio o di aggiungere altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le presenti clausole o ledano i diritti o le libertà fondamentali degli interessati.

Clausola 3 - Interpretazione

a) quando le presenti clausole utilizzano i termini definiti, rispettivamente, nel regolamento (UE) 2016/679, tali termini hanno lo stesso significato di cui al regolamento interessato.
b) le presenti clausole vanno lette e interpretate alla luce delle disposizioni del regolamento (UE) 2016/679.
c) le presenti clausole non devono essere interpretate in un senso che non sia conforme ai diritti e agli obblighi previsti dal regolamento (UE) 2016/679 o che pregiudichi i diritti o le libertà fondamentali degli interessati.

Clausola 4 - Gerarchia

In caso di contraddizione tra le presenti clausole e le disposizioni di accordi correlati, vigenti tra le parti al momento dell'accettazione delle presenti clausole, o conclusi successivamente, prevalgono le presenti clausole.

Clausola 5 - Clausola di adesione successiva (eventuale)

a) qualunque entità che non sia parte delle presenti clausole può, con l'accordo di tutte le parti, aderire alle presenti clausole in qualunque momento, in qualità di titolare del trattamento o di responsabile del trattamento, compilando gli allegati e firmando l'allegato I.
b) una volta compilati e firmati gli allegati di cui alla lettera a), l'entità aderente è considerata parte delle presenti clausole e ha i diritti e gli obblighi di un titolare del trattamento o di un responsabile del trattamento, conformemente alla sua designazione nell'allegato I.

c) l'entità aderente non ha diritti od obblighi derivanti a norma delle presenti clausole per il periodo precedente all'adesione.

SEZIONE II - OBBLIGHI DELLE PARTI

Clausola 6 - Descrizione del trattamento

I dettagli dei trattamenti, in particolare le categorie di dati personali e le finalità del trattamento per le quali i dati personali sono trattati per conto del titolare del trattamento, sono specificati nell'allegato II.

Clausola 7 - Obblighi delle parti

7.1. Istruzioni

a) il responsabile del trattamento tratta i dati personali soltanto su istruzione documentata del titolare del trattamento, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento. In tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto lo vieti per rilevanti motivi di interesse pubblico. Il titolare del trattamento può anche impartire istruzioni successive per tutta la durata del trattamento dei dati personali. Tali istruzioni sono sempre documentate.

b) il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, le istruzioni del titolare del trattamento violino il regolamento (UE) 2016/679 o le disposizioni applicabili, nazionali o dell'Unione, relative alla protezione dei dati.

7.2. Limitazione delle finalità

Il responsabile del trattamento tratta i dati personali soltanto per le finalità specifiche del trattamento di cui all'allegato II, salvo ulteriori istruzioni del titolare del trattamento.

7.3. Durata del trattamento dei dati personali

Il responsabile del trattamento tratta i dati personali soltanto per la durata specificata nell'allegato II.

7.4. Sicurezza del trattamento

a) il responsabile del trattamento mette in atto almeno le misure tecniche e organizzative specificate nell'allegato III per garantire la sicurezza dei dati personali. Ciò include la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati (violazione dei dati personali). Nel valutare l'adeguato livello di sicurezza, le parti tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per gli interessati.

b) il responsabile del trattamento concede l'accesso ai dati personali oggetto di trattamento ai membri del suo personale soltanto nella misura strettamente necessaria per l'attuazione, la gestione e il controllo del contratto. Il responsabile del trattamento garantisce che le persone autorizzate al trattamento dei dati personali ricevuti si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

7.5. Dati sensibili

Se il trattamento riguarda dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici o dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati relativi a condanne penali e a reati («dati sensibili»), il responsabile del trattamento applica limitazioni specifiche e/o garanzie supplementari.

7.6. Documentazione e rispetto

a) le parti devono essere in grado di dimostrare il rispetto delle presenti clausole.

b) il responsabile del trattamento risponde prontamente e adeguatamente alle richieste di informazioni del titolare del trattamento relative al trattamento dei dati conformemente alle presenti clausole.
c) il responsabile del trattamento mette a disposizione del titolare del trattamento tutte le informazioni necessarie a dimostrare il rispetto degli obblighi stabiliti nelle presenti clausole e che derivano direttamente dal regolamento (UE) 2016/679. Su richiesta del titolare del trattamento, il responsabile del trattamento consente e contribuisce alle attività di revisione delle attività di trattamento di cui alle presenti clausole, a intervalli ragionevoli o se vi sono indicazioni di inosservanza. Nel decidere in merito a un riesame o a un'attività di revisione, il titolare del trattamento può tenere conto delle pertinenti certificazioni in possesso del responsabile del trattamento.
d) il titolare del trattamento può scegliere di condurre l'attività di revisione autonomamente o incaricare un revisore indipendente. Le attività di revisione possono comprendere anche ispezioni nei locali o nelle strutture fisiche del responsabile del trattamento e, se del caso, sono effettuate con un preavviso ragionevole.
e) su richiesta, le parti mettono a disposizione della o delle autorità di controllo competenti le informazioni di cui alla presente clausola, compresi i risultati di eventuali attività di revisione.

7.7. Ricorso a sub-responsabili del trattamento
a) OPZIONE 1: AUTORIZZAZIONE PRELIMINARE SPECIFICA: Il responsabile del trattamento non può subcontrattare a un sub-responsabile del trattamento i trattamenti da effettuare per conto del titolare del trattamento conformemente alle presenti clausole senza la previa autorizzazione specifica scritta del titolare del trattamento. Il responsabile del trattamento presenta la richiesta di autorizzazione specifica almeno [SPECIFICARE IL PERIODO] prima di ricorrere al sub-responsabile del trattamento in questione, unitamente alle informazioni necessarie per consentire al titolare del trattamento di decidere in merito all'autorizzazione. L'elenco dei sub-responsabili del trattamento autorizzati dal titolare del trattamento figura nell'allegato IV. Le parti tengono aggiornato tale allegato.
OPZIONE 2: AUTORIZZAZIONE SCRITTA GENERALE: Il responsabile del trattamento ha l'autorizzazione generale del titolare del trattamento per ricorrere a sub-responsabili del trattamento sulla base di un elenco concordato. Il responsabile del trattamento informa specificamente per iscritto il titolare del trattamento di eventuali modifiche previste di tale elenco riguardanti l'aggiunta o la sostituzione di sub-responsabili del trattamento con un anticipo di almeno [SPECIFICARE IL PERIODO], dando così al titolare del trattamento tempo sufficiente per poter opporsi a tali modifiche prima del ricorso al o ai sub-responsabili del trattamento in questione. Il responsabile del trattamento fornisce al titolare del trattamento le informazioni necessarie per consentirgli di esercitare il diritto di opposizione.
b) qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento per l'esecuzione di specifiche attività di trattamento (per conto del responsabile del trattamento), stipula un contratto che impone al sub-responsabile del trattamento, nella sostanza, gli stessi obblighi in materia di protezione dei dati imposti al responsabile del trattamento conformemente alle presenti clausole. Il responsabile del trattamento si assicura che il sub-responsabile del trattamento rispetti gli obblighi cui il responsabile del trattamento è soggetto a norma delle presenti clausole e del regolamento (UE) 2016/679.
c) su richiesta del titolare del trattamento, il responsabile del trattamento gli fornisce copia del contratto stipulato con il sub-responsabile del trattamento e di ogni successiva modifica. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, il responsabile del trattamento può espungere informazioni dal contratto prima di trasmetterne una copia.
d) il responsabile del trattamento rimane pienamente responsabile nei confronti del titolare del trattamento dell'adempimento degli obblighi del sub-responsabile del trattamento derivanti dal contratto che questi ha stipulato con il responsabile del trattamento. Il responsabile del trattamento notifica al titolare del trattamento qualunque inadempimento, da parte del sub-responsabile del trattamento, degli obblighi contrattuali.
e) il responsabile del trattamento concorda con il sub-responsabile del trattamento una clausola del terzo beneficiario secondo la quale, qualora il responsabile del trattamento sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente, il titolare del trattamento ha diritto di risolvere

il contratto con il sub-responsabile del trattamento e di imporre a quest'ultimo di cancellare o restituire i dati personali.

7.8. Trasferimenti internazionali

a) qualunque trasferimento di dati verso un paese terzo o un'organizzazione internazionale da parte del responsabile del trattamento è effettuato soltanto su istruzione documentata del titolare del trattamento o per adempiere a un requisito specifico a norma del diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento, e nel rispetto del capo V del regolamento (UE) 2016/679.

b) il titolare del trattamento conviene che, qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento conformemente alla clausola 7.7 per l'esecuzione di specifiche attività di trattamento (per conto del titolare del trattamento) e tali attività di trattamento comportino il trasferimento di dati personali ai sensi del capo V del regolamento (UE) 2016/679, il responsabile del trattamento e il sub-responsabile del trattamento possono garantire il rispetto del capo V del regolamento (UE) 2016/679 utilizzando le clausole contrattuali tipo adottate dalla Commissione conformemente all'articolo 46, paragrafo 2, del regolamento (UE) 2016/679, purché le condizioni per l'uso di tali clausole contrattuali tipo siano soddisfatte.

Clausola 8 - Assistenza al titolare del trattamento

a) il responsabile del trattamento notifica prontamente al titolare del trattamento qualunque richiesta ricevuta dall'interessato. Non risponde egli stesso alla richiesta, a meno che sia stato autorizzato in tal senso dal titolare del trattamento.

b) il responsabile del trattamento assiste il titolare del trattamento nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti, tenuto conto della natura del trattamento. Nell'adempiere agli obblighi di cui alle lettere a) e b), il responsabile del trattamento si attiene alle istruzioni del titolare del trattamento.

c) oltre all'obbligo di assistere il titolare del trattamento in conformità della clausola 8, lettera b), il responsabile del trattamento assiste il titolare del trattamento anche nel garantire il rispetto dei seguenti obblighi, tenuto conto della natura del trattamento dei dati e delle informazioni a disposizione del responsabile del trattamento:

1) l'obbligo di effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali («valutazione d'impatto sulla protezione dei dati») qualora un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;

2) l'obbligo, prima di procedere al trattamento, di consultare la o le autorità di controllo competenti qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio;

3) l'obbligo di garantire che i dati personali siano esatti e aggiornati, informando senza indugio il titolare del trattamento qualora il responsabile del trattamento venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti o obsoleti;

4) gli obblighi di cui all'articolo 32 regolamento (UE) 2016/679.

d) le parti stabiliscono nell'allegato III le misure tecniche e organizzative adeguate con cui il responsabile del trattamento è tenuto ad assistere il titolare del trattamento nell'applicazione della presente clausola, nonché l'ambito di applicazione e la portata dell'assistenza richiesta.

Clausola 9 - Notifica di una violazione dei dati personali

In caso di violazione dei dati personali, il responsabile del trattamento coopera con il titolare del trattamento e lo assiste nell'adempimento degli obblighi che incombono a quest'ultimo a norma degli articoli 33 e 34 del regolamento (UE) 2016/679, tenuto conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento.

9.1. Violazione riguardante dati trattati dal titolare del trattamento

In caso di una violazione dei dati personali trattati dal titolare del trattamento, il responsabile del trattamento assiste il titolare del trattamento:

a) nel notificare la violazione dei dati personali alla o alle autorità di controllo competenti, senza ingiustificato ritardo dopo che il titolare del trattamento ne è venuto a conoscenza, se del caso (a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche);
b) nell'ottenere le seguenti informazioni che, in conformità dell'articolo 33, paragrafo 3, del regolamento (UE) 2016/679, devono essere indicate nella notifica del titolare del trattamento e includere almeno:
1) la natura dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
2) le probabili conseguenze della violazione dei dati personali;
3) le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali, se del caso anche per attenuarne i possibili effetti negativi.
Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.
c) nell'adempiere, in conformità dell'articolo 34 del regolamento (UE) 2016/679, all'obbligo di comunicare senza ingiustificato ritardo la violazione dei dati personali all'interessato, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

9.2. Violazione riguardante dati trattati dal responsabile del trattamento
In caso di una violazione dei dati personali trattati dal responsabile del trattamento, quest'ultimo ne dà notifica al titolare del trattamento senza ingiustificato ritardo dopo esserne venuto a conoscenza. La notifica contiene almeno:
a) una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati in questione);
b) i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;
c) le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi.
Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.
Le parti stabiliscono nell'allegato III tutti gli altri elementi che il responsabile del trattamento è tenuto a fornire quando assiste il titolare del trattamento nell'adempimento degli obblighi che incombono al titolare del trattamento a norma degli articoli 33 e 34 del regolamento (UE) 2016/679.

SEZIONE III - DISPOSIZIONI FINALI

Clausola 10 - Inosservanza delle clausole e risoluzione
a) fatte salve le disposizioni del regolamento (UE) 2016/679, qualora il responsabile del trattamento violi gli obblighi che gli incombono a norma delle presenti clausole, il titolare del trattamento può dare istruzione al responsabile del trattamento di sospendere il trattamento dei dati personali fino a quando quest'ultimo non rispetti le presenti clausole o non sia risolto il contratto. Il responsabile del trattamento informa prontamente il titolare del trattamento qualora, per qualunque motivo, non sia in grado di rispettare le presenti clausole.
b) il titolare del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali conformemente alle presenti clausole qualora:
1) il trattamento dei dati personali da parte del responsabile del trattamento sia stato sospeso dal titolare del trattamento in conformità della lettera a) e il rispetto delle presenti clausole non sia ripristinato entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;
2) il responsabile del trattamento violi in modo sostanziale o persistente le presenti clausole o gli obblighi che gli incombono a norma del regolamento (UE) 2016/679;
3) il responsabile del trattamento non rispetti una decisione vincolante di un organo giurisdizionale competente o della o delle autorità di controllo competenti per quanto riguarda i suoi obblighi in conformità delle presenti clausole o del regolamento (UE) 2016/679.

c) il responsabile del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali a norma delle presenti clausole qualora, dopo aver informato il titolare del trattamento che le sue istruzioni violano i requisiti giuridici applicabili in conformità della clausola 7.1, lettera b), il titolare del trattamento insista sul rispetto delle istruzioni.
d) dopo la risoluzione del contratto il responsabile del trattamento, a scelta del titolare del trattamento, cancella tutti i dati personali trattati per conto del titolare del trattamento e certifica a quest'ultimo di averlo fatto, oppure restituisce al titolare del trattamento tutti i dati personali e cancella le copie esistenti, a meno che il diritto dell'Unione o dello Stato membro non richieda la conservazione dei dati personali. Finché i dati non sono cancellati o restituiti, il responsabile del trattamento continua ad assicurare il rispetto delle presenti clausole.

ALLEGATO I
ELENCO DELLE PARTI

TITOLARE DEL TRATTAMENTO: [Identità e dati di contatto del/dei titolari del trattamento e, ove applicabile, del suo/loro responsabile della protezione dei dati]

1. DENOMINAZIONE ENTE:

.....
.....

Indirizzo e recapito PEC:

.....
.....

Nome, qualifica e dati di contatto della persona che sottoscrive l'accordo:

.....
.....

Nome e dati di contatto del responsabile della protezione dei dati (RPD):

.....
.....

Firma e data di adesione: .....

N.B.: in caso di contitolarità, indicare gli stessi campi in relazione a tutti i contitolari

** *** **

RESPONSABILE/I DEL TRATTAMENTO [Identità e dati di contatto del/dei responsabili del trattamento e, ove applicabile, del suo/loro responsabile della protezione dei dati]

1. DENOMINAZIONE ENTE / OPERATORE ECONOMICO:

.....
.....

Indirizzo e recapito PEC:

.....
.....

Nome, qualifica e dati di contatto della persona che sottoscrive l'accordo:

.....
.....

Nome e dati di contatto del responsabile della protezione dei dati (RPD):

.....
.....

Firma e data di adesione: .....

2. DENOMINAZIONE ENTE / OPERATORE ECONOMICO:

.....
.....

Indirizzo e recapito PEC:

.....
.....

Nome, qualifica e dati di contatto della persona che sottoscrive l'accordo:

.....
.....

Nome e dati di contatto del responsabile della protezione dei dati (RPD):

.....
.....

Firma e data di adesione: .....

N.B: In caso di Raggruppamento Temporaneo di Imprese (RTI), vanno indicati anche i mandanti che svolgano attività di trattamento di dati personali per conto del titolare del trattamento.

ALLEGATO II
DESCRIZIONE DEL TRATTAMENTO

Categorie di interessati i cui dati personali sono trattati:

[ ] Dipendenti/Consulenti
[ ] Utenti/Contraenti/Abbonati/Clienti (attuali o potenziali)
[ ] Associati, soci, aderenti, simpatizzanti, sostenitori
[ ] Soggetti che ricoprono cariche sociali
[ ] Beneficiari o assistiti
[ ] Pazienti
[ ] Minori
[ ] Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
[ ] Altro (specificare .....)

Categorie di dati personali trattati:

[ ] Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale)
[ ] Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
[ ] Dati di accesso e di identificazione (username, password, customer ID, altro…)
[ ] Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…)
[ ] Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro…)
[ ] Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza
[ ] Dati di profilazione
[ ] Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…)
[ ] Dati relativi all'ubicazione
[ ] Altro (specificare .....)

Dati sensibili trattati (se del caso) e limitazioni o garanzie applicate che tengono pienamente conto della natura dei dati e dei rischi connessi, ad esempio una rigorosa limitazione delle finalità, limitazioni all'accesso (tra cui accesso solo per il personale che ha seguito una formazione specializzata), tenuta di un registro degli accessi ai dati, limitazioni ai trasferimenti successivi o misure di sicurezza supplementari:

[ ] Dati che rivelano l'origine razziale o etnica
[ ] Dati che rivelano le opinioni politiche
[ ] Dati che rivelano le convinzioni religiose o filosofiche
[ ] Dati che rivelano l'appartenenza sindacale
[ ] Dati relativi alla vita sessuale o all'orientamento sessuale
[ ] Dati relativi alla salute
[ ] Dati genetici
[ ] Dati biometrici

Natura del trattamento

.....
.....

Finalità per le quali i dati personali sono trattati per conto del titolare del trattamento

.....
.....

Durata del trattamento

.....
.....

Per il trattamento da parte di (sub-)responsabili del trattamento, specificare anche la materia disciplinata, la natura e la durata del trattamento

.....
.....

ALLEGATO III
MISURE TECNICHE E ORGANIZZATIVE PER GARANTIRE LA SICUREZZA DEI DATI

Descrizione delle misure di sicurezza tecniche ed organizzative che devono essere messe in atto dal o dai responsabili del trattamento (comprese le eventuali certificazioni pertinenti) per garantire un adeguato livello di sicurezza, tenuto conto della natura, dell'ambito di applicazione, del contesto e della finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche.

[ ] misure generali
Registro dei trattamenti
Il responsabile del trattamento tiene per iscritto un registro delle attività relative al trattamento svolte per conto del Titolare e delle applicazioni informatizzate utilizzate, nel pieno rispetto del RGPD.
Persone autorizzate
Il Responsabile del Trattamento si impegna a tenere ed aggiornare, in caso di modifiche, l'elenco degli operatori autorizzati ed opportunamente formati in materia di protezione dei dati personali, impartendo loro, per iscritto, specifiche istruzioni su come trattare i dati personali nell'ambito della propria attività, curando, in particolare, il profilo della sicurezza dei dati, ai sensi dell'articolo 29 del RGPD. Il Titolare può richiedere una prova documentata al fine di verificare tali adempimenti.
Persone autorizzate in qualità di Amministratori di Sistema
Il Responsabile, qualora di avvalga di personale che svolga compiti riconducibili a quelli di Amministratori di Sistema, si impegna a conformarsi al Provvedimento generale del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", così come modificato dal Provvedimento del Garante del 25 giugno 2009 "Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento", così come eventualmente modificato o sostituito dallo stesso Garante, e ad ogni altro pertinente provvedimento dell'Autorità.
Il Titolare può richiedere una prova documentata al fine di verificare tali adempimenti.
Responsabilità
Il responsabile s'impegna a mantenere indenne il titolare da qualsiasi responsabilità, danno, incluse le spese legali od altro onere che possa derivare da pretese, azioni o procedimenti avanzate da terzi a seguito dell'eventuale illiceità o non correttezza delle operazioni di trattamento dei dati personali che sia imputabile a fatto, comportamento od omissione del responsabile (o di suoi dipendenti e/o collaboratori), ivi incluse le eventuali sanzioni che dovessero essere comminate ai sensi del RGPD.
Il responsabile si impegna a comunicare prontamente al titolare eventuali situazioni sopravvenute che, per il mutare delle conoscenze acquisite in base al progresso tecnico o per qualsiasi altra ragione, possano incidere sulla propria idoneità alla prestazione dei servizi dedotti nel presente accordo.
Il titolare ha il diritto di reclamare dal responsabile la parte dell'eventuale risarcimento di cui dovesse essere chiamato a rispondere nei confronti di terzi per le violazioni commesse dal responsabile ai sensi dell'art. 82, paragrafo 5, del RGPD.
Comunicazioni
Qualsiasi comunicazione relativa al presente accordo ed al sottostante contratto dovrà essere data per iscritto ed a mezzo di posta elettronica certificata, con ricevuta di accettazione e conferma di consegna, purché inviati o consegnati all'indirizzo indicato nell'accordo stesso. Tale indirizzo potrà essere modificato da ciascuna delle parti, dandone comunicazione all'altra ai sensi del presente comma.
Foro competente
Per qualsiasi controversia che dovesse sorgere tra le parti in ordine all'interpretazione del presente accordo e la corretta esecuzione delle disposizioni contrattuali in esso contenute sarà competente il Foro di _____. È esclusa qualsiasi forma di arbitrato.

[ ] procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative adottate, al fine di garantire la sicurezza del trattamento;

[ ] misure per garantire la **minimizzazione** dei dati quali, a titolo esemplificativo:
- definizione di policy interne che vietino la raccolta di dati non necessari;
- definizione chiara delle finalità: identificare in modo specifico e documentato le finalità per cui i dati personali sono necessari prima di raccoglierli, sulla base di un confronto puntuale con il titolare;
- analisi di necessità e proporzionalità: valutare attentamente se la raccolta di ciascun dato personale sia strettamente necessaria e proporzionata rispetto alle finalità identificate;
- evitare la raccolta di dati "per sicurezza" o "in caso possano servire in futuro";
- limitazione dei dati raccolti: raccogliere solo i dati personali strettamente necessari per le finalità dichiarate. Evitare di raccogliere dati superflui o non pertinenti;
- privacy by design e by default: integrare il principio di minimizzazione dei dati fin dalla progettazione di sistemi, processi e servizi che trattano dati personali, limitando la raccolta e il trattamento dei dati al minimo necessario per impostazione predefinita;
- analisi dettagliata delle effettive necessità di dati per ciascuna attività;
- revisione periodica dei dati raccolti per eliminare quelli superflui;
- formazione del personale sulla minimizzazione dei dati;
- previsione di Audit e controlli interni: eseguire audit e controlli interni per valutare l'implementazione e l'efficacia delle misure di minimizzazione dei dati.

[ ] misure per garantire la **qualità** dei dati quali, a titolo esemplificativo;
Validazione e Accuratezza dei dati
- implementare procedure di convalida dei dati in fase di inserimento per ridurre errori;
- implementare controlli automatici e/o manuali per controllare la coerenza e l'accuratezza dei dati;
- implementare meccanismi di controllo qualità durante le fasi di elaborazione, migrazione ed archiviazione dei dati per individuare e correggere eventuali errori o incongruenze;
- coinvolgere i dipendenti in sessioni di formazione su tecniche di inserimento corretto dei dati;
-rivedere regolarmente i set di dati per identificare e risolvere discrepanze in modo proattivo;
- implementare sistemi di data quality monitoring;
- implementare processi di escalation per problemi di data quality;
Aggiornamento Periodico dei dati
- stabilire procedure chiare per l'aggiornamento dei dati personali, garantendo che le informazioni trattate siano sempre accurate e attuali;
- programmare attività regolari di aggiornamento per garantire che i dati siano sempre attuali;
- implementare notifiche automatiche per avvisare il personale della necessità di aggiornare informazioni critiche;
- utilizzare procedure di confronto dei dati con il titolare per mantenerne l'attualità;
- stabilire un protocollo per la rimozione o l'archiviazione di dati obsoleti;
Uniformità e Consistenza dei dati
- creare standard di inserimento dei dati per assicurare coerenza in tutta l'organizzazione;
- utilizzare formati predefiniti per dati comuni (es. date, unità di misura) per evitare discrepanze;
- integrare sistemi di gestione dei dati per sincronizzare le informazioni tra diverse piattaforme;
- condurre sessioni di formazione per garantire che i dipendenti comprendano l'importanza della consistenza dei dati.
- monitorare regolarmente i dati per rilevare e correggere incongruenze;
Gestione delle duplicazioni
- definire processi di deduplicazione e pulizia dei dati;
- implementare software di deduplicazione per identificare e unire dati duplicati;
- utilizzare identificatori univoci per garantire che ciascun record nel sistema sia unico;
- eseguire scansioni periodiche per rilevare eventuali duplicati;
- stabilire procedure per la verifica manuale di duplicati segnalati da sistemi automatizzati;

- educare il personale sull'importanza di evitare l'inserimento duplicato di dati.
Formazione del personale sulla gestione dei dati
- organizzare corsi specifici sulle procedure di raccolta e inserimento dati;
- sensibilizzare il personale sull'importanza dell'accuratezza dei dati;
- addestrare il personale all'uso corretto dei sistemi informativi;
- condividere best practices per mantenere alta la qualità dei dati;

[ ] misure per garantire la **conservazione** limitata dei dati;
- redigere una policy interna che definisca in modo preciso e documentato i tempi di conservazione di ogni tipologia di dato personale trattato per conto del titolare;
- considerare eventuali obblighi legali per la conservazione dei dati, come quelli fiscali o contrattuali;
- documentare le ragioni per eventuali estensioni dei tempi di conservazione;
- applicare una politica di revisione periodica dei termini di conservazione per assicurare la loro attualità;
- evitare di conservare dati oltre il tempo necessario al raggiungimento delle finalità dichiarate;
- implementare sistemi, come scadenziari, sistemi automatici di notifica o flussi di lavoro automatizzati, che permettano di monitorare la data di scadenza dei termini di conservazione ed attivare le procedure di cancellazione o revisione;
- utilizzare database e sistemi di archiviazione che consentano di impostare regole automatiche per la conservazione e la cancellazione dei dati al termine del periodo prestabilito;
- definire processi strutturati di cancellazione;
- utilizzare strumenti certificati di data wiping o ricorrere a fornitori specializzati per la distruzione certificata;
- definire processi di gestione sicura dei supporti di memorizzazione dismessi;
- documentare le operazioni di distruzione dei dati;
- sensibilizzare e formare il personale sull'importanza della conservazione limitata dei dati e sulle procedure aziendali da seguire;
- eseguire verifiche a campione sul rispetto dei tempi di conservazione;
- valutare l'utilizzo di tecniche di pseudonimizzazione o anonimizzazione per ridurre la quantità di dati personali conservati ed il rischio per gli interessati;

[ ] misure per garantire la **cancellazione o la restituzione** dei dati al termine dell'accordo;
Al termine della prestazione dei servizi relativi al trattamento dei dati personali, il responsabile del trattamento ha l'obbligo di restituire tutti i dati personali al titolare del trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati.
Il responsabile, su richiesta del titolare, provvede a rilasciare apposita dichiarazione scritta contenente l'attestazione che, presso di sè, non esiste alcuna copia dei dati personali e delle informazioni trattate per conto del titolare. Sul contenuto di tale dichiarazione il titolare si riserva il diritto di effettuare controlli e verifiche volte ad accertarne la veridicità, anche ricorrendo ad una terza parte, a condizione che la terza parte non abbia una relazione competitiva con il Responsabile stesso.
In caso di fallimento o sottoposizione ad altra procedura concorsuale del responsabile, ovvero in caso di mancato assolvimento da parte di quest'ultimo degli obblighi previsti ai commi che precedono, ovvero ancora in caso di omissione ovvero di sospensione anche parziale, da parte del responsabile, dell'esecuzione delle obbligazioni oggetto del presente accordo, il titolare, ove possibile e dandone opportuna comunicazione, potrà sostituirsi al responsabile nell'esecuzione delle obbligazioni ovvero potrà avvalersi di soggetto terzo in danno ed a spese del responsabile, fatto salvo il risarcimento del maggior danno
Il responsabile è tenuto a non comunicare, trasferire o condividere, i dati personali trattati per conto del titolare a terze parti, salvo qualora legislativamente richiesto e, in ogni caso, informandone preventivamente il titolare.

[ ] azioni di **Valutazione e Mitigazione dei Rischi** quali, a titolo esemplificativo:
- condurre valutazioni per identificare e mitigare i rischi associati ai trattamenti effettuati per conto del titolare;
- adottare procedure interne per valutare la conformità delle pratiche di trattamento dei dati;

- utilizzare strumenti software per monitorare ed analizzare i rischi emergenti e le vulnerabilità;
- collaborare con esperti esterni per condurre audit indipendenti della sicurezza delle informazioni;
- implementare misure correttive tempestive in risposta ai risultati delle valutazioni del rischio;

[ ] misure di **gestione degli Accessi ai dati** (identificazione e autorizzazione dell'utente) quali, a titolo esemplificativo:
- implementare sistemi di controllo degli accessi basati sui ruoli (RBAC) per garantire che solo il personale autorizzato possa accedere ai dati personali (principio del privilegio minimo);
- stabilire procedure di autorizzazione multilivello per modifiche critiche ai dati;
- utilizzare l'autenticazione multi-fattore (MFA) per aumentare la sicurezza agli accessi;
- revisionare regolarmente i permessi di accesso per accertarsi che siano aggiornati e pertinenti;
- stabilire procedure di revoca degli accessi per dipendenti che abbia cessato il proprio rapporto o trasferiti ad altre posizioni;
- eseguire audit regolari per assicurarsi che le policy di accesso siano rispettate.

[ ] misure per garantire la **sicurezza fisica** dei luoghi in cui i dati personali sono trattati quali, a titolo esemplificativo:
Controllo degli Accessi Fisici
- implementare sistemi di controllo degli accessi come badge elettronici o codici di accesso per limitare l'accesso ai locali dove sono conservati i dati;
- monitorare e registrare chi accede alle aree sensibili attraverso log di accesso che possono essere verificati e revisionati;
- assicurarsi che solo il personale autorizzato possa entrare nelle aree in cui sono presenti dati personali o server;
- installare sistemi di videosorveglianza per monitorare continuamente le aree di accesso critico;
- effettuare controlli periodici per garantire che i dispositivi di accesso siano funzionanti e adeguati alle necessità di sicurezza.
Protezione dei dispositivi hardware
- mantenere un inventario aggiornato di tutti i supporti di memorizzazione (server, hard disk, chiavette USB, ecc.) che contengono dati personali, trattati per conto del titolare, tenendo traccia della loro posizione e del loro utilizzo;
- collocare server ed apparecchiature critiche in armadi o stanze chiuse a chiave per prevenire accessi non autorizzati;
- utilizzare allarmi e sistemi di rilevamento delle intrusioni per segnalare immediatamente accessi non autorizzati o forzature;
- assicurarsi che i dispositivi mobili contenenti dati personali (laptop, smartphone) abbiano misure di sicurezza come blocchi di sicurezza fisici e crittografia dei dati;
- implementare pratiche di gestione del ciclo di vita per dispositivi hardware, comprendendo la tracciabilità e la gestione appropriata dello smaltimento;
- predisporre ed osservare protocolli rigorosi per il trasporto e lo spostamento delle apparecchiature contenenti dati personali;
Protezione delle Strutture
- verificare che le strutture abbiano una protezione adeguata contro incendi, inondazioni e altre calamità naturali;
- installare rilevatori di fumo, sensori d'inondazione e sistemi di estinzione degli incendi per ridurre il rischio di danni fisici ai dati;
- implementare protezioni antisismiche nelle aree soggette a terremoti per prevenire danni strutturali;
- assicurare la tenuta e l'efficienza degli impianti elettrici e di climatizzazione per prevenire interruzioni che possano compromettere l'integrità delle apparecchiature;
- pianificare e testare regolarmente piani di risposta alle emergenze per mitigare l'impatto di disastri fisici;
Gestione dei visitatori
- stabilire politiche chiare per l'accesso dei visitatori alle aree sensibili delle strutture;

- richiedere ai visitatori di firmare registri di ingresso e di essere sempre accompagnati da personale autorizzato;
- fornire badge temporanei per i visitatori per distinguerli facilmente dal personale interno e monitorarne i movimenti;
- limitare le visite a orari specifici e solo alle aree pertinenti alla finalità della visita;
- educare il personale sulle procedure di gestione dei visitatori per garantire la conformità alle politiche aziendali;

[ ] misure di **pseudonimizzazione e cifratura** dei dati personali quali, a titolo esemplificativo:
- implementare la cifratura dei dati sia in transito che a riposo per proteggerli da accessi non autorizzati (utilizzo di protocolli HTTPS per le comunicazioni web, cifratura del disco rigido dei server che ospitano i dati personali, impiego di VPN per l'accesso remoto);
- utilizzare tecniche di hashing per oscurare gli identificativi diretti;
- utilizzare tecniche di pseudonimizzazione per separare l'identità degli utenti dai dati grezzi;
- cifratura dei database e dei backup;
- assicurarsi che le chiavi di cifratura siano gestite in modo sicuro e accessibili solo al personale autorizzato;
- effettuare audit regolari per verificare l'efficacia delle misure di cifratura;
- formare il personale su come maneggiare dati cifrati e pseudonimizzati, garantendo la loro corretta gestione;
[ ] misure di anonimizzazione dei dati, quando possibile, come l'aggregazione dei dati a livello statistico, la rimozione di informazioni direttamente identificative, ecc.

