Dipartimento
per le Politiche Giovanili
e il Servizio Civile Universale
Presidenza del Consiglio dei Ministri

Atto di designazione del Responsabile del trattamento dei dati personali ai sensi dell'art. 28 del Regolamento (UE) 2016/679 – GDPR

VISTA la legge 23 agosto 1988, n. 400, recante disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei ministri;

VISTA la legge 8 luglio 1998, n. 230, recante "*Nuove norme in materia di obiezione di coscienza*", e successive modificazioni ed integrazioni, in particolare gli articoli 8 e 19 che istituiscono presso la Presidenza del Consiglio dei ministri, rispettivamente, l'Ufficio nazionale per il servizio civile, successivamente confluito nel Dipartimento per le politiche giovanili e il servizio civile universale, e il Fondo nazionale per il servizio civile;

VISTA la legge 6 marzo 2001, n. 64, concernente "*Istituzione del servizio civile nazionale*" e successive modificazioni ed integrazioni;

VISTO il decreto del Presidente del Consiglio dei ministri in data 1° ottobre 2012, recante "*Ordinamento delle strutture generali della Presidenza del Consiglio dei ministri*", e s.m.i., da ultimo modificato con decreto del Presidente del Consiglio dei ministri 28 maggio 2020, che, all'articolo 15, definisce le competenze del Dipartimento per le politiche giovanili e il Servizio civile universale;

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;

VISTO il decreto legislativo 6 marzo 2017, n. 40, recante "*Istituzione e disciplina del servizio civile universale, a norma dell'articolo 8 della legge 6 giugno 2016, n. 106*" e successive modificazioni ed integrazioni;

VISTO il decreto del Presidente del Consiglio dei ministri in data 25 maggio 2018, recante *"Criteri e modalità per l'individuazione del responsabile della protezione dei dati personali, mediante il quale la Presidenza del Consiglio dei ministri esercita le funzioni di titolare del trattamento dei dati personali, ai sensi del regolamento (UE) n. 2016/679"* con il quale, all'articolo 3, vengono designati i Capi dei Dipartimenti, ciascuno nel rispettivo ambito di competenza, per l'esercizio delle predette funzioni di titolare del trattamento dei dati personali;

VISTO il Decreto del Presidente del Consiglio dei ministri 19 novembre 2021 recante: *"Modifiche al decreto del Presidente del Consiglio dei ministri 25 maggio 2018, concernente criteri e modalità per l'individuazione del responsabile della protezione dei dati personali,*

mediante il quale la Presidenza del Consiglio dei ministri esercita le funzioni di titolare del trattamento dei dati personali, ai sensi del regolamento";

CONSIDERATO che per l'attuazione del sistema del servizio civile, di cui al citato decreto legislativo 6 marzo 2017, n. 40 e s.m.i., la Presidenza del Consiglio dei ministri - Dipartimento per le politiche giovanili e il Servizio civile universale, deve provvedere alle attività di selezione e di gestione degli operatori volontari di servizio civile;

CONSIDERATO che, ai sensi del d.lgs. n.40/2017, le predette attività di selezione e di gestione dei volontari di servizio civile sono svolte tramite gli enti iscritti all'Albo degli enti di servizio civile universale;

CONSIDERATO, altresì, che dette attività richiedono il trattamento di dati personali, ai sensi del Regolamento (UE) 2016/679;

VISTO l'art. 4, paragrafo 1, n. 8) del Regolamento, che identifica il Responsabile del trattamento nella "*persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*";

VISTO l'art. 28, paragrafo 1, del Regolamento, secondo cui "*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 che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato*";

VISTO l'art. 28, paragrafo 2, del Regolamento, in base al quale "*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*";

CONSIDERATO che il Dipartimento per le Politiche Giovanili e il Servizio Civile Universale utilizza la piattaforma informatica *Helios* per la raccolta della documentazione inerente al Sistema di Servizio Civile Universale;

VISTO il Decreto del Capo Dipartimento n.705 del 29 luglio 2022 con il quale è stato adottato il Disciplinare per la protezione dei dati nell'ambito del Servizio Civile Universale (di seguito "Disciplinare");

VISTA la richiesta di iscrizione/l'iscrizione all'Albo degli enti di servizio civile universale in dell'ente titolare_____ eventualmente anche in forma associata con altri soggetti (enti di accoglienza);

CONSIDERATA l'idoneità del Sig. _____ (in qualità di Responsabile del trattamento dei dati) rispetto alle garanzie richieste dalla normativa regolamentare europea con riferimento all'adeguatezza delle misure tecniche e organizzative per la tutela dei diritti dell'interessato;

VISTO il decreto del Segretario generale della Presidenza del Consiglio dei ministri del 27 giugno 2025, regolarmente registrato dall'UBRRAC con il visto n. 2256 apposto in data 1° luglio 2025, con il quale le funzioni vicarie di Capo del Dipartimento sono state attribuite alla dott.ssa Laura Massoli, già coordinatrice dell'Ufficio per il servizio civile universale nell'ambito del Dipartimento medesimo, al fine di assicurare la continuità dei compiti della struttura;

le premesse formano parte integrante e sostanziale del presente atto:

la Presidenza del Consiglio dei ministri, con sede in Roma – Palazzo Chigi, Piazza Colonna n.370, codice fiscale 80188230587, in persona della dott.ssa Laura Massoli, Dirigente generale con funzioni vicarie di Capo del Dipartimento per le politiche giovanili e il Servizio civile universale, ex art. 3, comma 1, lett. b) del DPCM 25 maggio 2018, domiciliata per la carica presso la sede legale, in qualità di Titolare del trattamento, ai sensi dell'art. 28 del Regolamento.

DESIGNA

l'ente _____ (*indicare il nome dell' ente*), in fase di iscrizione/iscritto all'Albo degli enti di servizio civile universale come ente titolare, con sede legale in_____, codice fiscale _____, in persona del Sig. _____, in qualità di _____, [1] codice fiscale _____, quale Responsabile del trattamento dati, *ex* art. 28 del Regolamento.

A tale riguardo, il *Responsabile*, accettando la presente designazione:

- conferma la sua diretta e approfondita conoscenza degli obblighi che si assume in relazione a quanto disposto dal Regolamento e, più in generale, dalle Norme in materia di protezione dei dati personali;
- si obbliga a procedere al trattamento dei dati necessari all'esecuzione delle attività di competenza, nel rispetto della vigente normativa, dei provvedimenti dell'Autorità di Controllo, delle indicazioni del Titolare di cui al presente atto e relativi allegati, nonché di ogni altra istruzione comunque impartita dal Titolare che vigilerà sulla loro puntuale osservanza.

[1] In caso di nomina di un soggetto diverso dal Rappresentante Legale, al presente documento deve essere allegato l'atto di designazione per lo svolgimento di tale ruolo.

Con il presente atto di designazione il citato ente, in fase di iscrizione/iscritto all'Albo degli enti di servizio civile universale come ente titolare e *Responsabile*, è autorizzato, in via generale, a ricorrere, se presenti, agli "**enti di accoglienza**" iscritti presso il medesimo Albo in qualità di ***sub-Responsabili* del trattamento** dei dati *ex* art. 28, paragrafo 2 del Regolamento, previa autorizzazione del Titolare.

Il *Responsabile* verifica periodicamente l'adozione di misure tecniche organizzative e gestionali adeguate a garantire il rispetto della vigente normativa. Nel caso in cui, per l'esecuzione delle attività relative ai progetti finanziati, il *Responsabile* intenda ricorrere ad altro *sub-Responsabile* in aggiunta agli enti di accoglienza di cui sopra, deve informare il Titolare, ai sensi dell'art. 28, paragrafo 2 del Regolamento, al fine di consentirgli l'eventuale opposizione, ferma restando la necessità di un accordo scritto tra *Responsabile* e *sub-Responsabile*, nel rispetto dell'art. 28, paragrafo 4 del medesimo regolamento.