[ ] misure di **protezione dei dati durante la trasmissione** quali, a titolo esemplificativo:
- prevedere l'utilizzo di algoritmi di cifratura robusti e riconosciuti (es. AES-256) per la cifratura dei dati in transito;
- definire modalità sicure per lo scambio e la gestione delle chiavi di cifratura, ad esempio tramite protocolli di key agreement o sistemi di gestione delle chiavi centralizzati;
- utilizzare protocolli di cifratura come TLS per le comunicazioni via web (HTTPS);
- implementare della cifratura end-to-end per le comunicazioni e-mail;
- implementare sistemi di cifratura dei dati trasmessi su reti wireless;
- utilizzare VPN per le connessioni remote;
- imporre al proprio personale l'utilizzo di canali di trasmissione sicuri e controllati, limitando o vietando l'utilizzo di metodi di trasmissione non sicuri;
- effettuare una valutazione della sicurezza dei canali utilizzati, considerando fattori come la riservatezza, l'integrità e l'autenticazione;
- prevedere la cifratura dei dispositivi mobili e rimovibili;
- prevedere limitazioni al trasporto fisico di supporti con dati non cifrati;
- prevedere backup cifrati dei dati in transito;
- prevedere la segregazione dei dati personali da altri dati durante la trasmissione, ad esempio tramite l'utilizzo di VLAN dedicate o container crittografati;
- definire misure per proteggere i dati da accessi non autorizzati durante il transito, come l'autenticazione e l'autorizzazione a livello di dispositivo o di applicazione;
- prevedere la registrazione dettagliata di tutti gli accessi e le operazioni sui dati durante la trasmissione, includendo timestamp, utente, indirizzo IP e tipo di operazione;
- implementare sistemi di rilevamento delle intrusioni (IDS) per monitorare il traffico di rete e identificare attività sospette;
- assicurarsi che il personale, coinvolto nella trasmissione dei dati sia adeguatamente formato sulle procedure di sicurezza, sulle policy aziendali e sui rischi connessi alla trasmissione di dati personali;
- definire procedure chiare per la gestione degli incidenti di sicurezza durante la trasmissione dei dati, includendo la segnalazione tempestiva al titolare del trattamento e l'adozione di misure correttive;

[ ] piani di **Continuità Operativa e Ripristino dei dati** quali, a titolo esemplificativo:

- creare e mantenere aggiornati piani di continuità operativa che includano rapidi tempi di ripristino dei sistemi e dati critici;
- effettuare esercitazioni di simulazione per testare l'efficacia dei piani di continuità e ripristino;
- aggiornare regolarmente i piani di backup per includere nuove risorse e dati critici;
- definire una strategia di backup che preveda sia backup completi periodici che backup incrementali frequenti, in modo da ridurre la perdita di dati in caso di incidente e ottimizzare l'utilizzo dello spazio di archiviazione;
- eseguire regolarmente backup dei dati adottando il principio del "3-2-1": almeno tre copie dei dati; utilizzando almeno due sistemi differenti, di cui una copia deve essere conservata off-site, per assicurare la disponibilità dei dati anche in caso di disastro che comprometta la sede principale;
- utilizzare servizi e piattaforme di backup che rispettino gli standard di protezione dati;
- valutare l'utilizzo di soluzioni di backup che offrano funzionalità di sicurezza avanzate, come la cifratura end-to-end, l'autenticazione a più fattori, la gestione granulare degli accessi e la registrazione di tutte le attività;
- per le macchine virtuali, oltre al backup, effettuare repliche che permettano un rapido ripristino;
- garantire che i supporti di backup fisici e logici e le repliche siano protetti da accessi non autorizzati;
- implementare procedure regolari di revisione e test dei backup per verificare l'integrità e la disponibilità dei dati archiviati;
- prevedere report periodici che attestino l'esecuzione dei backup, l'integrità dei dati e la conformità alle policy definite.
- stabilire procedure di risposta agli incidenti per affrontare rapidamente eventuali violazioni della sicurezza dei dati;
- formare il personale sulle pratiche di gestione delle emergenze e sul loro ruolo nei piani di continuità;

[ ] misure per garantire la **registrazione degli eventi informatici** quali, a titolo esemplificativo:
Implementazione di Sistemi di Log
- definire le responsabilità in merito alla registrazione degli eventi e collaborare per garantire che i sistemi di log siano in grado di fornire le informazioni necessarie al titolare per l'analisi degli incidenti e la notifica alle autorità competenti;
- implementare sistemi centralizzati che registrino tutti gli eventi rilevanti per la sicurezza ed il trattamento dei dati, come accessi, modifiche, cancellazioni, tentativi di accesso non autorizzati, anomalie
- assicurarsi che i log siano completi e dettagliati, includendo data, ora, utente responsabile e dettagli delle azioni effettuate;
- utilizzare strumenti di correlazione degli eventi;
- eseguire controlli incrociati tra diverse fonti di log;
- predisporre backup regolari dei log per garantirne la disponibilità in caso di necessità di verifica o ripristino;
Determinazione dei Periodi di Conservazione dei Log
- definire chiare politiche di conservazione per i log degli eventi;
- automatizzare i processi di eliminazione dei log scaduti per ridurre il rischio di conservazione eccessiva di dati;
Monitoraggio e Revisione Periodica
- condurre regolari audit dei processi di registrazione degli eventi per assicurare che siano conformi agli standard di sicurezza ed alla normativa di protezione dei dati personali;
- implementare un piano di azione per correggere eventuali discrepanze o lacune identificate durante le revisioni;
- stabilire un sistema di revisione ed auditing dei log per identificare rapidamente eventuali attività sospette;
- documentare tutte le revisioni e le conclusioni per fornire un quadro chiaro delle pratiche di gestione dei log;
Utilizzo di Strumenti di Analytics
- implementare sistemi di monitoraggio in tempo reale che analizzino i log di sistema ed inviino allerte in caso di eventi sospetti o anomalie, consentendo un intervento tempestivo.
- utilizzare dashboard e report per monitorare l'integrità e la sicurezza dei dati continuamente;

- sviluppare indicatori di performance chiave (KPI) per valutare l'efficacia dei sistemi di registrazione degli eventi e l'aderenza alle compliance;
Protezione e Sicurezza dei Dati di Log
- adottare strumenti di sincronizzazione temporale di tutti i sistemi per una corretta cronologia degli eventi
- adottare misure per garantire l'integrità e l'immutabilità dei log, ad esempio tramite firme digitali, sistemi WORM (Write Once Read Many) o blockchain, per evitare la manipolazione o la cancellazione dei dati di log;
- crittografare i dati di log per proteggerli da accessi non autorizzati durante il transito ed a riposo;
- implementare rigide misure di controllo degli accessi per i sistemi di log, assicurando che solo personale qualificato possa visualizzare o modificare i dati;
- testare la sicurezza delle infrastrutture di registrazione degli eventi contro potenziali vulnerabilità;
- definire workflow di escalation per gli eventi rilevanti;
- effettuare simulazioni di incidenti per migliorare le risposte alle situazioni di compromissione dei dati di log;
- eseguire periodicamente revisioni e audit dei sistemi di log per verificarne l'efficacia, l'adeguatezza e la conformità alle normative vigenti;
- attivare procedure e strumenti di analisi forense dei log in caso di incidenti;
Formazione
- formare e sensibilizzazione del personale addetto alla gestione dei sistemi ed alla sicurezza informatica sulle corrette procedure di gestione dei log (lettura ed interpretazione) e sulla loro importanza per l'individuazione e la gestione degli incidenti.

[ ] attività di **Formazione e Consapevolezza del Personale**:
- organizzare sessioni di formazione regolari per tutto il personale sulla protezione dei dati personali e sulle proprie responsabilità, simulazioni di attacchi informatici e data breach;
- diffondere linee guida e politiche aziendali chiare relative alla gestione dei dati personali;
- sensibilizzare il personale sui rischi legati alla sicurezza informatica e su come prevenirli;
- istituire programmi di aggiornamento continuo per far fronte a cambiamenti normativi e tecnologici;
- monitorare l'efficacia dei programmi di formazione attraverso test e feedback dai partecipanti;

[ ] misure specifiche che il responsabile del trattamento deve adottare per essere in grado di fornire assistenza al titolare del trattamento in relazione ad una violazione di dati personali (**data breach**):
- attenersi alle prescrizioni contenute nella procedura di gestione delle violazioni di dati personali adottata dal titolare del trattamento;
Comunicazione Tempestiva
- informare tempestivamente il titolare del trattamento una volta rilevata una violazione dei dati personali;
- stabilire canali di comunicazione chiari e diretti con il titolare per garantire una rapida risposta in caso di incidente;
Coordinamento delle Attività di Risposta
- collaborare attivamente con il titolare per valutare l'entità della violazione e le sue potenziali conseguenze;
- partecipare alla stesura e all'esecuzione di un piano di risposta per mitigare i danni e ripristinare la sicurezza;
- eseguire simulazioni e test periodici del piano di risposta agli incidenti per verificarne l'efficacia e garantire che il personale sia pronto ad intervenire in caso di reale necessità;
Documentazione e Reporting
- tenere una documentazione dettagliata di tutti gli aspetti dell'incidente, comprese le cause, le misure adottate e l'interazione con il titolare;
- supportare il titolare nel compilare il registro delle violazioni, necessario per eventuali verifiche da parte del Garante per la protezione dei dati personali;
Implementazione di Misure Correttive
- collaborare con il titolare per identificare ed implementare misure correttive atte a prevenire future violazioni simili;
- partecipare all'aggiornamento delle politiche e procedure di sicurezza in base alle lezioni apprese dall'incidente;
Assistenza nella Notifica al Garante

- fornire al titolare tutte le informazioni necessarie per una tempestiva notifica della violazione al Garante, qualora la violazione possa comportare rischi significativi per i diritti e le libertà delle persone fisiche;
- fornire supporto al titolare del trattamento per l'eventuale comunicazione del data breach all'interessato;
Registro delle violazioni
- mantenere un registro degli incidenti di sicurezza, anche qualora non vi fossero violazioni di dati personali e le medesime non determinassero l'obbligo di notifica all'Autorità di controllo, per coadiuvare il Titolare nel suo obbligo relativo al paragrafo 5 dell'art. 33 del RGPD. A seguito del verificarsi di incidenti di sicurezza, il Titolare potrà:
1. condurre audit, anche senza preavviso e avvalendosi di soggetti terzi;
2. prescrivere ulteriori misure di sicurezza, anche apportando modifiche a quelle previste dal presente accordo;
3. esercitare azioni di rivalsa nei confronti del responsabile;
4. applicare le penali contrattuali;
5. risolvere il contratto in essere con il responsabile.

[ ] misure specifiche che il responsabile del trattamento deve adottare per essere in grado di fornire assistenza al titolare del trattamento in relazione alla **Valutazione d'impatto sulla protezione dei dati personali (DPIA)**:
Collaborazione nella Valutazione dei Rischi
- fornire al titolare una chiara descrizione dei tipi di trattamenti eseguiti e dei dati coinvolti, contribuendo all'identificazione dei possibili rischi;
- supportare il titolare nell'analisi delle specifiche tecniche ed organizzative già esistenti per mitigare tali rischi;
Raccolta e Condivisione delle Informazioni
- garantire la disponibilità di tutte le informazioni necessarie riguardanti le modalità di trattamento ed il workflow dei dati personali;
- contribuire alla raccolta dei feedback e delle osservazioni derivanti dai trattamenti già attivi per affinare l'analisi dei rischi;
- contribuire alla stesura e revisione della documentazione relativa alla DPIA, assicurando che i processi siano chiaramente definiti e completi;
- manutenere registrazioni dettagliate delle discussioni, decisioni e azioni intraprese durante la valutazione d'impatto.
- partecipare alla revisione periodica della DPIA, in un'ottica di miglioramento continuo, offrendo consulenza nelle aree identificate come problematiche o a rischio;
- essere proattivi nell'adeguare misure e procedure in base al feedback raccolto e alle evoluzioni normative;
- supportare il titolare nella comunicazione con l'autorità Garante per la protezione dei dati personali, qualora la DPIA evidenziasse la necessità di una consultazione preventiva;

[ ] misure specifiche in relazione al **trasferimento dei dati personali verso Paesi terzi e Organizzazioni internazionali**:
Sono vietati i trasferimenti extra SEE verso Paesi terzi e Organizzazioni internazionali.
Salvo che il titolare del trattamento non fornisca, nel presente accordo o successivamente, istruzioni documentate riguardanti il trasferimento dei dati personali verso un paese terzo od una organizzazione internazionale, il responsabile del trattamento non ha diritto di eseguire tale trasferimento.

[ ] misure specifiche che il responsabile del trattamento deve adottare per essere in grado di fornire assistenza al titolare del trattamento in relazione alle istanze di **esercizio dei diritti riconosciuti all'interessato**:
- rendere all'interessato l'informativa sulla base del modello e delle informazioni fornite dal titolare del trattamento;
- ove necessario, acquisire dall'interessato il consenso al trattamento dei dati personali, sulla base della modulistica e delle informazioni fornite dal titolare;

- conservare, per conto del titolare del trattamento, il consenso espresso dall'interessato, garantendone l'integrità, la disponibilità e la riservatezza;
- fornire al titolare tutte le informazioni necessarie per rispondere alle richieste degli interessati nei tempi previsti dal RGPD;
- inoltrare tempestivamente al titolare tutte le richieste ricevute direttamente dagli interessati, fornendo tutte le informazioni in suo possesso e la documentazione di supporto;
- fornire al titolare il proprio supporto tecnico e specialistico per valutare l'ammissibilità delle richieste e verificare la corretta applicazione del RGPD, in particolare per quanto riguarda le basi giuridiche del trattamento, le eventuali limitazioni all'esercizio dei diritti e le modalità di risposta;
- collaborare attivamente con il titolare per dare seguito alle richieste degli interessati, fornendo l'accesso ai dati, apportando le modifiche richieste od eseguendo le altre operazioni necessarie nel rispetto della normativa e degli accordi contrattuali;
- mettere a disposizione del titolare strumenti e risorse tecniche necessarie per facilitare l'adempimento delle richieste, come meccanismi per l'estrazione e la consegna sicura dei dati;
- implementare tecnologie che permettano la cancellazione o l'anonimizzazione automatizzata dei dati su richiesta;

Qualora il responsabile riceva richieste provenienti dall'interessato, finalizzate all'esercizio dei propri diritti, esso dovrà:
- darne tempestiva comunicazione scritta al titolare via posta elettronica certificata, allegando copia delle richieste ricevute;
- coordinarsi, ove necessario e per quanto di propria competenza, con le funzioni interne designate dal titolare per gestire le relazioni con l'interessato.

[ ] misure tecniche ed organizzative specifiche che un eventuale **sub-responsabile** del trattamento deve prendere per essere in grado di fornire assistenza al titolare del trattamento:
- sottoscrivere un accordo scritto con il responsabile principale che definisca chiaramente i compiti, le responsabilità e le misure di sicurezza da adottare. Questo include anche l'obbligo di ricevere autorizzazione scritta dal titolare per eventuali sub-nomine;
- garantire che tutte le operazioni di trattamento rispettino le norme del RGPD e le istruzioni specifiche ricevute dal responsabile principale;
- prevedere audit regolari e verifiche interne per assicurarsi che le politiche di conformità siano efficacemente applicate;
- adottare misure tecniche ed organizzative adeguate per proteggere i dati trattati, come la crittografia, la pseudonimizzazione e restrizioni di accesso, in linea con l'articolo 32 del RGPD;
- assicurare la riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di trattamento;
- supportare il responsabile principale nel fornire accesso ai dati o rettificarli, cancellarli o limitarli su richiesta degli interessati;
- assistere il responsabile principale nella conduzione delle Valutazioni di Impatto sulla Protezione dei Dati (DPIA) se richiesto, fornendo tutta la documentazione necessaria;
- informare immediatamente il responsabile principale di eventuali violazioni della sicurezza che comportino la perdita, la modifica o l'accesso non autorizzato ai dati personali, fornendo tutte le informazioni necessarie per consentire una risposta tempestiva;
- tenere aggiornato un registro delle attività di trattamento per dimostrare la conformità con il RGPD, specificando la natura, la durata, la finalità del trattamento, e le categorie di dati trattati;
- fornire continua formazione al proprio personale sulle normative in materia di protezione dei dati personali e cibersicurezza e sulle migliori pratiche di gestione dei dati;
- mantenersi aggiornato sulle ultime evoluzioni in materia di sicurezza dei dati per migliorare continuamente la protezione;

ALLEGATO IV
ELENCO DEI SUB-RESPONSABILI DEL TRATTAMENTO

NOTA ESPLICATIVA:

Il presente allegato deve essere compilato in caso di autorizzazione specifica di sub-responsabili del trattamento [clausola 7.7, lettera a), opzione 1].

Il titolare del trattamento ha autorizzato il ricorso ai seguenti sub-responsabili del trattamento:

1. DENOMINAZIONE ENTE / OPERATORE ECONOMICO:

……

Indirizzo e recapito PEC:

……

Nome, qualifica e dati di contatto della persona che sottoscrive l'accordo:

……

Nome e dati di contatto del responsabile della protezione dei dati (RPD):

……

Descrizione del trattamento (compresa una chiara delimitazione delle responsabilità qualora siano autorizzati più sub-responsabili del trattamento):
……
……
……

Firma e data di adesione: ……

2. DENOMINAZIONE ENTE / OPERATORE ECONOMICO:

……

Indirizzo e recapito PEC:

……

Nome, qualifica e dati di contatto della persona che sottoscrive l'accordo:

……

Nome e dati di contatto del responsabile della protezione dei dati (RPD):

……

Descrizione del trattamento (compresa una chiara delimitazione delle responsabilità qualora siano autorizzati più sub-responsabili del trattamento):

……
……
……

Firma e data di adesione: ……

COMUNE DI GENOVA

DISPOSIZIONI OPERATIVE
IN MATERIA DI INCIDENTI DI SICUREZZA E DI VIOLAZIONE DI DATI PERSONALI (c.d. DATA BREACH)

Sommario

FINALITÀ E AMBITO DI APPLICAZIONE

Il Comune di Genova, ai sensi del Regolamento Europeo 2016/679 (da qui in avanti **RGPD**), in quanto Titolare del trattamento (di seguito, per brevità, "**Titolare del trattamento**" o anche solo "**Titolare**" o "**Comune**") è tenuto a mantenere sicuri i dati personali trattati nell'ambito delle proprie attività istituzionali e ad agire senza ingiustificato ritardo in caso di violazione dei dati stessi (di seguito, per comodità, "**data breach**"), incluse eventuali notifiche all'Autorità di controllo competente ed eventuali comunicazioni agli interessati.

Il mancato rispetto dell'obbligo di notifica ex articolo 33 del RGPD comporta l'applicabilità da parte dell'autorità di controllo delle sanzioni amministrative previste dall'art. 83 del RGPD. **L'autorità potrebbe inoltre applicare le misure correttive previste dall'art. 58 del RGPD e, quindi, rivolgere al Titolare avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti provvisori o definiti al trattamento e di divieti, ordini di rettifica e cancellazione dei dati, revoche di certificazioni, ordini di sospendere i flussi di dati verso paesi terzi o organizzazioni internazionali**.

Il RGPD prevede poi espressamente che al momento della decisione in merito alla sanzione amministrativa pecuniaria da infliggere ed alla definizione del suo ammontare, è necessario tenere conto nel caso concreto anche delle misure adottate dal Titolare per attenuare il danno subito dagli interessati, come pure del grado di responsabilità del Titolare (o del responsabile) alla luce delle misure tecniche e organizzative messe in atto ai sensi degli artt. 25 e 32. La stessa mancata notifica all'autorità di controllo, e/o comunicazione all'Interessato, potrebbero d'altro canto essere considerate nel caso specifico indici di una mancata adozione di misure di sicurezza che potrebbe portare all'irrogazione di specifiche sanzioni al riguardo.

Inoltre, **l'articolo 82 del RGPD prevede che chiunque subisca un danno materiale o immateriale causato da una violazione del RGPD ha il diritto di ottenere il risarcimento del danno dal soggetto al quale l'obbligo (violato) era imposto (salvo che quest'ultimo dimostri che l'evento dannoso non gli è imputabile)**.

E' pertanto di fondamentale importanza predisporre una procedura organizzativa interna per la gestione di eventuali violazioni concrete, potenziali o sospette di dati personali per adempiere agli obblighi imposti dalla normativa europea ed evitare rischi per i diritti e le libertà degli interessati, nonché danni economici per l'Ente (**data breach policy**). A tale riguardo si precisa che, presso il Comune di Genova, sono state attivate procedure a tutela della sicurezza dei dati, tra cui:

− l'adozione di misure organizzative e tecniche per garantire un livello di sicurezza adeguato al rischio connesso al trattamento dei dati personali e alle altre informazioni trattate, comprese misure volte al tempestivo ripristino della disponibilità in caso di incidente sulla sicurezza;

− l'organizzazione, a cadenza periodica, di corsi di formazione per i dipendenti/collaboratori sui principi cardine della normativa sul trattamento dati, sulla sicurezza dei dati personali e dei sistemi.

I dati oggetto di riferimento sono i dati personali trattati "*da* "e "*per conto*" del Comune di Genova, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo.

Il presente documento ha lo scopo di indicare le **modalità di gestione di un data breach**, ovvero di un episodio di violazione di dati personali (come meglio spiegato nel prosieguo), nel rispetto dei principi e delle disposizioni contenute nel Regolamento (UE) 679/2016 sulla protezione dei dati personali (RGPD).

L'obiettivo del presente documento è, pertanto:

- **sensibilizzare** il personale in ordine alle responsabilità in materia di protezione dei dati personali ed all'importanza della collaborazione nella tempestiva segnalazione e risoluzione degli incidenti sulla sicurezza (inclusi i data breach);
- **definire processi** per identificare, tracciare e reagire ad un incidente sulla sicurezza e ad un data breach, per valutarne il rischio, contenere gli effetti negativi e porvi rimedio nonché stabilire se, in caso di data breach, si renda necessario procedere alla (i) notifica al Garante e (ii) comunicazione agli Interessati;
- **definire ruoli e responsabilità** per la risposta agli incidenti sulla sicurezza ed i data breach;
- **assicurare un adeguato flusso comunicativo** all'interno della struttura del Comune, tra le figure coinvolte.

Le procedure qui contemplate sono applicabili a tutte le attività svolte dal Comune di Genova, con particolare riferimento alla gestione di tutti gli archivi e documenti cartacei e di tutti i sistemi informatici, attraverso i quali vengono trattati dati personali degli interessati, anche con il supporto di soggetti esterni.

Le procedure descritte nel presente documento sono rivolte a tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del Comune di Genova, quali:
a) I lavoratori dipendenti, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto contrattuale intercorrente - abbiano accesso ai dati personali trattati nel corso delle prestazioni rese all'interno della struttura organizzativa comunale;
b) qualsiasi soggetto (persona fisica o persona giuridica) diverso da quelli indicati alla lettera precedente che, in ragione del rapporto contrattuale in essere con il Comune di Genova abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento (art. 28 del RGPD). In particolare, ogniqualvolta il Comune si trovi ad affidare il trattamento di dati ad un soggetto terzo, in qualità di responsabile del trattamento, è tenuto a stipulare con tale soggetto uno specifico accordo che lo vincoli al rispetto delle istruzioni impartitegli dal Titolare in materia di protezione dati: è necessario che la presente procedura di segnalazione di data breach sia inclusa nel suddetto accordo. Ciò al fine di obbligare il responsabile ad informare il Comune senza ingiustificato ritardo, di ogni potenziale evento di data breach;

Il rispetto della presente procedura è obbligatorio per tutti i soggetti coinvolti e **la mancata conformità alle regole di comportamento previste dalla stessa potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia**.

In questo documento si sintetizzano le regole per garantire la realizzabilità tecnica e la sostenibilità organizzativa nella gestione del data breach, sotto i diversi aspetti relativi a:

- modalità e profili di segnalazione al Comune di Genova;
- valutazione dell'evento accaduto;
- modalità e profili di notificazione all'Autorità di controllo;
- eventuale comunicazione agli interessati

garantendo al tempo stesso:

- l'identificazione della violazione;
- l'analisi delle cause della violazione;
- la definizione delle misure da adottare per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi;
- la registrazione delle informazioni relative alla violazione, delle misure identificate e dell'efficacia delle stesse.

Le disposizioni contenute nel presente documento sono applicabili, in quanto compatibili, anche in relazione alle violazioni di dati personali verificatesi nel contesto delle attività di trattamento dei dati personali che il Comune di Genova svolga in quanto **Autorità competente a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, in conformità alle previsioni di cui al Decreto Legislativo 18 maggio 2018, n. 51**.

Articolo 26 del D.Lgs. 51/2018:
"*1. Salvo quanto previsto dall'articolo 37, comma 6, in caso di violazione di dati personali, il titolare del trattamento notifica la violazione al Garante con le modalità di cui all'articolo 33 del regolamento UE.*
2. Se la violazione dei dati personali riguarda dati personali che sono stati trasmessi dal o al titolare del trattamento di un altro Stato membro, le informazioni previste dal citato articolo 33 del regolamento UE sono comunicate, senza ingiustificato ritardo, al titolare del trattamento di tale Stato membro."

Articolo 27 del D.Lgs. 51/2018:
"*1. Quando la violazione di dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, si osservano le disposizioni in tema di comunicazioni di cui all'articolo 34 del regolamento UE.*
2. La comunicazione all'interessato di cui al comma 1 può essere ritardata, limitata od omessa alle condizioni e per i motivi di cui all'articolo 14, comma 2."

DEFINIZIONI

Fermo restando che le uniche definizioni "ufficiali" e vincolanti sono quelle contenute nell'articolo 4 del RGPD e quelle contenute nel Codice per la protezione dei dati personali (D.Lgs. 30 giugno 2003 n. 196), si riporta la terminologia maggiormente utilizzata nel contesto del presente documento, per semplificarne la lettura.

«**GDPR**» o «**RGPD**» o «**Regolamento**»: il Regolamento (UE) n. 679/2016 "General Data Protection Regulation", in italiano indicato come "Regolamento generale sulla protezione dei dati";
«**CODICE PRIVACY**»: il Decreto Legislativo 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali";
«**DATO PERSONALE**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («Interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
«**CATEGORIE PARTICOLARI DI DATI PERSONALI**»: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
«**DATI RELATIVI ALLA SALUTE**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
«**DATI GENETICI**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
«**DATI BIOMETRICI**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
«**ARCHIVIO**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
«**TRATTAMENTO**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
«**PSEUDONIMIZZAZIONE**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un Interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
«**COMUNICAZIONE**»: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'Interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies del Codice privacy, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;
«**DIFFUSIONE**»: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
«**INTERESSATO**»: la persona fisica cui si riferiscono i dati personali;
«**TITOLARE DEL TRATTAMENTO**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare

del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
«**RESPONSABILE DEL TRATTAMENTO**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
«**RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI**» o «**RPD**» o «**RPD**»: soggetto cui è attribuito dal Titolare del trattamento il compito di informare e fornire consulenza sugli obblighi derivanti dal RGPD e di sorvegliarne l'osservanza. Fornisce, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati (PIA) e ne sorveglia lo svolgimento. Coopera con l'Autorità di controllo e funge da punto di contatto con essa (RGPD, art. 37, 38, 39);
«**DESTINATARIO**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
«**TERZO**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'Interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
«**VIOLAZIONE DEI DATI PERSONALI**»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
«**MINACCIA**»: una serie di eventi dannosi che possono compromettere le caratteristiche di integrità, riservatezza e disponibilità del dato personale;
«**DANNO**»: conseguenza negativa derivante dal verificarsi di una determinata minaccia; il danno può qualificarsi come materiale quando determina una concreta lesione all'ambito fisico o patrimoniale dell'Interessato oppure immateriale quando riguarda le possibili conseguenze dannose derivanti dal trattamento di dati personali, di natura non patrimoniale e che affliggono la sfera interiore del soggetto Interessato;
«**MALWARE**»: software di tipo malevolo che causa danni ai sistemi informativi;
«**MISURA DI SICUREZZA**»: accorgimento tecnico e organizzativo utilizzato per garantire che i dati non vadano distrutti o persi anche in modo accidentale, per garantire che solo le persone autorizzate possano avere accesso ai dati e che non siano effettuati trattamenti contrari alle norme di legge o diversi da quelli per cui i dati erano stati raccolti;
«**CRITTOGRAFIA**»: tecnica che permette di "cifrare" un messaggio rendendolo incomprensibile a tutti fuorché al suo destinatario;
«**DECRITTOGRAFIA**»: il processo per "sbloccare" i dati criptati, cioè cifrati;
«**AUTORITÀ DI CONTROLLO**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del RGPD. In Italia, il Garante per la Protezione dei Dati Personali;
«**WP ARTICOLO 29**»: gruppo di lavoro indipendente con funzioni consultive dell'UE nell'ambito della protezione dei dati personali e della vita privata, istituito ai sensi dell'art. 29 della direttiva 95/45/CE. A decorrere dal 25 maggio 2018 è stato sostituito dal Comitato europeo per la protezione dei dati (EDPB) ai sensi del regolamento generale sulla protezione dei dati dell'UE (RGPD) (regolamento (UE) 2016/679);
«**EDPB**» o «**EUROPEAN DATA PROTECTION BOARD**»: Il Comitato europeo per la protezione dei dati (EDPB) è un organismo europeo indipendente. È l'organizzazione sotto la cui egida si riuniscono le Autorità nazionali per la protezione dei dati personali (Autorità nazionali di controllo) dei paesi dello Spazio economico europeo, nonché il Garante europeo della protezione dei dati (EDPS). L'EDPB garantisce che il Regolamento generale sulla protezione dei dati e la Direttiva "polizia e giustizia" siano applicati in modo coerente; inoltre, l'EDPB garantisce la cooperazione, anche in materia di attuazione della normativa;
«**LINEE GUIDA**»: con questo termine si intende riferirsi al documento denominato "*Linee guida 9/2022 sulla notifica di violazione dei dati personali ai sensi del GDPR*", versione 2.0, adottato dall'EDPB in data 28 marzo 2023[1]. Si ricorda, tuttavia, che il Gruppo di lavoro ex art. 29 ("WP29") ha adottato il 6 febbraio 2018 la versione definitiva delle linee guida sulla notifica delle violazioni dei dati personali (cd. "data breach") ai sensi

[1] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_it.

del Regolamento UE n. 679/2016 (cd. "RGPD")[2]. Durante la prima riunione plenaria del 25/05/2018 il Comitato europeo per la protezione dei dati aveva approvato le linee-guida relative al regolamento generale sulla protezione dei dati messe a punto dal gruppo di lavoro "Articolo 29"[3].
Successivamente, in data 14 dicembre 2021, l'EDPB ha pubblicato le "*Linee-guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali*"[4]. Tale testo (**ALLEGATO F** al presente documento) mantiene la propria utilità quanto alle fattispecie esemplificative elencate.

[2] Linee guida WP29 sulla notifica di violazione dei dati personali ai sensi del regolamento 2016/679 (WP250 rev.01) (ultima revisione e aggiornamento il 6 febbraio 2018), disponibile all'indirizzo https://ec.europa.eu/newsroom/article29/items/612052.
[3] https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en.
[4] https://www.edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_it.pdf

PIANO DI AZIONE

E' individuato il seguente piano d'azione per assicurare la conformità (compliance) del Comune di Genova alle previsioni normative in tema di protezione dei dati personali. Il piano evidenzia in rosso le azioni "obbligatorie" ed in giallo quelle "non obbligatorie ma, vivamente, consigliate". Trattasi ovviamente di **indicazioni di massima**, debitamente integrate dalle regole contenute nel prosieguo del documento, che sono suscettibili di modifica ed integrazione in considerazione dell'evoluzione normativa e tecnica e delle peculiari caratteristiche organizzative del Comune.

Azione	Annotazioni
Adottare una procedura interna di gestione dei data breach (obbligatorio)	Attraverso la presente policy sono definiti i ruoli e le responsabilità nella gestione degli incidenti e delle violazioni
Istruire il personale autorizzato al trattamento dei dati in materia di sicurezza e gestione di possibili violazioni (obbligatorio)	Il personale dev'essere in grado di identificare e gestire eventuali violazioni di dati personali
Verificare lo stato delle misure di sicurezza implementate presso l'Ente (consigliato)	Condurre audit sui sistemi informatici e non. Il RGPD richiede infatti che siano implementate tutte le misure tecnologiche ed organizzative per valutare se sia avvenuta una violazione di dati; tali misure aiutano anche a stabilire se sia necessaria o meno la notifica
Cifrare o pseudonimizzare i dati di cui agli articoli 9 e 10 del RGPD (obbligatorio)	
Limitare l'accesso ai dati personali solo al personale autorizzato (obbligatorio)	E' opportuno limitare l'accesso per ridurre le possibilità di eventuali violazioni, che spesso sono provocate anche da errore umano
Verificare le misure di sicurezza installate sui computer al fine di eliminare le vulnerabilità ed implementare misure di sicurezza logiche e fisiche adeguate (obbligatorio)	Occorre valutare le misure di sicurezza anche al fine di dimostrare la c.d. "accountability"
Preparare un piano di risposta alle violazioni (obbligatorio)	Il piano dovrebbe prevedere le seguenti azioni: – assicurare che i dati non siano più compressi; – mettere in sicurezza tutti i dati ed i sistemi; – identificare i dati compromessi, le categorie di Interessati coinvolte, la tipologia di violazione; – isolare i dati compromessi; – modificare le chiavi di codifica e le relative password immediatamente; – documentare tutte le fasi di gestione della violazione e tutte le informazioni relative alla violazione stessa; – determinare quando sia effettivamente avvenuta la violazione (al fine di notificare la violazione entro 72 ore)
Coinvolgere le autorità competenti ove si sospettino attività illecite (obbligatorio)	Non è strettamente richiesto dal RGPD, ma è opportuno notificare la violazione anche ad altre autorità, ove applicabile e richiesto dalla normativa vigente

Selezionare adeguatamente i fornitori che erogano attività che comportano un trattamento di dati (obbligatorio)	E' opportuno verificare e selezionare il fornitore e assicurare che la designazione come Responsabile contenga previsioni e istruzioni specifiche in materia di data breach
Conclusa la gestione urgente della violazione, valutare i "gaps" e l'efficacia dei sistemi interni, della formazione del personale e delle ulteriori procedure che mirano a tutelare i dati personali (obbligatorio)	Tale attività potrebbe essere inclusa in una fase di post-assessment
Testare frequentemente i sistemi interni (consigliato)	
Conservare un registro dei data breach ed aggiornarlo frequentemente (obbligatorio)	Il Titolare è tenuto a comunicare ogni informazione sulla violazione all'Autorità di controllo e per tale motivo è opportuno implementare un registro di data breach

PROCEDURA

Considerando 85, del RGPD:
"*Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata. Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo.*"

Si individuano di seguito i soggetti coinvolti ed il flusso delle principali attività previste per la rilevazione e gestione di un incidente di sicurezza che possa comportare una violazione di dati personali (si veda la **rappresentazione grafica nell'ALLEGATO A**).

La **tempestività** è un fattore determinante nella risposta agli incidenti sulla sicurezza ed ai data breach ed è dovere di ciascun soggetto, nell'ambito del proprio ruolo nella struttura e nella catena di comunicazione, non ritardare iniziative di reazione all'incidente e rispettare le procedure e le tempistiche di comunicazione individuate dal presente documento.

La risposta a un Incidente sulla sicurezza o ad un data breach deve avvenire secondo le fasi descritte di seguito. Considerando, tuttavia, che gli Incidenti possono avere molteplici cause o coinvolgere diversi soggetti ed avere conseguenze caratterizzate da vari livelli di gravità, tali fasi potrebbero sovrapporsi o richiedere tempistiche differenti o aggiornamenti. È tuttavia fatto obbligo ad ogni soggetto operante sotto la responsabilità del Comune di Genova di collaborare e seguire le istruzioni che di volta in volta gli vengano fornite dallo stesso Comune o dal RPD.

Considerati i rischi e, in caso di data breach, le ridotte tempistiche per effettuare la notifica e per la comunicazione agli interessati, occuparsi degli incidenti di sicurezza deve essere obiettivo prioritario per tutti i soggetti coinvolti nella loro gestione. Nella gestione di un qualunque incidente di sicurezza devono essere considerate le seguenti due priorità:

prima priorità: proteggere tutti gli assets del Comune di Genova, incluse le risorse colpite dall'incidente, fino al ripristino della normale operatività;

seconda priorità: raccogliere informazioni e prove per supportare le eventuali e appropriate azioni correttive, disciplinari o legali;

Tutti gli incidenti di sicurezza ed i data breach devono essere trattati con il **massimo livello di riservatezza**: le informazioni devono essere condivise esclusivamente con il personale identificato nella presente procedura e solo quando strettamente necessario. Eventuali comunicazioni a soggetti non coinvolti nella gestione dell'Incidente dovranno limitarsi all'indicazione che si è verificato un problema e che lo stesso è in fase di gestione.

Tutte le attività di gestione devono essere **tracciate e documentate** per quanto possibile a partire dall'istante di rilevazione.

Il coordinamento delle attività di gestione di una violazione di dati personali, con particolare riferimento agli obblighi di comunicazione e notifica imposti dal RGPD, è assicurato dal RPD con il supporto dell'Area Technology Office (Sistemi Informativi) od altra struttura organizzativa equivalente, per gli aspetti tecnici e dell'Avvocatura per gli aspetti giuridici, nonché dal Dirigente competente in ragione del servizio o settore coinvolto. Il RPD ha, comunque, piena facoltà di suggerire la convocazione ed il coinvolgimento di altri soggetti che ritenga utili alle necessità del caso.

1. Individuazione della violazione

Articolo 33, par. 1, del RGPD:
"*In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'Autorità di controllo competente a norma dell'art. 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo*"

Articolo 4, par. 1, n. 2, del RGPD:
"*Ai fini del presente regolamento s'intende per:*
(…)
«violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati"

Considerando 87 del RGPD:
"*È opportuno verificare se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali e informare tempestivamente l'autorità di controllo e l'interessato.*"

Le violazioni dei dati personali sono una tipologia di incidente per la sicurezza delle informazioni nel quale sia coinvolto qualsiasi genere di dato di natura personale (anagrafici, numeri di carte personali, codici identificativi, dati sanitari, dati biometrici, dati relativi a conti correnti, ecc.). **Tuttavia, come indicato all'articolo 4, punto 12, il RGPD si applica soltanto in caso di violazione di dati personali**.

La conseguenza di tale violazione è che il Titolare del trattamento non è più in grado di garantire l'osservanza dei principi relativi al trattamento dei dati personali di cui all'articolo 5 del RGPD. Questo punto mette in luce la differenza tra un incidente di sicurezza e una violazione dei dati personali: mentre tutte le violazioni dei dati personali sono incidenti di sicurezza, non tutti gli incidenti di sicurezza sono necessariamente violazioni dei dati personali.

Non è da ritenersi corretta la comune associazione tra data breach ed attacco o problema informatico poiché tale violazione può avvenire anche (ad esempio) a causa di un dipendente infedele che sottragga documentazione cartacea ovvero un di dipendente disattento che la smarrisca.

Le violazioni dei dati personali sono, di per sé, problematiche, ma possono anche essere sintomi di un regime di sicurezza dei dati vulnerabile e forse obsoleto, oppure segnalare carenze del sistema, da affrontare. In linea generale, è sempre meglio prevenire le violazioni dei dati preparandosi in anticipo, dal momento che diverse conseguenze sono per loro natura irreversibili. Prima che il Comune di Genova possa valutare appieno il rischio derivante da una violazione causata da una qualche forma di attacco, occorre individuare la causa alla radice del problema, al fine di stabilire se le vulnerabilità che hanno determinato l'incidente siano ancora presenti e siano pertanto ancora sfruttabili.

Le Linee Guida precisano la nozione di violazione in base ai seguenti **tre principi di sicurezza delle informazioni**:

Violazione della riservatezza *(Confidentiality breach)*	**divulgazione o accesso non autorizzato o accidentale** ai dati personali come, ad esempio: • quando nella redazione di un atto non si redige la versione con omissione dei dati da non pubblicare e l'atto viene pubblicato nella sua interezza; • quando si inoltrano messaggi contenenti dati a soggetti non interessati al trattamento; • quando un operatore abbandona la propria postazione di lavoro senza prima prendere le opportune precauzioni (riporre la documentazione, lasciare attive procedure sulla risorsa informatica utilizzata, ecc..) e terze persone prendono visione di informazioni; • quando un soggetto in malafede comunica dei dati non pubblici a terzi in modo non autorizzato. Per "**divulgazione**" si intende la trasmissione non autorizzata o impropria dei dati personali degli interessati verso terze parti (persone fisiche, persone giuridiche, gruppi di soggetti, pubblico) anche non precisamente identificabili. Per "**accesso**" si intende l'accesso non autorizzato o improprio ai dati degli interessati. Accessi ai dati (anche in sola visualizzazione, sia in caso di accessi logici ai sistemi informatici sia agli archivi cartacei) effettivamente avvenuti al di fuori dei processi operativi di trattamento dei dati previsti e autorizzati. Un **trattamento non autorizzato o illecito** può includere la divulgazione di dati personali a (o l'accesso da parte di) destinatari non autorizzati a ricevere (o ad accedere a) i dati oppure qualsiasi altra forma di trattamento in violazione del RGPD.

Violazione dell'integrità *(Integrity breach)*	**alterazione non autorizzata o accidentale** dei dati personali La "***alterazione***" è la situazione in cui i dati sono danneggiati, corrotti o non più completi. L'alterazione non autorizzata può essere la conseguenza di un attacco esterno o di una manipolazione inconsapevole da parte di personale non competente. Un'alterazione accidentale si può verificare per errore umano (ad es. nel momento di un aggiornamento delle informazioni) o per un disguido tecnico quando all'interno di una base dati si perdono i collegamenti a determinate informazioni (integrità referenziale).

Violazione della disponibilità *(Availability breach)*	**accidentale o non autorizzata perdita di accesso** o **distruzione** di dati personali (Fattispecie non sempre di facile individuazione). La "***perdita di dati***" è la situazione in cui i dati, presumibilmente, esistono ancora, ma il Titolare ne ha perso il controllo o la possibilità di accedervi. Perdita del supporto fisico di memorizzazione dei dati (dischi esterni, pendrive ecc.) in termini di privazione, sottrazione, smarrimento dei dispositivi contenenti i dati degli interessati oppure dei documenti cartacei. La perdita può essere anche temporanea ma superiore ad un termine ragionevole. Può riguardare le copie o gli originali dei supporti contenenti i dati personali dei soggetti interessati. La "***distruzione***" dei dati personali è la condizione in cui i dati non esistono più o non esistono più in un formato che sia utilizzabile dal Titolare. La violazione può essere determinata da una eliminazione logica (es. cancellazione dei dati) oppure fisica (es. rottura dei supporti di memorizzazione) non autorizzata e relativa impossibilità di ripristinare i dati entro un termine ragionevole. Ci sarà sempre una violazione della Disponibilità del dato nel caso di **perdita o distruzione permanente** dei dati. L'indisponibilità dei dati è quindi da considerare una violazione quando potrebbe avere un impatto significativo sui diritti e le libertà delle persone fisiche. Non si tratta invece di una violazione quando l'indisponibilità è dovuta a interruzioni programmate per la manutenzione). Ci si potrebbe chiedere se una **perdita temporanea della disponibilità** dei dati personali costituisca una violazione e, in tal caso, se si tratti di una violazione che richiede la notifica. L'articolo 32 del RGPD ("Sicurezza del trattamento") spiega che nell'attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, si dovrebbe prendere in considerazione, tra le altre cose, "*la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento*" e "*la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico*". Di conseguenza, un incidente di sicurezza che determini l'indisponibilità dei dati personali per un certo periodo di tempo costituisce una violazione, in quanto la mancanza di accesso ai dati può avere un impatto significativo sui diritti e sulle libertà delle persone fisiche. Va precisato che l'indisponibilità dei dati personali dovuta allo svolgimento di un intervento di manutenzione programmata del sistema non costituisce una "violazione della sicurezza" ai sensi dell'articolo 4, n. 12 del RGPD. Va notato che, sebbene una perdita di disponibilità dei sistemi del Titolare del trattamento possa essere solo temporanea e non

	avere un impatto sulle persone fisiche, è importante che il Titolare consideri tutte le possibili conseguenze della violazione, poiché quest'ultima potrebbe comunque dover essere segnalata per altri motivi.

A seconda delle circostanze, una violazione può riguardare uno o tutti gli aspetti sopra indicati o una combinazione di essi.

La violazione dei dati può avvenire a seguito di un attacco informatico, di un accesso abusivo, di un incidente (es. incendio, allagamento, etc.) o per la perdita di un supporto informatico (smartphone, notebook, chiavetta USB, etc.) o per la sottrazione o perdita di documenti con dati personali (furto, smarrimento, abbandono, etc.). La casistica è molto ampia.

A mero **titolo esemplificativo** e senza pretesa di esaustività, l'oggetto della segnalazione di un data breach può essere:

- l'accesso abusivo (ad esempio: accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
- dati cancellati accidentalmente o da soggetti non autorizzati;
- perdita della chiave di decriptazione;
- dati persi dall'ambiente di produzione che non possano essere ripristinati integralmente dalle copie di sicurezza e si debba provvedere manualmente alla loro ricostruzione;
- interruzione significativa di un servizio ("*black out*" elettrico o attacchi di tipo "*denial of service*");
- divulgazione di dati confidenziali a persone non autorizzate;
- errori nell'implementazione di una policy di controllo e verifica periodica delle abilitazioni degli accessi;
- divulgazione accidentale di credenziali di accesso a colleghi o personale non autorizzato;
- pubblicazione erronea delle informazioni personali (non di dominio pubblico) sul portale web istituzionale del Comune;
- infedeltà aziendale (ad esempio: data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico);
- perdita o il furto di dati o di strumenti nei quali i dati sono memorizzati;
- perdita o il furto di documenti cartacei;
- pirateria informatica;
- virus o altri attacchi al sistema informatico o alla rete dell'Ente;
- banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo "*owner*";
- violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);
- smarrimento di pc portatili, devices o attrezzature informatiche aziendali;
- formattazione di dispositivi di memorizzazione;
- malfunzionamenti software quali esecuzione di uno script automatico non autorizzato; errori di programmazione che causano output errati, ecc.;
- distruzione dolosa dei documenti: ad esempio incendio doloso provocato da personale interno o soggetti esterni che rende indisponibile in modo definitivo i documenti contenenti dati personali;
- distruzione dei supporti di memorizzazione a causa di sbalzi di temperatura e di elettricità, umidità, corto circuito, caduta accidentale, eventi catastrofici/incendi, ecc.;
- guasti alla rete informatica: a titolo di esempio caduta delle comunicazioni durante il trasferimento di dati e perdita di dati durante la trasmissione, ecc.;
- invio di e-mail contenenti dati personali e/o particolari ad erroneo destinatario.

2. Rilevazione della violazione

La prima fase nella gestione del data breach è quella che conduce alla rilevazione della violazione o presunta violazione di sicurezza e della sua comunicazione al **Dirigente competente in ragione del servizio o settore coinvolto**. Nell'ipotesi in cui ci si dovesse accorgere di essere stati vittima di un data breach la prima cosa da fare è quella di **non farsi prendere dal panico ed agire in modo scomposto** ma, anzi, applicare subito le procedure previste dalla presente policy.

2.1. Acquisizione della notizia

In caso di concreta, sospetta e/o avvenuta violazione dei dati personali, è di estrema importanza assicurare che la stessa sia **affrontata immediatamente e correttamente** al fine di minimizzare l'impatto della violazione e prevenire che si ripeta. Ai fini di una corretta analisi della segnalazione, è necessario raccogliere fatti concreti prima di segnalare qualsiasi tipo di violazione, illecito ed irregolarità in ambito di tutela dei dati personali.

È importante che la raccolta della segnalazione o l'esecuzione della segnalazione da parte degli uffici avvenga **raccogliendo quante più informazioni possibili** (identificazione dei segnalatori, data ed ora in cui la segnalazione è avvenuta, dati descrittivi sulla violazione segnalata ecc..). **Le segnalazioni, pertanto, devono essere fondate su elementi di fatto precisi, circostanziati e concordanti**.

Se al momento della rilevazione dell'incidente di sicurezza non è disponibile una descrizione particolareggiata dell'evento, è comunque essenziale procedere immediatamente alla comunicazione dell'incidente al **Dirigente competente in ragione del servizio o settore coinvolto**, per una prima valutazione d'impatto, anche con **informazioni incomplete**. Laddove necessario, alla prima valutazione possono seguirne altre, in base alle informazioni che vengono acquisite nella prosecuzione dell'indagine.

2.2. Fonte della notizia

La segnalazione di un data breach può essere **interna** (da personale dipendente, convenzionato, stagisti, tirocinanti, amministratori, RPD, …) o **esterna all'Ente** (Agid, ACN, Polizia, altre Forze dell'Ordine, giornalisti, utenti di servizi, RPD, Responsabili del trattamento, ecc.). Inoltre, ogni **Interessato** può segnalare, anche solo in caso di sospetto, che i propri dati personali siano stati utilizzati abusivamente o fraudolentemente da un terzo; in tal caso, l'Interessato può richiedere al Comune di Genova la verifica dell'eventuale violazione.

Il pubblico e, in genere, i soggetti che non sono legati al Comune di Genova del trattamento da rapporti contrattuali od altrimenti vincolanti, possono segnalare anomalie, disservizi o potenziali incidenti sulla sicurezza mediante comunicazione scritta inviata al protocollo. Il Comune di Genova rende disponibili presso i propri uffici e sul **sito web istituzionale**, la **modulistica** e le **informazioni** utili allo scopo. Sebbene la segnalazione possa avvenire in forma libera, si ritiene opportuno suggerire al segnalante l'utilizzo di un apposito modello **ALLEGATO B - "*Modulo di segnalazione di una potenziale violazione di dati personali*"**, predisposto in modo tale da agevolare l'attività istruttoria e valutativa da parte del Comune.

Nel caso in cui la segnalazione sia raccolta presso persone fisiche, senza l'utilizzo della modulistica e delle procedure di cui sopra, è opportuno che chi riceve la segnalazione provveda anche a raccogliere informazioni di contatto sul segnalante (indirizzo di reperibilità, numeri telefonici, indirizzo di posta elettronica) che potranno, nel caso, essere utili durante la fase di gestione tecnica, per reperire maggiori informazioni circa la violazione segnalata. Ove possibile è

sempre opportuno invitare il segnalante a rendere la propria dichiarazione per iscritto, anche in forma libera. In questa fase è opportuno non raccogliere dati personali appartenenti alle categorie particolari di cui all'art. 9 del RGPD, se non strettamente necessari.

Qualora la segnalazione pervenisse per **posta elettronica** certificata od ordinaria su una casella qualsiasi (istituzionale o meno) non è sufficiente il solo inoltro del messaggio ma occorre, comunque, seguire le modalità di seguito riportate. Allo stesso modo, ove la segnalazione pervenisse su **supporto cartaceo** non è sufficiente la sua mera registrazione al protocollo, occorrendo comunque che si segua la procedura di cui *infra*. Questo per accertarsi che la segnalazione non passi inosservata.

Anche le **segnalazioni anonime e/o verbali** devono essere raccolte e trasmesse conformemente a quanto *infra*, al fine di accertare la reale sussistenza della violazione, disporre l'eventuale notifica o le comunicazioni ed assumere i provvedimenti atti ad evitare l'aggravamento della situazione.

La **segnalazione di una potenziale violazione di dati personali da parte del personale operante all'interno della struttura organizzativa del Comune di Genova** deve avvenire solamente utilizzando l'apposito modello **ALLEGATO B - "*Modulo di segnalazione di una potenziale violazione di dati personali*"**.

2.3. Il monitoraggio degli eventi di sicurezza con impatto sulla protezione dei dati personali

L'individuazione di potenziali violazioni dei dati personali può anche avvenire a seguito di **attività di monitoraggio** degli eventi che possono arrecare violazioni dei dati, sia digitale ed automatizzata che cartacea. Il monitoraggio viene effettuato tramite il controllo delle attività di trattamento definite nel Registro dei trattamenti, in particolare per quei trattamenti che sono stati valutati con rischio non trascurabile in fase di valutazione d'impatto.

Le attività di monitoraggio si possono suddividere in due tipologie:

A) Il monitoraggio degli eventi generati dai sistemi ICT: tale monitoraggio include l'insieme delle attività di controllo finalizzate al rilevamento degli eventi tracciati dai sistemi informatici e dalle infrastrutture di sicurezza perimetrale che assumono carattere di rilevanza ai fini della sicurezza informatica. Tali eventi relativi ai sistemi ICT sono monitorati e gestiti dalla Direzione di Area Technology Office od altra similare, alla quale è assegnato il compito di identificare le categorie di eventi che dovrebbero essere sottoposte a monitoraggio, sulla scorta della seguente elencazione (meramente esemplificativa):

- log generati dalle attività svolte con account riconducibili agli amministratori di sistema, con particolare attenzione a:
  - orari di connessione/disconnessione (log-on / log-off);
  - log afferenti alla gestione dei profili utente (es. creazione di nuove utenze, modifica dei privilegi di accesso, blocco di utenze, forzato cambio password, riassegnazione di account ad altro utente);
  - modifiche alle configurazioni di sistema;
  - escalation o tentata escalation a profili con privilegi di accesso superiori;
  - qualsiasi attività svolta da remoto al di fuori dei consueti orari di lavoro;
  - qualsiasi attività bloccata dalle misure di sicurezza e controllo accessi (es. accessi negati; user-id o password errata);
- log generati dalle attività svolte da utenti ordinari, con particolare attenzione a:
  - orari di connessione/disconnessione (log-on / log-off);
  - accessi negati;
  - escalation o tentata escalation a profili con privilegi di accesso superiori;

  - qualsiasi attività svolta da remoto al di fuori dei consueti orari di lavoro;
  - qualsiasi attività bloccata dalle misure di sicurezza e controllo accessi (es. accessi negati; user-id o password errata);
- log generati dai sistemi di sicurezza:
  - tentativi di violazione delle politiche di firewalling (es. drop/reject);
  - allarmi generati dai sistemi antivirus;
  - allarmi generati dai sistemi antispamming;
  - allarmi generati dai directory server/service.

B) Il monitoraggio dei luoghi fisici del trattamento e dell'archiviazione di dati personali. I luoghi fisici preposti al trattamento di informazioni personali riconducibili alle categorie di cui agli articoli 9 e 10 del RGPD, con particolare riferimento agli eventuali archivi cartacei, devono essere controllati periodicamente dal personale preposto alla vigilanza, ove previsto, ed anche con l'ausilio di eventuali dispositivi di videosorveglianza. In ogni caso sia il personale di guardiania o di vigilanza, sia il personale operativo, autorizzato all'accesso ai locali o al trattamento dei dati personali, è tenuto a comunicare tempestivamente qualsiasi evento di presunta o palese violazione della privacy come ad esempio:

- smarrimento o furto di documenti cartacei contenenti informazioni personali;
- smarrimento o furto di supporti digitali o di computer fissi o mobili contenenti dati personali;
- constatazione di effrazione o tentativi di effrazione alle porte di accesso od alle serrature di chiusura degli armadi che custodiscono documenti;
- presenza di personale non autorizzato nei locali preposti al trattamento di informazioni personali.

Qualunque constatazione di violazione o sospetta violazione, emersa in sede di monitoraggio, deve essere comunicata al **Dirigente competente in ragione del servizio o settore coinvolto, senza ritardo**.

2.4. Trasmissione della notizia

Ricevuta, da chiunque ed in qualunque modo, la segnalazione di un potenziale od effettivo incidente sulla sicurezza, la medesima è immediatamente **trasmessa al Dirigente competente in ragione del servizio o settore coinvolto o, in caso di incertezza sulla sua individuazione, assenza o indisponibilità**, **al RPD**, compilando il documento di cui all'**ALLEGATO C - "Modulo di inoltro di segnalazione di una potenziale violazione di dati personali"**, **senza ritardo**. Il modello di segnalazione, debitamente compilato e sottoscritto, dovrà essere consegnato con le modalità più idonee (posta elettronica, consegna a mani, …) a garantirne la pronta e puntuale conoscenza in quanto permetterà di condurre una valutazione iniziale riguardante la notizia dell'incidente occorso e, ciò, al fine di stabilire se si sia effettivamente verificata un'ipotesi di data breach (violazione) e se sia necessaria un'indagine più approfondita dell'accaduto. Contestualmente alla **trasmissione documentale** della segnalazione è necessario **l'avvertimento** del destinatario anche in modo **verbale** allo scopo di assicurarsi che quanto comunicato non passi inosservato.

Ricevuta la segnalazione, il **Dirigente competente in ragione del servizio o settore coinvolto**, provvede ad **informarne prontamente e, comunque non oltre 12 ore dalla conoscenza della segnalazione, il RPD,** al seguente indirizzo: rpd@comune.genova.it

Il **Dirigente competente in ragione del servizio o settore coinvolto**, anche insieme ai soggetti coinvolti nell'incidente e sotto la supervisione del RPD, coordina la raccolta delle informazioni nel più breve tempo possibile.

Nel caso la violazione coinvolga più servizi o settori del Comune, il coordinamento dei Dirigenti avviene a cura del Dirigente competente in ragione del servizio o settore maggiormente coinvolto. In casi di incertezza o contrasto, spetta al RPD individuare la figura del coordinatore. Resta inteso che, l'utilizzo nel presente documento, della terminologia "Dirigente competente in ragione del servizio o settore coinvolto" sta ad indicare altresì la figura del coordinatore di cui sopra.

Nel caso in cui si tratti di violazione di dati contenuti in un sistema informatico, il Dirigente competente in ragione del servizio o settore coinvolto dovrà coinvolgere in tutta la procedura indicata nel presente documento anche l'Area Technology Office (Sistemi Informativi) od altra struttura organizzativa equivalente.

3. Analisi e Valutazione della violazione

Questa fase si compone di tutte quelle operazioni, accertamenti e verifiche tese a supportare la valutazione dell'accaduto.

Una volta stabilito che un data breach è avvenuto, il **Dirigente competente in ragione del servizio o settore coinvolto, insieme al RPD ed all'Area Technology Office od altra figura equivalente**, dovrà stabilire:

a) se sia probabile o meno che la violazione dei dati personali presenti un **rischio per i diritti e le libertà delle persone fisiche**;
b) se esistano e quali siano le **misure efficaci** per contenere ed affrontare la violazione;
c) una volta identificate tali misure, quali siano i **soggetti che devono agire** per contenere ed affrontare la violazione;
d) se sia necessario **notificare** la violazione all'Autorità di controllo;
e) se sia necessario **comunicare** la violazione agli interessati.

Il Dirigente competente in ragione del servizio o settore coinvolto e tutti i soggetti coinvolti nella gestione degli incidenti (a mero titolo esemplificativo, Area Technology Office od altra figura equivalente, Amministratore di sistema, altri dirigenti, ecc.) sono responsabili, sulla base delle rispettive competenze ed in base alla tipologia della violazione, dell'analisi tecnica dell'evento e delle azioni da mettere in atto tempestivamente per il contenimento del danno.

È importante che questa fase, nella sua prima esecuzione, **si concluda nel più breve tempo possibile, massimo 24/48 ore**, per consentire il primo processo decisionale di valutazione da parte del **Dirigente competente in ragione del servizio o settore coinvolto** e permettergli di eseguire le eventuali notifiche e comunicazioni entro i termini previsti.

In questa fase, è fondamentale raccogliere il maggior numero di informazioni relative alla violazione di dati personali e, anche in caso queste non siano per il momento ritenute esaustive, effettuare comunque la notificazione all'Autorità di controllo. Si veda il successivo paragrafo 4.2.2. in ordine alla possibilità di effettuare la notifica all'Autorità di controllo "per fasi".

3.1. Analisi tecnica dell'evento

Per identificare le modalità di gestione di una violazione e gli eventuali obblighi di notifica e/o di comunicazione, il **Dirigente competente in ragione del servizio o settore coinvolto** (con il supporto dell'Area Technology Office od altra figura equivalente) effettua, anzitutto, un'analisi tecnica della segnalazione, all'interno della quale, **dovrà essere accertato se la violazione segnalata sia considerabile o meno un data breach**.

Questa fase dev'essere condotta con **estrema celerità**, anche se non si riescono ad individuare tutti gli elementi utili, ad eccezione della determinazione della sussistenza della violazione. Le verifiche potranno eventualmente proseguire anche dopo una prima valutazione. Inoltre, l'Autorità di controllo o gli alti organi nazionali (polizia, magistratura, CSIRT Italia, CNAIPIC, ecc.) potrebbero richiedere o ritenere necessari approfondimenti. Dunque, l'incompletezza delle informazioni, così come la necessità di approfondimenti potrebbero rendere necessario ripetere la fase anche più volte.

Nessuna segnalazione deve concludersi in questa fase unicamente sulla base di un giudizio di inaffidabilità del segnalante: occorrerà comunque appurare se la violazione si sia effettivamente verificata. **Parimenti, nessuna segnalazione che sia relativa unicamente ad operazioni svolte con strumenti informatici potrà concludersi durante l'analisi tecnica per il solo fatto che non sussiste**

una violazione di dati personali, in quanto potrebbe in ogni caso rendersi necessario informare altre Autorità competenti (ad es., CSIRT Italia, CNAIPIC, ecc.).

Cons specifico riferimento agli incidenti di sicurezza "tecnologici" si dovranno, ove possibile, rilevare:
• la causa e la natura del disservizio, della rottura e, in generale, dell'incidente di sicurezza;
• le eventuali vulnerabilità collegate con l'incidente e le azioni di mitigazione delle vulnerabilità individuate;
• l'esistenza di misure adottate precedentemente all'evento per contrastare il rischio;
• la valutazione dei tempi e modalità di riparazione e ripristino dei sistemi, dell'infrastruttura e delle configurazioni;
• la verifica dei sistemi recuperati;
• l'eventualità di perdita di dati durante il ripristino, la loro tipologia, se i dati sono reperibili in altre aree dei sistemi o presso terzi e le tempistiche per il recupero.

3.2. Valutazione della violazione al fine del rispetto degli obblighi di notifica e comunicazione

Esaurita l'analisi tecnica, il **Dirigente competente in ragione del servizio o settore coinvolto**, dovrà svolgere tutte le operazioni necessarie a raccogliere gli elementi per l'ulteriore valutazione dell'evento, ai fini dell'adempimento degli obblighi imposti dal RGPD. Più precisamente il **Dirigente competente in ragione del servizio o settore coinvolto** (con il supporto dell'Area Technology Office od altra figura equivalente) dovrà **accertare che i dati oggetto di violazione siano dati personali nonché la probabilità o meno che l'evento abbia comportato dei rischi per i diritti e la libertà delle persone e la gravità del rischio così identificato**. Nello specifico verrà effettuato:
a) il riconoscimento della categoria della violazione (se di riservatezza, di integrità o di disponibilità) o altro evento;
b) l'identificazione dei dati violati/distrutti/compromessi e relativi trattamenti;
c) l'identificazione degli interessati;
d) il contenimento del danno;

Tutte le operazioni effettuate devono essere tracciate e documentate.

3.2.1. valutazione dell'impatto sugli interessati

Considerando 75 del RGPD:
"*I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.*"

Considerando 76 del RGPD:
"*La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.*"

Nella fase di valutazione, sulla base delle informazioni rinvenute, occorre innanzitutto stabilire se nell'incidente sono coinvolti i **dati personali**. In caso di risposta positiva occorre valutare l'impatto sugli interessati:

a) ove si tratta di una *violazione di riservatezza* occorre verificare che le misure di sicurezza (es.: cifratura dei dati) in uso rendano improbabile l'identificazione degli Interessati (non compromissione della chiave, algoritmo di cifratura o impronta senza vulnerabilità note);
b) in caso di *perdita di integrità o disponibilità* di dati occorre valutare se è possibile il recupero degli stessi in tempi compatibili con i diritti degli Interessati.

Si noti che **la valutazione del rischio per i diritti e le libertà delle persone, a seguito di una violazione, ha un focus diverso rispetto al rischio considerato nell'ambito di una Valutazione d'impatto sulla Protezione dei Dati Personali (c.d. DPIA)**.
La DPIA considera sia i rischi derivanti dal trattamento dei dati effettuato come previsto, sia i rischi in caso di violazione. Quando si valuta una potenziale violazione, si considera in termini generali la probabilità che questa si verifichi ed il danno che potrebbe derivarne all'Interessato; in altre parole, si tratta di una valutazione di un evento ipotetico.
Nel caso di una violazione effettiva, l'evento si è già verificato e, quindi, l'attenzione deve concentrarsi tutta sul rischio derivante dall'impatto della violazione sui singoli individui.

I fattori da considerare nella valutazione del rischio per i diritti e le libertà delle persone fisiche interessate dalla violazione possono così essere esemplificati (trattasi di elencazione non esaustiva né vincolante):

FATTORE	OSSERVAZIONI
Aspetti **generali**	Valutazione della gravità dell'impatto potenziale sui diritti e sulle libertà delle persone fisiche e della probabilità che tale impatto si verifichi. Se le conseguenze di una violazione sono più gravi, il rischio è più elevato; analogamente, se la probabilità che tali conseguenze si verifichino è maggiore, maggiore sarà anche il rischio
Tipo di **violazione**	Distruzione, modifica, perdita, divulgazione (ad esempio, una violazione della riservatezza può avere conseguenze diverse rispetto ad una violazione in cui i dati siano stati persi e non più disponibili)
Natura, carattere sensibile e volume dei **dati** personali	Alcuni tipi di dati personali possono sembrare relativamente innocui, tuttavia occorre valutare attentamente ciò che questi dati possono rivelare sull'Interessato a malintenzionati. Quando la violazione riguarda categorie particolari di dati personali (art. 9 del RGPD) e dati relativi a condanne penale e reati (art. 10 del RGPD), il rischio per i diritti e le libertà degli Interessati dovrebbe essere, sempre, considerato presente. Inoltre, di norma, una combinazione di dati personali ha un carattere più sensibile rispetto a un singolo dato personale. Una violazione che interessi grandi quantità di dati personali relative a molte persone può avere ripercussioni su un numero corrispondentemente elevato di persone.
Facilità di **identificazione** delle persone fisiche	Facilità di identificazione, diretta o indiretta tramite abbinamento con altre informazioni, di specifiche persone fisiche sulla base dei dati personali compromessi dalla violazione. L'identificazione può essere direttamente o indirettamente possibile a partire dai dati oggetto di violazione; tuttavia, può dipendere anche dal contesto specifico della violazione e dalla disponibilità pubblica dei corrispondenti dettagli personali. Ciò potrebbe essere più rilevante per le violazioni della riservatezza e della disponibilità. Sebbene i dati personali protetti da un adeguato livello di crittografia siano incomprensibili a persone non autorizzate, senza la chiave di decrittazione, le sole tecniche di pseudonimizzazione non possono essere considerate tali da rendere i dati incomprensibili.

FATTORE	OSSERVAZIONI
Gravità delle **conseguenze** per le persone fisiche	Danno potenziale alle persone fisiche che potrebbe derivare dalla violazione, comprese le categorie degli interessati e dei dati personali coinvolti e la permanenza a lungo termine delle conseguenze del danno (furto di identità, danni fisici, disagio psicologico, danni reputazionali). A seconda della natura dei dati personali coinvolti in una violazione (ad esempio, categorie particolari di dati), il potenziale danno che potrebbe derivare alle persone può essere particolarmente grave, in particolare laddove la violazione possa comportare il furto o frode di identità, danni fisici, disagio psicologico, umiliazione o danno alla reputazione. Il fatto che si sappia o meno che i dati personali sono nelle mani di persone le cui intenzioni sono sconosciute o potenzialmente dannose può incidere sul livello di rischio potenziale. Si dovrebbe altresì tener conto della permanenza delle conseguenze per le persone fisiche laddove l'impatto possa essere considerato maggiore qualora gli effetti siano a lungo termine.
Caratteristiche particolari del **Titolare**	La natura e il ruolo del Titolare del trattamento e delle sue attività possono influire sul livello di rischio per le persone fisiche in seguito a una violazione.
Caratteristiche particolari dell'**Interessato**	Se la violazione riguarda dati personali relativi a persone fisiche vulnerabili (minori, anziani, pazienti, …), queste ultime potrebbero essere esposte a un rischio maggiore di danni.
Numero di persone fisiche interessate	Di norma, maggiore è il numero di persone fisiche interessate, maggiore è l'impatto che una violazione può avere. Tuttavia, una violazione può avere ripercussioni gravi anche su una sola persona fisica, a seconda della natura dei dati personali e del contesto nel quale i dati sono stati compromessi.

Qualora il numero degli interessati (anche potenziali) dalla violazione sia ridotto e questi siano identificabili è opportuno stilare degli elenchi da utilizzare nel caso in cui il sia necessario inviare loro delle comunicazioni personalizzate.

3.2.2. valutazione della probabilità e gravità del rischio

La gravità di una violazione di dati personali è definita come la **stima dell'entità del potenziale impatto sulle persone fisiche derivante dalla violazione medesima**. Tale valutazione di impatto permette di stabilire la necessità di notifica della violazione all'Autorità di controllo, in particolare se sia probabile un rischio per la libertà e diritti delle persone fisiche, e la comunicazione anche agli Interessati, nel caso in cui tale rischio sia elevato.

La violazione dei dati può comportare **rischi per i diritti e le libertà delle persone** fisiche. I rischi principali sono connessi alla possibilità che l'Interessato subisca danni fisici, materiali o immateriali connessi perdita del controllo dei dati personali quali, ad esempio:

a) limitazione dei diritti;
b) discriminazione;
c) furto o usurpazione di identità;
d) perdite finanziarie;
e) decifratura non autorizzata della pseudonimizzazione;
f) pregiudizio alla reputazione;
g) perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari);
h) qualsiasi altro danno economico o sociale, significativo.

la **tabella** che segue rappresenta visivamente i livelli di gravità del rischio "*per i diritti e le libertà delle persone fisiche*" coinvolte:

	Impatto della violazione sui diritti e le libertà delle persone coinvolte
GRAVITÀ	**BASSO**: gli individui possono andare incontro a *disagi minori*, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.);
	MEDIO: gli individui possono andare incontro a *significativi disagi*, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.);
	ALTO: gli individui possono andare incontro a *conseguenze significative*, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.);
	MOLTO ALTO: gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.)

Nel valutare il livello complessivo di rischio che potrebbe derivare da una violazione, il **Dirigente competente in ragione del servizio o settore coinvolto** deve considerare una combinazione tra la gravità del potenziale impatto sui diritti e sulle libertà delle persone e la probabilità che esso si verifichi.

Con specifico riferimento alla violazione di dati personali, il livello di probabilità è ritenuto rilevante secondo il seguente schema:

PROBABILITÀ	**Possibilità che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche**
	IMPROBABILE
	PROBABILE

Le Linee Guida suggeriscono di ritenere, il rischio elevato per i diritti e le libertà delle persone fisiche, quantomeno come "probabile" quando la violazione riguardi dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, oppure che includono dati genetici, dati relativi alla salute o dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza.

RIASSUMENDO

	Descrizione	Notifica all'Autorità	Comunicazione agli interessati
Rischio	**BASSO**: nessun pregiudizio sui diritti e sulle libertà degli interessati né sulla sicurezza dei dati personali coinvolti	NO	NO
	MEDIO: probabile pregiudizio sui diritti e sulle libertà degli interessati e sulla sicurezza dei dati personali coinvolti	SI	NO
	ALTO e MOLTO ALTO: pregiudizio certo sui diritti e sulle libertà degli interessati e sulla sicurezza dei dati personali coinvolti	SI	SI

Sulla base degli elementi di cui sopra, acquisito un ragionevole grado di certezza del fatto che sia avvenuto un incidente per la sicurezza delle informazioni che abbia compromesso dati personali, il **Dirigente competente in ragione del servizio o settore coinvolto**:
a) stima la gravità e la probabilità della violazione e classifica il rischio;
b) documenta la decisione presa a seguito della valutazione del rischio nel Registro delle violazioni.

Gli elementi a supporto del procedimento e degli esiti della valutazione del rischio sono documentati utilizzando il modello **ALLEGATO D – "Modulo di valutazione del rischio connesso al violazione di dati personali"** e tale documentazione è conservata in apposito archivio.

SCENARI AL TERMINE DELLA FASE VALUTATIVA

A) ove i **rischi per gli interessati siano trascurabili**, la procedura può terminare, dopo aver documentato il processo e le scelte operate: le misure messe in atto sono state adeguate alla minaccia. Una eventuale fase di miglioramento può essere innescata per incrementare ulteriormente la protezione del dato, ma non è obbligatoria.