Di seguito sono definite le istruzioni di carattere generale, che possono essere integrate e modificate per iscritto dal Titolare.

ISTRUZIONI

1. Elementi essenziali dei trattamenti che il Responsabile è autorizzato a svolgere

Il *Responsabile* è autorizzato a trattare, per conto del Titolare, tutti i dati personali necessari per la corretta esecuzione delle attività connesse all'attuazione del servizio civile universale e alle relative finalità, come previste dal d.lgs. n. 40/2017 e dal Disciplinare.

La durata del trattamento, con riferimento alla documentazione caricata sul sistema Helios, coincide con la durata dei singoli progetti, ovvero di loro eventuali proroghe, fatti salvi gli adempimenti richiesti da specifici obblighi di legge o da documentate istruzioni impartite dal Titolare ed è finalizzata all'adempimento degli obblighi assunti con la realizzazione dei progetti stessi.

Fermo restando che, in attuazione del **principio della minimizzazione**, di cui al GDPR, i dati vanno conservati per il tempo strettamente necessario, che il Titolare valuta in relazione alle specifiche esigenze, ulteriori documenti contenenti dati personali, comunque acquisiti dall'ente *Responsabile* e dal sub Responsabile (a titolo esemplificativo e non esaustivo, fogli firma dei volontari, ordini di servizio, turnazioni, certificazioni sanitarie, scambi di e-mail ecc.) di cui il Dipartimento non ha contezza o non possiede copia, devono essere conservati dall'ente medesimo, *Responsabile* o sub responsabile, per un periodo di anni 10 (dieci) per essere resi disponibili a prima richiesta del Titolare.

È fatta salva l'eventuale durata superiore di conservazione degli atti fissata dalle Pubbliche Amministrazioni che partecipano al Servizio civile universale.

Il Dipartimento si impegna a creare le condizioni operative per consentire la completa dematerializzazione della gestione documentale degli operatori volontari promuovendo, in via pressoché esclusiva, l'utilizzo degli strumenti telematici così da ridurre gli oneri della conservazione.

I dati personali trattati possono essere ai sensi del GDPR, i seguenti:

- dati anagrafici dei rappresentanti legali dell'ente;
- dati anagrafici delle persone fisiche facenti parte della struttura organizzativa dell'ente, anche al fine dello svolgimento dei controlli svolti dal Dipartimento ai sensi della vigente normativa antimafia;
- dati anagrafici e di esperienza professionale (CV) dei candidati;
- dati anagrafici degli operatori volontari;
- dati anagrafici, dati di genere (uomo/donna), codice fiscale, numero telefonico, indirizzo mail, titolo di studio, codice IBAN per pagamenti (dati inseriti nella scheda personale dell'operatore volontario nel Sistema Unico di SCU);
- certificazioni mediche per malattia, L.104/92, maternità, covid-19, nelle modalità stabilite dalla normativa vigente.

Le categorie di interessati sono:

- i candidati al bando per la selezione di operatori volontari da impiegare in progetti di servizio civile universale;
- gli operatori volontari di servizio civile;
- eventuali beneficiari diretti delle attività progettuali di servizio civile laddove specificatamente individuati.
- qualunque persona fisica che possa essere identificata, direttamente o indirettamente, con particolare riferimento ad un dato 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, genetica, psichica, economica, culturale, sociale o politica nell'ambito del Sistema di servizio civile universale.

2. Obblighi del Responsabile del trattamento nei confronti del Titolare e limiti e termini del trattamento dei dati personali

Il *Responsabile* è tenuto a trattare i dati personali solo in relazione alle attività di competenza, ossia nei limiti necessari per lo svolgimento delle attività connesse all'attuazione del servizio civile universale e alle relative finalità, come previste dal d.lgs. n. 40/2017 e dal Disciplinare, secondo le indicazioni ricevute dal Titolare.
Il *Responsabile* è tenuto a garantire che il trattamento dei dati personali, per quanto di propria competenza, sia effettuato in modo lecito e secondo correttezza, nel rispetto dei principi di cui all'art. 5 del Regolamento.

Il *Responsabile*, qualora intenda trattare i dati personali per finalità ultronee al servizio civile deve chiederne esplicito consenso all'interessato, specificando la propria posizione di Titolare del trattamento, nonché fornire idonea e adeguata informativa all'interessato medesimo nella quale vengano specificate le finalità e la liceità del trattamento. In mancanza di detto consenso, ogni attività di trattamento deve ritenersi inibita.

2.1 Istruzioni del Titolare

Il *Responsabile* non può trasferire i dati personali verso un paese terzo o un'organizzazione internazionale, salvo che non abbia preventivamente ottenuto un'**autorizzazione scritta** del Titolare.
Tale autorizzazione, con la sottoscrizione del presente atto, si intende concessa al *Responsabile*, e quindi ai suoi Sub-Responsabili individuati nei propri enti di accoglienza, **solo** in tutti quei casi in cui questi ultimi, in base al progetto da realizzare, ne abbiano necessità per il corretto espletamento delle attività di competenza.
Anche nelle ipotesi in cui, ai sensi della vigente normativa nazionale o dell'Unione europea, il responsabile sia obbligato a trasferire dati personali verso un paese terzo o un'organizzazione internazionale, il *Responsabile* è tenuto ad **informare il Titolare** circa tale obbligo giuridico, prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico.
Ove il *Responsabile* rilevi la sua impossibilità a rispettare le istruzioni impartite dal Titolare deve attuare, comunque, le possibili e ragionevoli **misure di salvaguardia** e deve avvertire immediatamente il Titolare e concordare eventuali ulteriori **misure di protezione**.
Qualora il *Responsabile* ritenga che una delle istruzioni violi il Regolamento o altre disposizioni nazionali o comunitarie deve informare immediatamente il Titolare.

2.2 Fornitura dei dati al Titolare

Le richieste di fornitura di documenti da acquisire in esecuzione di attività ispettive e/o di controllo, anche da remoto, devono essere evase contestualmente alla richiesta, fatti salvi impedimenti di natura tecnica o fisica (a titolo esemplificativo e non esaustivo, archivio documentale posto in un sito diverso dalla sede di ispezione) che dovranno essere motivati per iscritto, e non soggiacciono a formalità specifiche. Qualora, per motivi diversi dalle attività ispettive e/o di controllo, il Titolare o soggetto da esso incaricato abbia necessità, per lo svolgimento dei propri compiti istituzionali, di accedere a dati non disponibili attraverso i servizi applicativi, può richiederli per iscritto al *Responsabile,* il quale è tenuto a renderli disponibili nel più breve tempo possibile.

2.3 Registro dei trattamenti

Il *Responsabile* tiene un Registro di tutte le categorie di attività relative al trattamento (o ai trattamenti) svolto per conto del *Titolare,* mediante l'adozione del modello allegato.
Il *Responsabile* ed il *Titolare* devono assicurare la coerenza reciproca dei propri Registri.
Il *Responsabile* mette a disposizione dell'Autorità di controllo il Registro, ove richiesto, dandone al contempo informazione al *Titolare*.