L'art. 33 paragrafo 1 chiarisce, infatti, che **non vi è obbligo di notifica della violazione quando è "*improbabile*" che questa comporti un rischio per i diritti e le libertà delle persone fisiche**. Tuttavia, si ricorda che, sebbene inizialmente la notifica possa non essere richiesta in quanto non esiste un rischio probabile per i diritti e le libertà delle persone fisiche, la situazione potrebbe cambiare nel corso del tempo e **il rischio dovrebbe essere rivalutato**.

B) nel caso in cui i **rischi per l'Interessato non siano trascurabili** occorre procedere alla notificazione all'Autorità di controllo sulla scorta delle indicazioni di cui al successivo paragrafo 4. In questo caso, la procedura deve dare le giuste priorità agli sforzi di contenimento dell'incidente. In ogni caso, andrà condotta una successiva fase di miglioramento.

C) qualora i **rischi per l'Interessato siano elevati** occorre procedere alla comunicazione della violazione alle persone fisiche interessate, di cui al successivo paragrafo 6, in aggiunta alla notificazione all'Autorità di controllo, salvo che quest'ultima richieda di omettere o ritardare la comunicazione stessa. In ogni caso, andrà condotta una fase di miglioramento.

3.3. Tool di autovalutazione del Garante privacy

Il Garante per la Protezione dei Dati Personali ha reso disponibile uno specifico Tool che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza.

Mediante alcuni semplici quesiti, il **Dirigente competente in ragione del servizio o settore coinvolto** viene guidato nell'assolvimento degli obblighi in materia di «Notifica di una violazione dei dati personali all'autorità di controllo» (articolo 33 del RGPD) e di «Comunicazione di una violazione dei dati personali all'interessato» (articolo 34 del RGPD). Tale strumento è da considerarsi esclusivamente quale ausilio al processo decisionale del Dirigente e non rappresenta un pronunciamento del Garante sulle informazioni fornite e sulle valutazioni effettuate. Le informazioni fornite durante il suo utilizzo non saranno conservate.
LINK al **sito web**: https://servizi.gpdp.it/databreach/s/self-assessment

3.4. Valutazioni supplementari

Ulteriori analisi dell'accaduto possono rendersi necessarie qualora:

a) il **Dirigente competente in ragione del servizio o settore coinvolto** ritenga necessario un approfondimento finalizzato ad es. all'integrazione di una precedente notifica all'Autorità di controllo;
b) l'Autorità di controllo, gli organi di polizia o la magistratura ritengano necessarie informazioni aggiuntive od approfondimenti di informazioni già fornite;
c) durante una delle fasi del processo di gestione del data breach siano emerse situazioni non approfondibili o non sia stato possibile coinvolgere pienamente responsabili esterni o questi non abbiano comunicato in tempo utile i risultati delle loro analisi.

L'analisi supplementare può essere attivata più volte per la stessa violazione, secondo necessità.

4. Notifica della violazione dei dati personali all'Autorità di controllo

Considerando 88 del RGPD:
"Nel definire modalità dettagliate relative al formato e alle procedure applicabili alla notifica delle violazioni di dati personali, è opportuno tenere debitamente conto delle circostanze di tale violazione, ad esempio stabilire se i dati personali fossero o meno protetti con misure tecniche adeguate di protezione atte a limitare efficacemente il rischio di furto d'identità o altre forme di abuso. Inoltre, è opportuno che tali modalità e procedure tengano conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali."

4.1. Quando effettuare la notificazione

Articolo 33, par. 1, del RGPD
"In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo"

Considerando 87 del RGPD:
"È opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione dei dati personali e delle sue conseguenze e effetti negativi per l'interessato. Siffatta notifica può dar luogo a un intervento dell'autorità di controllo nell'ambito dei suoi compiti e poteri previsti dal presente regolamento."

La normativa prevede che, **non appena si venga a conoscenza di una violazione dei dati personali che presenti un rischio per i diritti e le libertà delle persone coinvolte**, sia obbligatorio effettuare la notifica all'Autorità. Pertanto, **la notifica all'Autorità dell'avvenuta violazione non è un processo automatico, essendo subordinata alla valutazione del rischio per gli interessati che spetta al Dirigente**.

Le Linee guida chiariscono quando il Titolare del trattamento possa considerarsi "*a conoscenza*" di una violazione.

L'EDPB ritiene che il Titolare del trattamento debba considerarsi "*a conoscenza*" nel momento in cui sia ragionevolmente certo che si è verificato un incidente di sicurezza che abbia portato alla compromissione dei dati personali. Tuttavia, va considerato che il RGPD impone al Titolare del trattamento di attuare tutte le misure tecniche ed organizzative di protezione adeguate a stabilire, immediatamente, se si sia verificata una violazione ed informare tempestivamente l'Autorità di controllo e gli interessati. L'EDPB afferma, inoltre, che è opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione e delle sue conseguenze e dei suoi effetti negativi per l'Interessato.

Il Comune di Genova è quindi tenuto a prendere le misure necessarie per assicurarsi di venire "a conoscenza" di eventuali violazioni in maniera tempestiva, in modo da poter adottare le misure appropriate.

Il momento esatto in cui il Comune possa considerarsi "*a conoscenza*" di una particolare violazione dipenderà dalle circostanze della violazione.

Nella pratica, rilevazione e valutazione dell'evento sono spesso interconnesse e già nell'immediato può essere riscontrato un rischio ragionevole di violazione e, anche se non sono disponibili subito maggiori informazioni di dettaglio, si rende necessaria una preventiva notificazione all'Autorità di controllo. Vi sono casi, tuttavia, in cui è possibile definire se l'evento costituisca una violazione ai sensi del RGPD solo al termine della fase di valutazione. Acquisita la notizia di un possibile data breach il Comune può aver necessità di un breve periodo nel quale effettuare indagini, proprio al fine di stabilire se si sia verificata, o meno, una violazione. Durante questo periodo di indagine il Comune non può essere considerato "consapevole".

Le Linee Guida prevedono, tuttavia, che l'indagine iniziale venga avviata quanto prima e stabilisca con un ragionevole grado di certezza se si sia verificata una violazione; potrà poi seguire un'indagine più approfondita. In questo caso la decorrenza della tempistica per la notificazione all'Autorità di controllo è, comunque, dal momento della constatazione.

Qualora i contorni della violazione non siano chiari si può attendere fino ad **un massimo di 72 ore** prima di effettuare una notifica (Non si tratta di un termine puramente indicativo ma **categorico**, il cui mancato rispetto se non adeguatamente motivato, integra una situazione sanzionabile). Alla scadenza delle 72 ore è comunque necessario fare una comunicazione, significando che questa è l'inizio di una notifica in fasi. Il RGPD consente infatti una notifica per fasi, a condizione che il Titolare indichi i motivi del ritardo, in conformità all'articolo 33, paragrafo 1.

In ogni caso, l'accento dovrebbe essere posto sulla tempestività dell'azione per indagare su un incidente per stabilire se i dati personali sono stati effettivamente violati e, in caso affermativo, prendere misure correttive ed effettuare la notifica, se necessario.

Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, essa va corredata dei **motivi del ritardo**. Si suggerisce in ogni caso di procedere comunque all'effettuazione della notifica entro il termine, fatto salvo quanto *infra* con riferimento alla notifica per fasi.

L'obiettivo dell'obbligo di notifica è incoraggiare i Titolari del trattamento ad agire tempestivamente in caso di violazione, a contenerla e, se possibile, a recuperare i dati personali compromessi, nonché a chiedere il parere pertinente all'Autorità di controllo. La notifica all'Autorità di controllo entro le prime 72 ore può, inoltre, consentire al Titolare del trattamento di assicurarsi che le decisioni in merito alla comunicazione od alla mancata comunicazione all'Interessato siano corrette.

Si ricorda che **l'obbligo di effettuare la notifica all'Autorità di controllo, ricorre solo quando:**

a) il Comune di Genova è Titolare del trattamento di dati coinvolti nell'incidente;

b) il Comune di Genova è Contitolare del trattamento e l'accordo di contitolarità prevede che spetti ad esso procedere alla notifica, anche per conto dell'altro Contitolare;

c) il Comune di Genova è Responsabile del trattamento con delega alla notifica. Il Comune non ha il dovere di notificare la violazione all'Autorità di controllo quando agisce come Responsabile del trattamento per conto di altro Titolare, senza delega alla notifica. In questo caso il Comune deve comunicare al Titolare del trattamento la sospetta violazione e/o l'incidente di sicurezza riguardante dati personali, nei modi convenuti, con la massima tempestività e mettersi a disposizione di quest'ultimo per approfondimenti e contenimento dei danni.

4.2. Come effettuare la notificazione

Per le violazioni identificate, il **Dirigente competente in ragione del servizio o settore coinvolto** provveda alla notifica della violazione, **utilizzando gli strumenti ed in conformità alle istruzioni rese disponibili dall'Autorità di controllo**, **previa consultazione ed in collaborazione con il RPD**.

Alla data di redazione del presente documento il Garante della Protezione dei Dati Personali ha reso disponibile un **servizio di notificazione telematica**, raggiungibile al seguente indirizzo web: https://servizi.gpdp.it/databreach/s/
Nella stessa pagina è disponibile un modello facsimile, da NON utilizzare per la notifica al Garante, ma utile per vedere in anteprima i contenuti che andranno comunicati all'Autorità.

Si ricorda che, per semplificare gli adempimenti previsti per i Titolari del trattamento, il Garante ha ideato e messo disposizione un apposito **strumento di autovalutazione (self assessment)** che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza. Lo strumento è presente all'interno della pagina web sopra indicata.

4.2.1. Informazioni da fornire

Articolo 33, par. 3, del RGPD
"*La notifica di cui al paragrafo 1 deve almeno:*
a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi."

L'articolo sopra riportato stabilisce che il Titolare del trattamento debba "***almeno***" fornire queste informazioni all'Autorità di controllo mediante lo strumento della notifica, in modo che il Titolare possa, se necessario, scegliere di fornire ulteriori dettagli. Differenti tipi di violazioni (riservatezza, integrità o disponibilità) potrebbero richiedere di fornire ulteriori informazioni per spiegare puntualmente le circostanze di ciascuna fattispecie.
In ogni caso, l'Autorità di controllo potrà richiedere **ulteriori dettagli** nell'ambito della propria attività d'indagine.

Il RGPD non definisce le "*categorie di interessati*" o cosa si intenda per "*registrazioni di dati personali*".
Tuttavia, l'EDPB suggerisce, quanto alle categorie di interessati, di fare riferimento ai vari tipi di soggetti i cui dati personali siano stati colpiti da una violazione: a seconda dei descrittori utilizzati, ciò potrebbe includere, tra gli altri, bambini ed altri gruppi vulnerabili, persone con disabilità, dipendenti o fruitori di particolari servizi.
Allo stesso modo, in relazione alle categorie di registrazioni di dati personali, si potrebbe fare riferimento ai diversi tipi di record che il Titolare del trattamento si trovi a trattare, come dati

sanitari, documenti scolastici, informazioni sull'assistenza sociale, informazioni relativi a provvedimenti dell'Autorità giudiziaria, dettagli finanziari, numeri di conto bancario, numeri di carta d'identità, passaporto e così via.

Il considerando 85 del RGPD chiarisce che uno degli scopi della notifica è limitare i danni alle persone. Di conseguenza, se le tipologie di Interessati o di dati personali implicano un rischio di danno particolare che si verifica a seguito di una violazione (ad esempio, furto di identità, frode, perdita finanziaria, minaccia al segreto professionale), ecc., allora è importante che la notifica indichi queste categorie. Ad esso si collega, in tal modo, l'obbligo di descrivere le probabili conseguenze della violazione.

Laddove non fossero disponibili informazioni precise (ad esempio, il numero esatto degli interessati o di registrazioni), ciò non dovrebbe costituire un ostacolo alla tempestiva notifica della violazione. L'EDPB consente di effettuare approssimazioni nel numero di persone interessate e nel numero di registrazioni di dati personali coinvolti. L'attenzione dovrebbe essere rivolta ad affrontare gli effetti negativi della violazione piuttosto che fornire cifre precise. Pertanto, quando fosse evidente che si è verificata una violazione, ma la sua portata non fosse ancora nota, la notifica in fasi (di cui al successivo paragrafo) sarebbe un modo sicuro per soddisfare gli obblighi di notifica.

4.2.2. Notifica "per fasi"

Articolo 33, par. 4 del RGPD:
"*Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente,* ***le informazioni possono essere fornite in fasi successive*** *senza ulteriore ingiustificato ritardo*"

A seconda della natura della violazione, potrebbero essere necessarie ulteriori indagini da parte del **Dirigente competente in ragione del servizio o settore coinvolto** (anche valendosi della collaborazione di eventuali Responsabili del trattamento) per stabilire tutti i fatti rilevanti relativi all'incidente.

È probabile che ciò avvenga nel caso di violazioni più complesse, come alcuni tipi di incidenti che coinvolgono la sicurezza informatica nei quali, ad esempio, potrebbe essere necessaria un'indagine forense approfondita per stabilire puntualmente la natura della violazione e la misura in cui i dati personali siano stati violati o compromessi. Di conseguenza, in questi casi il Titolare del trattamento dovrà svolgere ulteriori indagini e fornire ulteriori informazioni in un secondo momento.
Ciò è consentito, a condizione che il Titolare del trattamento giustifichi il ritardo, ai sensi dell'articolo 33, paragrafo 1, del RGPD.
L'EDPB raccomanda che, quando il Titolare del trattamento notifica per la volta l'Autorità di controllo, esso possa precisare anche se non dispone ancora di tutte le informazioni richieste, impegnandosi a fornire maggiori dettagli in seguito. L'Autorità di controllo dovrebbe concordare su "come" e "quando" andrebbero fornite informazioni aggiuntive; ciò, tuttavia, non impedisce al Titolare del trattamento di fornire ulteriori informazioni in qualsiasi altra fase, qualora venga a conoscenza di ulteriori dettagli rilevanti sulla violazione che debbano essere forniti all'Autorità di controllo.

Dopo aver effettuato una notifica "iniziale", il Titolare del trattamento potrebbe, inoltre, informare l'Autorità di controllo del fatto che, a fronte di un'indagine successiva, siano emersi elementi tali da far ritenere che l'incidente di sicurezza fosse di minor impatto per l'Interessato o, anche, che non si fosse verificata alcuna violazione.

Non è prevista alcuna sanzione per la segnalazione di un incidente che, a seguito di indagini più approfondite, non risultasse essere una violazione.

4.2.3. Notifiche "ritardate" e "cumulative"

Articolo 33, par. 1 del RGPD:
"(…) *Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei* ***motivi del ritardo***"

Detta previsione, unitamente alla possibilità di effettuare una notifica "per fasi", rende evidente il fatto che il Titolare del trattamento potrebbe non essere sempre in grado di notificare una violazione "*senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza*" e che, pertanto, una notifica tardiva sia da considerarsi ammissibile.

L'EDPB segnala che uno scenario di questo tipo potrebbe verificarsi laddove, ad esempio, il Titolare del trattamento subisse molteplici violazioni simili, in un breve periodo di tempo, che colpissero allo stesso modo un gran numero di Interessati. Il Titolare potrebbe, in tal caso, venire a conoscenza di una violazione e, avviando l'indagine e prima della notifica, individuare ulteriori violazioni simili, dovute a cause diverse. A seconda delle circostanze, il Titolare del trattamento potrebbe impiegare del tempo per stabilire l'entità delle violazioni e, invece di notificare ciascuna violazione individualmente, potrebbe decidere di procedere con una notifica unitaria che rappresentasse le diverse violazioni. Ciò, potrebbe comportare un ritardo nella notifica all'Autorità di controllo.
Sebbene ogni singola violazione costituisca un incidente da segnalare, per evitare di essere eccessivamente formalista, l'EDPB ammette che il Titolare del trattamento possa procedere ad una notifica "cumulativa" che rappresenti tutte queste violazioni, a condizione che riguardi lo stesso tipo di dati personali, violati nello stesso modo, in un arco di tempo relativamente breve.
Laddove, invece, si trattasse di una serie di violazioni che riguardasse diversi tipi di dati personali, violati in modi diversi, la notifica dovrebbe procedere normalmente, segnalando ciascuna violazione in conformità a quanto previsto dall'articolo 33 del RGPD.

Sebbene la normativa consenta, in una certa misura, notifiche tardive, ciò non dev'essere visto come qualcosa che possa avvenire nell'ordinario.
Vale la pena di precisare che è sempre possibile inviare notifiche "cumulative", inerenti più violazioni simili "*senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza*".

4.3. Condizioni per le quali non è richiesta la notifica

Articolo 33, par. 1, del RGPD:
"*In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza,* ***a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche***."

Un esempio potrebbe essere il caso in cui i dati personali fossero già disponibili al pubblico e la divulgazione di tali dati non costituisse un probabile rischio per l'individuo.

Nel parere 03/2014 sulla notifica delle violazioni, il WP29 ha spiegato che una violazione della riservatezza dei dati personali crittografati con un algoritmo all'avanguardia costituisca pur sempre una violazione dei dati personali e debba essere notificata. Tuttavia, ove la riservatezza della chiave fosse intatta (cioè, la chiave non fosse stata compromessa in alcuna violazione della sicurezza e fosse stata generata in modo tale da non poter essere scoperta con i mezzi tecnici disponibili da qualsiasi persona non autorizzata ad accedervi) allora i dati potrebbero essere, in linea di principio, considerati incomprensibili. Pertanto, sarebbe improbabile che la violazione potesse incidere negativamente sugli individui e, ciò, renderebbe non necessaria la notifica.
Ciò nonostante, anche quando i dati fossero crittografati, una perdita od un'alterazione potrebbe avere conseguenze negative per gli Interessati qualora il Titolare del trattamento non disponesse di backup adeguati (perdita di disponibilità).
A conclusioni analoghe il WP29 è pervenuto in relazione alla fattispecie in cui dati personali, come le password, fossero sottoposti ad "hashing" con "salt", il valore di hash fosse calcolato con una funzione hash con chiave crittografica all'avanguardia, la chiave utilizzata per eseguire l'hashing dei dati non fosse compromesse in alcuna violazione e la chiave utilizzata per eseguire l'hashing dei dati fosse stata generata in modo tale da non poter essere accertata con i mezzi tecnologici disponibili da alcuna persona non autorizzata ad accedervi.

Secondo l'EDPB, ove i dati personali fossero stati resi sostanzialmente incomprensibili a soggetti non autorizzati ed ove dei dati medesimi esistesse una copia od un backup, potrebbe non essere necessario notificare all'Autorità di controllo la violazione della riservatezza. Questo in quanto sarebbe improbabile che una tale violazione possa rappresentare un rischio i diritti e le libertà degli individui.

Tuttavia, va tenuto presente che, sebbene inizialmente la notifica potrebbe non essere richiesta (non essendo probabile un rischio per i diritti e le libertà degli individui), ciò potrebbe cambiare nel tempo ed il rischio dovrebbe essere rivalutato (ad esempio, se, successivamente, si scopre che la chiave fosse stata compromessa o venisse scoperta una vulnerabilità nel software di crittografia) e potrebbe rendersi, comunque, necessaria una notifica.
Inoltre, va notato che laddove si verificasse una violazione in cui non esistessero backup dei dati personali crittografati, allora si sarebbe in presenza di una violazione della disponibilità, che potrebbe comportare rischi per le persone e, pertanto, potrebbe rendersi necessaria una notifica.

Allo stesso modo, laddove si verificasse una violazione che comportasse la perdita di dati crittografati, anche in presenza di un backup dei dati personali, ciò potrebbe comunque costituire una violazione da notificare, a seconda del tempo impiegato per ripristinare i dati da tale backup e dell'effetto che la mancanza di disponibilità avrebbe sugli Interessati.

4.4. Eventuali ulteriori notificazioni all'Autorità di controllo

Effettuata la notifica in favore dell'Autorità di controllo, è poi opportuno verificare se sia necessaria una *seconda notifica*, più approfondita, quale conseguenza di un'analisi tecnica supplementare ovvero di elementi ed informazioni successivamente acquisiti.

È opportuno inoltre precisare che se, dopo la notifica iniziale, una successiva indagine dimostrasse che l'incidente di sicurezza è stato contenuto e che non si è verificata alcuna violazione, il **Dirigente competente in ragione del servizio o settore coinvolto** dovrebbe informarne l'Autorità di controllo. Tali informazioni possono quindi essere aggiunte alle informazioni già fornite all'Autorità di controllo e l'incidente può essere quindi registrato come un evento che non costituisce una violazione.

Non si incorre in alcuna sanzione se si segnala un incidente che alla fine si rivela non essere una violazione.

5. Recepimento della eventuale risposta dell'Autorità di controllo

Il **Dirigente competente in ragione del servizio o settore coinvolto** dispone con sollecitudine ulteriori indagini o eventuali misure correttive, secondo le disposizioni ricevute dall'Autorità di controllo. Parimenti, provvede a seguito del ricevimento di indicazioni od ordini relativamente alla comunicazione da effettuare o non effettuare in favore degli interessati.

6. Comunicazione della violazione dei dati personali all'Interessato

Articolo 34, par. 1, del RGPD:
"*Quando la violazione dei dati personali è* ***suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche****, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo*"

Considerando 86 del RGPD:
"Il titolare del trattamento dovrebbe comunicare all'interessato la violazione dei dati personali senza indebito ritardo, qualora questa violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, al fine di consentirgli di prendere le precauzioni necessarie. La comunicazione dovrebbe descrivere la natura della violazione dei dati personali e formulare raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi. Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge. Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione."

Contestualmente alla decisione di notificare all'Autorità di controllo, occorre valutare se sia il caso di informare anche gli Interessati. Il modello di notificazione predisposto dall'Autorità di controllo richiede infatti una specifica indicazione e descrizione delle circostanze e valutazioni che abbiano condotto ad effettuare o non effettuare siffatta comunicazione agli interessati.

La soglia di rischio determinante per rendere necessaria la comunicazione di una violazione ai singoli Interessati è più elevata rispetto a quella utilizzata come indicatore della necessità della notifica all'Autorità di controllo e, pertanto, non tutte le violazioni dovranno essere comunicate all'Interessato. **A tale scopo va valutata la gravità del rischio per gli interessati ed i loro diritti**.

Nel caso di accertamento di una **violazione di dati personali che sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche**, come valutato secondo quanto indicato al precedente paragrafo 3, il **Dirigente competente in ragione del servizio o settore coinvolto**, provvederà ad informare gli Interessati sul fatto avvenuto, sui dati violati e sulle procedure necessarie a ridurre il rischio. In tale ipotesi occorre quindi valutare:

a) la fattibilità di contattarli singolarmente oppure la necessità di procedere con pubblicazioni su diversi mezzi di comunicazione (sito web, quotidiani, radio, tv);
b) le misure di contenimento che gli stessi interessati possano mettere in atto per minimizzare i rischi;
c) le forme di comunicazione più comprensibili per gli interessati (mezzi, lingue, linguaggio) come indicato nelle Linee guida elaborate dal Gruppo ex art. 29 in materia di trasparenza (WP 260), aggiornate in base alle previsioni del Regolamento (UE) 2016/679.

Anche di questa fase deve essere prodotta e conservata appropriata documentazione.

6.1. Quando effettuare la comunicazione

Articolo 34, par. 1, del RGPD:
"*Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato* ***senza ingiustificato ritardo.***"

Il RGPD afferma che la comunicazione di una violazione agli interessati dovrebbe avvenire "***senza ingiustificato ritardo***", il che significa il prima possibile. **L'obiettivo principale della comunicazione agli interessati consiste nel fornire loro informazioni specifiche sulle misure che questi possono prendere per proteggersi**. A seconda della natura della violazione e del rischio presentato, la comunicazione tempestiva aiuterà le persone a prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione.

Da notare inoltre che il Considerando 86 suggerisce che "T*ali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge*". Parallelamente, il Considerando 88 indica che la notifica di una violazione dovrebbe tenere "*conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali*".

Conseguentemente si ritiene suggeribile, **nel contesto della notifica all'Autorità di controllo, formulare espressa richiesta di indicazioni in tal senso** (non soltanto se provvedere alla comunicazione o no, ma anche quale contenuto della comunicazione e quali canali suggeriti).

Le Linee Guida emanate dall'EDPB, suggeriscono le seguenti fattispecie, quali indicatori del fatto che la violazione possa comportare un "*rischio elevato per i diritti e le libertà delle persone fisiche*":

- attacco informatico ad un servizio online, con esfiltrazione dei dati personali ivi presenti (anche se riguardanti le credenziali di accesso e/o la cronologia e/o i log);
- attacco mediante ransomware agli archivi del Comune, in assenza di backup o, comunque, in caso di impossibilità di ripristino;
- i dati personali di un interessato sono stati erroneamente comunicati ad altro Interessato;
- comunicazioni e-mail a destinatari errati;
- indisponibilità di dati e/o documenti protratta per un periodo di tempo significativo;

6.2. Come effettuare la comunicazione

Considerando 86 del RGPD:
"(…) *Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e* ***in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti*** *quali le autorità incaricate dell'applicazione della legge. Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione*"

Per la comunicazione, è possibile identificare **uno o più canali di comunicazione**, a seconda delle circostanze, quali comunicazioni e-mail, comunicazioni PEC, SMS, posta ordinaria, comunicati

istituzionali, banner o notifiche su siti web, scegliendo il canale che massimizza la probabilità che tutti gli interessati siano raggiunti dal messaggio.

Di regola, la violazione dovrebbe essere comunicata direttamente a ciascun Interessato, a meno che ciò comporti uno sforzo sproporzionato. In tal caso, è tuttavia prevista una comunicazione pubblica od un provvedimento analogo, con il quale gli interessati vengano informati in modo altrettanto efficace (articolo 34, paragrafo 3, lettera c), del RGPD).

Caso per caso, il **Dirigente competente in ragione del servizio o settore coinvolto**, dovrà **sempre privilegiare la modalità di comunicazione diretta** con i soggetti interessati (quali e- mail, PEC, SMS o messaggi diretti) eventualmente anche combinando modalità differenti. Inoltre, nel contesto della notificazione all'Autorità di controllo, potranno essere richiesti suggerimenti in ordine ai tempi, alla modalità preferibile ed al contenuto della comunicazione agli Interessati.

Il messaggio dovrà essere comunicato in maniera evidente e trasparente, evitando quindi di inviare le informazioni nel contesto di update generali o newsletter, che potrebbero essere facilmente fraintesi dai lettori.

Non dovrà essere utilizzato il canale di contatto compromesso dalla violazione, in quanto tale canale potrebbe essere utilizzato anche da autori di attacchi che si presentino come Comune di Genova.

Ove non si abbia la possibilità di comunicare una violazione all'Interessato perché non si disponga di dati sufficienti per contattarlo, questi sarà informato non appena sia ragionevolmente possibile farlo (ad esempio quando l'Interessato esercita il proprio diritto. ai sensi dell'articolo 15 del RGPD, di accedere ai dati personali e fornisce le informazioni necessarie per essere contattato).

6.3. Quali informazioni comunicare

Articolo 34, par. 2, del RGPD:
"*La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e* ***contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).***"

Sebbene sia preferibile utilizzare il modello **ALLEGATO E – "Comunicazione all'Interessato della violazione dei dati personali"**, la comunicazione in altra forma deve comunque contenere, ai sensi dell'art. 34, le seguenti **informazioni**:

1) il nome ed i dati di contatto del RPD o di altro punto di contatto presso cui ottenere più informazioni;
2) una descrizione della natura della violazione;
3) una descrizione delle probabili conseguenze della violazione dei dati personali;
4) una descrizione delle misure adottate o di cui si propone l'adozione da parte del Comune per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi;
5) se l'Autorità di controllo abbia suggerito od ordinato misure di gestione della violazione e sull'attenuazione del suo impatto;
6) eventuali indicazioni al destinatario sul modo in cui proteggersi dalle possibili conseguenze negative della violazione

Particolare attenzione dev'essere prestata con riferimento alle "*eventuali indicazioni al destinatario sul modo in cui proteggersi dalle possibili conseguenze negative della violazione*".

6.4. Quando non effettuare la comunicazione

Articolo 34, parr. 3 e 4, del RGPD:
"3. ***Non è richiesta la comunicazione all'interessato*** *di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:*
a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, ***l'autorità di controllo può richiedere****, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi* ***provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.***"

Il **Dirigente competente in ragione del servizio o settore coinvolto**, il quale ritenga di non procedere con la comunicazione agli Interessati, dovrà essere in grado di dimostrare all'Autorità di controllo la ricorrenza di una o più delle condizioni di cui all'articolo 34, par. 3 del RGPD.
Si consideri, peraltro che, sebbene inizialmente la notifica possa essere ritenuta come non necessaria per assenza di rischio per i diritti e libertà delle persone fisiche, ciò potrebbe cambiare nel tempo a seguito del sopravvenire di ulteriori elementi informativi: in tal caso, il rischio dovrà essere rivalutato.

7. Altre segnalazioni

Il **Dirigente competente in ragione del servizio o settore coinvolto** dovrà verificare la necessità di informare altri organi quali, a mero titolo esemplificativo:
- CSIRT Italia (https://www.csirt.gov.it/segnalazione);
- Organi di Polizia (in caso di violazioni di dati conseguenza di comportamenti illeciti o fraudolenti);
- CNAIPC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche).
- Gestore di Identità Digitale ed AgID nel caso in cui si individui un uso anomalo di un'identità SPID, CIE, CNS, ecc.

Ciascuna segnalazione dovrà avvenire nel rispetto delle procedure ed utilizzando la modulistica all'uopo eventualmente predisposta da ciascuna Autorità di vigilanza o controllo.

8. Documentazione della violazione

Articolo 33, par. 5, del RGPD:
*"Il titolare del trattamento **documenta qualsiasi violazione** dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo."*

La necessità di documentare le violazioni di dati personali è attuativa del principio di "accountability" (c.d. responsabilizzazione), contenuto nell'articolo 5, paragrafo 2, del RGPD. Lo scopo della registrazione delle violazioni non notificabili, nonché delle violazioni notificabili, si riferisce anche agli obblighi del Titolare del trattamento previsti dall'articolo 24 del RGPD e l'Autorità di controllo può richiedere di vedere tali registrazioni.

Si ricorda che **la mancata corretta documentazione di una violazione può comportare l'esercizio da parte dell'Autorità di controllo dei suoi poteri ai sensi dell'articolo 58 del RGPD e l'imposizione di una sanzione amministrativa pecuniaria ai sensi dell'articolo 83 del RGPD**.

Il Comune di Genova stabilisce di documentare gli incidenti di sicurezza e le violazioni di dati personali come segue:

a) adozione, di un registro "interno" delle (sole) violazioni di dati personali, intendendosi per tale un inventario aggiornato delle violazioni contenente tutte le informazioni necessarie a chiarire le circostanze nelle quali si sono verificate, le conseguenze che le stesse hanno avuto ed i provvedimenti adottati per porvi rimedio. Esso tiene traccia anche delle varie fasi di gestione dell'evento, dalla rilevazione, all'analisi e alla sua risoluzione e conclusione;
b) adozione di modulistica, anche a rilevanza esterna, idonea a documentare gli incidenti di sicurezza e le violazioni di dati personali.

Il RGPD non specifica un **periodo di conservazione** per tale documentazione. Essa sarà dunque conservata nel rispetto dei termini e delle norme di legge sulla conservazione della documentazione amministrativa, anche in considerazione del fatto che la conservazione è necessaria, in conformità dell'articolo 33, paragrafo 5, nella misura in cui il Comune potrà essere chiamato a fornire prove all'Autorità di controllo in merito al rispetto di tale articolo oppure, più in generale, del principio di responsabilizzazione.

8.1. il Registro delle violazioni

Il Dirigente competente in ragione del servizio o settore coinvolto è responsabile della tenuta e dell'aggiornamento del Registro delle violazioni, sulla scorta delle informazioni e della documentazione fornita dal Dirigente competente in ragione del servizio o settore coinvolto.

Poiché il RGPD non specifica quale debba essere il **contenuto** e la **forma** del Registro delle violazioni né il tipo di supporto sul quale debba essere redatto, per estensione delle disposizioni contenute nell'art. n. 30 del RGPD (relativamente al registro delle attività di trattamento e registro delle categorie di attività di trattamento) si presume che tale registro possa anche essere **di tipo elettronico**. Il Comune di Genova ha quindi deciso di adottarlo in tale forma.

Il registro dovrà essere accompagnato da idonee misure di sicurezza atte a garantire **l'integrità e l'immodificabilità dei dati in esso registrati** quali ad esempio la protocollazione, la

stampa, …). I dati presenti nel registro sono trattati nel rispetto del **principio di minimizzazione** e secondo le misure necessarie per mitigare i rischi di violazione dei dati personali.

Ogni segnalazione, comprese quelle **non veritiere**, deve essere soggetta a registrazione nel registro delle violazioni. Per ogni violazione di cui sia accertata l'esistenza, anche se non notificata all'Autorità di controllo e non comunicata agli interessati, **il registro ripoterà (almeno)**:

(con riferimento alla segnalazione)
- numerazione progressiva;
- data ed ora della segnalazione;
- dati identificative del segnalante;
- unità organizzativa coinvolta;
- organi informati;
- valutazione circa la rilevanza (o meno) della segnalazione quale violazione di dati personali;

(con riferimento alla violazione)
- luogo violazione;
- modalità della violazione;
- descrizione dei sistemi, apparati, reti, banche dati oggetto di data breach;
- la natura della violazione dei dati personali;
- altri elementi utili alla descrizione della violazione;

(con riferimento agli interessati)
- indicazione delle categorie di interessati coinvolti;
- indicazione del numero approssimativo di interessati coinvolti;

(con riferimento ai dati personali coinvolti)
- indicazione delle categorie dei dati personali coinvolte;
- indicazione del numero approssimativo di dati personali coinvolti;

(con riferimento alle conseguenze)
- descrizione delle previste (o verificate) conseguenze;

(con riferimento ai rimedi)
- indicazione delle misure adottate per porre rimedio alla violazione;
- indicazione delle misure proposte per porre rimedio alla violazione;

(con riferimento all'attenuazione delle conseguenze)
- indicazione delle misure adottate per attenuare i possibili effetti negativi;
- indicazione delle misure proposte per attenuare i possibili effetti negativi;

(con riferimento ai tempi di ripristino)
- indicazione della tempistica stimata

(con riferimento alla notifica all'Autorità di controllo)
- valutazione circa la probabilità (o improbabilità) che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche;
- effettuazione o meno della notificazione;
- ragioni della omessa notificazione all'Autorità di controllo;
- ragioni della tardiva notificazione all'Autorità di controllo;

(con riferimento alla comunicazione agli interessati)
- valutazione circa la possibilità che la violazione sia (o meno) suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- effettuazione o meno della comunicazione;
- ragioni della omessa comunicazione agli interessati;

8.2. Altri documenti ed informazioni

Ad integrazione di quanto riportato nel registro, il **Dirigente competente in ragione del servizio o settore coinvolto** raccoglie e **conserva tutti i documenti relativi ad ogni violazione**, compresi quelli inerenti alle circostanze ad essa relative, le sue conseguenze ed i provvedimenti adottati per porvi rimedio.

Spetta all'**Area Technology Office (Sistemi Informativi) od altra struttura organizzativa equivalente documentare tutti gli incidenti di sicurezza informatica**, le circostanze ad essi relative, le conseguenze, le misure tecniche ed i provvedimenti adottati per porvi rimedio.

9. Fase di miglioramento

Una volta contenuti i rischi o le conseguenze della violazione ed adempiuto agli obblighi di notificazione e comunicazione previsti dal RGPD occorre dedicare attenzione alla fase di miglioramento delle misure tecniche ed organizzative in uso presso il Comune, al fine di evitare il ripetersi di incidenti analoghi.

Le azioni previste in questa fase sono:

- l'analisi della relazione dettagliata sull'incidente;
- la reiterazione del processo di Gestione del rischio;
- l'eventuale revisione di questo documento (se necessario) e di eventuali altri documenti collegati (es. analisi del rischio, misure di sicurezza, modulistica, ecc.);
- l'individuazione di controlli che diminuiscano la probabilità dell'incidente o i relativi impatti sul sistema colpito e su sistemi analoghi;
- la revisione del sistema di gestione della protezione dei dati;
- la revisione con cadenza almeno annuale della procedura descritta nel presente documento.

10. Fattispecie di contitolarità e responsabilità del trattamento

10.1. Contitolari del trattamento

Articolo 26 del RGPD
"1. Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati.
2. L'accordo di cui al paragrafo 1 riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.
(…)"

Sulla scorta della previsione sopra riportata, laddove il Comune di Genova si trovasse ad operare, unitamente ad altri soggetti, in fattispecie classificabili in termini di **contitolarità del trattamento** dei dati personali, il relativo accordo o convenzione dovrà contenere espressa determinazione di chi assumerà il comando o sarà responsabile del rispetto degli obblighi di cui agli articoli 33 e 34 del medesimo RGPD.

Si riporta, a titolo esemplificativo, una bozza di clausola:
"1. In eventuali casi di violazione della sicurezza dei dati personali che comportino, accidentalmente od in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati e tali da mettere a rischio i diritti e le libertà degli individui i cui dati personali sono trattati nel contesto del progetto comune, l'attività di coordinamento ai fini dell'adempimento degli obblighi di cui agli articoli 33 e 34 del RGPD è affidata a _____ il quale curerà la predisposizione di un apposito documento (data breach policy), ove non già esistente ed adottato.
2. Al verificarsi di una violazione di dati personali, il Contitolare non assegnatario dell'attività di coordinamento provvederà:
a) ad informare l'altro Contitolare tempestivamente ed in ogni caso entro e non oltre 24 ore dalla scoperta dell'evento, tramite PEC, di essere venuto a conoscenza di una violazione, fornendogli tutti i dettagli della violazione subita, in particolare una descrizione della natura della violazione dei dati personali, le categorie e il numero approssimativo di interessati coinvolti, nonché le categorie e il numero approssimativo di registrazioni dei dati in questione, l'impatto della violazione dei dati personali sugli Interessati coinvolti e le misure adottate per mitigare i rischi;
b) fornire assistenza per far fronte alla violazione ed alle sue conseguenze soprattutto in capo agli Interessati coinvolti. Esso, inoltre, si attiverà per mitigare gli effetti delle violazioni, proponendo tempestive azioni correttive ed attuando tutte le azioni correttive approvate e/o richieste dal Contitolare assegnatario dell'attività di coordinamento. Tali misure sono richieste al fine di garantire un livello di sicurezza adeguato al rischio correlato al Trattamento eseguito.
3. Ciascun Contitolare si impegna a predisporre e tenere aggiornato un registro interno delle violazioni di dati personali nonché a raccogliere e conservare tutti i documenti relativi ad ogni violazione, compresi quelli inerenti alle circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio."

10.1. Responsabili del trattamento

Articolo 28, par. 3 del RGPD
"I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:
(…)
f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
(…)"

Sulla scorta della previsione di cui sopra, laddove il Comune di Genova necessiti che il trattamento di dati personali venga effettuato per suo conto ad opera di altri soggetti qualificabili come **responsabili del trattamento**, il contratto od altro atto giuridico che vincoli tale soggetto al Comune dovrà contenere espressa previsione che il responsabile assista il Comune nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del RGPD, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento.

È opportuno notare che il Responsabile del trattamento non è tenuto a valutare preventivamente la probabilità del rischio derivante da una violazione prima di avvisare il Titolare del trattamento in quanto solo quest'ultimo deve effettuare tale valutazione nel momento in cui viene a conoscenza della violazione. Il Responsabile deve solo stabilire se si sia verificata una violazione ed avvisare il Titolare del trattamento.

Il Titolare del trattamento si avvale del Responsabile del trattamento per il raggiungimento delle proprie finalità; pertanto, in linea di principio, il Titolare dovrebbe essere considerato "consapevole" una volta che il Responsabile lo abbia informato della violazione. L'obbligo del Responsabile di informare il proprio Titolare del trattamento consente a quest'ultimo di affrontare la violazione e di determinare se sia tenuto o meno ad informare l'Autorità di controllo e le persone interessate.

Il Comune potrebbe anche voler indagare sulla violazione, poiché il Responsabile del trattamento potrebbe non essere in grado di conoscere tutti i fatti rilevanti relativi alla questione, ad esempio, se sia ancora conservata una copia od un backup dei dati personali distrutti o persi dal Responsabile del trattamento. Ciò potrebbe influire sulla necessità o meno del Comune di effettuare la notifica.

Il RGPD non prevede un termine esplicito entro il quale il Responsabile del trattamento debba avvisare il Titolare, salvo che debba farlo "*senza ingiustificato ritardo*". Pertanto, l'EDPB raccomanda al Responsabile del trattamento di informare tempestivamente il Titolare, fornendo ulteriori informazioni sulla violazione man mano che maggiori dettagli diventino disponibili. Ciò, è importante per aiutare il Titolare del trattamento a soddisfare l'obbligo di notifica all'Autorità di controllo entro 72 ore.

Un Responsabile del trattamento potrebbe effettuare una notifica per conto del Comune di Genova, nel caso in cui quest'ultimo gli avesse concesso un'adeguata autorizzazione e, ciò, rientrasse negli accordi contrattuali tra Titolare e Responsabile. Tuttavia, è importante ricordare che la responsabilità legale di notificare rimarrebbe in capo al Comune di Genova.

Anche in questo caso, si riporta, a titolo esemplificativo, una bozza di clausola:

"1. In eventuali casi di violazione della sicurezza dei dati personali che comportino, accidentalmente od in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati e tali da mettere a rischio i diritti e le libertà degli individui i cui dati personali sono trattati dal Responsabile per conto del Titolare (c.d. data breach), il Responsabile deve osservare le disposizioni organizzative contenute nella data breach policy adottata dal Titolare e, in ogni caso:

a) informare il Titolare tempestivamente ed in ogni caso entro e non oltre 24 ore dalla scoperta dell'evento, tramite PEC, di essere venuto a conoscenza di una violazione e fornire al Titolare tutti i dettagli della violazione subita, in particolare una descrizione della natura della violazione dei dati personali, le categorie e il numero approssimativo di interessati coinvolti, nonché le categorie e il numero approssimativo di registrazioni dei dati in questione, l'impatto della violazione dei dati personali sul Titolare e sugli Interessati coinvolti e le misure adottate per mitigare i rischi. Spetta unicamente al Titolare del trattamento di effettuare la valutazione circa la probabilità di rischio derivante dalla violazione stessa;

b) fornire assistenza al Titolare per far fronte alla violazione ed alle sue conseguenze soprattutto in capo agli Interessati coinvolti. Il Responsabile si attiverà per mitigare gli effetti delle violazioni, proponendo tempestive azioni correttive al Titolare ed attuando tutte le azioni correttive approvate e/o richieste dal Titolare. Tali misure sono richieste al fine di garantire un livello di sicurezza adeguato al rischio correlato al Trattamento eseguito;

2. I Responsabile del trattamento si impegna a predisporre e tenere aggiornato un registro interno delle violazioni di dati personali nonché a raccogliere e conservare tutti i documenti relativi ad ogni violazione, compresi quelli inerenti alle circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.".

ALLEGATI

ALLEGATO A – “DIAGRAMMA DI FLUSSO”

ALLEGATO B – “Modulo di segnalazione di una potenziale violazione di dati personali”

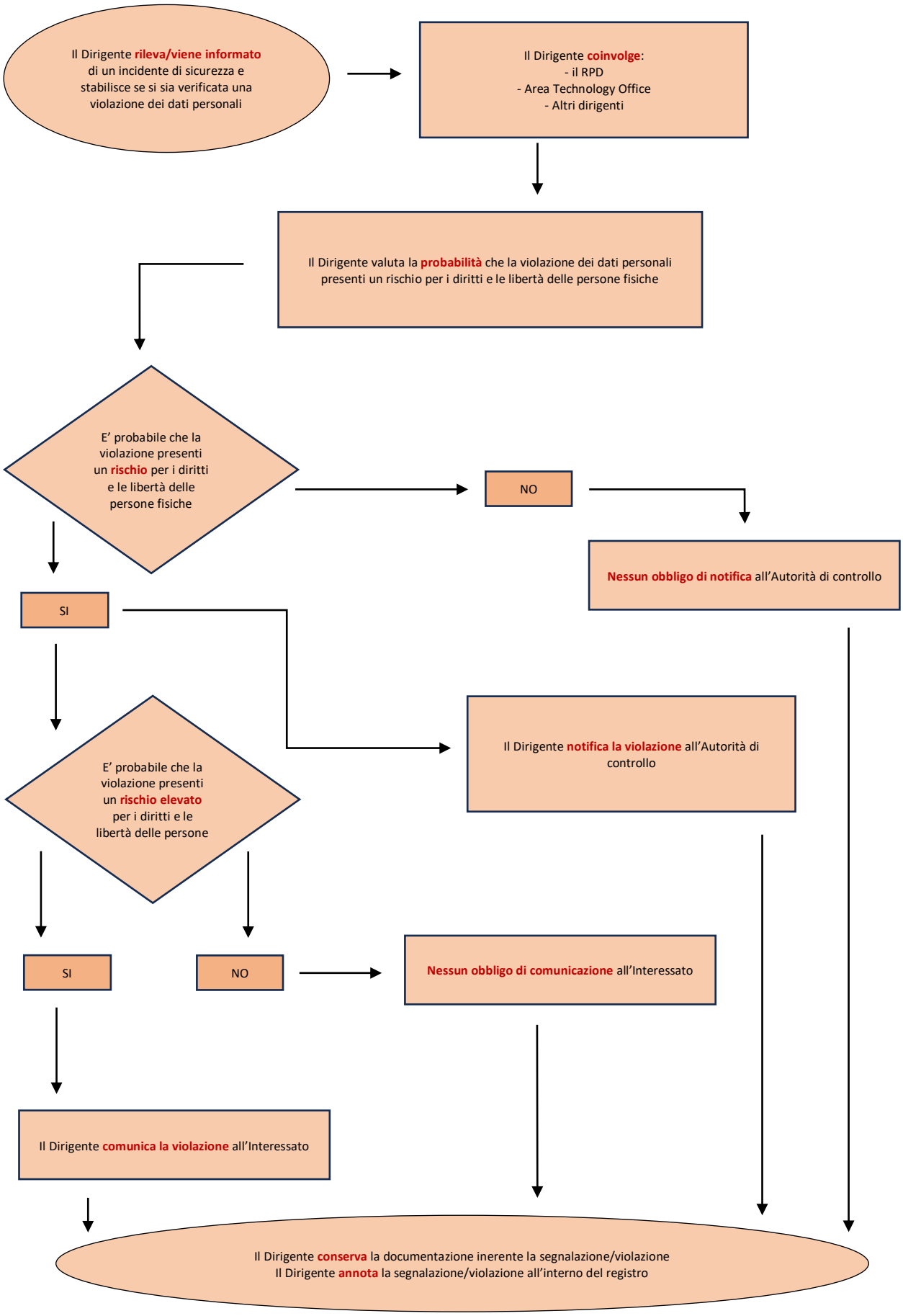
ALLEGATO C – “Modulo di inoltro di segnalazione di una potenziale violazione di dati personali”

ALLEGATO D – “Modulo di valutazione del rischio connesso al violazione di dati personali”

ALLEGATO E – “Comunicazione all’Interessato della violazione dei dati personali”

ALLEGATO F – “Linee-guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali”

ALLEGATO A - DIAGRAMMA DI FLUSSO



ALLEGATO B

MODULO DI SEGNALAZIONE DI UNA POTENZIALE VIOLAZIONE DI DATI PERSONALI

ai sensi dell'art. 33 del Regolamento Generale sulla Protezione dei Dati

(Il presente modello non è vincolante, ben potendo la segnalazione essere fornita in forma libera)

Il presente modulo va compilato da chiunque constati un effettivo o potenziale incidente di sicurezza che possa comportare una violazione di dati personali, al fine di consentire al Titolare del trattamento la valutazione e gestione dell'incidente stesso e, in caso di violazione accertata, di notifica al Garante e di comunicazione agli interessati.

Il modulo, compilato in ogni sua parte e debitamente sottoscritto, dev'essere consegnato al più presto con le seguenti alternative modalità:

a) consegna a mani presso l'Ufficio protocollo;
b) consegna via email all'indirizzo:
c) consegna via PEC all'indirizzo:

Ove al momento della rilevazione dell'incidente di sicurezza non sia possibile una descrizione particolareggiata dell'evento, è comunque essenziale procedere immediatamente alla sua segnalazione, anche con informazioni incomplete. Sarà cura del Titolare del trattamento accertare quanto necessario, anche contattando il segnalante ai recapiti forniti.

Dati identificativi del SEGNALANTE ed informazioni di contatto					
Cognome					
Nome					
Documento di identità N.		rilasciato da		scadenza	
Servizio o settore di appartenenza	(questo campo dev'essere compilato solo in caso di segnalazione ad opera di un dipendente/collaboratore del Titolare. In tale ipotesi non vanno indicati i riferimenti al documento di identità)				
Telefono		cellulare			
E-mail		PEC			

Informazioni sulla VIOLAZIONE	
Quando mi sono accorto della violazione?	
Come mi sono accorto della violazione?	

Breve **descrizione** della violazione	

Quali strutture sono coinvolte (locali, archivi, web, dispositivi elettronici, etc)?	

Quale tipo di violazione?	In caso di perdita di **confidenzialità**	
		I dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento
		I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati
		I dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito
		Altro (specificare)
	In caso di perdita di **integrità**	
		I dati sono stati modificati e resi inconsistenti
		I dati sono stati modificati mantenendo la consistenza
		Altro (specificare)
	In caso di perdita di **disponibilità**	
		Mancato accesso a servizi
		Malfunzionamento e difficoltà nell'utilizzo di servizi
		Altro (specificare)

Quali soggetti coinvolti?		Il segnalante
		Cittadini
		Dipendenti e titolari di incarichi di collaborazione
		Utenti di servizi pubblici
		Soggetti che ricoprono cariche istituzionali
		Beneficiari o assistiti
		Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
		Minori
		Categorie ancora non determinate
		Altro (specificare)

Sono coinvolti cittadini di altri paesi?	(in caso affermativo, indicare i paesi di riferimento)

Quali dati personali sono coinvolti?		Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale, altro...)
		Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
		Dati di accesso e di identificazione (username, password, customer ID, altro...)
		Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro...)
		Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro...)
		Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza o di prevenzione
		Dati di profilazione
		Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro...)
		Dati di localizzazione
		Dati che rivelino l'origine razziale o etnica
		Dati che rivelino opinioni politiche
		Dati che rivelino convinzioni religiose o filosofiche
		Dati che rivelino l'appartenenza sindacale
		Dati relativi alla vita sessuale o all'orientamento sessuale
		Dati relativi alla salute
		Dati genetici
		Dati biometrici
		Categorie ancora non determinate
		Altro, descrivere:

Quali potenziali effetti negativi per le persone coinvolte?		Perdita del controllo dei dati personali
		Limitazione dei diritti
		Discriminazione
		Furto o usurpazione d'identità
		Frodi
		Perdite finanziarie
		Decifratura non autorizzata della pseudonimizzazione
		Pregiudizio alla reputazione
		Perdita di riservatezza dei dati personali protetti da segreto professionale
		Conoscenza da parte di terzi non autorizzati
		Qualsiasi altro danno economico o sociale significativo (specificare)

E' già stata fatta una segnalazione al Garante della privacy?	(in caso affermativo, allegare la relativa documentazione)
E' già stata fatta una segnalazione alle forze dell'ordine o all'Autorità giudiziaria?	(in caso affermativo, allegare la relativa documentazione)

Documentazione che si allega	(diversa da quella indicata al punto precedente. Indicare anche eventuali fogli aggiuntivi necessari per ragioni di spazio)	
	X	Fotocopia del documento di identità (solo per soggetti esterni al Titolare)
Numero dei documenti allegati		

ANNOTAZIONI

Firma

_____, lì _____ _____

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI

Ai sensi dell'articolo 13 del Regolamento (UE) 2016/679 si rappresenta che il Comune di Genova, in qualità di Titolare del trattamento (con sede in Via Garibaldi 9, Palazzo Tursi, 16124 Genova; Email: urp@comune.genova.it; PEC: comunegenova@postemailcertificata.it), tratterà i dati personali conferiti con il presente modulo per le finalità previste dal Regolamento (UE) 2016/679 e dal Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196 e s.m.i.), in particolare per l'esecuzione dei propri compiti di interesse pubblico o comunque connessi all'esercizio dei propri pubblici poteri e, segnatamente, al solo scopo di acquisire ogni necessaria informazione in merito all'evento segnalato, adottare le conseguenti procedure di tutela ed effettuare le comunicazioni previste dalla normativa vigente.
Il conferimento dei dati, fermo restando quanto previsto dall'art. 33, par. 4, del Regolamento (UE) 2016/679, è obbligatorio al fine della ricevibilità della segnalazione, ferma restando la facoltà del Titolare di istruire comunque il procedimento volto all'accertamento della violazione di dati personali. I dati acquisiti nell'ambito della procedura saranno conservati in conformità alle norme sulla conservazione della documentazione amministrativa. I dati saranno trattati esclusivamente dal personale e da collaboratori del Titolare o delle imprese espressamente designate come responsabili del trattamento. Al di fuori di queste ipotesi, i dati non saranno diffusi, né saranno comunicati a terzi, fatti salvi i casi in cui si renda necessario comunicarli al Garante per la protezione dei dati personali, all'Autorità giudiziaria e ad altri soggetti coinvolti nell'attività istruttoria e nei casi specificamente previsti dal diritto nazionale o dell'Unione europea. Gli interessati hanno il diritto di ottenere dal Titolare, nei casi previsti, l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt.15 e ss. del Regolamento UE 2016/679). L'apposita istanza è presentata contattando il Responsabile della protezione dei dati ai seguenti indirizzi (e-mail rpd@comune.genova.it, PEC dpo.comge@postecert.it). Gli interessati che ritengono che il trattamento dei dati personali a loro riferiti avvenga in violazione di quanto previsto dalla disciplina in materia di protezione dei dati personali hanno il diritto di proporre reclamo al Garante, come previsto dall'art. 77 del Regolamento (UE) 2016/679, o di adire le opportune sedi giudiziarie ai sensi dell'art. art. 79 del Regolamento citato.

ALLEGATO C

MODULO DI INOLTRO DI SEGNALAZIONE DI UNA POTENZIALE VIOLAZIONE DI DATI PERSONALI

ai sensi dell'art. 33 del Regolamento Generale sulla Protezione dei Dati

Ricevuta, da chiunque ed in qualunque modo, la segnalazione di un potenziale od effettivo incidente sulla sicurezza la medesima è immediatamente **trasmessa al Dirigente competente in ragione del servizio o settore coinvolto o, in caso di incertezza sulla sua individuazione, assenza o indisponibilità**, **al DPO**, esclusivamente utilizzando il presente modulo, senza ritardo e, comunque, entro 4 ore dalla conoscenza dei fatti.

Il modello di segnalazione, debitamente compilato e sottoscritto, dovrà essere consegnato con le modalità più idonee (posta elettronica, consegna a mani, …) a garantirne la pronta e puntuale conoscenza in quanto permetterà di condurre una valutazione iniziale riguardante la notizia dell'incidente occorso e, ciò, al fine di stabilire se si sia effettivamente verificata un'ipotesi di data breach (violazione) e se sia necessaria un'indagine più approfondita dell'accaduto. Ove possibile, devono essere in questo modello integrate le informazioni richieste e non già fornite dal segnalante.

Contestualmente alla comunicazione scritta della segnalazione è necessario l'**avvertimento** del destinatario **anche in modo verbale** allo scopo di assicurarsi che quanto comunicato non passi inosservato.

Dati identificativi del soggetto che INOLTRA			
Cognome			
Nome			
Servizio o settore di appartenenza			
E-mail		Telefono	

Dati identificativi del soggetto DESTINATARIO				
Cognome				
Nome				
Servizio o settore di appartenenza				
E-mail		Telefono		
Modalità di inoltro segnalazione		A mani	data e ora	
		E-mail	data e ora	
		Avviso orale	data e ora	
		Altro (specificare)		

Informazioni sulla SEGNALAZIONE	
Da chi ho ricevuto la segnalazione?	
Quando ho ricevuto la segnalazione?	
Come ho ricevuto la segnalazione?	
(eventuali) ulteriori **informazioni** ricevute oralmente dal segnalante	

(eventuali) **Osservazioni** rispetto al contenuto della segnalazione ricevuta (anche in punto **descrizione** della violazione)	

ATTIVITA' DI RILEVAZIONE INTERNA

Competenza in merito alla segnalazione ricevuta (anche di più uffici)		Servizio o settore che l'ha ricevuta
		Altro/i servizio/i o settore/i (specificare)

Presenza di **Contitolari** del trattamento		NO
		SI (per ciascuno specificare denominazione e tipologia servizio affidato)

Presenza di **Responsabili** del trattamento		NO
		SI (per ciascuno specificare denominazione e tipologia servizio affidato)

descrizione delle **strutture** fisiche e tecnologiche coinvolte	

istruttoria condotta con indicazione delle relative evidenze	

Quale tipo di violazione?	In caso di perdita di **confidenzialità**	
		I dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento
		I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati
		I dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito
		Altro (specificare)
	In caso di perdita di **integrità**	
		I dati sono stati modificati e resi inconsistenti
		I dati sono stati modificati mantenendo la consistenza
		Altro (specificare)
	In caso di perdita di **disponibilità**	
		Mancato accesso a servizi
		Malfunzionamento e difficoltà nell'utilizzo di servizi
		Altro (specificare)

Possibili **cause** della violazione		Azione intenzionale interna
		Azione accidentale interna
		Azione intenzionale esterna
		Azione accidentale esterna
		Sconosciuta
		Altro (specificare)

Volume (anche approssimativo) dei **soggetti** coinvolti		Numero
		Circa numero
		Numero (ancora) non definito (specificare)

Quali soggetti coinvolti?		Il segnalante
		Cittadini
		Dipendenti e titolari di incarichi di collaborazione
		Utenti di servizi pubblici
		Soggetti che ricoprono cariche istituzionali
		Beneficiari o assistiti
		Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
		Minori
		Categorie ancora non determinate
		Altro (specificare)

Sono coinvolti cittadini di altri paesi?	(in caso affermativo, indicare i paesi di riferimento)

Volume (anche approssimativo) dei **dati** coinvolti		Numero
		Circa numero
		Numero (ancora) non definito (specificare)

Quali dati personali sono coinvolti?		Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale, altro...)
		Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
		Dati di accesso e di identificazione (username, password, customer ID, altro...)
		Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro...)
		Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro...)
		Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza o di prevenzione
		Dati di profilazione
		Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro...)
		Dati di localizzazione
		Dati che rivelino l'origine razziale o etnica
		Dati che rivelino opinioni politiche
		Dati che rivelino convinzioni religiose o filosofiche
		Dati che rivelino l'appartenenza sindacale
		Dati relativi alla vita sessuale o all'orientamento sessuale
		Dati relativi alla salute
		Dati genetici
		Dati biometrici
		Categorie ancora non determinate
		Altro, descrivere:

Quali potenziali effetti negativi per le persone coinvolte?		Perdita del controllo dei dati personali
		Limitazione dei diritti
		Discriminazione
		Furto o usurpazione d'identità
		Frodi
		Perdite finanziarie
		Decifratura non autorizzata della pseudonimizzazione
		Pregiudizio alla reputazione
		Perdita di riservatezza dei dati personali protetti da segreto professionale
		Conoscenza da parte di terzi non autorizzati
		Qualsiasi altro danno economico o sociale significativo (specificare)

Stima della **Gravità** della violazione		Trascurabile
		Basso
		Medio
		Alto
	Motivazione:	

AZIONI INTRAPRESE O SUGGERITE

Misure tecniche ed organizzative adottate (o di cui si propone l'adozione) **per porre rimedio** alla violazione e ridurne gli effetti negativi per gli interessati	

Misure tecniche e organizzative adottate (o di cui si propone l'adozione) **per prevenire** simili violazioni future	

ALLEGATI E NOTE

Documentazione che si allega	X	Modulo di segnalazione di una potenziale violazione di dati personali e relativi allegati
Numero dei documenti allegati		

ANNOTAZIONI

Firma

_____, lì _____ _____

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI

Ai sensi dell'articolo 13 del Regolamento (UE) 2016/679 si rappresenta che il Comune di Genova, in qualità di Titolare del trattamento (con sede in Via Garibaldi 9, Palazzo Tursi, 16124 Genova; Email: urp@comune.genova.it; PEC: comunegenova@postemailcertificata.it), tratterà i dati personali conferiti con il presente modulo per le finalità previste dal Regolamento (UE) 2016/679 e dal Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196 e s.m.i.), in particolare per l'esecuzione dei propri compiti di interesse pubblico o comunque connessi all'esercizio dei propri pubblici poteri e, segnatamente, al solo scopo di acquisire ogni necessaria informazione in merito all'evento segnalato, adottare le conseguenti procedure di tutela ed effettuare le comunicazioni previste dalla normativa vigente.
Il conferimento dei dati, fermo restando quanto previsto dall'art. 33, par. 4, del Regolamento (UE) 2016/679, è obbligatorio al fine della ricevibilità della segnalazione, ferma restando la facoltà del Titolare di istruire comunque il procedimento volto all'accertamento della violazione di dati personali. I dati acquisiti nell'ambito della procedura saranno conservati in conformità alle norme sulla conservazione della documentazione amministrativa. I dati saranno trattati esclusivamente dal personale e da collaboratori del Titolare o delle imprese espressamente designate come responsabili del trattamento. Al di fuori di queste ipotesi, i dati non saranno diffusi, né saranno comunicati a terzi, fatti salvi i casi in cui si renda necessario comunicarli al Garante per la protezione dei dati personali, all'Autorità giudiziaria e ad altri soggetti coinvolti nell'attività istruttoria e nei casi specificamente previsti dal diritto nazionale o dell'Unione europea. Gli interessati hanno il diritto di ottenere dal Titolare, nei casi previsti, l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt.15 e ss. del Regolamento UE 2016/679). L'apposita istanza è presentata contattando il Responsabile della protezione dei dati ai seguenti indirizzi (e-mail rpd@comune.genova.it, PEC dpo.comge@postecert.it). Gli interessati che ritengono che il trattamento dei dati personali a loro riferiti avvenga in violazione di quanto previsto dalla disciplina in materia di protezione dei dati personali hanno il diritto di proporre reclamo al Garante, come previsto dall'art. 77 del Regolamento (UE) 2016/679, o di adire le opportune sedi giudiziarie ai sensi dell'art. art. 79 del Regolamento citato.

ALLEGATO D

MODULO DI VALUTAZIONE DEL RISCHIO CONNESSO ALLA VIOLAZIONE DI DATI PERSONALI

ai sensi dell'art. 33 del Regolamento Generale sulla Protezione dei Dati

Ricevuta la documentazione relativa alla segnalazione di una potenziale violazione di dati personali ed effettuata la prescritta analisi tecnica, il **Dirigente competente in ragione del servizio o settore coinvolto** deve stabilire la probabilità o meno che l'evento abbia comportato dei rischi per i diritti e la libertà delle persone e la gravità del rischio così identificato.

Il modello, debitamente compilato e sottoscritto, dovrà essere conservato a documentazione delle valutazioni e decisioni prese.

Dati identificativi del soggetto che effettua l'ANALISI				
Cognome				
Nome				
Servizio o settore di appartenenza				
E-mail			Telefono	
Ricevuta la segnalazione		A mani	data e ora	
		E-mail	data e ora	
		Avviso orale	data e ora	
		Altro (specificare)		

Dati identificativi del soggetto che effettua la VALUTAZIONE (se diverso)				
Cognome				
Nome				
Servizio o settore di appartenenza				
E-mail			Telefono	
Ricevuta la segnalazione		A mani	data e ora	
		E-mail	data e ora	
		Avviso orale	data e ora	
		Altro (specificare)		

ATTIVITA' DI ANALISI

Osservazioni rispetto al contenuto della segnalazione ricevuta (anche in punto **descrizione** della violazione)	

Data della violazione		il	
		Dal	(violazione ancora in corso)
		Dal	Al
		In un tempo non ancora determinato (specificare)	

Natura della violazione		**Riguarda dati personali**		**Non Riguarda dati personali**
		Perdita di confidenzialità		
		Perdita di integrità		
		Perdita di disponibilità		

Competenza in merito alla segnalazione ricevuta (anche di più uffici)		Servizio o settore che l'ha ricevuta
		Altro/i servizio/i o settore/i (specificare)

Presenza di **Contitolari** del trattamento		NO
		SI

Presenza di **Responsabili** del trattamento		NO
		SI

Descrizione dei **sistemi e delle infrastrutture IT coinvolti** nell'incidente, con indicazione della loro ubicazione e	

Misure di sicurezza tecniche e organizzative adottate per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture IT coinvolti (**in essere** al momento della violazione)	

istruttoria condotta con indicazione delle relative evidenze	

Possibili **cause** della violazione		Azione intenzionale interna
		Azione accidentale interna
		Azione intenzionale esterna
		Azione accidentale esterna
		Sconosciuta
		Altro (specificare)

Possibili conseguenze della violazione?	In caso di perdita di **confidenzialità**	
		I dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento
		I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati
		I dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito
		Altro (specificare)
	In caso di perdita di **integrità**	
		I dati sono stati modificati e resi inconsistenti
		I dati sono stati modificati mantenendo la consistenza
		Altro (specificare)
	In caso di perdita di **disponibilità**	
		Mancato accesso a servizi
		Malfunzionamento e difficoltà nell'utilizzo di servizi
		Altro (specificare)

Volume (anche approssimativo) dei **soggetti** coinvolti		Numero
		Circa numero
		Numero (ancora) non definito (specificare)

Quali soggetti coinvolti?		Il segnalante
		Cittadini
		Dipendenti e titolari di incarichi di collaborazione
		Utenti di servizi pubblici
		Soggetti che ricoprono cariche istituzionali
		Beneficiari o assistiti
		Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
		Minori
		Categorie ancora non determinate
		Altro (specificare)

Sono coinvolti cittadini di altri paesi?	(in caso affermativo, indicare i paesi di riferimento)

Volume (anche approssimativo) dei **dati** coinvolti		Numero
		Circa numero
		Numero (ancora) non definito (specificare)

Quali dati personali sono coinvolti?		Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale, altro...)
		Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
		Dati di accesso e di identificazione (username, password, customer ID, altro...)
		Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro...)
		Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro...)
		Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza o di prevenzione
		Dati di profilazione
		Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro...)
		Dati di localizzazione
		Dati che rivelino l'origine razziale o etnica
		Dati che rivelino opinioni politiche
		Dati che rivelino convinzioni religiose o filosofiche
		Dati che rivelino l'appartenenza sindacale
		Dati relativi alla vita sessuale o all'orientamento sessuale
		Dati relativi alla salute
		Dati genetici
		Dati biometrici
		Categorie ancora non determinate
		Altro, descrivere:

Quali potenziali **effetti negativi** per le persone coinvolte?		Perdita del controllo dei dati personali
		Limitazione dei diritti
		Discriminazione
		Furto o usurpazione d'identità
		Frodi
		Perdite finanziarie
		Decifratura non autorizzata della pseudonimizzazione
		Pregiudizio alla reputazione
		Perdita di riservatezza dei dati personali protetti da segreto professionale
		Conoscenza da parte di terzi non autorizzati
		Qualsiasi altro danno economico o sociale significativo (specificare)

Stima della **Gravità** della violazione		Trascurabile (no notifica, né comunicazione)
		Basso (no notifica, né comunicazione)
		Medio (si notifica, no comunicazione)
		Alto e Molto Alto (si notifica e comunicazione)
	Motivazione:	

AZIONI INTRAPRESE O SUGGERITE	
Misure tecniche ed organizzative adottate (o di cui si propone l'adozione) **per porre rimedio** alla violazione e ridurne gli effetti negativi per gli interessati	
Misure tecniche e organizzative adottate (o di cui si propone l'adozione) **per prevenire** simili violazioni future	

ADEMPIMENTI

NOTIFICAZIONE ALL'AUTORITA' DI CONTROLLO

	Effettuata	in data e ora	

	No e non sarà effettuata in quanto si ritiene che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche (specificare):

NOTIFICAZIONE O SEGNALAZIONE AD ALTRI ORGANISMI

Autorità giudiziaria			
	Effettuata	in data e ora	
	Modalità (specificare):		

Forze di polizia			
	Effettuata	in data e ora	
	Modalità (specificare):		

Altri organismi di vigilanza o controllo			
	Effettuata	in data e ora	
	Specificare l'organismo e le modalità di segnalazione		

COMUNICAZIONE AGLI INTERESSATI

	Effettuata	data e ora	
	Modalità e numero destinatari (specificare):		

	Non ancora effettuata
	in quanto tuttora in corso di valutazione
	Sarà effettuata in data da definire
	Sarà effettuata il

	No e non sarà effettuata in quanto:
	a) si ritiene che la violazione dei dati personali **non presenti un rischio elevato** per i diritti e le libertà delle persone fisiche (specificare):
	b) sono state **messe in atto le misure** tecniche ed organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi (specificare):
	c) sono state **successivamente adottate misure** atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati (specificare):
	d) detta comunicazione avrebbe richiesto **sforzi sproporzionati**. Gli interessati sono stati informati con altre modalità, quali:

ALLEGATI E NOTE

Documentazione che si allega	X	Modulo di segnalazione di una potenziale violazione di dati personali e relativi allegati
	X	Modulo di inoltro di una segnalazione di una potenziale violazione di dati personali e relativi allegati
	X	Copia notificazione all'Autorità di controllo (eventuale)
	X	Copia comunicazione agli interessati (eventuale)
Numero dei documenti allegati		

ANNOTAZIONI

Firma

_____, lì _____ _____

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI

Ai sensi dell'articolo 13 del Regolamento (UE) 2016/679 si rappresenta che il Comune di Genova, in qualità di Titolare del trattamento (con sede in Via Garibaldi 9, Palazzo Tursi, 16124 Genova; Email: urp@comune.genova.it; PEC: comunegenova@postemailcertificata.it), tratterà i dati personali conferiti con il presente modulo per le finalità previste dal Regolamento (UE) 2016/679 e dal Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196 e s.m.i.), in particolare per l'esecuzione dei propri compiti di interesse pubblico o comunque connessi all'esercizio dei propri pubblici poteri e, segnatamente, al solo scopo di acquisire ogni necessaria informazione in merito all'evento segnalato, adottare le conseguenti procedure di tutela ed effettuare le comunicazioni previste dalla normativa vigente.
Il conferimento dei dati, fermo restando quanto previsto dall'art. 33, par. 4, del Regolamento (UE) 2016/679, è obbligatorio al fine della ricevibilità della segnalazione, ferma restando la facoltà del Titolare di istruire comunque il procedimento volto all'accertamento della violazione di dati personali. I dati acquisiti nell'ambito della procedura saranno conservati in conformità alle norme sulla conservazione della documentazione amministrativa. I dati saranno trattati esclusivamente dal personale e da collaboratori del Titolare o delle imprese espressamente designate come responsabili del trattamento. Al di fuori di queste ipotesi, i dati non saranno diffusi, né saranno comunicati a terzi, fatti salvi i casi in cui si renda necessario comunicarli al Garante per la protezione dei dati personali, all'Autorità giudiziaria e ad altri soggetti coinvolti nell'attività istruttoria e nei casi specificamente previsti dal diritto nazionale o dell'Unione europea. Gli interessati hanno il diritto di ottenere dal Titolare, nei casi previsti, l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt.15 e ss. del Regolamento UE 2016/679). L'apposita istanza è presentata contattando il Responsabile della protezione dei dati ai seguenti indirizzi (e-mail rpd@comune.genova.it, PEC dpo.comge@postecert.it). Gli interessati che ritengono che il trattamento dei dati personali a loro riferiti avvenga in violazione di quanto previsto dalla disciplina in materia di protezione dei dati personali hanno il diritto di proporre reclamo al Garante, come previsto dall'art. 77 del Regolamento (UE) 2016/679, o di adire le opportune sedi giudiziarie ai sensi dell'art. art. 79 del Regolamento citato.