2.4 Autorità di controllo

Il *Responsabile* è tenuto in ogni caso a cooperare, su richiesta, con l'Autorità di controllo nell'esecuzione dei suoi compiti.
Il *Responsabile* si obbliga a cooperare con il *Titolare* al fine di fornire tutte le informazioni, i dati e la documentazione necessaria affinché il *Titolare* possa adempiere alle richieste dell'Autorità di controllo ovvero qualora si rendessero necessarie informazioni in caso di precontenzioso o contenzioso.

2.5 Comunicazione e diffusione di dati

Il *Responsabile* non può comunicare e/o diffondere dati senza l'esplicita autorizzazione del *Titolare*, fatte salve le comunicazioni di dati personali necessarie alla realizzazione diretta di attività progettuali (a titolo esemplificativo non esaustivo, acquisto titoli di viaggio nominativi) per le quali il consenso è stato raccolto in sede di avvio al servizio civile del volontario, nonché le particolari esigenze di riservatezza espressamente esplicitate dall'Autorità Giudiziaria.

2.6 Ricorso a Sub-Responsabili del trattamento

Il *sub-Responsabile* del trattamento, dovrà rispettare gli obblighi in materia di protezione dei dati personali imposti al *Responsabile* dalla normativa in materia di protezione dei dati personali e dal *Titolare* con il presente atto e le eventuali ulteriori istruzioni documentate che lo stesso dovesse impartire.
Al *sub-Responsabile*, verranno imposti i medesimi obblighi e le medesime istruzioni ricevute dal *Titolare*. Il Responsabile del trattamento verifica periodicamente l'adozione di misure tecniche organizzative e gestionali adeguate a garantire il rispetto della vigente normativa.
Qualora il *sub-Responsabile* ometta di adempiere ai propri obblighi in materia di protezione dei dati, il *Responsabile iniziale del trattamento* conserva nei confronti del *Titolare* l'intera responsabilità dell'adempimento degli obblighi del *sub-Responsabile*.
Il *Responsabile* si impegna a informare preventivamente il *Titolare* di eventuali modifiche riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento dando così al *Titolare* l'opportunità di opporsi a tali modifiche.
Il *Responsabile* si impegna comunque a rispettare le condizioni di cui ai paragrafi 2 e 4 dell'art. 28 del Regolamento, per quanto applicabili.

2.7 Riservatezza e formazione delle persone autorizzate al trattamento

Il Responsabile garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza e che siano adeguatamente formate in relazione alle Norme in materia di protezione dei dati personali e pienamente edotte rispetto alle istruzioni impartite dal Titolare.

2.8 Obblighi del Responsabile nell'ambito dei diritti esercitati dagli Interessati

Il *Responsabile*, ove richiesto, deve collaborare e supportare nel dare riscontro scritto, anche di

mero diniego, alle istanze trasmesse dagli *Interessati* nell'esercizio dei diritti previsti dagli. artt.15-23 del GDPR, vale a dire alle istanze per l'esercizio del diritto di accesso, di rettifica, di integrazione, di cancellazione e di opposizione, diritto alla limitazione del trattamento, diritto alla portabilità dei dati, diritto a non essere oggetto di un processo decisionale automatizzato, compresa la profilazione.
Qualora gli interessati trasmettano la richiesta per l'esercizio dei loro diritti al *Responsabile*, quest'ultimo deve inoltrarla tempestivamente al *Titolare*.

2.9 Misure di sicurezza

Il *Responsabile*, sulla base delle indicazioni del *Titolare*, adotta le misure richieste dall'art. 32 del Regolamento. Al fine di ridurre e mantenere, per quanto più possibile, al minimo i rischi e i pericoli derivanti dal trattamento dei dati personali, il *Responsabile*, fatto salvo quanto previsto al par. 2.7, si impegna ad individuare le misure tecniche e organizzative più adeguate da mettere in atto nel rispetto dei vincoli del presente *Atto di designazione* e sulla base delle indicazioni del *Titolare* di cui all'allegato **documento di policy**, recante gli standard di sicurezza minimi, con riferimento anche all'adeguatezza delle misure tecniche e organizzative per la tutela dei diritti dell'interessato, in modo tale che il trattamento soddisfi i requisiti del *Regolamento* e garantisca la tutela dei diritti degli interessati.

2.10 Cancellazione e distruzione dei dati

Fermo restando quanto previsto dall'articolo 1, il *Titolare*, terminato il progetto di servizio civile relativo al trattamento, ottiene in qualunque momento, e comunque entro sei mesi, dal Responsabile del Trattamento la cancellazione o la restituzione di tutti i dati personali e la cancellazione totale di tutte le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati.

2.11 Ispezioni e revisione

Il *Responsabile* mette a disposizione del *Titolare* tutte le informazioni necessarie per dimostrare il rispetto degli obblighi a suo carico, consente e contribuisce alle attività di revisione, comprese le ispezioni, realizzate dal *Titolare* o da altro soggetto da questi incaricato, anche attraverso periodiche attività di *audit*, con modalità che saranno, di volta in volta, concordate.

2.12 Codici di condotta

Nel caso in cui il *Responsabile* aderisca a un codice di condotta approvato ai sensi dell'articolo 40 del *Regolamento* o a un meccanismo di certificazione approvato ai sensi dell'articolo 42 del *Regolamento*, tale adesione può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 dell'art. 28 del *Regolamento*.

2.13 Violazioni dei dati

Il *Responsabile* si dichiara consapevole degli obblighi che incombono sul *Titolare* del

trattamento, ai sensi dell'art. 33 del *Regolamento*, in caso di violazione dei dati che sia tale da presentare un rischio per i diritti e le libertà fondamentali delle persone.
Il *Responsabile* si impegna a comunicare al *Titolare* la violazione dei dati personali "senza ingiustificato ritardo", ai sensi e nei termini previsti dall'art. 33 del *Regolamento*. Tale obbligo di cooperazione si impone anche nel caso in cui il *Titolare* debba comunicare la violazione all'interessato.
In ogni caso, il Responsabile si impegna ad adottare le linee guida della PCM in caso di violazione dei dati.

2.14 Modifiche normative

Nell'eventualità di qualsiasi modifica delle *Norme in materia di protezione dei dati personali*, il *Responsabile* supporta, nel rispetto dei vincoli del presente atto di designazione e nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse, il *Titolare* negli adeguamenti necessari.

3. Rinvio

Per tutto quanto non espressamente disciplinato nel presente atto, si richiamano gli obblighi previsti a carico del *Responsabile* dalla normativa in materia di protezione dei dati personali.

(Data) _____

PRESIDENZA
DEL CONSIGLIO DEI MINISTRI
Il Dirigente Generale con funzioni
vicarie di Capo del Dipartimento per
le politiche giovanili e il Servizio
civile universale
Dott.ssa Laura MASSOLI

Firmato digitalmente da
MASSOLI LAURA
C=IT
O=PRESIDENZA
CONSIGLIO DEI MINISTRI

Per accettazione
(Responsabile del trattamento
dei dati personali)

Allegati
- 1. Policy recante gli standard minimi di sicurezza informatica
- 2. Scheda registro dei trattamenti
- 3. Linee guida per la gestione delle violazioni di dati personali (data breach) in PCM

Allegato 1

Policy recante gli standard minimi di sicurezza informatica

1. Premessa

Il Dipartimento delle politiche giovanili e il Servizio civile universale, analizzate le misure di cui alla Circolare AGID del 18 aprile 2017, n. 2/2017 pubblicata sulla Gazzetta Ufficiale, serie generale n. 103 del 5 maggio 2017, valutato il contesto tecnico ed organizzativo in cui opera il servizio civile universale, definisce il presente documento di policy per l'adozione delle misure di sicurezza informatica nella formulazione **minima,** per ridurre l'impatto dell'applicazione sugli enti di servizio civile universale a cui la policy si applica.

Il *Responsabile* e il s*ub Responsabile* del trattamento dei dati personali sono tenuti a recepire le misure indicate nel presente documento di policy, al fine di ridurre e mantenere, per quanto più possibile, al minimo i rischi e i pericoli derivanti dal trattamento stesso.

Il documento individua linee di intervento specifiche la cui implementazione si rende necessaria anche per la tutela dei diritti dell'interessato

2. Misure minime di sicurezza ICT

Le misure, in piena conformità con l'enunciazione formulata dall'AgID, vengono articolate nei seguenti item generali "AgID Basic Security Control(s)" (ABSC):

- ABSC1(CSC1): inventario dei dispositivi autorizzati e non autorizzati;
- ABSC2(CSC2): inventario dei software autorizzati e non autorizzati;
- ABSC3(CSC3): proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server;
- ABSC4(CSC4): valutazione e correzione continua della vulnerabilità;
- ABSC5(CSC5): uso appropriato dei privilegi di amministratore;
- ABSC8(CSC8): difese contro i malware;
- ABSC10(CSC10): copie di sicurezza;
- ABSC13(CSC13): protezione dei dati.

Per ogni linea di intervento sono individuate le sole misure definite minime da applicare:

ABSC1(CSC1): inventario dei dispositivi autorizzati e non autorizzati

- Implementare un inventario delle risorse attive correlato a quello ABSC 1.4
- Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.
- Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.

ABSC 2 (CSC 2): inventario dei software autorizzati e non autorizzati

- Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.
- Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.

ABSC 3 (CSC 3): proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server

- Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.
- Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.
- Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.
- Le immagini d'installazione devono essere memorizzate offline.
- Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).

ABSC 4 (CSC 4): valutazione e correzione continua della vulnerabilità

- Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.
- Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.
- Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.
- Assicurare l'aggiornamento dei sistemi separati dalla rete adottando misure adeguate al loro livello di criticità.
- Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.
- Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).
- Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare, applicare le patch per le vulnerabilità a partire da quelle più critiche.

ABSC 5 (CSC 5): uso appropriato dei privilegi di amministratore

- Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.
- Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.
- Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.
- Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.
- Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).
- Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).
- Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).
- Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.
- Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.
- Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.
- Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.
- Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.

ABSC 8 (CSC 8): difese contro i malware

- Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.
- Installare su tutti i dispositivi firewall ed IPS personali.
- Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.
- Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.
- Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.
- Disattivare l'apertura automatica dei messaggi di posta elettronica.
- Disattivare l'anteprima automatica dei contenuti dei file.
- Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.
- Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.
- Filtrare il contenuto del traffico web.

- Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).

ABSC 10 (CSC 10): copie di sicurezza

- Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.
- Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.
- Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.

ABSC 13 (CSC 13): protezione dei dati

- Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica
- Bloccare il traffico da e verso url presenti in una blacklist.

3. Sicurezza fisica dei luoghi

Le norme prevedono che i luoghi in cui sono presenti le infrastrutture informatiche o comunque postazioni che trattano dati personali devono essere protetti da accessi non autorizzati anche dal punto di vista fisico. Nel caso di luoghi in cui sono presenti server o infrastrutture di rete i locali devono essere chiusi a chiave e deve essere registrato ogni accesso di personale riportando ora e data nel registro suddetto.

Anche le stanze in cui avviene un trattamento dati devono essere dotate di chiave e normalmente chiuse. Occorre, inoltre, dotarle di un registro degli accessi per le persone che normalmente non sono autorizzate ad entrare e non devono accedere ai dati presenti sugli apparati informatici.

4. Responsabilità

Il *Responsabile* e il s*ub Responsabile* del trattamento dei dati personali hanno la responsabilità dell'attuazione delle misure minime di cui al presente documento.

Il *Responsabile* e il s*ub Responsabile* hanno l'obbligo di compilare annualmente il modulo di implementazione delle misure minime in cui si descrive le azioni intraprese per l'adeguamento a quanto indicato nel presente documento di policy. Il modulo è costituito da una checklist che, firmata digitalmente deve essere inviata al Dipartimento.

DIPARTIMENTO PER LE POLITICHE GIOVANILI E IL SERVIZIO CIVILE UNIVERSALE

Allegato 2

SCHEDA REGISTRO DEI TRATTAMENTI DEL RESPONSABILE/SUB-RESPONSABILE			
per i contenuti vedi Faq sul registro delle attività di trattamento: https://www.garanteprivacy.it/regolamentoue/registro			
RESPONSABILE *[inserire la denominazione e i* ***dati di contatto: indirizzo, email, tel., pec, ecc.]***			
TITOLARE/CONTITOLARE/RAPPRESENTANTE DEL TITOLARE *inserire la denominazione e i* ***dati di contatto: indirizzo, email, tel., pec, ecc.***			
RESPONSABILE DELLA PROTEZIONE DEI DATI *[inserire la denominazione e i dati di contatto]*			
CATEGORIA DI TRATTAMENTO	**TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI** *[indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]*	**MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE**	**NOMI DEI SOGGETTI ADDETTI AL TRATTAMENTO DEI DATI**
Il Registro dell'Ente **in qualità di Responsabile** deve contenere tutte le categorie di attività relative al trattamento svolti per conto del Titolare; i dati minimi sono quelli indicati all'art. 30, paragrafo 2 del GDPR (denominazione + dati contatto responsabile, denominazione + dati contatto del titolare del cui trattamento è responsabile, del rappresentante del titolare e del suo RPD, le categorie di trattamento, eventuali trasferimenti verso Paesi terzi e le misure di sicurezza tecniche e organizzative). Possono, inoltre, essere inserite indicazioni aggiuntive, anche per assicurare la coerenza con il Registro del Titolare.			

Presidenza del Consiglio dei Ministri

Allegato 3

Linee guida per la gestione delle violazioni di dati personali (*data breach*) in PCM

Roma, luglio 2024, Versione 1

Revisionato e approvato dalla dott.ssa **Stefania Tilia**, Responsabile della Protezione dei Dati della Presidenza del Consiglio dei Ministri

Il presente documento è stato redatto dal **Gruppo di Supporto Privacy** della PCM:

dott.ssa **Paola Colangelo** (USG), ing. **Marco Carbonelli** (DCI), dott.ssa **Assunta Polito** (USG), dott. **Andrea Giubilei** (USG), dott. **Stefano Tribuz**i (USG)

Sommario

1 Introduzione

1.1 Premessa

Finalità del presente documento è indicare il processo di gestione delle violazioni dei dati personali (in inglese "data breach") trattati all'interno delle strutture della Presidenza del Consiglio dei ministri (art. 3 del DPCM del 25 maggio 2018) definendo i principi generali, i ruoli, le responsabilità e le attività da svolgere allorché si verifichi una violazione. Nel documento vengono date anche indicazioni per la compilazione del Registro dei data breach e per la valutazione del livello di gravità della violazione.

Il processo di gestione delle violazioni dei dati personali qui analizzato considera le due casistiche, indicate nel dettaglio nel par. 1.4, legate alla "Notifica delle violazioni e Registro dei data breach", ovvero:

- **violazioni** che, a fronte di una valutazione approfondita che escluda effetti negativi sugli interessati in termini di rischio per i diritti e le libertà delle persone fisiche, **non comportano segnalazioni al Garante o agli interessati** stessi ma necessitano di archiviazione all'interno di un "Registro dei data breach"
- **violazioni** che per i loro effetti **rendono necessaria una comunicazione al Garante e potenzialmente anche agli interessati coinvolti** nonché la registrazione all'interno di un "Registro dei data breach".