ALLEGATO E

COMUNICAZIONE ALL'INTERESSATO DELLA VIOLAZIONE DEI DATI PERSONALI
(ai sensi del Regolamento Europeo 2016/679 sulla Protezione dei dati "GDPR")

(il presente modello costituisce una traccia liberamente modificabile e personalizzabile in considerazione delle circostanze di fatto coinvolte. Esso individua tuttavia il contenuto minimo che dev'essere in ogni caso garantito)

Gentile Signore/a,
Secondo quanto prescritto dall'articolo 34 del GDPR, La informiamo essersi verificato un accidentale ed imprevedibile evento che ha comportato una possibile violazione di dati dei Suoi dati personali. Dagli accertamenti, tuttora in corso, è emerso che l'evento si sarebbe verificato in data _____, alle ore_____ e se ne è avuta conoscenza in data_____, alle ore_____.

DESCRIZIONE DELLA NATURA DELLA VIOLAZIONE

DOVE È AVVENUTA LA VIOLAZIONE
(Specificare ove sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

_____
_____
_____
_____

TIPO DI VIOLAZIONE

Per esempio: Lettura (presumibilmente i dati non sono stati copiati); Copia (i dati sono ancora presenti sui sistemi del Titolare); Alterazione (i dati sono presenti sui sistemi del Titolare ma sono stati alterati); Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione); Furto (i dati non sono più sui sistemi del Titolare e li ha l'autore della violazione)

_____
_____
_____
_____

DISPOSITIVO OGGETTO DI VIOLAZIONE

Per esempio: Computer; Rete; Dispositivo mobile; Strumento di backup; Documento cartaceo

_____
_____
_____
_____

TIPO DI DATI OGGETTO DI VIOLAZIONE

Per esempio: Dati anagrafici (nome, cognome, telefono, mail, CF, indirizzo…); Dati di accesso e di identificazione (username, password, ID,…); Dati personali idonei a rivelare l'origine razziale ed etnica; Dati personali idonei a rivelare le convinzioni religiose; Dati personali idonei a rivelare convinzioni filosofiche o di altro genere; Dati personali idonei a rivelare le opinioni politiche; Dati personali idonei a rivelare l'adesione a partiti; Dati personali idonei a rivelare l'adesione a sindacati; Dati personali idonei a rivelare l'adesione ad associazioni od organizzazioni a carattere religioso; Dati personali idonei a rivelare l'adesione ad associazioni od organizzazioni a carattere filosofico; Dati personali idonei a rivelare l'adesione ad associazioni od organizzazioni a carattere sindacale; Dati personali idonei a rivelare lo stato di

salute; Dati personali idonei a rivelare la vita sessuale; Dati giudiziari; Dati genetici; Dati biometrici; Copia per immagine su supporto informatico di documenti analogici; Ancora sconosciuto.

_____
_____
_____
_____

Tale violazione è suscettibile di presentare un rischio elevato per Suoi diritti e le libertà.

DESCRIZIONE DELLE CONSEGUENZE DELLA VIOLAZIONE

_____
_____
_____
_____

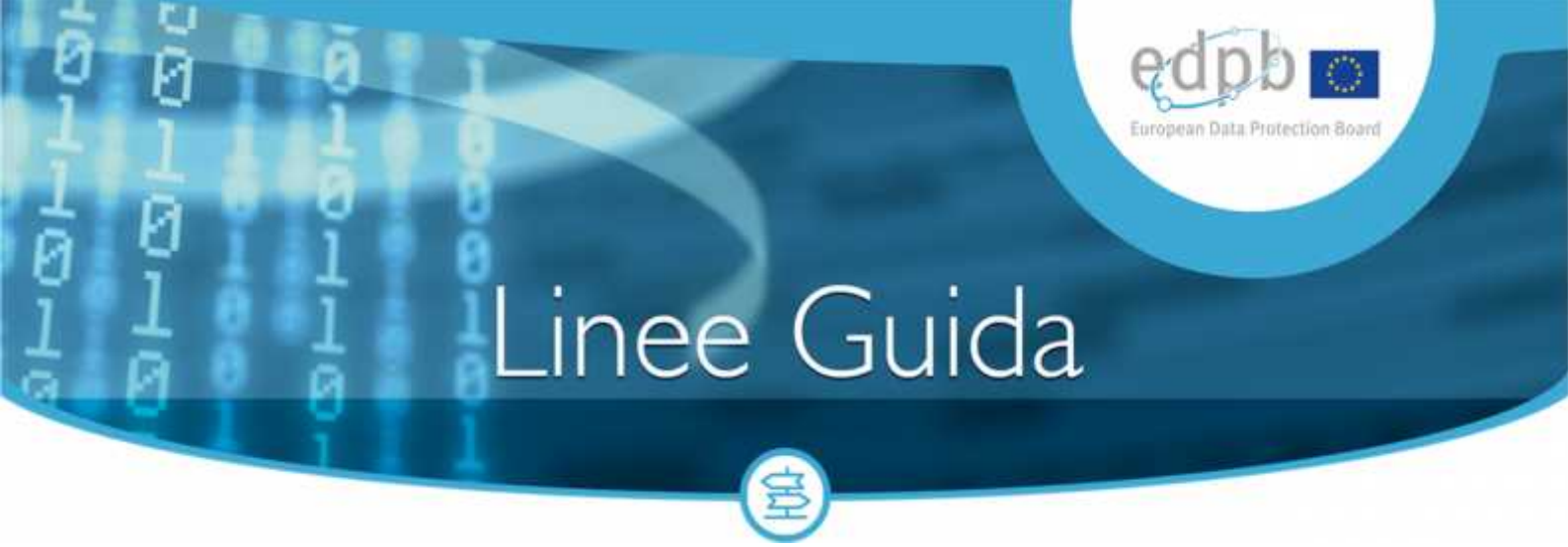
DESCRIZIONE DELLE MISURE TECNOLOGICHE E ORGANIZZATIVE ASSUNTE

_____
_____
_____
_____

Per poter ottenere maggiori **informazioni** relativamente alla violazione in oggetto, può contattare lo scrivente Ufficio, nonché il Responsabile della Protezione dei Dati, i cui dati di contatto sono i seguenti: e-mail rpd@comune.genova.it, PEC dpo.comge@postecert.it

Luogo e data

Firma del ____



Linee-guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali

Adottate il 14 dicembre 2021

Cronologia delle versioni

Versione 2.0	14 12 2021	Adozione delle linee guida dopo la consultazione pubblica
Versione 1.0	14 01 2021	Adozione delle linee guida per consultazione pubblica

Indice

IL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

Visto l'articolo 70, paragrafo 1, lettera e), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (in appresso "GDPR"),

Visto l'accordo SEE, in particolare l'allegato XI e il protocollo 37 dello stesso, modificati dalla Decisione del 6 luglio 20181,

Visti l'articolo 12 e l'articolo 22 del suo regolamento,

Vista la comunicazione della Commissione al Parlamento europeo e al Consiglio dal titolo "La protezione dei dati quale pilastro della responsabilizzazione dei cittadini e dell'approccio dell'UE alla transizione digitale — due anni di applicazione del regolamento generale sulla protezione dei dati"2,

HA ADOTTATO LE SEGUENTI LINEE-GUIDA

1 INTRODUZIONE

1. Il GDPR introduce, in alcuni casi, l'obbligo di notificare una violazione dei dati personali all'autorità nazionale di controllo competente e di comunicare la violazione alle persone i cui dati personali sono stati interessati dalla violazione (articoli 33 e 34).

2. Nell'ottobre 2017 il gruppo di lavoro "Articolo 29" ha già elaborato linee-guida generali sulla notifica delle violazioni dei dati, analizzando le sezioni pertinenti del regolamento generale sulla protezione dei dati (Linee-guida sulla notifica delle violazioni dei dati personali a norma del regolamento (UE) 2016/679, WP 250) (di seguito "Linee-guida WP250"3). Tuttavia, a causa della loro natura e della tempistica prevista, tali linee-guida non hanno affrontato tutte le questioni pratiche in modo sufficientemente dettagliato. Pertanto, è emersa la necessità di una guida pratica e basata su casi concreti, che utilizzi le esperienze acquisite dalle autorità di controllo da quando GDPR è divenuto pienamente applicabile.

3. Il presente documento è inteso a integrare gli orientamenti WP 250 e rispecchia le esperienze comuni delle autorità di controllo dello Spazio Economico Europeo (SEE) successivamente alla piena applicabilità del regolamento generale sulla protezione dei dati. Il suo obiettivo è aiutare i titolari del trattamento a decidere come gestire le violazioni dei dati e quali fattori prendere in considerazione durante la valutazione del rischio.

4. Qualsiasi tentativo di porre rimedio a una violazione presuppone che il titolare e il responsabile del trattamento siano in grado di riconoscerla. L'articolo 4, paragrafo 12, del regolamento generale sulla protezione dei dati definisce una "violazione dei dati personali" come "una violazione della sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o altrimenti trattati".

5. Nel suo parere 03/2014 sulla notifica delle violazioni4 e nelle Linee-guida WP 250, il WP29 ha spiegato che le

1 I riferimenti agli "Stati membri" nel presente documento sono da intendersi come riferimenti agli "Stati membri del SEE".
2 COM (2020) 264 final del 24 giugno 2020.
3 WP29 WP250 rev.1, 6 febbraio 2018, Linee guida sulla notifica delle violazioni dei dati personali a norma del regolamento 2016/679 — approvate dal comitato europeo per la protezione dei dati, https://ec.europa.eu/newsroom/article29/item-detail.cfm7item id = 612052.
4 WP29 WP213, 25 marzo 2014, Parere 03/2014 sulla notifica di una violazione dei dati personali, pag. 5,

violazioni possono essere classificate in base ai seguenti tre noti principi di sicurezza delle informazioni:

- "Violazione della riservatezza" — in caso di divulgazione non autorizzata o accidentale di dati personali o di accesso non autorizzato o accidentale agli stessi.
- "Violazione dell'integrità" — in caso di modifica non autorizzata o accidentale di dati personali.
- "Violazione della disponibilità" — in caso di perdita accidentale o non autorizzata dell'accesso ai dati personali o di loro distruzione accidentale o non autorizzata.5

6. Una violazione può avere potenzialmente numerosi effetti negativi significativi sulle persone fisiche, che possono causare danni fisici, materiali o immateriali. Il GDPR spiega che ciò può includere la perdita del controllo da parte degli interessati sui loro dati personali, la limitazione dei loro diritti, la discriminazione, il furto o l'usurpazione d'identità, perdite finanziarie, la decifratura non autorizzata della pseudonimizzazione, il pregiudizio alla reputazione e la perdita di riservatezza dei dati personali protetti da segreto professionale, nonché qualsiasi altro danno economico o sociale significativo per le persone fisiche interessate. Uno degli obblighi più importanti del titolare del trattamento è valutare tali rischi per i diritti e le libertà degli interessati e attuare misure tecniche e organizzative adeguate per affrontarli.

7. Di conseguenza, il GDPR impone al titolare del trattamento di:

- documentare le violazioni dei dati personali, comprese le circostanze della violazione dei dati personali, le sue conseguenze e le azioni correttive adottate6;
- notificare la violazione dei dati personali all'autorità di controllo, a meno che sia improbabile che la violazione dei dati presenti un rischio per i diritti e le libertà delle persone fisiche7;
- comunicare la violazione dei dati personali all'interessato quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche8.

8. Le violazioni dei dati sono di per sé problematiche, ma possono anche essere sintomi di un regime di sicurezza dei dati vulnerabile e forse obsoleto, oppure segnalare carenze del sistema da affrontare. In linea generale, è sempre meglio prevenire le violazioni dei dati preparandosi in anticipo, dal momento che diverse conseguenze sono per loro natura irreversibili. Prima che un titolare del trattamento possa valutare *appieno* il rischio derivante da una violazione causata da una qualche forma di attacco, occorre individuare la causa alla radice del problema, al fine di stabilire se le vulnerabilità che hanno determinato l'incidente siano ancora presenti e siano pertanto ancora sfruttabili. In molti casi il titolare del trattamento è in grado di individuare che l'incidente può comportare un rischio e deve pertanto essere notificato. In altri casi non si dovrà rinviare la notifica fino a quando il rischio e l'impatto della violazione non siano stati pienamente valutati, poiché la valutazione completa del rischio può avvenire parallelamente alla notifica e le informazioni così ottenute possono essere fornite all'autorità di controllo in fasi successive senza ulteriore e ingiustificato ritardo9.

9. La violazione dovrebbe essere notificata quando il titolare del trattamento ritiene che possa comportare un rischio per i diritti e le libertà dell'interessato. I titolari dovrebbero effettuare tale valutazione nel momento in cui vengono a conoscenza della violazione. Un titolare non dovrebbe attendere gli esiti di un'analisi forense dettagliata e l'applicazione di azioni di mitigazione del rischio (precoci) prima di valutare se la violazione dei dati possa comportare un rischio e debba pertanto essere notificata.

10. Se un titolare del trattamento valuta autonomamente che un rischio sia improbabile, ma tale rischio di fatto

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index en.htm # maincontentSec4.

5 Cfr. le Linee-guida WP 250, pag. 7. — Occorre tener conto del fatto che una violazione dei dati può riguardare una o più categorie simultaneamente.

6 Articolo 33, paragrafo 5, del GDPR.

7 Articolo 33, paragrafo 1, del GDPR.

8 Articolo 34, paragrafo 1, del GDPR.

9 Articolo 33, paragrafo 4, del GDPR.

si concretizza, l'autorità di controllo competente può avvalersi dei suoi poteri correttivi e può decidere di comminare sanzioni.

11. Ogni titolare e responsabile del trattamento dovrebbe disporre di piani e procedure per la gestione di eventuali violazioni dei dati. Si dovrebbero prevedere linee gerarchiche chiare e specifiche figure responsabili di determinati aspetti del processo di recupero.

12. Anche la formazione e la sensibilizzazione in materia di protezione dei dati per il personale del titolare e del responsabile del trattamento sono essenziali, concentrandosi sulla gestione delle violazioni dei dati personali (identificazione di un incidente di violazione dei dati personali e ulteriori azioni da intraprendere, ecc.). Tale formazione dovrebbe essere ripetuta periodicamente, a seconda del tipo di trattamento e delle dimensioni della struttura del titolare, esaminando le più recenti tendenze e segnalazioni derivanti da attacchi informatici o altri incidenti di sicurezza.

13. Il principio di responsabilizzazione e il concetto di protezione dei dati fin dalla progettazione potrebbero contemplare un'analisi intesa a confluire in una sorta di "Manuale per la gestione delle violazioni dei dati" messo a punto dal titolare e dal responsabile del trattamento, in cui definire gli elementi fattuali in rapporto a ogni sfaccettatura del trattamento in ciascuna delle fasi principali dell'operazione. Tale manuale, ove redatto preventivamente, fornirebbe una fonte di informazioni molto più rapida per consentire ai titolari e ai responsabili del trattamento di mitigare i rischi e di adempiere ai rispettivi obblighi senza indebito ritardo. Così facendo, in caso di violazione dei dati personali, il personale saprà cosa fare e l'incidente potrà essere gestito più rapidamente di quanto avverrebbe in assenza di misure di mitigazione o dei predetti piani.

14. Sebbene i casi presentati di seguito siano fittizi, essi si basano su casi tipici tratti dall'esperienza collettiva delle autorità di controllo in materia di notifiche di violazioni dei dati. Le analisi proposte si riferiscono esplicitamente ai casi in esame, ma con l'obiettivo di fornire assistenza ai titolari del trattamento per la valutazione delle violazioni dei dati che li riguardino. Qualsiasi modifica delle circostanze riferite alle fattispecie descritte di seguito può comportare livelli di rischio diversi o più significativi, e quindi rendere necessarie misure diverse o supplementari. In queste linee-guida, i casi sono presentati in base a determinate categorie di violazioni (ad esempio "attacchi ransomware"). Alcune misure di mitigazione sono necessarie in tutte le fattispecie appartenenti a una determinata categoria di violazioni. Tali misure non sono necessariamente ripetute in ciascuna analisi riferita a un caso appartenente alla stessa categoria di violazioni. Per i casi appartenenti alla stessa categoria sono indicate solo le differenze. Pertanto, il lettore dovrebbe tenere conto dell'intera casistica riferita alla pertinente categoria di violazione al fine di individuare e distinguere tutte le misure corrette da adottare.

15. La documentazione interna di una violazione è un obbligo indipendente dai rischi connessi alla violazione stessa e deve essere predisposta in ogni singolo caso. I casi presentati di seguito cercano di chiarire se notificare o meno la violazione all'autorità di controllo e comunicarla agli interessati coinvolti.

2 RANSOMWARE

16. Una causa frequente di notifica di violazione dei dati è un attacco ransomware subito dal titolare del trattamento. In questi casi un codice malevolo cifra i dati personali e successivamente l'autore dell'attacco chiede al titolare del trattamento un riscatto in cambio della chiave di decifratura. Questo tipo di attacco può di norma essere classificato come una violazione della disponibilità, ma spesso potrebbe comportare anche una violazione della riservatezza.

2.1 Caso n. 01: Ransomware in presenza di backup adeguato e senza esfiltrazione

I sistemi informatici di una piccola impresa manifatturiera sono stati esposti a un attacco ransomware e i dati memorizzati in tali sistemi sono stati cifrati. Il titolare ha utilizzato la cifratura dei dati memorizzati (at rest), per cui tutti i dati ai quali ha avuto accesso il ransomware erano conservati in forma cifrata utilizzando

un algoritmo di cifratura conforme allo stato dell'arte. La chiave di decifratura non è stata compromessa nell'attacco, ossia l'autore dell'attacco non ha potuto accedervi né utilizzarla indirettamente. Di conseguenza, l'autore dell'attacco ha avuto accesso solo a dati personali cifrati. In particolare, né il sistema di posta elettronica della società né i sistemi clienti utilizzati per accedervi sarebbero stati interessati. L'impresa si avvale delle competenze di una società esterna di cybersecurity per indagare sull'incidente. Sono disponibili le registrazioni (log) di tutti i flussi dati in uscita dall'impresa (compresa la posta elettronica in uscita). Dopo aver analizzato i log e i dati raccolti dai sistemi di rilevazione utilizzati dall'impresa, un'indagine interna supportata dalla società esterna di cybersecurity ha stabilito *con certezza* che l'autore del reato si è limitato a cifrare i dati, senza esfiltrarli. I log non mostrano alcun flusso di dati verso l'esterno nell'arco di tempo dell'attacco. I dati personali interessati dalla violazione riguardano i clienti e i dipendenti dell'impresa, per un totale di poche decine di persone. Un backup era prontamente disponibile e i dati sono stati ripristinati poche ore dopo l'attacco. La violazione non ha avuto alcuna conseguenza sull'operatività del titolare del trattamento. Non vi sono stati ritardi nei pagamenti dei dipendenti o nella gestione delle richieste dei clienti.

17. In questo caso, rispetto alla definizione di "violazione dei dati personali" si sono concretizzati i seguenti elementi: una violazione della sicurezza ha comportato una modifica illecita e l'accesso non autorizzato ai dati personali conservati.

2.1.1 Caso n. 01 — Misure in essere e valutazione del rischio

18. Come per tutti i rischi posti da attori esterni, la probabilità che un attacco ransomware abbia successo può essere drasticamente ridotta rafforzando la sicurezza dei dati mediante controllo del contesto. La maggior parte di queste violazioni può essere evitata garantendo l'adozione di adeguate misure di sicurezza organizzative, fisiche e tecnologiche. Esempi di tali misure sono la corretta gestione delle patch e l'uso di un adeguato sistema di rilevamento di malware. Disporre di un backup adeguato e separato contribuirà ad attenuare le conseguenze di un eventuale attacco riuscito. Inoltre, un programma di istruzione, formazione e sensibilizzazione dei dipendenti in materia di sicurezza (SETA) contribuirà a prevenire e riconoscere questo tipo di attacco. (Un elenco di misure consigliate è riportato nella sezione 2.5.) Tra tali misure, una delle più importanti è una corretta gestione delle patch che assicuri che i sistemi siano aggiornati e che tutte le vulnerabilità note dei sistemi installati siano state corrette poiché la maggior parte degli attacchi ransomware sfrutta proprio vulnerabilità ben note.

19. Nel valutare i rischi, il titolare del trattamento dovrebbe indagare sulla violazione e individuare il tipo di codice malevolo per comprendere le possibili conseguenze dell'attacco. Tra i rischi da considerare figura il rischio che i dati siano stati esfiltrati senza lasciare traccia nei log dei sistemi.

20. In questo esempio, l'attaccante ha avuto accesso ai dati personali ed è stata compromessa la riservatezza del testo cifrato contenente dati personali in forma cifrata. Tuttavia, i dati che potrebbero essere stati esfiltrati non possono essere letti o utilizzati dall'autore dell'attacco, almeno per il momento. La tecnica di cifratura utilizzata dal titolare è conforme allo stato dell'arte. La chiave di decifratura non è stata compromessa e presumibilmente non può essere determinata con altri mezzi. Di conseguenza, i rischi in termini di riservatezza per i diritti e le libertà delle persone fisiche sono ridotti al minimo, salvi i progressi delle tecniche crittografiche che in futuro potrebbero rendere i dati cifrati intelligibili.

21. Il titolare del trattamento dovrebbe considerare il rischio per le persone fisiche dovuto alla violazione10. In questo caso, sembra che i rischi per i diritti e le libertà degli interessati derivino dalla mancanza di disponibilità

10 Per orientamenti sui trattamenti *"che possono comportare un rischio elevato"*, si veda il gruppo di lavoro A29 "Guidelines on Data Protection Impact Assessment (DPIA) and determining if processing is likely to be a high risk" (Linee guida sulla valutazione d'impatto sulla protezione dei dati e sulla determinazione della probabilità che il trattamento possa comportare un rischio elevato) ai fini del regolamento 2016/679, WP248 rev. 01, approvato dall'EDPB, https://ec.europa.eu/newsroom/article29/items/611236, pag. 9.

dei dati personali e che la riservatezza dei dati personali non sia compromessa11. In questo esempio, gli effetti negativi della violazione sono stati attenuati in tempi contenuti dopo il verificarsi della violazione stessa. Disporre di un adeguato regime di backup12 riduce gli effetti negativi della violazione e in questo caso il titolare del trattamento è stato in grado di avvalersene in modo efficace.

22. Per quanto riguarda la gravità delle conseguenze per gli interessati, è stato possibile individuare solo conseguenze minori, poiché i dati sono stati ripristinati in poche ore e la violazione non ha avuto conseguenze sull'operatività del titolare del trattamento né effetti significativi sugli interessati (ad esempio pagamenti ai dipendenti o gestione delle richieste dei clienti).

2.1.2 Caso n. 01 — Misure di mitigazione e obblighi

23. In assenza di un backup, il titolare del trattamento può adottare poche misure per porre rimedio alla perdita di dati personali e i dati devono essere nuovamente raccolti. In questo caso particolare, tuttavia, gli effetti dell'attacco potrebbero essere contenuti efficacemente "ripulendo" tutti i sistemi compromessi dal codice malevolo, correggendo le vulnerabilità e ripristinando i dati interessati entro breve tempo dall'attacco. In assenza di backup, i dati sarebbero andati persi e la gravità può aumentare di pari passo con i rischi o gli impatti per le persone.

24. La tempestività di un ripristino efficace dei dati utilizzando un backup prontamente disponibile è una variabile fondamentale nell'analisi della violazione. La definizione di una tempistica adeguata per il ripristino di dati compromessi dipende dalle circostanze specifiche della violazione. Il regolamento generale sulla protezione dei dati stabilisce che una violazione dei dati personali deve essere notificata senza ingiustificato ritardo e, ove possibile, entro 72 ore. Si potrebbe pertanto stabilire che in nessun caso è consigliabile superare il termine di 72 ore, ma quando si tratta di casi caratterizzati da un rischio elevato, anche il rispetto di tale termine può risultare insoddisfacente.

25. In questo caso, grazie a procedure dettagliate per la valutazione d'impatto e la risposta agli incidenti, il titolare del trattamento ha stabilito che era improbabile che la violazione comportasse un rischio per i diritti e le libertà delle persone fisiche; pertanto non è necessaria alcuna comunicazione agli interessati, né la violazione richiede una notifica all'autorità di controllo. Tuttavia, come tutte le violazioni dei dati, è necessario conservarne la documentazione conformemente all'articolo 33, paragrafo 5. La struttura del titolare potrebbe anche necessitare di (o essere successivamente tenuta a effettuare, su disposizione dell'autorità di controllo) aggiornamenti e correzioni delle misure e procedure organizzative e tecniche messe in atto per la gestione della sicurezza dei dati personali e la mitigazione dei rischi. Nell'ambito di tale aggiornamento e revisione, si dovrebbe indagare approfonditamente sulla violazione individuandone le cause e definendo i metodi utilizzati dall'autore dell'attacco al fine di prevenire eventi analoghi in futuro.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati

11 Dal punto di vista tecnico, la cifratura dei dati comporta l' "accesso" ai dati originali e, nel caso di ransomware, la cancellazione dei dati originali — il codice ransomware deve accedere ai dati per cifrarli e rimuovere i dati originali. L'autore di un attacco può effettuare una copia dell'originale prima dell'eliminazione, ma i dati personali non verranno sempre estratti.. Con l'avanzare delle indagini svolte dal titolare, potrebbero emergere nuove informazioni tali da modificare la suddetta valutazione. L'accesso che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata dei dati personali o un rischio per la sicurezza dell'interessato, anche in assenza di interpretazione dei dati, può essere tanto grave quanto l'accesso seguito da interpretazione dei dati personali.

12 Le procedure di backup dovrebbero essere strutturate, coerenti e ripetibili. Esempi di procedure di backup sono il metodo 3-2-1 e il metodo grandfather-father-son. Qualsiasi metodo dovrebbe sempre essere testato per verificarne l'efficacia in termini di copertura nonché in sede di ripristino dei dati. I test dovrebbero inoltre essere ripetuti a intervalli regolari, in particolare quando intervengono cambiamenti nel trattamento o nelle sue circostanze, al fine di garantire l'integrità del sistema.

✓	X	X

2.2 Caso n. 02: Ransomware senza un adeguato backup

Uno dei computer utilizzati da un'azienda agricola è stato esposto a un attacco ransomware e i dati sono stati cifrati dall'attaccante. L'impresa si avvale delle competenze di una società esterna di cybersecurity per monitorare la propria rete. Sono disponibili log che tracciano tutti i flussi di dati in uscita dall'impresa (comprese le e-mail in uscita). Dopo aver analizzato i log e i dati raccolti dagli altri sistemi di rilevamento, l'indagine interna condotta con l'ausilio dell'impresa di cybersecurity ha stabilito che l'autore dell'attacco ha soltanto cifrato i dati, senza esfiltrarli. I log non mostrano alcun flusso di dati verso l'esterno nell'arco di tempo dell'attacco. I dati personali interessati dalla violazione riguardano i dipendenti e i clienti dell'impresa, per un totale di poche decine di persone. Non sono state interessate categorie particolari di dati. Non era disponibile alcun backup in formato elettronico. La maggior parte dei dati è stata ripristinata da backup cartacei. Il ripristino dei dati ha richiesto 5 giorni lavorativi e ha comportato lievi ritardi nella consegna degli ordini ai clienti.

2.2.1 Caso n. 02 — Misure in essere e valutazione del rischio

26. Il titolare del trattamento avrebbe dovuto adottare le stesse misure di cui alla parte 2.1 e alla sezione 2.9. La principale differenza rispetto al caso precedente è la mancanza di un backup in formato elettronico e la mancanza di cifratura dei dati memorizzati (at rest). Ciò comporta differenze critiche nelle fasi successive.

27. Nel valutare i rischi, il titolare del trattamento dovrebbe indagare sul metodo di infiltrazione e individuare la tipologia di codice malevolo per comprendere le possibili conseguenze dell'attacco. In questo esempio il ransomware cifrava i dati personali senza esfiltrarli. Di conseguenza, i rischi per i diritti e le libertà degli interessati sembrano derivare dalla mancanza di disponibilità dei dati personali e la riservatezza dei dati personali non risulterebbe compromessa. Per determinare il rischio è essenziale un esame approfondito dei log dei firewall e delle relative implicazioni. Su richiesta, il titolare del trattamento dovrebbe presentare le risultanze documentate di tali indagini.

28. Il titolare del trattamento deve tenere presente che, se l'attacco è più sofisticato, il malware è in grado di modificare i file di log e rimuovere le tracce. Pertanto, poiché i log non sono trasmessi o replicati a un server centrale, anche dopo un'indagine approfondita che ha accertato che i dati personali non sono stati esfiltrati dall'attaccante, il titolare del trattamento non può affermare che l'assenza di log dimostri l'assenza di esfiltrazione; ne consegue l'impossibilità di escludere in via assoluta la probabilità di una violazione della riservatezza.

29. Il titolare del trattamento dovrebbe valutare i rischi di questa violazione13 se l'attaccante ha avuto accesso ai dati. Nel corso della valutazione del rischio, il titolare dovrebbe tenere conto anche della natura, della sensibilità, del volume e del contesto dei dati personali interessati dalla violazione. In questo caso non sono coinvolte categorie particolari di dati personali e la quantità di dati violati e il numero di interessati colpiti sono ridotti.

30. La raccolta di informazioni esatte sull'accesso non autorizzato è fondamentale per determinare il livello di rischio e prevenire un nuovo attacco o la prosecuzione di un attacco in corso. Se i dati fossero stati copiati dalla banca dati, ciò sarebbe stato ovviamente un fattore di incremento del rischio. In caso di incertezza circa le specificità dell'accesso illegittimo, si dovrebbe prendere in considerazione lo scenario peggiore e il rischio dovrebbe essere valutato in termini conseguenti.

31. L'assenza di un backup può essere considerata un fattore di incremento del rischio a seconda della gravità delle conseguenze derivanti per gli interessati dall'indisponibilità dei dati.

13 Per indicazioni sulle operazioni di trattamento "che possono comportare un rischio elevato ", cfr. la nota 10.

2.2.2 Caso n. 02 — Misure di mitigazione e obblighi

32. In assenza di un backup, sono poche le misure che il titolare del trattamento può adottare per porre rimedio alla perdita di dati personali e i dati devono essere nuovamente raccolti, a meno che sia disponibile un'altra fonte (ad esempio, e-mail di conferma degli ordini). Senza un backup, i dati possono andare persi e la gravità dipenderà dall'impatto per le persone.

33. Il ripristino dei dati non dovrebbe rivelarsi eccessivamente problematico14 se i dati sono ancora disponibili su supporto cartaceo; tuttavia, data la mancanza di un backup in formato elettronico , si ritiene necessaria una notifica all'autorità di controllo, in quanto il ripristino dei dati ha richiesto un certo tempo e potrebbe causare ritardi nella consegna degli ordini ai clienti mentre potrebbe risultare impossibile recuperare una notevole quantità di metadati (ad esempio log, marcatura temporale).

34. La comunicazione agli interessati in merito alla violazione può dipendere anche dal periodo di indisponibilità dei dati personali e dalle difficoltà che ne potrebbero derivare per l'operatività del titolare del trattamento (ad esempio ritardi nel trasferimento dei pagamenti ai dipendenti). Poiché tali ritardi nei pagamenti e nelle consegne possono comportare perdite finanziarie per le persone i cui dati sono stati compromessi, si potrebbe anche sostenere che la violazione comporti un rischio elevato. Inoltre, potrebbe risultare impossibile evitare di informare gli interessati se il loro contributo è necessario per ripristinare i dati cifrati.

35. Questo caso è un esempio di attacco ransomware con rischi per i diritti e le libertà degli interessati, senza che si raggiunga un rischio elevato. La violazione dovrebbe essere documentata conformemente all'articolo 33, paragrafo 5, e notificata all'autorità di controllo a norma dell'articolo 33, paragrafo 1. La struttura del titolare può anche necessitare di (o ricevere disposizioni dall'autorità di controllo per) aggiornare e correggere le misure e procedure organizzative e tecniche di gestione della sicurezza dei dati personali e di mitigazione dei rischi.

Azioni necessarie sulla base dei rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	✓	X

2.3 Caso n. 03: Attacco ransomware nei confronti di un ospedale con backup e senza esfiltrazione

Il sistema informativo di un ospedale/centro sanitario è stato esposto a un attacco ransomware e una parte significativa dei dati è stata cifrata dall'attaccante. L'azienda sanitaria si avvale delle competenze di una società esterna di cybersecurity per monitorare la propria rete. Sono disponibili log che tracciano tutti i flussi di dati in uscita dall'azienda (comprese le e-mail in uscita). Dopo aver analizzato i log e i dati raccolti dagli altri sistemi di rilevamento, l'indagine interna svolta con l'ausilio della società di cybersecurity ha stabilito che l'autore dell'attacco ha soltanto cifrato i dati senza esfiltrarli. I log non mostrano alcun flusso di dati verso l'esterno nell'arco di tempo dell'attacco. I dati personali interessati dalla violazione riguardano i dipendenti e i pazienti, complessivamente varie migliaia di persone. I backup erano disponibili in formato elettronico. La maggior parte dei dati è stata ripristinata, ma questa operazione ha richiesto 2 giorni lavorativi, causando notevoli ritardi nelle cure rese ai pazienti con annullamento o rinvio di interventi chirurgici e un abbassamento del livello di servizio a causa dell'indisponibilità dei sistemi.

2.3.1 Caso n. 03 — Misure in essere e valutazione del rischio

36. Il titolare del trattamento avrebbe dovuto adottare le stesse misure di cui alla parte 2.1 e alla sezione 2.5. La principale differenza rispetto al caso precedente è l'elevata gravità delle conseguenze per un numero

14 Ciò dipenderà dalla complessità e dalla struttura dei dati personali. Negli scenari più complessi, il ripristino dell'integrità dei dati, la coerenza con i metadati, la garanzia della correttezza delle relazioni all'interno delle strutture di dati e il controllo dell'accuratezza dei dati possono richiedere risorse e sforzi significativi.

sostanziale di interessati15.

37. La quantità di dati violati e il numero di interessati colpiti dalla violazione sono elevati, in quanto gli ospedali generalmente trattano grandi quantità di dati. L'indisponibilità dei dati ha un forte impatto su una parte sostanziale degli interessati. Esiste inoltre un rischio residuo di elevata gravità per la riservatezza dei dati dei pazienti.