1.2 Contesto normativo e procedurale di riferimento in caso di data breach

Di seguito è riportato l'elenco degli atti e dei documenti che costituiscono il riferimento per l'analisi svolta in queste Linee guida per la gestione delle violazioni di dati personali (data breach) in PCM:

- 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
- Decreto legislativo 10 agosto 2018, n. 101 recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679
- 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
- Decreto Legislativo 30 giugno 2003 n. 196, recante il "Codice in materia di protezione dei dati personali
- Decreto legislativo 7 marzo 2005, n. 82 e successive modifiche e integrazioni (CAD-Codice dell'amministrazione digitale)
- DPCM 25 maggio 2018, novellato dal DPCM 19 novembre 2021, in particolare l'art. 9
- Linee Guida per la DPIA in PCM (versione marzo 2024)
- Linee guida 9/2022 in materia di notifica delle violazioni di dati personali (data breach) - WP 250, adottate dal Gruppo di lavoro Articolo 29 ("WP29")
- Linee guida 01/2021 in materia di notifica delle violazioni di dati personali (Examples regarding Data Breach Notification), adottate dall'European Data Protection Board (EDPB)
- Linee guida 2/2018 in materia di notifica delle violazioni di dati personali (Data Breach Notification) - WP250, adottate dal Gruppo di lavoro Articolo 29 ("WP29")
- Provvedimento n. 209 del Garante del 27 maggio 2021 sulla Procedura telematica per la notifica di violazioni di dati personali (data breach);
- Provvedimento n. 157 del Garante del 30 luglio 2019 sulla notifica delle violazioni dei dati personali

- Agenzia UE ENISA dicembre 2013, Recommendations for a methodology of the assessment of severity of personal data breaches, https://www.enisa.europa.eu/publications/dbn-severity.

1.3 Definizione di una violazione dei dati personali (data breach)

Ai sensi dell'articolo 4 («Definizioni») del Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (di seguito, "GDPR" o "Regolamento"), per violazione dei dati personali si intende «**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**» per mezzo di sistemi informatici o di altra natura.

In tale contesto, il Regolamento sancisce l'obbligo per il Titolare del trattamento di notificare tempestivamente l'avvenuta violazione dei dati personali all'autorità di controllo e, in casi determinati e con specifiche modalità, di procedere alla comunicazione direttamente agli interessati (artt. 33 e 34).

Coerentemente al Provvedimento n. 157 del Garante del 30 luglio 2019, alle Linee Guida WP250 del 3 ottobre 2017 sulla notifica delle violazioni dei dati personali ai sensi del Regolamento, nonché alle linee guida 9/2022 del Comitato europeo per la protezione dei dati (EDPB), la natura della violazione può essere classificata in base ai seguenti principi di sicurezza delle informazioni (noti come RID: Riservatezza, Integrità, Disponibilità):

• "perdita di riservatezza" (*Confidentiality Breach*): quando vi è un accesso o una diffusione accidentale o abusiva a dati personali;

• "perdita di disponibilità" (*Availability Breach*): quando vi è una perdita o distruzione accidentale o non autorizzata del dato personale;

• "perdita di integrità" *(Integrity Breach*): quando vi è un'alterazione accidentale o non autorizzata del dato personale con conseguente impossibilità di accesso, perdita, distruzione non autorizzata o accidentale del dato.

Vengono forniti, di seguito, alcuni esempi di data breach, tra i più significativi:

- furto o smarrimento di beni della PCM connesso ad un comportamento negligente di dipendenti/collaboratori, che può verificarsi nel caso in cui venga meno il controllo degli strumenti utilizzati per elaborare i dati personali (ad esempio Server, PC/laptop, smartphone, device per l'archiviazione di dati esterni);
- accesso illegale da parte di soggetti terzi, ossia accesso abusivo da parte di terzi, non autorizzati, ai sistemi informatici, ad esempio, mediante un attacco ransomware, mirato al furto di documenti o alla indisponibilità degli stessi mediante azioni di crittografia sui dati e successiva richiesta di riscatto. Questo tipo di attacco di solito può essere classificato come violazione della disponibilità dei dati personali, ma spesso potrebbe verificarsi anche una violazione della riservatezza degli stessi dati;
- attacchi informatici a sistemi e piattaforme applicative. Tali attacchi sfruttano la vulnerabilità dei sistemi e delle piattaforme al fine di ottenere l'accesso a dati memorizzati su Database o aree condivise in rete. Si tratta principalmente di violazioni della riservatezza, ma spesso potrebbe verificarsi anche una violazione dell'integrità degli stessi dati;
- attacchi *phishing,* ossia truffe informatiche effettuate inviando un'e-mail da indirizzi che in prima analisi possono anche apparire leciti, in cui si invita il destinatario a fornire dati riservati, motivando tale richiesta con ragioni di ordine tecnico. Tali attacchi sono classificati come violazioni della riservatezza dei dati personali;
- errore accidentale da parte di uno dei soggetti che trattano dati personali (ad esempio, l'invio di una mail contenente dati personali ad un destinatario errato);

- furto di informazioni, può verificarsi, ad esempio, nel caso in cui un dipendente (o ex dipendente) sfrutti la propria conoscenza o le proprie autorizzazioni per sottrarre dolosamente dati/informazioni di carattere personale;
- mancata vigilanza/adozione di misure di sicurezza, qualora, a causa di un'erronea valutazione sul livello di criticità dei dati personali, non siano poste in essere le necessarie precauzioni volte alla salvaguardia dei dati medesimi.

1.4 Notifica delle violazioni e Registro dei data breach

Il Regolamento afferma che 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 d'identità, perdite finanziarie, decifratura non autorizzata, perdita della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Pertanto, il Titolare del trattamento, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, **è tenuto a notificare la violazione dei dati personali al Garante**, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, **a meno che 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 deve essere **corredata delle ragioni del ritardo** e le informazioni possono essere fornite in fasi successive, senza ulteriore ingiustificato ritardo.

Inoltre, è espressamente previsto un onere informativo anche in capo al Responsabile del trattamento, ove presente: questi, infatti, è tenuto ad informare il Titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

In merito ai tempi di rilevazione della violazione, il Gruppo di lavoro articolo 29 ritiene che il Titolare del trattamento debba considerarsi "a conoscenza" nel momento in cui è **ragionevolmente certo che si è verificato un incidente di sicurezza** che ha portato alla compromissione dei dati personali.

Il momento esatto in cui il Titolare del trattamento può considerarsi "a conoscenza" di una particolare violazione dipenderà dalle circostanze della violazione: in alcuni casi sarà relativamente evidente, fin dall'inizio, che c'è stata una violazione, mentre in altri potrebbe occorrere del tempo per stabilire se i dati personali siano stati compromessi. Tuttavia, l'accento deve essere posto sulla tempestività dell'azione di indagine sull'incidente al fine di stabilire se i dati personali siano stati effettivamente violati e, in caso affermativo, prendere misure correttive ed effettuare la notifica, ove necessario.

Il Titolare del trattamento 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.

In ogni caso il Titolare del trattamento, a prescindere dalla notifica al Garante, deve **documentare tutte le violazioni dei dati personali** in un **apposito registro**. Tale documentazione consente all'Autorità sulla protezione dei dati personali di effettuare eventuali verifiche sul rispetto della normativa.

Spetta al Titolare del trattamento determinare quale metodo e struttura utilizzare per documentare una violazione tenendo conto che determinate informazioni chiave dovrebbero essere sempre incluse. Ad esempio, il Titolare del trattamento è tenuto a registrare i dettagli relativi alla violazione, comprese le cause, i fatti e i dati personali interessati e dovrebbe altresì indicare gli effetti e le conseguenze della violazione e i provvedimenti adottati per porvi rimedio.

Il Regolamento non specifica un periodo di conservazione della documentazione; pertanto, spetta al Titolare del trattamento stabilire un periodo appropriato di conservazione del registro, preferibilmente non inferiore a 10 anni, al fine di fornire prove all'Autorità di controllo in merito al rispetto del Regolamento.

Infine, richiamando le citate Linee Guida WP 250, il Titolare e il Responsabile del trattamento dovrebbero, al fine di agevolare il rispetto degli artt. 33 e 34 del GDPR, disporre di una procedura di notifica documentata, che stabilisca gli adempimenti da seguire una volta individuata una violazione, compreso come contenere, gestire e porre rimedio all'incidente, valutare il rischio e notificare la violazione. A questo proposito, per dimostrare il rispetto del Regolamento potrebbe anche essere utile dimostrare che i dipendenti sono stati informati dell'esistenza di tali procedure e meccanismi e che sanno come reagire alle violazioni.

La mancata corretta documentazione di una violazione **può comportare l'esercizio da parte del Garante dei poteri indicati dall'articolo 58 del Regolamento e l'imposizione di una sanzione amministrativa pecuniaria** ai sensi dell'articolo 83 del Regolamento.

2 Il processo di gestione degli eventi in PCM in caso di data breach

2.1 Descrizione del processo

2.1.1 Ruoli e responsabilità

In conformità a quanto disposto dal Regolamento (UE)2016/679 e in particolare con le Linee Guida 9/2022-WP250, nonché coerentemente con il modello organizzativo in ambito privacy adottato dalla Presidenza del Consiglio dei ministri con DPCM 25 maggio 2018 e s.m.i., si riportano di seguito i ruoli e le responsabilità di ciascuna figura coinvolta nel processo di gestione e segnalazione delle violazioni:

- Garante: autorità di controllo italiana incaricata di sorvegliare l'applicazione delle disposizioni del Regolamento GDPR e delle altre normative nazionali applicabili alla protezione dei dati;
- Titolare del trattamento: è il responsabile ultimo della tenuta del/i Registro/i di trattamento del processo/i che trattano dati personali all'interno della struttura di appartenenza e di cui è referente. Valuta gli impatti di una violazione dei dati, la sua portata e il livello di rischio della avvenuta violazione di dati personali. Si occupa di individuare e adottare possibili misure di rimedio e, ove necessario, di notificare la violazione all'autorità di controllo competente entro 72 ore dal momento in cui ne è venuto a conoscenza, salvo che si riveli improbabile che la violazione medesima possa presentare un rischio per i diritti e le libertà delle persone fisiche. Comunica la violazione agli interessati, qualora la stessa sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Prevede attività di verifiche periodiche volte a garantire l'efficacia delle procedure e degli strumenti di risposta agli incidenti relativi alle violazioni di dati personali. In PCM esercitano le funzioni di Titolare i soggetti di cui agli articoli 2 e 3 del DPCM 25 maggio 2018;
- Responsabile della Transizione Digitale (RTD): figura dirigenziale, interna a tutte le PA prevista dal Codice dell'Amministrazione Digitale, D.lgs. 82/2005. In PCM tale figura è individuata nel Direttore Ufficio informatica e telematica;
- Responsabile dei sistemi informativi: in PCM è il Direttore Ufficio informatica e telematica e coincide con RTD;
- Referente privacy: svolge attività di supporto al Titolare del trattamento per le questioni relative alla tutela dei dati personali trattati e rappresenta il punto di contatto con il RPD (art. 5, comma 3, lettera e), del DPCM 25 maggio 2018);
- Responsabile protezione dati (RPD): ha il compito di: a) informare e fornire consulenza al Titolare del trattamento o al responsabile del trattamento; b) sorvegliare l'osservanza della normativa applicabile; c) fornire, se richiesto, un parere in merito alla DPIA; d) cooperare e fungere da punto di contatto per l'autorità di controllo (Garante). Nella struttura organizzativa della PCM, tale ruolo è stabilito all'art. 6 del DPCM 25 maggio 2018;
- 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;
- Autorizzati al trattamento: soggetti preposti materialmente ad una o più attività di trattamento che coadiuvano il Titolare e il Responsabile del trattamento coerentemente con le responsabilità attribuitegli, in PCM, dal DPCM 25 maggio 2018.

2.1.2 Identificazione di un potenziale data breach

La fase di identificazione di una violazione di dati personali ha l'obiettivo di rilevare un potenziale data breach derivante dalla perdita, divulgazione non autorizzata, trattamento illecito e/o perdita di disponibilità di dati personali di cui la Presidenza del Consiglio dei ministri è Titolare.

La rilevazione/segnalazione di un data breach può provenire da fonte interna o esterna all'Amministrazione quale, ad esempio:

FONTE INTERNA:

- dipendenti e personale esterno in servizio presso la Presidenza del Consiglio dei ministri[1]
- figure preposte alla gestione dei sistemi e dei servizi IT (personale interno ed esterno)

FONTE ESTERNA:

- Autorità di vigilanza o Enti preposti alla segnalazione di eventi (es: CSIRT)
- Cittadini/Imprese che utilizzano i servizi forniti on line sui siti della Presidenza
- Responsabili del Trattamento
- Fornitori e terze parti.

La segnalazione, qualsiasi sia la forma, può raggiungere un qualunque soggetto (o Unità organizzativa) dell'Amministrazione. Al fine di gestire il flusso di comunicazione interna, occorre distinguere:

- segnalazione recapitata al RPD: il RPD individua la Struttura competente e trasmette tempestivamente i dati al Titolare del trattamento per l'avvio delle attività di gestione del data breach;
- segnalazione recapitata ad una Struttura: il Titolare del trattamento accerta la propria competenza e avvia le attività di gestione del data breach, informandone il RPD; nel caso in cui il Titolare accerti che la segnalazione non è riferita a dati personali di propria competenza, informa immediatamente il RPD, che individua il Titolare del trattamento competente.

La comunicazione può contenere indicazioni generiche e pertanto dovrà essere oggetto di indagini e approfondimento successivi al fine di individuare gli effettivi dati personali coinvolti e le loro caratteristiche. In una prima fase, ove possibile, occorre individuare la struttura organizzativa o il sistema informatico (sito web, applicazione) interessato dalla violazione.

Qualora la presunta violazione di dati personali venga rilevata da un Responsabile del trattamento, sarà dovere dello stesso informare tempestivamente il Titolare del trattamento che lo ha designato con atto formale ai sensi dell'art. 28 del GDPR e il RPD, fornendo tutte le informazioni di cui dispone circa l'evento e assicurando la massima solerzia nell'applicare le misure necessarie per la riduzione dei rischi e dell'impatto dovuto alla violazione. Dal momento della ricezione di tale comunicazione da parte del Titolare decorrono le tempistiche previste dal Regolamento per la gestione degli adempimenti connessi alle violazioni accertate.