38. La tipologia della violazione, la natura, la sensibilità e il volume dei dati personali interessati dalla violazione sono importanti. Sebbene esistesse un backup per i dati e questi abbiano potuto essere ripristinati in pochi giorni, sussiste un rischio elevato a causa della gravità delle conseguenze per gli interessati derivanti dall'indisponibilità dei dati al momento dell'attacco e nei giorni successivi.

2.3.2 Caso n. 03 — Misure di mitigazione e obblighi

39. Si ritiene necessaria una notifica all'autorità di controllo, in quanto si tratta di categorie particolari di dati personali e il ripristino dei dati potrebbe richiedere molto tempo, con notevoli ritardi nelle cure dei pazienti. Comunicare la violazione agli interessati è necessario a causa dell'impatto sui pazienti, anche dopo il ripristino dei dati cifrati. Anche se sono stati criptati dati relativi a tutti i pazienti trattati in ospedale negli ultimi anni, la violazione ha interessato soltanto i dati relativi ai pazienti che dovevano essere sottoposti a terapie in ospedale durante il periodo di indisponibilità del sistema informatico. Il titolare del trattamento dovrebbe comunicare la violazione dei dati direttamente a tali pazienti. L'eccezione di cui all'articolo 34, paragrafo 3, lettera c), può non rendere necessaria la comunicazione diretta agli altri pazienti, alcuni dei quali possono non essere stati ricoverati in ospedale da più di venti anni. In tal caso, si procede invece a una comunicazione pubblica16 o a una misura analoga, tramite la quale gli interessati sono informati con pari efficacia. In tal caso, l'ospedale dovrebbe rendere pubblico l'attacco ransomware e i suoi effetti.

40. Questo caso serve da esempio di un attacco ransomware con un rischio elevato per i diritti e le libertà degli interessati. La violazione dovrebbe essere documentata conformemente all'articolo 33, paragrafo 5, notificata all'autorità di controllo in conformità dell'articolo 33, paragrafo 1, e comunicata agli interessati in conformità dell'articolo 34, paragrafo 1. L'azienda sanitaria deve inoltre aggiornare e correggere le misure e procedure organizzative e tecniche di gestione della sicurezza dei dati personali e di mitigazione dei rischi.

Azioni necessarie sulla base dei rischi individuati		
Documentazione interna	Notifica all' autorità di controllo	Comunicazione agli interessati
✓	✓	✓

2.4 Caso n. 04: Attacco ransomware senza backup e con esfiltrazione

Il server di una società di trasporto pubblico è stato esposto a un attacco ransomware e i dati sono stati cifrati dall'autore dell'attacco. Secondo i risultati dell'indagine interna, l'autore dell'attacco non solo ha cifrato i dati, ma li ha anche esfiltrati. La tipologia dei dati violati consiste nei dati personali di clienti e dipendenti e delle diverse migliaia di persone che utilizzano i servizi della società (ad esempio, per l'acquisto di biglietti online). Oltre ai dati identificativi di base, sono coinvolti nella violazione i numeri dei documenti d'identità e dati finanziari come i dati della carta di credito. Era disponibile un backup, ma anch'esso è stato

15 Per indicazioni sulle operazioni di trattamento "che possono comportare un rischio elevato ", cfr. la nota 10.

16 Il considerando 86 del regolamento generale sulla protezione dei dati spiega che *"Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta cooperazione con l'autorità di controllo, nel rispetto degli orientamenti forniti da quest'ultima o da altre autorità competenti, quali le autorità di contrasto. Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione con gli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione".*

criptato dall'aggressore.

2.4.1 Caso n. 04 — Misure in essere e valutazione del rischio

41. Il titolare del trattamento avrebbe dovuto adottare le stesse misure di cui alla parte 2.1 e alla sezione 2.5. Sebbene disponibile, anche il backup è stato compromesso dall'attacco. Questa circostanza di per sé solleva interrogativi sulla qualità delle misure di sicurezza informatica in essere e dovrebbe essere oggetto di approfondimenti ulteriori durante l'indagine poiché, in un regime di backup ben progettato, devono essere conservati in modo sicuro più backup senza consentire l'accesso dal sistema principale, altrimenti potrebbero essere compromessi nello stesso attacco. Inoltre, gli attacchi ransomware possono rimanere occulti per giorni cifrando lentamente dati utilizzati di rado. Ciò può rendere inutile l'esecuzione di più backup, per cui dovrebbero essere eseguiti anche backup periodici e poi essere isolati. In tal modo si aumenterebbe la probabilità di recupero seppur con una perdita maggiore di dati.

42. La violazione riguarda non solo la disponibilità dei dati, ma anche la riservatezza, in quanto l'autore dell'attacco può aver modificato e/o copiato i dati dal server. Pertanto, il tipo di violazione comporta un rischio elevato17.

43. La natura, la sensibilità e il volume dei dati personali aumentano ulteriormente i rischi, poiché il numero di persone interessate è elevato, così come la quantità complessiva di dati personali compromessi. Al di là dei dati identificativi di base, sono coinvolti anche documenti di identità e dati finanziari come i dati della carta di credito. Una violazione dei dati relativa a queste categorie di informazioni presenta di per sé un rischio elevato e i dati oggetto di compromissione, se utilizzati congiuntamente, potrebbero servire, tra l'altro, a realizzare furti di identità o frodi.

44. A causa di errori dei controlli logici o organizzativi del server, i backup sono stati compromessi dal ransomware e ciò ha impedito il ripristino dei dati e aumentato il rischio.

45. Questa violazione dei dati presenta un rischio elevato per i diritti e le libertà delle persone, in quanto potrebbe comportare sia un danno materiale (ad esempio una perdita finanziaria dovuta alla compromissione dei dati della carta di credito) sia immateriale (ad esempio furto o usurpazione d'identità in quanto i dati della carta d'identità sono stati compromessi).

2.4.2 Caso n. 04 — Misure di mitigazione e obblighi

46. La comunicazione agli interessati è essenziale affinché possano adottare le misure necessarie per evitare danni materiali (ad esempio bloccare le loro carte di credito).

47. Oltre a documentare la violazione ai sensi dell'articolo 33, paragrafo 5, anche in questo caso la notifica all'autorità di controllo è obbligatoria (articolo 33, paragrafo 1) e il titolare del trattamento è altresì tenuto a comunicare la violazione agli interessati (articolo 34, paragrafo 1). Quest'ultima comunicazione potrebbe essere effettuata a ogni singolo interessato, ma per le persone in cui i dati di contatto non sono disponibili, il titolare del trattamento dovrebbe dare pubblica comunicazione purché ciò non sia suscettibile di determinare ulteriori conseguenze negative per gli interessati - ad esempio mediante una notifica sul suo sito web. In quest'ultimo caso è necessaria una comunicazione chiara e precisa, ben visibile sulla homepage del titolare del trattamento, con riferimenti esatti alle pertinenti disposizioni del GDPR. La società può inoltre dover aggiornare e correggere le misure e procedure organizzative e tecniche di gestione della sicurezza dei dati personali e di mitigazione dei rischi.

Azioni necessarie sulla base dei rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati

17 Per indicazioni sulle operazioni di trattamento *"che possono comportare un rischio elevato* ", cfr. la nota 10.

✓	✓	✓

2.5 Misure organizzative e tecniche per prevenire/mitigare gli effetti degli attacchi di ransomware

48. Il fatto che si sia verificato un attacco ransomware è solitamente la spia dell'esistenza di una o più vulnerabilità del sistema del titolare del trattamento. Ciò vale anche nei casi di attacchi ransomware con cifratura dei dati personali ma senza esfiltrazione. Indipendentemente dall'esito e dalle conseguenze dell'attacco, non si evidenzierà mai a sufficienza quanto sia cruciale una valutazione complessiva del sistema di sicurezza dei dati, con particolare riguardo alla sicurezza informatica. Le debolezze individuate e le lacune di sicurezza devono essere documentate e affrontate senza indugio.

49. Misure consigliate:

(L'elenco delle seguenti misure non è da considerarsi assolutamente esaustivo né tassativo. L'obiettivo è piuttosto quello di fornire suggerimenti di prevenzione e possibili soluzioni. Ogni attività di trattamento è diversa, pertanto il titolare del trattamento dovrebbe decidere quali misure siano più idonee nella specifica situazione)

- Mantenere aggiornato il firmware, il sistema operativo e il software applicativo sui server, sui client, sui componenti attivi di rete e su ogni altra macchina presente dulla stessa LAN (compresi i dispositivi Wi-Fi). Garantire l'esistenza di adeguate misure di sicurezza informatica, accertarne l'efficacia e mantenerle regolarmente aggiornate quando il trattamento o le circostanze cambiano o evolvono. Ciò comprende la conservazione di log dettagliati dei patch applicati e della rispettiva marcatura temporale.
- Progettazione e organizzazione di sistemi e infrastrutture di trattamento in modo da segmentare o isolare sistemi e reti di dati per evitare la propagazione di software malevolo all'interno dell'organizzazione e verso sistemi esterni.
- Esistenza di una procedura di backup aggiornata, sicura e testata. I mezzi di supporto per il back-up a medio e lungo termine dovrebbero essere tenuti separati dalla conservazione dei dati operativi e fuori dalla portata di soggetti terzi anche in caso di attacco riuscito (per esempio, un backup incrementale giornaliero e un backup settimanale completo).
- Disporre di/procurarsi un software antimalware adeguato, aggiornato, efficace e integrato.
- Disporre di un firewall e sistemi per il rilevamento e la prevenzione delle intrusioni adeguati, aggiornati, efficaci e integrati. Instradare il traffico di rete attraverso il firewall/il sistema rilevamento intrusioni, anche in caso di lavoro agile o in mobilità (ad esempio utilizzando connessioni VPN dotate di meccanismi organizzativi di sicurezza per l'accesso a Internet).
- Formazione dei dipendenti sui metodi di riconoscimento e prevenzione degli attacchi informatici. Il titolare del trattamento dovrebbe fornire gli strumenti per stabilire se le e-mail e i messaggi ottenuti con altri mezzi di comunicazione siano autentici e affidabili. I dipendenti dovrebbero essere formati per riconoscere quando si verifica un attacco del genere, sapere come rimuovere dalla rete l'endpoint ed essere tenuti a segnalarlo immediatamente al responsabile della sicurezza.
- Sottolineare la necessità di individuare il tipo di codice malevolo per comprendere le conseguenze dell'attacco ed essere in grado di individuare le misure giuste per attenuare il rischio. Nel caso in cui un attacco ransomware abbia avuto successo e non sia disponibile alcun back-up, per recuperare i dati possono essere utilizzati strumenti come quelli del progetto "no more ransom" (nomoreransom.org). Tuttavia, nel caso in cui sia disponibile un backup sicuro, è consigliabile ripristinare i dati attraverso il backup.
- Inoltrare o replicare tutti i log a un server centrale (compresa eventualmente la marcatura temporale crittografica o la firma delle registrazioni dei log).
- Cifratura robusta e autenticazione a più fattori, in particolare per l'accesso amministrativo ai sistemi informatici, adeguata gestione delle chiavi e delle password.

- Test di vulnerabilità e di penetrazione a cadenze regolari.
- Istituire un gruppo di risposta agli incidenti di sicurezza (CSIRT) o un gruppo di risposta alle emergenze informatiche (CERT) all'interno dell'organizzazione o aderire a un CSIRT/CERT collettivo. Creare un piano di risposta agli incidenti, un piano di *disaster recovery* (ripristino in caso di evento catastrofico) e un piano di continuità operativa e assicurarsi che tali piani siano testati in modo approfondito.
- Nel valutare le contromisure, si dovrebbe riesaminare, testare e aggiornare l'analisi dei rischi.

3 ATTACCHI DI ESFILTRAZIONE DEI DATI

50. Gli attacchi che sfruttano le vulnerabilità dei servizi offerti dal titolare del trattamento a terzi su Internet, ad esempio mediante attacchi di *injection* (es. attacchi SQL *injection*, *path traversal*), compromissione di siti web e simili, possono assomigliare ad attacchi ransomware in quanto il rischio deriva dall'azione di un terzo non autorizzato, ma mirano generalmente a copiare, esfiltrare e utilizzare dati personali per fini dolosi. Si tratta quindi principalmente di violazioni della riservatezza e, eventualmente, anche dell'integrità dei dati. Allo stesso tempo, se il titolare del trattamento è a conoscenza delle caratteristiche di questo tipo di violazioni, vi sono numerose misure che possono ridurre considerevolmente il rischio di un attacco efficace.

3.1 Caso n. 05: Esfiltrazione dei dati delle domande di impiego da un sito web

Un'agenzia per l'impiego è stata vittima di un attacco informatico, che ha inserito un codice malevolo sul suo sito web. Questo codice ha reso accessibili a soggetti non autorizzati le informazioni personali contenute nei moduli di richiesta di impiego conservati sul server web. 213 di tali moduli potrebbero essere interessati, e le analisi hanno accertato che nessuna categoria particolare di dati era oggetto della violazione. Il i malware installato aveva funzionalità che consentivano all'attaccante di rimuovere qualsiasi traccia di esfiltrazione e di monitorare il trattamento effettuato sul server e di carpire dati personali. Il malware è stato individuato solo un mese dopo la sua installazione.

3.1.1 Caso n. 05 — Misure in essere e valutazione del rischio

51. La sicurezza dell'ambiente del titolare del trattamento è estremamente importante, dal momento che la maggior parte di queste violazioni può essere evitata garantendo che tutti i sistemi siano costantemente aggiornati, che i dati sensibili siano cifrati e che le applicazioni siano sviluppate secondo elevati standard di sicurezza quali autenticazione forte, misure contro attacchi di forza bruta, "escape" (evasione) o "sanitizing" (sanificazione) "18 degli input degli utenti, ecc. . Anche gli audit periodici di sicurezza informatica, le valutazioni delle vulnerabilità e i test di penetrazione sono necessari per individuare e correggere tali tipi di vulnerabilità. Nel caso specifico, l'impiego di strumenti di monitoraggio dell'integrità dei file nell'ambiente di produzione avrebbe potuto facilitare l'individuazione dell'iniezione del codice (un elenco delle misure consigliate figura nella sezione 3.7).

52. Nell'indagare sulla violazione, il titolare del trattamento dovrebbe sempre partire dall'identificazione della tipologia e della metodica dell'attacco, al fine di valutare le misure da adottare. Per garantire rapidità ed efficacia di tale valutazione, il titolare dovrebbe disporre di un piano di risposta agli incidenti che specifichi le misure necessarie da adottare rapidamente per assumere il controllo dell'incidente. In questo caso particolare, il tipo di violazione costituiva un fattore di incremento del rischio, in quanto non solo veniva compromessa la riservatezza dei dati, ma il soggetto infiltrato era anche in grado di apportare modifiche al sistema cosicché veniva messa in discussione anche l'integrità dei dati.

53. Si dovrebbe tenere conto della natura, della sensibilità e del volume dei dati personali colpiti dalla violazione per determinare in che misura quest'ultima abbia inciso sugli interessati. Sebbene non siano state

18 La sanificazione degli input dell'utente è una forma di convalida degli input finalizzata ad assicurare che solo dati adeguatamente formattati siano inseriti in un sistema IT.

compromesse categorie particolari di dati personali, i dati oggetto della violazione contengono importanti informazioni sulle persone che hanno compilato i moduli online e tali dati potrebbero essere utilizzati impropriamente in vari modi (marketing indesiderato, furto di identità, ecc.), per cui la gravità delle conseguenze dovrebbe aumentare il rischio per i diritti e le libertà degli interessati19.

3.1.2 Caso n. 05 — Misure di mitigazione e obblighi

54. Se possibile, una volta risolto il problema, la banca dati dovrebbe essere confrontata con quella memorizzata in un backup sicuro. Le esperienze tratte dalla violazione dovrebbero essere utilizzate per aggiornare l'infrastruttura informatica. Il titolare del trattamento dovrebbe riportare tutti i sistemi informatici interessati a uno stato pulito noto, porre rimedio alla vulnerabilità e attuare nuove misure di sicurezza per evitare analoghe violazioni dei dati in futuro, ad esempio controlli di integrità dei file e audit di sicurezza. Se i dati personali sono stati non solo esfiltrati, ma anche cancellati, il titolare del trattamento deve intraprendere un'azione sistematica per ripristinare i dati personali nello stato in cui si trovavano prima della violazione. Potrebbe essere necessario applicare backup completi, modifiche incrementali ed eventualmente ripetere il trattamento dall'ultimo backup incrementale, il che richiede che il titolare sia in grado di replicare le modifiche apportate dopo l'ultimo backup. Ciò potrebbe necessitare che il titolare del trattamento disponga di un sistema progettato per conservare i file di input giornalieri nel caso in cui questi debbano essere nuovamente elaborati; tutto ciò richiede una tecnica robusta di memorizzazione e un'adeguata politica di conservazione prolungata dei dati.

55. Alla luce di quanto precede, poiché la violazione può comportare un rischio elevato per i diritti e le libertà delle persone fisiche, gli interessati dovrebbero esserne informati (articolo 34, paragrafo 1), il che significa naturalmente che anche le autorità di controllo competenti dovrebbero essere coinvolte attraverso una notifica di violazione dei dati. Documentare la violazione è obbligatorio ai sensi dell'articolo 33, paragrafo 5, del regolamento generale sulla protezione dei dati e facilita la valutazione del caso specifico.

Azioni necessarie sulla base dei rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	✓	✓

3.2 Caso n. 06: Esfiltrazione da un sito web di password sottoposte ad hashing

Una vulnerabilità SQL Injection è stata sfruttata per accedere a un database sul server di un sito web dedicato alla cucina. Agli utenti è stato consentito di scegliere solo pseudonimi arbitrari come nomi utente. È stato scoraggiato l'uso di indirizzi di posta elettronica a tal fine. Le password memorizzate nella banca dati sono state sottoposte ad hashing con un algoritmo robusto e il *salt* non è stato compromesso. Dati interessati: password *hashed* di 1.200 utenti. Per motivi di sicurezza, il titolare del trattamento ha informato gli interessati della violazione tramite posta elettronica e ha chiesto loro di modificare le password, soprattutto se la stessa password è stata utilizzata per altri servizi.

3.2.1 Caso n. 06 — Misure in essere e valutazione del rischio

56. In questo caso particolare, la riservatezza dei dati è compromessa, ma le password nel database sono state sottoposte ad hashing con un metodo conforme allo stato dell'arte, il che ridurrebbe il rischio per quanto riguarda la natura, la sensibilità e il volume dei dati personali. Il caso non presenta rischi per i diritti e le libertà degli interessati.

57. Inoltre, non sono state compromesse le informazioni di contatto (ad esempio indirizzi di posta elettronica o numeri di telefono) degli interessati, il che significa che non vi è alcun rischio significativo per gli interessati di essere oggetto di tentativi di frode (ad esempio, messaggi di posta elettronica di phishing o telefonate e SMS fraudolenti). Non sono state coinvolte categorie particolari di dati personali.

19 Per indicazioni sulle operazioni di trattamento *"che possono comportare un rischio elevato"*, cfr. la nota 10.

58. Alcuni nomi utente potrebbero essere considerati dati personali, ma la materia trattata dal sito web non genera connotazioni negative. Tuttavia, si deve osservare che la valutazione del rischio può essere diversa20, se la natura del sito web e i dati consultati possono rivelare categorie particolari di dati personali (ad esempio il sito web di un partito politico o di un sindacato). L'uso di tecniche di cifratura conformi allo stato dell'arte potrebbe attenuare gli effetti negativi della violazione. Consentire un numero limitato di tentativi di login impedirà il successo degli attacchi di forza bruta sul login, riducendo in larga misura i rischi generati da i attaccanti che già conoscono i nomi utente.

3.2.2 Caso n. 06 — Misure di mitigazione e obblighi

59. In alcuni casi la comunicazione agli interessati potrebbe essere considerata un fattore di mitigazione del rischio, dal momento che anche gli interessati sono in grado di adottare le misure necessarie per evitare ulteriori danni derivanti dalla violazione, ad esempio modificando la loro password. In questo caso, la comunicazione non era obbligatoria, ma in molti casi può essere considerata una buona pratica.

60. Il titolare del trattamento dovrebbe correggere la vulnerabilità e implementare nuove misure di sicurezza per evitare in futuro analoghe violazioni dei dati, ad esempio attraverso audit sistematici di sicurezza sul sito web.

61. La violazione dovrebbe essere documentata conformemente all'articolo 33, paragrafo 5, ma non è necessaria alcuna notifica o comunicazione.

62. Inoltre, è fortemente consigliabile comunicare agli interessati una violazione che riguardi password anche se le password sono state memorizzate utilizzando un hash con l'impiego di *salt* attraverso un algoritmo conforme allo stato dell'arte. È preferibile utilizzare metodi di autenticazione che evitino la necessità di trattare password lato server. Gli interessati dovrebbero avere la possibilità di adottare misure adeguate per quanto riguarda le proprie password.

Azioni necessarie sulla base dei rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	X	X

3.3 Caso n. 07: Attacco del tipo *credential stuffing* su un sito web bancario

Una banca ha subito un attacco informatico contro uno dei suoi siti web di servizi bancari online. L'attacco mirava a elencare tutti gli identificativi utente di accesso possibili utilizzando una banale password fissa. Le password sono composte da 8 cifre. A causa di vulnerabilità del sito web, in alcuni casi l'autore dell'attacco ha potuto accedere a informazioni riguardanti gli interessati (nome, cognome, sesso, data e luogo di nascita, codice fiscale, codici di identificazione dell'utente), anche se la password utilizzata non era corretta o il conto bancario non era più attivo. Ciò ha interessato circa 100.000 soggetti. Fra questi, l'autore dell'attacco si è connesso con successo a circa 2.000 account che utilizzavano la password banale da questi processata . Successivamente il titolare del trattamento è stato in grado di individuare tutti i tentativi illegittimi di log-on. Il titolare ha potuto verificare che, in base ai controlli antifrode, su tali account non è stata effettuata alcuna transazione durante l'attacco. La banca era a conoscenza della violazione dei dati in quanto il suo centro operativo di sicurezza ha individuato un numero elevato di richieste di login dirette verso il sito web. In risposta, il titolare del trattamento ha disattivato temporaneamente la possibilità di connettersi al sito web e ha forzato il cambio password degli account compromessi. Il titolare ha comunicato la violazione solo agli utenti con account compromessi, ossia agli utenti le cui password sono state compromesse o i cui dati sono stati divulgati.

3.3.1 Caso n. 07 — Misure in essere e valutazione del rischio

63. È importante ricordare che i titolari che trattano dati di natura estremamente personale21 hanno maggiori

20 Per indicazioni sulle operazioni di trattamento *"che possono comportare un rischio elevato* ", cfr. la nota 10.

21 Quali le informazioni degli interessati relative a metodi di pagamento come numeri di carta, conti bancari,

responsabilità in termini di garanzia di un'adeguata sicurezza dei dati, ad esempio predisponendo un centro operativo di sicurezza e attuando altre misure di prevenzione, rilevamento e risposta agli incidenti. Il mancato rispetto di questi standard più elevati comporterà certamente l'adozione di misure più severe durante l'indagine di un'autorità di controllo.

64. La violazione riguarda dati finanziari che vanno al di là dell'identità e delle informazioni identificative dell'utente, il che la rende particolarmente grave. Il numero di persone interessate è elevato.

65. Il fatto che una violazione possa verificarsi in un ambiente così sensibile segnala la presenza di notevoli lacune della sicurezza dei dati nel sistema del titolare del trattamento e può essere un indicatore della necessità di un riesame e di un aggiornamento delle misure in questione, in linea con gli articoli 24 (1), 25 (1) e 32 (1) del GDPR. I dati violati consentono l'identificazione univoca degli interessati e contengono altre informazioni su di essi (tra cui sesso, data e luogo di nascita); inoltre possono essere utilizzati dall'autore dell'attacco per ricavare le password dei clienti o per condurre una campagna di phishing mirata ai clienti della banca.

66. Per questi motivi, la violazione dei dati è stata ritenuta suscettibile di comportare un rischio elevato per i diritti e le libertà di tutti gli interessati22. Pertanto, è ipotizzabile il verificarsi di un danno materiale (ad esempio una perdita finanziaria) e immateriale (ad esempio furto d'identità o frode) in conseguenza della violazione.

3.3.2 Caso n. 07 — Misure di mitigazione e obblighi

67. Le misure del titolare del trattamento menzionate nella descrizione del caso sono adeguate. A seguito della violazione, ha inoltre corretto la vulnerabilità del sito web e ha adottato altre misure per prevenire analoghe violazioni dei dati in futuro, come l'aggiunta di un'autenticazione a due fattori al sito web interessato e il passaggio a un'autenticazione forte del cliente.

68. In questo scenario la documentazione della violazione a norma dell'articolo 33, paragrafo 5, del GDPR e la notifica all'autorità di controllo non sono lasciate alla discrezione del titolare. Inoltre, il titolare del trattamento dovrebbe informare tutti i 100.000 interessati (compresi gli interessati i cui account non sono stati compromessi) a norma dell'articolo 34 del GDPR.

Azioni necessarie sulla base dei rischi individuati		
Documentazione	Notifica all'autorità	Comunicazione agli interessati
✓	✓	✓

3.4 Misure organizzative e tecniche per prevenire/mitigare gli effetti degli attacchi di hacker

69. Come nel caso degli attacchi ransomware, indipendentemente dall'esito e dalle conseguenze dell'attacco, i titolari sono tenuti a riconsiderare le misure di sicurezza dei sistemi informativi in casi analoghi.

70. Misure consigliate:23

(L'elenco delle seguenti misure non è da considerarsi assolutamente esaustivo né tassativo. L'obiettivo è piuttosto quello di fornire suggerimenti di prevenzione e possibili soluzioni. Ogni attività di trattamento è diversa, pertanto il titolare del trattamento dovrebbe decidere quali misure siano più idonee nella specifica situazione)

- Cifratura e gestione delle chiavi conformi allo stato dell'arte, in particolare quando si trattano password, dati sensibili o finanziari. L'hashing e l'utilizzo di salt crittografici sono sempre preferibili in caso di informazioni riservate (password) rispetto alla cifratura delle password. È preferibile utilizzare metodi di autenticazione che evitino la necessità di trattare password lato server.
- Aggiornamento del sistema (software e firmware). Garantire l'applicazione di tutte le misure di sicurezza

pagamenti online, cedolini degli stipendi, estratti conto bancari, studi economici o qualsiasi altro elemento che possa rivelare informazioni economiche relative agli interessati.

22 Per indicazioni sulle operazioni di trattamento *"che possono comportare un rischio elevato"*, cfr. la nota 10.

23 Per lo sviluppo sicuro di applicazioni web si veda anche: https://www.owasp.org/index.php/Main page.

informatica, garantirne l'efficacia e mantenerle regolarmente aggiornate quando il trattamento o le circostanze cambiano o evolvono. Per essere in grado di dimostrare la conformità all'articolo 5, paragrafo 1, lettera f), a norma dell'articolo 5, paragrafo 2, del GDPR, il titolare del trattamento dovrebbe conservare un registro di tutti gli aggiornamenti effettuati, compreso il momento in cui sono stati applicati.

- Uso di metodi di autenticazione forte quali autenticazione a due fattori e server di autenticazione, integrati da una politica aggiornata in materia di password.
- Gli standard sicuri di sviluppo comprendono l'applicazione di un filtro agli input utente (utilizzando per quanto possibile una *white list*), la sanificazione degli input utente e misure di prevenzione degli attacchi di forza bruta (come limitare il numero massimo di tentativi ripetuti). L'impiego di Web Application Firewall (WAF - firewall per le applicazioni web) può supportare l'implementazione efficace di questa tecnica.
- Politiche robuste per i privilegi utente e la gestione del controllo degli accessi.
- Uso di sistemi di protezione, di rilevamento delle intrusioni e di difesa perimetrale adeguati, aggiornati, efficaci e integrati.
- Audit sistematici della sicurezza informatica e valutazioni delle vulnerabilità (test di penetrazione).
- Revisioni e test periodici per garantire l'utilizzabilità dei backup al fine di ripristinare i dati la cui integrità o disponibilità siano state compromesse.
- Nessun identificativo di sessione nell'URL in chiaro.

4 FONTI DI RISCHIO INTERNE LEGATE AL FATTORE UMANO

71. Occorre evidenziare il ruolo dell'errore umano nelle violazioni dei dati personali a causa della sua frequenza. Poiché queste violazioni possono essere sia intenzionali che accidentali, è molto difficile per i titolari del trattamento individuare le vulnerabilità e adottare misure per evitarle. La Conferenza internazionale delle autorità per la protezione dei dati e la privacy ha riconosciuto l'importanza di affrontare tali fattori umani e ha adottato, nell'ottobre 2019, una risoluzione concernente il ruolo dell'errore umano nelle violazioni dei dati personali24. La risoluzione sottolinea la necessità di adottare misure di salvaguardia adeguate al fine di prevenire gli errori umani e fornisce un elenco non esaustivo di garanzie e approcci.

4.1 Caso n. 08: Esfiltrazione di dati aziendali da parte di un dipendente

Durante il suo periodo di preavviso, il dipendente di una società copia i dati aziendali dalla banca dati della società. Il dipendente è autorizzato ad accedere ai dati solo per svolgere le sue mansioni. Vari mesi dopo aver cessato il lavoro alle dipendenze della società, utilizza i dati così ottenuti (dati di contatto di base) per alimentare un nuovo trattamento dei dati per il quale è il titolare, al fine di contattare i clienti della società e invitarli a rivolgersi alla sua nuova impresa.

4.1.1 Caso n. 08 — Misure in essere e valutazione del rischio

72. Nel caso di specie non sono state adottate misure preventive per impedire al dipendente di copiare i dati di contatto della clientela della società, in quanto il dipendente aveva bisogno legittimamente di accedere – e di fatto accedeva – a tali informazioni per le sue mansioni. Poiché la gestione dei clienti richiede nella maggior parte dei casi un qualche tipo di accesso dei dipendenti ai dati personali, tali violazioni possono essere le più difficili da prevenire. Limitando la portata dell'accesso si rischia di limitare il lavoro che il dipendente è in grado di svolgere. Tuttavia, politiche di accesso ben concepite e un controllo costante possono contribuire a prevenire tali violazioni.

73. Come di consueto, durante la valutazione del rischio devono essere presi in considerazione il tipo di violazione e la natura, la sensibilità e il volume dei dati personali interessati. Queste violazioni sono generalmente

24 http://globalprivacyassembly.org/wp-content/uploads/2019/10/AOIC-Resolution-FINAL-ADOPTED.pdf

violazioni della riservatezza, in quanto la banca dati è solitamente lasciata intatta e il suo contenuto è "semplicemente" copiato in vista di un ulteriore utilizzo. La quantità di dati interessati è solitamente bassa o media. In questo caso particolare non sono state coinvolte categorie particolari di dati personali, il dipendente aveva bisogno soltanto delle informazioni di contatto dei clienti per essere in grado di contattarli dopo aver lasciato la società. Pertanto, i dati in questione non sono sensibili.

74. Sebbene l'unico obiettivo dell'ex-dipendente che ha copiato in modo fraudolento i dati possa consistere nell'ottenere le informazioni di contatto della clientela della società per i propri scopi di natura commerciale, il titolare del trattamento non può considerare basso il rischio per gli interessati poiché non dispone di alcuna certezza sulle intenzioni del dipendente. Pertanto, sebbene le conseguenze della violazione possano limitarsi all'esposizione alle attività di autopromozione svolte dall'ex-dipendente, non è escluso un ulteriore e più grave abuso dei dati copiati, a seconda della finalità del trattamento messo in atto dall'ex-dipendente25.

4.1.2 Caso n. 08 — Misure di mitigazione e obblighi

75. Nel caso di specie è difficile mitigare gli effetti negativi della violazione. Potrebbe essere necessario avviare un'azione legale immediata per impedire all'ex-dipendente di utilizzare impropriamente e diffondere ulteriormente i dati. In seconda battuta, l'obiettivo dovrebbe essere quello di evitare situazioni analoghe in futuro. Il titolare del trattamento potrebbe chiedere un'ingiunzione che imponga all'ex-dipendente di astenersi dall'utilizzo dei dati, ma le probabilità che ciò risulti efficace sono, nella migliore delle ipotesi, opinabili. Possono essere utili misure tecniche adeguate, come l'impossibilità di copiare o scaricare dati su dispositivi amovibili.

76. Non esiste una soluzione unica per tutti i casi di questo tipo, ma un approccio sistematico può contribuire a prevenirli. Ad esempio, l'impresa può prendere in considerazione, ove possibile, la limitazione degli accessi per i dipendenti che hanno segnalato l'intenzione di licenziarsi, oppure prevedere log degli accessi in modo da registrare e segnalare ogni accesso indesiderato. Il contratto firmato con i dipendenti dovrebbe includere clausole che vietino attività del genere descritto.

77. Nel complesso, poiché la violazione in questione non comporterà un rischio elevato per i diritti e le libertà delle persone fisiche, è sufficiente una notifica all'autorità di controllo. Tuttavia, informarne gli interessati potrebbe essere vantaggioso anche per il titolare del trattamento, in quanto sarebbe meglio che gli interessati ricevano la notizia della violazione dall'azienda piuttosto che apprenderla quando l'ex-dipendente cercherà di contattarli. La documentazione della violazione a norma dell'articolo 33, paragrafo 5, è un obbligo giuridico.

Azioni necessarie sulla base dei rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	✓	X

4.2 Caso n. 09: Trasmissione accidentale di dati a un terzo fidato

Un agente assicurativo ha notato che — a causa dalle impostazioni difettose di un file Excel ricevuto per posta elettronica — era in grado di accedere alle informazioni relative a una ventina di clienti non appartenenti al suo portafoglio. Egli è vincolato dal segreto professionale ed è stato l'unico destinatario del messaggio di posta elettronica. L'accordo tra il titolare del trattamento e l'agente assicurativo obbliga quest'ultimo a segnalare senza ingiustificato ritardo una violazione dei dati personali al titolare stesso. Pertanto, l'agente ha immediatamente segnalato l'errore al titolare, che ha corretto il file e lo ha inviato nuovamente, chiedendo all'agente di cancellare il messaggio precedente. In base all'accordo di cui sopra, l'agente deve confermare la cancellazione per iscritto, cosa che ha fatto. Le informazioni raccolte non comprendono categorie particolari di dati personali, solo dati di contatto e dati relativi all'assicurazione stessa (tipo di assicurazione, importo). Dopo aver analizzato i dati personali interessati dalla violazione, il titolare del trattamento non ha individuato elementi particolari, sia per quanto riguarda gli interessati sia

25 Per indicazioni sulle operazioni di trattamento *"che possono comportare un rischio elevato"*, cfr. la nota 10.

per quanto riguarda lo stesso titolare, tali da incidere sul livello di impatto della violazione.

4.2.1 Caso n. 09 — Misure in essere e valutazione del rischio

78. In questo caso la violazione non deriva da un'azione deliberata di un dipendente, ma da un errore umano accidentale causato da disattenzione. Questo tipo di violazione può essere evitato o reso meno frequente: a) applicando programmi di formazione, istruzione e sensibilizzazione cosicché i dipendenti acquisiscano una migliore comprensione dell'importanza della protezione dei dati personali; b) riducendo lo scambio di file tramite posta elettronica, e utilizzando invece sistemi dedicati per il trattamento dei dati dei clienti; c) verificando due volte i file prima dell'invio; d) separando il momento della creazione da quello dell'invio di file.