2.1.3 Analisi dell'evento

Di seguito sono riportate le azioni fondamentali del "Processo di gestione dei data breach". Questo processo prevede due fasi distinte di analisi dell'evento:

- **ANALISI DI PRIMO LIVELLO:** il Titolare del trattamento, informato di una presunta violazione, convoca il referente privacy, individua il dirigente/i dirigenti della Struttura che svolgono attività di trattamento sui dati per i quali è intervenuta la segnalazione e tutte le competenze a sua disposizione nella struttura al fine di avviare questa fase dell'analisi. Con l'ausilio di questo gruppo, nelle successive ore, nel minor tempo consentito, e comunque non oltre 12 ore, analizza i dati della violazione e raccoglie, per quanto possibile, le informazioni di seguito elencate, anche al fine di applicare un primo tool di autovalutazione di data breach messo a disposizione dal Garante (https://servizi.gpdp.it/databreach/s/):
    a. la struttura coinvolta;

[1] V. DPCM 25 maggio 2018, art. 9.

b. la data dell'evento e l'ora della violazione anche solo presunta (specificando se è presunta);
c. la data e ora in cui si è avuto conoscenza della violazione[2];
d. la fonte di segnalazione;
e. la natura dell'evento anomalo;
f. la categoria e il volume di dati personali di cui si presume la violazione;
g. il numero e la categoria di interessati coinvolti;
h. una sintetica descrizione dell'evento anomalo specificando se si tratta di:
    - Violazione non occorsa: in questo caso, l'incidente si chiude. Il Titolare con il supporto del Referente privacy provvede a inserire i dati nel Registro dei data breach e dà contestuale comunicazione al RPD e agli eventuali soggetti segnalanti il problema della natura della presunta violazione.
    - Violazione accertata o non chiarita nella analisi di primo livello: in questo caso, il Titolare del trattamento informa tempestivamente il RPD e valuta l'opportunità, sulla base delle caratteristiche e della severità della violazione subita, di costituire un **Team di data breach** a supporto delle successive attività, composto a titolo esemplificativo dal Responsabile della transizione digitale, dal Responsabile del trattamento (se presente), dai tecnici preposti alla gestione di servizi e sistemi IT (es.: amministratori di sistema), oltre che dai dirigenti della Struttura, dal Referente privacy e dalle figure già coinvolte nella fase 1.

- **ANALISI DI SECONDO LIVELLO:** L'analisi di secondo livello è svolta dal Titolare del trattamento, con il supporto del **Team di data breach** da questi individuato, e comporta a cura del Titolare stesso:
    - l'eventuale notifica al Garante entro le 72 ore e la contestuale comunicazione al Segretario Generale della PCM (come da art. 9, comma 5, del DPCM 25 maggio 2018) e al RPD della PCM
    - l'eventuale comunicazione agli interessati
    - la definizione delle misure necessarie per porre rimedio alla violazione. Tali misure correttive tecniche e organizzative dovranno essere adottate nel minor tempo consentito al fine di mitigare i relativi effetti e ridurre la probabilità di impatto e ricorrenza e dovranno essere adeguate alla natura della violazione dei dati personali
    - l'individuazione dei dati da comunicare al Garante e (eventualmente, secondo il dettato del regolamento) agli interessati
    - l'individuazione dei dati da inserire nel Registro dei data breach.

  In questa fase si raccolgono i dati di dettaglio indicati dal Garante nel fac-simile riportato al seguente link: https://servizi.gpdp.it/databreach/resource/1629905132000/DB_Istruzioni.

  Tali dati vengono caricati sul sito del Garante tramite una procedura informatica, disponibile al seguente link: https://servizi.gpdp.it/databreach/s/scelta-auth.

  Tra i dati da raccogliere indicati dal Garante, si segnalano, a titolo esemplificativo e non esaustivo, le seguenti informazioni:

    - la categoria e il volume di dati personali di cui si presume la violazione;
    - la descrizione dei sistemi di elaborazione e/o memorizzazione dei dati coinvolti, con indicazione della loro ubicazione;
    - indicazione dell'eventuale Responsabile del trattamento coinvolto nella gestione del sistema informatico;
    - analisi tecnica della violazione occorsa in termini di cause, effetti e impatto;

[2] Rappresentano data e ora a partire dalle quali si misurano le 72h (massime) richieste per le comunicazioni al Garante.

- misure di sicurezza adottabili e adottate al fine di interrompere gli effetti della violazione e impedire nuove violazioni della stessa natura;
- misure ulteriori proposte per la mitigazione dell'impatto della violazione;
- valutazione della gravità della violazione avvenuta sui dati personali.

2.1.4 Valutazione della gravita dell'impatto della violazione

Il Titolare del trattamento valuta la gravità della violazione basandosi sulle informazioni raccolte con il supporto del **Team di data breach** attivato per l'analisi di secondo livello.

Al fine di valutare la gravità della violazione e, quindi, il grado di rischio per gli interessati, il board europeo EDPB suggerisce[3] di prendere in considerazione:

- le caratteristiche particolari del Titolare del trattamento e degli interessati;
- il numero delle persone fisiche coinvolte;
- il tipo di violazione;
- la natura della violazione;
- il carattere sensibile e il volume dei dati personali violati;
- la facilità di identificazione delle persone fisiche interessate.

Per calcolare il rischio, l'ENISA propone, ad esempio, di determinare la gravità del data breach tenendo in considerazione tre variabili:

- il contesto del trattamento (ad esempio: dati finanziari, dati sanitari, dati particolari ecc.);
- la facilità di identificazione dell'interessato coinvolto;
- le circostanze del data breach.

A queste variabili viene attribuito un valore (sintetizzati nella fig.1 che riassume in tre tabelle la metodologia proposte da ENISA) tenuto conto della stima specifica del caso. Il grado di rischio è determinato in questa metodologia moltiplicando il dato relativo al *contesto di trattamento* a quello della *facilità di identificazione* dell'interessato sommato alla *valutazione delle circostanze* del data breach. Per la metodologia e l'algoritmo completo da applicare fare comunque riferimento al documento di ENISA del dicembre 2013.

CONTESTO DEL TRATTAMENTO	
Classe dei dati violati	*Punteggio di base **
Dati semplici	1
Dati comportamentali	2
Dati finanziari	3
Dati sensibili	4

FACILITÀ DI IDENTIFICAZIONE	
Livello di identificabilità	*Moltiplicatore*
Trascurabile	0,25
Limitato	0,5
Significativo	0,75
Massimo	1

CIRCOSTANZE DELLA VIOLAZIONE	
Circostanza	*Correzione*
Perdita di riservatezza	Da +0 a +0.50
Perdita di integrità	Da +0 a +0.50
Perdita di disponibilità	Da +0 a +0.50
Intenzioni malevole	+0.50

[3] V. le raccomandazioni proposte nel 2013 dall'Agenzia dell'Unione Europea per la sicurezza delle reti e dell'informazione (ENISA) in merito ad una possibile metodologia di valutazione della gravità di una violazione, consultabili al seguente link: https://www.enisa.europa.eu/publications/dbn-severity.

* Il punteggio di base rientrerà sempre in un valore da 1 a 4, a seconda delle successive correzioni. Ad esempio: a dati semplici potrebbe essere attribuito un punteggio di base = 4 qualora a causa di determinate caratteristiche dell'individuo l'informazione possa essere critica per la sicurezza personale o per le condizioni fisiche/psicologiche. Analogamente, anche a dati sensibili potrebbe essere attribuito un punteggio di base = 1, quando la natura dei dati non fornisce alcuna comprensione sostanziale delle informazioni comportamentali dell'individuo. Per l'algoritmo completo da applicare fare in ogni caso riferimento al documento di ENISA del dicembre 2013.

Fig.1 - Sintesi in tabelle per il calcolo delle variabili del data breach proposto da ENISA.

In ogni caso, la misura qualitativa della *gravità della violazione* potrà fare riferimento alla classificazione qualitativa generale (riportata in Tab.1), ricavata a partire dal documento di ENISA del dicembre 2013.

Tab.1 – Definizioni adottate in PCM per la misura qualitativa della gravità di una violazione (data breach).