79. La violazione riguarda solo la riservatezza dei dati, e l'integrità e l'accessibilità degli stessi non sono compromesse. La violazione dei dati riguardava solo una ventina di clienti, per cui è contenuto il volume dei dati interessati. Inoltre, non sono coinvolti dati sensibili. Il fatto che il responsabile del trattamento abbia contattato immediatamente il titolare dopo essere venuto a conoscenza della violazione dei dati può essere considerato un fattore di mitigazione del rischio. (Sarebbe da valutare anche l'eventualità che i dati siano stati trasmessi ad altri agenti assicurativi e, in caso di conferma, si dovrebbero adottare misure adeguate.) Grazie alle misure appropriate adottate successivamente alla violazione dei dati, probabilmente quest'ultima non avrà alcun impatto sui diritti e sulle libertà degli interessati.

80. Il basso numero di persone interessate, la rilevazione immediata della violazione e le misure adottate per minimizzarne gli effetti rendono il caso in questione privo di rischi.

4.2.2 Caso n. 09 — Misure di mitigazione e obblighi

81. Vi sono altri elementi di mitigazione del rischio nel caso in esame: l'agente è vincolato al segreto professionale; egli stesso ha segnalato il problema al titolare del trattamento e ha cancellato il file su richiesta. La sensibilizzazione ed eventualmente la previsione di ulteriori misure di controllo dei documenti contenenti dati personali potranno contribuire a evitare il ripetersi di situazioni simili in futuro.

82. Oltre a documentare la violazione a norma dell'articolo 33, paragrafo 5, non sono necessarie altre azioni.

Azioni necessarie sulla base dei rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	X	X

4.3 Misure organizzative e tecniche per prevenire/attenuare l'impatto delle fonti interne di rischio legate al fattore umano

83. L'applicazione congiunta delle misure indicate di seguito, in funzione delle caratteristiche specifiche del caso, dovrebbe contribuire a ridurre le probabilità di una recidiva analoga.

84. Misure consigliate:

(L'elenco delle seguenti misure non è da considerarsi assolutamente esaustivo né tassativo. L'obiettivo è piuttosto quello di fornire suggerimenti di prevenzione e possibili soluzioni. Ogni attività di trattamento è diversa, pertanto il titolare del trattamento dovrebbe decidere quali misure siano più idonee nella specifica situazione)

- Attuazione periodica di programmi di formazione, istruzione e sensibilizzazione per i dipendenti sugli obblighi in materia di privacy e sicurezza e sulla rilevazione e la segnalazione di minacce alla sicurezza dei dati personali26. Messa a punto di un programma di sensibilizzazione per ricordare ai dipendenti gli errori

26 Sezione 2) sottosezione i) della risoluzione per affrontare il ruolo dell'errore umano nelle violazioni dei dati personali.

più comuni che portano a violazioni dei dati personali e come evitarli.

- Istituzione di pratiche, procedure e sistemi solidi ed efficaci in materia di protezione dei dati e di tutela della vita privata27.
- Valutazione delle pratiche, delle procedure e dei sistemi in materia di tutela della vita privata per garantirne l'efficacia nel tempo28.
- Elaborazione di adeguate politiche di controllo dell'accesso e obbligo per gli utenti di rispettare le norme.
- Tecniche per forzare l'autenticazione dell'utente quando accede a dati personali sensibili.
- Disabilitazione dell'account aziendale non appena il dipendente lascia l'azienda.
- controllo dei flussi di dati insoliti tra il file server e le postazioni di lavoro dei dipendenti.
- impostazione della sicurezza dell'interfaccia I/O nel BIOS o mediante l'uso di software che controlla l'uso delle interfacce del computer (blocco o sblocco, ad esempio USB/CD/DVD, ecc.).
- revisione delle politiche in materia di accesso dei dipendenti (ad esempio, registrare l'accesso a dati sensibili chiedendo all'utente di inserire una motivazione di ordine aziendale, in modo che sia disponibile per gli audit).
- Disabilitazione dei servizi di cloud aperti.
- Vietare e impedire l'accesso a servizi di posta elettronica aperta noti.
- Disattivazione della funzione *print screen* [stampa schermata] nel sistema operativo (OS).
- Applicazione rigorosa di una politica della “scrivania sgombra” (c.d. *clean desktop*).
- Blocco automatico di tutti i computer dopo un certo periodo di inattività.
- Utilizzo di meccanismi (ad esempio token (wireless) per accedere a/aprire account bloccati) per cambi rapidi di utente in ambienti condivisi.
- Utilizzo di sistemi dedicati per la gestione dei dati personali che prevedano adeguati meccanismi di controllo dell'accesso e siano in grado di prevenire errori umani, come l'invio di comunicazioni al soggetto sbagliato. L'uso di fogli di calcolo e di altri documenti d'ufficio non è adeguato al fine di gestire i dati dei clienti.

5 SMARRIMENTO O FURTO DI DISPOSITIVI O DI DOCUMENTI CARTACEI

85. Un caso frequente è lo smarrimento o il furto di dispositivi portatili. In questi casi, il titolare del trattamento deve prendere in considerazione le circostanze del trattamento, quali le categorie dei dati conservati sul dispositivo, nonché le risorse di supporto, e le misure adottate precedentemente alla violazione per garantire un livello di sicurezza adeguato. Tutti questi elementi incidono sui potenziali impatti della violazione dei dati. La valutazione dei rischi potrebbe risultare difficile, in quanto il dispositivo non è più disponibile.

86. Questo tipo di violazione può essere classificato in tutti i casi come violazione della riservatezza. Tuttavia, se non esiste un backup per il database sottratto, può configurarsi anche una violazione della disponibilità e dell'integrità.

87. Gli scenari descritti di seguito illustrano in che modo le circostanze di cui sopra determinano la probabilità e la gravità della violazione dei dati.

5.1 Caso n. 10: Furto di supporti sui quali sono memorizzati dati personali cifrati

A seguito di un’effrazione compiuta in un asilo, sono stati rubati due tablet. Nei tablet era installata un'app contenente dati personali sui bambini che frequentano l’asilo: nome, data di nascita, dati personali relativi alle attività educative. Sia i tablet cifrati, che erano spenti al momento dell’effrazione, sia l'app erano protetti da una password robusta. Per il titolare era prontamente ed efficacemente disponibile il back-up. Subito

27 Sezione 2) sottosezione ii) della risoluzione per affrontare il ruolo dell'errore umano nelle violazioni dei dati personali.

28 Sezione 2) sottosezione iii) della risoluzione per affrontare il ruolo dell'errore umano nelle violazioni dei dati personali.

dopo essere venuto a conoscenza dell'effrazione, l'asilo ha inviato un comando a distanza per rimuovere il contenuto dei tablet.

5.1.1 Caso n. 10 — Misure in essere e valutazione del rischio

88. In questo caso particolare, il titolare del trattamento ha adottato misure adeguate per prevenire e mitigare gli effetti di una potenziale violazione dei dati utilizzando la cifratura dei dispositivi, introducendo un'adeguata protezione delle password e garantendo il back-up dei dati conservati sui tablet. (Un elenco delle misure consigliate figura nella sezione 5.7).

89. Dopo essere venuto a conoscenza di una violazione, il titolare del trattamento dovrebbe valutare la fonte di rischio, i sistemi a supporto del trattamento dei dati, il tipo di dati personali coinvolti e gli impatti potenziali della violazione sulle persone interessate. La violazione dei dati sopra descritta avrebbe riguardato la riservatezza, la disponibilità e l'integrità dei dati; tuttavia, grazie alle idonee misure adottate dal titolare precedentemente e successivamente alla violazione dei dati, nessuna di tali compromissioni si è verificata.

5.1.2 Caso n. 10 — Misure di mitigazione e obblighi

90. La riservatezza dei dati personali sui dispositivi non è stata compromessa grazie alla protezione delle password robuste sia sui tablet che sulle app. I tablet sono stati configurati in modo tale che la l'impostazione di una password comporti la cifratura dei dati nel dispositivo. A ciò si aggiunga il tentativo del titolare di cancellare da remoto tutte le informazioni nei tablet rubati.

91. Grazie alle misure adottate, anche la riservatezza dei dati non è stata compromessa. Inoltre, il backup garantiva la costante disponibilità dei dati personali, pertanto non si sarebbe potuto verificare alcun potenziale impatto negativo.

92. Ne deriva l'improbabilità che la violazione dei dati sopra descritta comporti un rischio per i diritti e le libertà degli interessati, pertanto non occorre alcuna notifica all'autorità di controllo o agli interessati. Tuttavia, anche una violazione di questo tipo deve essere documentata, a norma dell'articolo 33, paragrafo 5.

Azioni necessarie sulla base dei rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	X	**X**

5.2 Caso n. 11: Furto di supporti sui quali sono memorizzati dati personali non cifrati

Il computer portatile di un dipendente di una società di servizi è stato rubato. Il notebook rubato conteneva nomi, cognomi, sesso, indirizzi e data di nascita di oltre 100.000 clienti. A causa dell'indisponibilità del dispositivo rubato non è stato possibile individuare se fossero interessate anche altre categorie di dati personali. L'accesso al disco rigido del notebook non era protetto da alcuna password. È possibile ripristinare i dati personali attraverso i backup giornalieri disponibili.

5.2.1 Caso n. 11 — Misure in essere e valutazione del rischio

93. Poiché il titolare del trattamento non ha adottato alcuna misura di sicurezza, i dati personali memorizzati nel notebook rubato erano facilmente accessibili all'autore del furto o a qualsiasi altra persona che successivamente entrasse in possesso del dispositivo.

94. Questa violazione riguarda la riservatezza dei dati conservati sul dispositivo rubato.

95. In questo caso il notebook contenente i dati personali era vulnerabile in quanto non disponeva di alcuna password di protezione né di cifratura. La mancanza di misure di sicurezza di base aumenta il livello di rischio per gli interessati. Un'ulteriore criticità è rappresentata dall'identificazione degli interessati, il che aumenta anche la gravità della violazione. Il numero considerevole di persone interessate comporta un incremento del

rischio; tuttavia, nella violazione non sono coinvolte categorie particolari di dati personali.

96. Nel corso della valutazione del rischio29, il titolare del trattamento dovrebbe prendere in considerazione le potenziali conseguenze e gli effetti negativi della violazione della riservatezza. A causa della violazione, gli interessati possono subire furti di identità sulla base dei dati disponibili nel notebook sottratto, per cui il rischio è da ritenersi elevato.

5.2.2 Caso n. 11 — Misure di mitigazione e obblighi

97. La cifratura del dispositivo e l'uso della protezione di una password robusta del database memorizzato nel dispositivo avrebbero potuto impedire che la violazione dei dati comportasse un rischio per i diritti e le libertà degli interessati.

98. Alla luce di tali circostanze, è necessaria la notifica all'autorità di controllo competente nonché la comunicazione agli interessati.

Azioni necessarie sulla base dei rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	✓	✓

5.3 CASO n. 12 – FURTO DI FASCICOLI CARTACEI CONTENENTI DATI SENSIBILI

Un registro cartaceo è stato rubato da un centro per la riabilitazione dalle tossicodipendenze. Il registro conteneva dati identificativi e sanitari di base relativi ai pazienti del centro. I dati erano memorizzati solo sul supporto cartaceo e i medici che trattavano i pazienti non dispongono di un backup. Il registro non era conservato in un cassetto chiuso a chiave né in una stanza chiusa a chiave; il titolare non aveva previsto politiche per il controllo degli accessi né altre misure a protezione della documentazione cartacea.

5.3.1 Caso n. 12 — Misure in essere e valutazione del rischio

99. Poiché il titolare del trattamento dei dati non ha adottato alcuna misura di sicurezza, i dati personali conservati nel registro erano facilmente accessibili alla persona che lo ha trovato. Inoltre, la natura dei dati personali conservati nel registro rende la mancanza di un backup un fattore di rischio molto grave.

100. Questo caso esemplifica una violazione dei dati ad alto rischio. A causa della mancanza di adeguate precauzioni a, sono andati perduti dati sanitari sensibili a norma dell'articolo 9, paragrafo 1, del GDPR. Poiché in questo caso si trattava di una categoria particolare di dati personali, i rischi potenziali per gli interessati sono maggiori, e tale circostanza deve essere tenuta in considerazione anche dal titolare del trattamento nell'effettuare la valutazione del rischio30.

101. La violazione riguarda la riservatezza, la disponibilità e l'integrità dei dati personali in questione. La violazione compromette la segretezza del rapporto medico-paziente, e terzi non autorizzati possono accedere alle informazioni sanitarie riguardanti i pazienti, il che può avere gravi ripercussioni sulla loro vita. La violazione della disponibilità può anche compromettere la continuità delle cure prestate. Non potendosi escludere la modifica/cancellazione di parti del contenuto del registro, risulta compromessa anche l'integrità dei dati personali.

5.3.2 Caso n. 12 — Misure di mitigazione e obblighi

102. In fase di valutazione delle misure di salvaguardia dovrebbe essere presa in considerazione anche la natura del supporto utilizzato. Poiché il registro dei pazienti era un documento fisico, la sua protezione avrebbe dovuto essere organizzata in modo diverso rispetto a un dispositivo elettronico. La pseudonimizzazione dei nomi dei pazienti, la conservazione del registro in un locale protetto e in un cassetto o una stanza chiusi a

29 Per indicazioni sulle operazioni *di trattamento "che possono comportare un rischio elevato* ", cfr. la nota 10.
30 Per indicazioni sulle operazioni di trattamento *"che possono comportare un rischio elevato* ", cfr. la nota 10.

chiave, e un adeguato controllo degli accessi che prevedesse l'autenticazione al momento dell'accesso avrebbero potuto impedire la violazione dei dati.

103. La violazione dei dati di cui sopra può avere gravi ripercussioni sugli interessati; di conseguenza, la notifica dell'autorità di controllo e la comunicazione della violazione agli interessati sono obbligatorie.

Azioni necessarie sulla base dei rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	✓	✓

5.4 Misure organizzative e tecniche per prevenire/attenuare le conseguenze della perdita o del furto di dispositivi

104. L'applicazione congiunta delle misure indicate di seguito, in funzione delle caratteristiche specifiche del caso, dovrebbe contribuire a ridurre la probabilità del ripetersi di incidenti analoghi.

105. Misure consigliate:

(L'elenco delle seguenti misure non è da considerarsi assolutamente esaustivo né tassativo. L'obiettivo è piuttosto quello di fornire suggerimenti di prevenzione e possibili soluzioni. Ogni attività di trattamento è diversa, pertanto il titolare del trattamento dovrebbe decidere quali misure siano più idonee nella specifica situazione)

- Attivare sistemi di cifratura del dispositivo (come BitLocker, Veracript o DM-Crypt).
- Utilizzare un codice di accesso/password su tutti i dispositivi. Cifrare tutti i dispositivi elettronici mobili prevedendo l'inserimento di una password complessa per la decifratura.
- Utilizzare l'autenticazione a più fattori.
- Attivare le funzionalità dei dispositivi ad alta mobilità che ne consentono la localizzazione in caso di perdita o smarrimento.
- Utilizzare software/app e localizzazione MDM (Mobile Devices Management). Utilizzare filtri antiriflesso. Chiudere tutti i dispositivi incustoditi.
- Se possibile e opportuno per il trattamento dei dati in questione, salvare i dati personali non su un dispositivo mobile, ma su un server centrale di back-end.
- Se la postazione di lavoro è collegata alla LAN aziendale, eseguire un backup automatico dalle cartelle di lavoro, a condizione che sia ineludibile che i dati personali siano ivi conservati.
- Utilizzare una VPN sicura (ad esempio, che richieda un secondo fattore di autenticazione separato per stabilire una connessione sicura) per collegare i dispositivi mobili ai server back-end.
- Fornire dispositivi di blocco fisico ai dipendenti per consentire loro di mettere fisicamente in sicurezza i dispositivi mobili che utilizzano quando rimangono incustoditi.
- Corretta regolamentazione dell'uso del dispositivo al di fuori dell'azienda.
- Corretta regolamentazione dell'uso dei dispositivi all'interno dell'azienda.
- Utilizzare software/app MDM (Mobile Devices Management) e attivare la funzione wipe da remoto.
- Utilizzare una gestione centralizzata dei dispositivi con diritti minimi per l'installazione di software da parte degli utenti finali.
- Installare controlli di accesso fisico.
- Evitare di conservare informazioni sensibili in dispositivi mobili o dischi rigidi. Se è necessario accedere al sistema interno dell'impresa, si dovrebbero utilizzare canali sicuri come indicato in precedenza.

6 ERRATO INVIO DI CORRISPONDENZA

106. Anche in questo caso la fonte di rischio è un errore umano interno, ma nessun atto doloso ha portato alla violazione. È il risultato di una disattenzione. Ben poco può fare il titolare del trattamento una volta che la violazione si sia verificata, pertanto la prevenzione in questi casi è ancora più importante.

6.1 Caso n. 13: Errore nella corrispondenza postale

Due ordini per l'acquisto di calzature sono stati evasi da una società di vendita al dettaglio. A causa di un errore umano, è stata fatta confusione con le due fatture per cui sia i prodotti che le relative fatture sono stati inviati alla persona sbagliata. Ciò significa che i due clienti hanno ricevuto gli ordini l'uno dell'altro, comprese le fatture contenenti i dati personali. Dopo essere venuto a conoscenza della violazione, il titolare del trattamento ha richiamato gli ordini e li ha inviati ai destinatari corretti.

6.1.1 Caso n. 13 — Misure in essere e valutazione del rischio

107. Le fatture contenevano i dati personali necessari per la consegna (nome, indirizzo, oltre all'articolo acquistato e il suo prezzo). È importante individuare in primo luogo come abbia potuto verificarsi l'errore umano e, se del caso, come avrebbe potuto essere evitato. Nel caso specifico, il rischio è basso, poiché non sono state coinvolte categorie particolari di dati personali o altri dati il cui abuso potrebbe avere effetti negativi rilevanti, la violazione non consegue a un errore sistemico da parte del titolare del trattamento e sono interessate solo due persone. Non sono stati rilevati effetti negativi sugli interessati.

6.1.2 Caso n. 13 — Misure di mitigazione e obblighi

108. Il titolare del trattamento dovrebbe prevedere la restituzione gratuita degli articoli e delle relative fatture, nonché chiedere ai destinatari errati di distruggere/cancellare tutte le eventuali copie delle fatture contenenti i dati personali dell'altro destinatario.

109. Anche se la violazione non comporta di per sé un rischio elevato per i diritti e le libertà delle persone interessate e, di conseguenza, la comunicazione agli interessati non è richiesta ai sensi dell'articolo 34 del GDPR, tale comunicazione di fatto è inevitabile in quanto è necessaria la cooperazione degli interessati per la mitigazione del rischio.

Azioni necessarie sulla base dei rischi individuati		
Documentazione	Notifica all'autorità	Comunicazione agli interessati
✓	X	X

6.2 Caso n. 14: Dati personali altamente riservati inviati erroneamente per posta elettronica

Il dipartimento risorse umane di una pubblica amministrazione ha inviato un messaggio di posta elettronica — sulle attività formative previste — alle persone registrate nel sistema come in cerca di occupazione. Per errore, all'e-mail è stato allegato un documento contenente tutti i dati personali di tali soggetti (nome, indirizzo e-mail, indirizzo postale, numero di previdenza sociale). Gli interessati coinvolti sono oltre 60.000. Successivamente, l'Ufficio ha contattato tutti i destinatari chiedendo loro di cancellare il messaggio precedente e di non utilizzare le informazioni in esso contenute.

6.2.1 Caso n. 14 — Misure in essere e valutazione del rischio

110. Per l'invio di messaggi di questo genere avrebbero dovuto essere applicate regole più rigorose. Occorre prendere in considerazione l'introduzione di meccanismi di controllo supplementari.

111. Il numero di persone interessate è considerevole e il coinvolgimento del loro numero di previdenza sociale, insieme ad altri dati personali più basilari, aumenta ulteriormente il rischio, che può essere classificato come elevato31. Il titolare non può implementare misure tese a contenere l'eventuale diffusione dei dati da parte di uno qualsiasi dei destinatari.

6.2.2 Caso n. 14 — Misure di mitigazione e obblighi

112. Come indicato in precedenza, sono pochi gli strumenti utili a mitigare efficacemente i rischi di una violazione analoga. Sebbene il titolare del trattamento abbia chiesto la cancellazione del messaggio, non può costringere

31 Per indicazioni sulle operazioni di trattamento *"che possono comportare un rischio elevato* ", cfr. la nota 10.

i destinatari a farlo e, di conseguenza, non può essere certo che essi adempiano a quanto richiesto.

113. In un caso del genere non dovrebbero esservi dubbi sulla necessità di tutte e tre le azioni indicate di seguito.

Azioni necessarie sulla base dei rischi individuati		
Documentazione	Notifica all'autorità	Comunicazione agli interessati
✓	✓	✓

6.3 Caso n. 15: Dati personali inviati per errore tramite posta elettronica

Un elenco dei partecipanti a un corso di inglese giuridico tenuto presso un albergo e della durata di 5 giorni è inviato per errore a 15 partecipanti a un precedente e analogo corso anziché all'albergo. L'elenco contiene nomi, indirizzi di posta elettronica e preferenze alimentari dei 15 partecipanti. Solo due partecipanti hanno indicato le loro preferenze alimentari, dichiarando di essere intolleranti al lattosio. Nessuno dei partecipanti ha un'identità protetta. Il titolare del trattamento scopre l'errore subito dopo l'invio dell'elenco e ne informa i destinatari chiedendo loro di cancellare l'elenco.

6.3.1 Caso n. 15 — Misure in essere e valutazione del rischio

114. Avrebbero dovuto essere applicate regole rigorose per l'invio di messaggi contenenti dati personali. Occorre prendere in considerazione l'introduzione di meccanismi di controllo supplementari.

115. I rischi derivanti dalla natura, dalla sensibilità, dal volume e dal contesto dei dati personali sono bassi. I dati personali comprendono dati sensibili sulle preferenze alimentari di due dei partecipanti. Anche se l' informazione relativa all'intolleranza al lattosio è un dato sanitario, il rischio che tali dati siano utilizzati in modo dannoso dovrebbe essere considerato relativamente basso. Mentre nel caso di dati relativi alla salute si presume solitamente che la violazione possa comportare un rischio elevato per l'interessato32, nel caso di specie non è possibile individuare il rischio che la violazione comporti danni fisici, materiali o immateriali all'interessato a causa della divulgazione non autorizzata di informazioni sull'intolleranza al lattosio. Contrariamente ad altre preferenze alimentari, l'intolleranza al lattosio non può di norma essere collegata a convinzioni religiose o filosofiche. Anche la quantità di dati violati e il numero di interessati coinvolti sono molto bassi.

6.3.2 Caso n. 15 — Misure di mitigazione e obblighi

116. In sintesi, si può affermare che la violazione non ha avuto effetti significativi sugli interessati. Il fatto che il titolare del trattamento abbia contattato immediatamente i destinatari dopo essere venuto a conoscenza dell'errore può essere considerato un fattore di mitigazione.

117. Se un messaggio di posta elettronica è inviato a un destinatario errato/non autorizzato, si raccomanda al titolare del trattamento di inviare un'e-mail di follow-up, in copia nascosta, ai destinatari non corretti, scusandosi per l'errore, invitando a cancellare l'e-mail inviata erroneamente e informando i destinatari che non hanno il diritto di utilizzare ulteriormente gli indirizzi di posta elettronica loro comunicati.

118. Alla luce delle circostanze descritte, era improbabile che la violazione dei dati comportasse un rischio per i diritti e le libertà degli interessati, pertanto non si è resa necessaria alcuna notifica all'autorità di controllo o agli interessati. Tuttavia, anche una violazione dei dati di questo tipo deve essere documentata a norma dell'articolo 33, paragrafo 5.

Azioni necessarie sulla base dei rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	X	X

6.4 Caso n. 16: Errore nell'invio di corrispondenza postale

Un gruppo assicurativo offre assicurazioni auto. A tal fine, invia per posta aggiornamenti periodici sulle

32 Cfr. le Linee-guida WP 250, pag. 23.

prestazioni assicurative. Oltre al nome e all'indirizzo dell'assicurato, la lettera contiene la targa del veicolo in chiaro, gli importi del premio assicurativo per l'anno in corso e per quello successivo, il chilometraggio annuo approssimativo e la data di nascita dell'assicurato. Non sono inclusi dati sanitari ai sensi dell'articolo 9 del GDPR, né dati relativi ai pagamenti (coordinate bancarie) o dati economici e finanziari.

Le lettere sono imbustate automaticamente. A causa di un errore meccanico, due lettere destinate a contraenti diversi sono inserite in una stessa busta e inviate per posta ordinaria a uno dei due. Il contraente apre la lettera a casa e legge la lettera a lui correttamente indirizzata nonché quella erroneamente consegnata e indirizzata a un diverso contraente.

6.4.1 Caso n. 16 — Misure in essere e valutazione del rischio

119. La lettera erroneamente consegnata contiene il nome, l'indirizzo, la data di nascita, il numero di immatricolazione in chiaro del veicolo e la classe attribuita per il premio assicurativo dell'anno in corso e dell'anno successivo. Gli effetti sulla persona interessata devono ritenersi di media entità, in quanto sono comunicate a una persona non autorizzata informazioni non accessibili al pubblico, quali la data di nascita o i numeri di immatricolazione in chiaro dei veicoli, nonché i dettagli relativi all'aumento del premio assicurativo. La probabilità di un uso improprio di questi dati è da valutarsi tra bassa e media. Tuttavia, mentre molti destinatari probabilmente cestineranno la lettera ricevuta per errore, non si può escludere del tutto che, in determinati casi, la lettera sia pubblicata sui social network o che l'assicurato sia contattato.

6.4.2 Caso n. 16 — Misure di mitigazione e obblighi

120. Il titolare del trattamento deve chiedere che, a sue spese, gli sia reinviato il documento originale. Inoltre, dovrebbe informare il destinatario errato del fatto che non può utilizzare in modo improprio le informazioni cui ha avuto accesso.

121. Probabilmente non sarà mai possibile prevenire del tutto errori di spedizione in una postalizzazione massiva effettuata in forma completamente automatizzata. Tuttavia, se tali errori avvengono con una certa frequenza, è necessario verificare se i dispositivi di imbustamento siano impostate e sottoposte a manutenzione in modo corretto o se vi siano altri problemi di natura sistemica alla base della violazione.

Azioni necessarie sulla base dei rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	✓	X

6.5 Misure organizzative e tecniche per prevenire/attenuare gli effetti di un'errata postalizzazione

122. L'applicazione congiunta delle misure indicate di seguito, in funzione delle caratteristiche specifiche del caso, dovrebbe contribuire a ridurre le probabilità del ripetersi di eventi analoghi.

123. Misure consigliate:

(L'elenco delle seguenti misure non è da considerarsi assolutamente esaustivo né tassativo. L'obiettivo è piuttosto quello di fornire suggerimenti di prevenzione e possibili soluzioni. Ogni attività di trattamento è diversa, pertanto il titolare del trattamento dovrebbe decidere quali misure siano più idonee nella specifica situazione.)

- Definizione di standard specifici — che non lascino spazi all'interpretazione — per l'invio di lettere/e-mail.
- Formazione adeguata del personale sull'invio di lettere/e-mail.
- Quando si inviano messaggi di posta elettronica a più destinatari, questi sono inseriti nel campo "Ccn" per impostazione predefinita.
- Necessità di una conferma supplementare prima di inviare messaggi di posta elettronica a più destinatari senza inserirli nel campo "Ccn".
- Applicazione del principio del doppio livello di controllo.

- Inserimento automatico anziché manuale dei recapiti, con dati estratti da una banca dati disponibile e aggiornata; il sistema di inserimento automatico dovrebbe essere riesaminato periodicamente per verificare eventuali errori nascosti e impostazioni errate.
- Applicazione della funzionalità di invio ritardato (che consente di cancellare/modificare il messaggio entro un determinato periodo di tempo dopo aver premuto il pulsante "Invio").
- Disabilitazione del completamento automatico quando si digitano indirizzi e-mail.
- Sessioni di sensibilizzazione sugli errori più comuni che generano una violazione dei dati personali.
- Sessioni di formazione e manuali sulla gestione di incidenti che generano una violazione dei dati personali, compresa l'indicazione dei soggetti da informare (coinvolgimento del responsabile della protezione dei dati).

7 ALTRI CASI — INGEGNERIA SOCIALE (*Social Engineering*)

7.1 Caso n. 17: Furto d'identità

Il centro di contatto di un'impresa di telecomunicazioni riceve una telefonata da una persona che si presenta come cliente. Il presunto cliente chiede alla società di modificare l'indirizzo e-mail al quale inviare le informazioni di fatturazione. L'operatore convalida l'identità del cliente chiedendo alcuni dati personali, quali definiti dalle procedure dell'impresa. Il chiamante indica correttamente il codice fiscale e l'indirizzo postale del cliente (perché ha avuto accesso a tali informazioni). Dopo la convalida, l'operatore effettua la modifica richiesta e, successivamente, le informazioni di fatturazione sono inviate al nuovo indirizzo e-mail. La procedura non prevede alcuna notifica al precedente contatto e-mail. Il mese successivo il cliente legittimo contatta la società, chiedendo perché non riceva la fattura al suo indirizzo di posta elettronica, e nega qualsiasi richiesta da parte sua di modificare l'email di contatto. La società si rende conto che le informazioni sono state inviate a un utente illegittimo e annulla la modifica.

7.1.1 Caso n. 17 — Valutazione del rischio, misure di mitigazione e obblighi

124. Questo caso ben esemplifica l'importanza delle misure preventive. La violazione presenta un elevato livello di rischio33, in quanto i dati di fatturazione possono fornire informazioni sulla vita privata dell'interessato (ad esempio, abitudini, contatti) e potrebbero causare danni materiali (ad esempio stalking, rischio per l'integrità fisica). I dati personali ottenuti durante l'attacco possono essere utilizzati anche per facilitare l'acquisizione di account all'interno della specifica organizzazione o per testare ulteriori misure di autenticazione in altre organizzazioni. Tenuto conto di tali rischi, la soglia di "adeguatezza" delle misure di autenticazione dovrebbe essere fissata a un livello elevato in rapporto alla natura dei dati personali cui è possibile accedere una volta effettuata l'autenticazione.

125. Di conseguenza, sono necessarie sia una notifica all'autorità di controllo sia una comunicazione all'interessato da parte del titolare del trattamento.

126. È chiaro che il processo di convalida preventiva del cliente necessita di perfezionamenti, alla luce di questo caso. I metodi utilizzati per l'autenticazione non erano sufficienti. La parte malintenzionata è riuscita a fingere di essere l'utente legittimo utilizzando informazioni pubblicamente disponibili e altre informazioni cui aveva altrimenti accesso.5

127. Non si raccomanda l'uso di questa forma di autenticazione statica basata su elementi di conoscenza (in cui la risposta non cambia e non ci sono informazioni "segrete", come invece sarebbe nel caso di una password).

128. L'organizzazione dovrebbe invece utilizzare una forma di autenticazione altamente affidabile quanto alla dimostrazione che l'utente autenticato sia realmente chi afferma di essere, e non altri. L'introduzione di un metodo di autenticazione a più fattori fuori banda risolverebbe il problema, ad esempio per verificare

eventuali richieste di variazioni, attraverso l'invio di una richiesta di conferma al precedente indirizzo di contatto; oppure aggiungendo ulteriori domande di controllo e chiedendo informazioni presenti solo sulle fatture precedenti. Spetta al titolare del trattamento decidere quali misure introdurre, in quanto conosce meglio di chiunque altro i dettagli e le esigenze della sua operatività interna.

Azioni necessarie sulla base dei rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	✓	✓

[33] Per indicazioni *sui trattamenti "che possono comportare un rischio elevato"*, cfr. la precedente nota 10.

7.2 Caso n. 18: Esfiltrazione di e-mail

Una catena di ipermercati ha rilevato, 3 mesi dopo la configurazione, che alcuni account di posta elettronica erano stati modificati attraverso la creazione di regole per cui ogni e-mail contenente determinate espressioni (ad esempio "fattura", "pagamento", "bonifico bancario", "autenticazione della carta di credito", "coordinate bancarie") veniva trasferita in una cartella non utilizzata e trasmessa anche a un indirizzo di posta elettronica esterno. Inoltre, a quella data, era già stato commesso un attacco di ingegneria sociale, vale a dire che l'attaccante, che fingeva di essere un fornitore, aveva modificato le coordinate bancarie di tale fornitore sostituendovi le proprie. Infine, a quella data, erano state inviate diverse fatture false che includevano i nuovi dati relativi alle coordinate bancarie. Il sistema di monitoraggio della piattaforma di posta elettronica aveva segnalato, in ultima istanza, un problema sulle cartelle. La società non è stata in grado di individuare in che modo l'attaccante fosse riuscito ad accedere agli account di posta elettronica, ma ha ritenuto che attraverso un'email infetta fosse avvenuto l'accesso al gruppo di utenti incaricati dei pagamenti.

A seguito della trasmissione di e-mail contenenti determinate parole-chiave, l'attaccante ha ricevuto informazioni su 99 dipendenti: nome e salario riferito a uno specifico mese per 89 soggetti; nome, stato civile, numero di figli, retribuzione, ore di lavoro e altre informazioni sulla retribuzione di 10 dipendenti il cui contratto era terminato. Il titolare ha comunicato la violazione soltanto ai 10 dipendenti appartenenti a quest'ultimo gruppo.

7.2.1 Caso n. 18 — Valutazione del rischio, misure di mitigazione e obblighi

129. Anche se l'attaccante non mirava probabilmente a raccogliere dati personali, la violazione potrebbe comportare sia un danno materiale (ad esempio, perdite finanziarie) che un danno immateriale (ad esempio furto o usurpazione di identità), e i dati potrebbero essere utilizzati per facilitare altri attacchi (ad esempio phishing); pertanto, la violazione potrebbe comportare un rischio elevato per i diritti e le libertà delle persone fisiche e dovrebbe essere comunicata a tutti i 99 dipendenti e non solo ai 10 dei quali sono state divulgate le retribuzioni.

130. Una volta venuto a conoscenza della violazione, il titolare del trattamento ha forzato la modifica della password per gli account compromessi, ha bloccato l'invio di e-mail all'account dell'attaccante, ha informato il fornitore del servizio di posta elettronica utilizzato dall'autore dell'attacco in merito alle azioni compiute da quest'ultimo, ha rimosso le regole stabilite dall'attaccante e perfezionato le segnalazioni del sistema di monitoraggio così da generare una segnalazione non appena venga creata una regola automatica. In alternativa, il titolare del trattamento potrebbe eliminare il diritto degli utenti di stabilire regole sull'inoltro dei messaggi di posta elettronica, prevedendo la necessità di un intervento del team del servizio informatico su specifica richiesta, oppure potrebbe introdurre una politica in base alla quale gli utenti dovrebbero verificare e comunicare le regole stabilite sui loro account una volta alla settimana o con maggiore frequenza, nei settori che trattano dati finanziari.

131. Il fatto che una violazione abbia potuto verificarsi e sfuggire al rilevamento per un periodo così prolungato, e la circostanza per cui, se la violazione fosse proseguita, le tecniche di ingegneria sociale avrebbero consentito di modificare un volume di dati ancora più consistente, evidenziano notevoli criticità nel sistema di sicurezza informatica del titolare del trattamento. Tali criticità dovrebbero essere affrontate senza indugio, ad esempio rivedendo le procedure automatizzate e le verifiche dei cambiamenti, le misure di rilevazione degli incidenti e di risposta agli incidenti. I titolari del trattamento di dati sensibili, informazioni finanziarie, ecc. hanno maggiori responsabilità nel garantire un'adeguata sicurezza dei dati.

Azioni necessarie sulla base dei rischi individuati			
	Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
	✓	✓	✓