Gravità/Rischio	Descrizione
Nullo	Gli utenti interessati non sono influenzati dalla violazione dei dati personali
Basso	Gli utenti interessati potranno incontrare solo qualche inconveniente che supereranno senza problemi (ad esempio: tempo impiegato per reinserire informazioni, fastidi, ecc.)
Medio	Gli utenti interessati possono incontrare inconvenienti non trascurabili che comunque riusciranno a superare nonostante alcune difficoltà (ad esempio: costi aggiuntivi, rifiuto di accesso ai servizi aziendali/pubblici, paura, incomprensione, stress, piccoli disturbi fisici, ecc.)
Alto	Gli utenti interessati possono andare incontro a conseguenze significative che dovrebbero essere in grado di superare anche se con gravi difficoltà (ad esempio: appropriazione indebita di fondi, inserimento in liste nere da parte delle banche, danni materiali, perdita di lavoro, mandato di comparizione, peggioramento della salute, ecc.)
Molto alto	Gli utenti interessati possono andare incontro a conseguenze molto gravi o addirittura irreversibili, che non riusciranno a superare (ad esempio: difficoltà finanziarie come debiti considerevoli o incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.)

Nel caso in cui non ricorrano le caratteristiche di gravità dal valore ***Medio*** fino a ***Molto alto***, ossia qualora, ad esempio, i sistemi informativi coinvolti siano limitati e/o protetti da misure adeguate (ad esempio cifratura), o qualora non siano coinvolti interessati, se non in numero limitato e i dati personali siano parziali e non associati ad altre informazioni (ad esempio nome e cognome senza codice fiscale o carta di credito o numeri telefonici), **la violazione può essere definita a gravità dal valore *Nullo* o *Basso*, quindi da non comunicare al Garante**.

Qualora, invece, la violazione presenti caratteristiche di gravità dal valore ***Medio*** fino a ***Molto alto***, **la violazione dovrà essere notificata al Garante entro il termine di 72 ore** (secondo la procedura sopra indicata) **e, contestualmente, comunicata al Segretario Generale della PCM** (come da art. 9, comma 5, del DPCM 25 maggio 2018) **e al RPD della PCM, predisponendo comunque la sua immissione nel Registro dei data breach**.

Nel caso in cui **la violazione determini un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento comunica la violazione all'interessato, senza ingiustificato ritardo**, secondo le indicazioni e le modalità descritte nel paragrafo successivo.

2.1.5 Comunicazione agli interessati

Secondo quanto previsto dall'art. 34, par.1, del GDPR, «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», fornendo agli stessi interessati informazioni specifiche sulle misure che questi possono prendere per proteggersi.

Per cui, mentre la notifica all'Autorità di controllo è obbligatoria a meno che sia improbabile che la violazione possa presentare un rischio per i diritti e le libertà delle persone fisiche, **la comunicazione di una violazione alle persone fisiche diventa necessaria soltanto laddove la violazione possa presentare un rischio elevato per i loro diritti e le loro libertà**. Per la valutazione della gravità di una violazione il Titolare del trattamento può utilizzare le raccomandazioni elaborate nel 2013 dall'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) (vedi par. 2.1.4).

La comunicazione deve fornire, «con un linguaggio semplice e chiaro» (art. 34 GDPR), i seguenti dati:

- una descrizione della natura della violazione;
- il nome e i dati di contatto del RPD o di altro punto di contatto presso cui ottenere più informazioni;
- una descrizione delle probabili conseguenze della violazione dei dati personali;
- una descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e anche, se del caso, per attenuare i possibili effetti negativi per gli interessati.

Il Titolare del trattamento deve dare comunicazione direttamente agli interessati coinvolti (ad esempio mediante messaggi di posta elettronica, SMS, comunicazione postale), fornendo altresì consulenza specifica alle persone fisiche sul modo in cui proteggersi dalle possibili conseguenze negative della violazione.

Si rammenta che non si procede, invece, con la comunicazione all'interessato qualora ricorra una delle tre condizioni indicate dall'art. 34, par. 3, del GDPR, ovvero quando:

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;

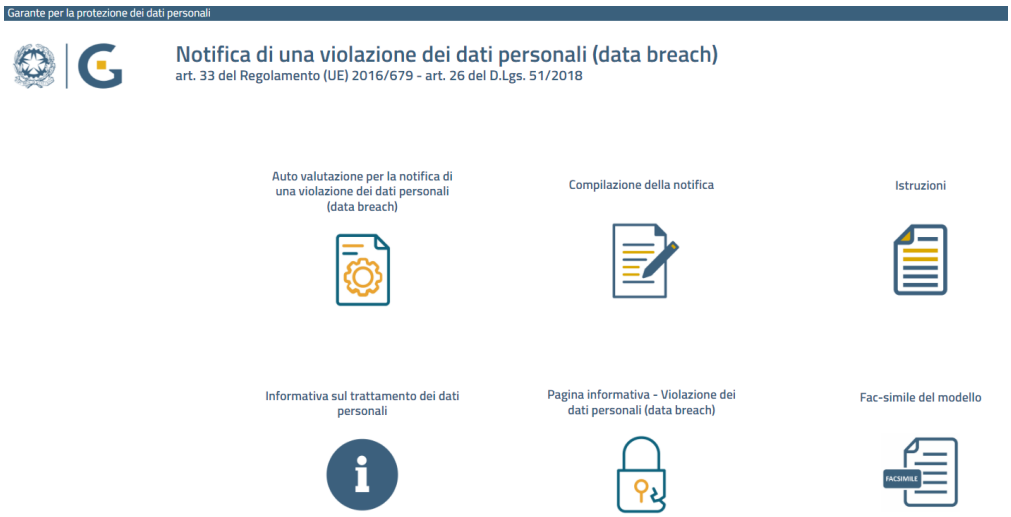
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia» (ad esempio banner o notifiche sul sito web istituzionale).

Conformemente al principio di responsabilizzazione, il Titolare del trattamento deve essere in grado di dimostrare all'Autorità di controllo la sussistenza di una delle tre condizioni sopra indicate. Pertanto, nel caso in cui il soggetto che esercita le funzioni di Titolare del trattamento abbia deciso di non comunicare la violazione di dati personali agli interessati, deve far menzione all'interno del Registro delle violazioni delle ragioni a fondamento della propria decisione. In tal caso, l'Autorità di controllo, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato per i diritti e le libertà degli interessati, può chiedere a chi esercita le funzioni di Titolare di provvedere alla comunicazione ovvero può ritenere che una delle condizioni più sopra menzionate sia soddisfatta.

3 Strumenti e documentazione di supporto predisposta dal Garante sul data breach

Il Titolare del trattamento dovrà avvalersi durante le sue analisi del supporto di alcuni tool e di ulteriori documenti messi a disposizione dal Garante per la Protezione dei Dati personali (https://servizi.gpdp.it/databreach/s/). In particolare, trovano specifica utilità i seguenti 5 elementi.

1. Percorso di **Auto valutazione per la notifica** di una violazione dei dati personali (data breach): questo strumento del Garante, messo a disposizione di ciascun Titolare del trattamento, consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza. È uno strumento di ausilio al processo decisionale del Titolare del trattamento e le informazioni fornite durante il suo utilizzo non saranno conservate sul portale del Garante.
2. Supporto digitale per la **Compilazione della notifica**: applicativo messo a disposizione del Garante per effettuare la notifica della violazione a seguito di autenticazione sul sistema del Titolare del trattamento (attualmente, tramite firma digitale).
3. **Istruzioni** per l'utilizzo della procedura telematica per la notifica delle violazioni dei dati personali: documento in cui il Garante descrive nel dettaglio le funzionalità e i flussi della procedura telematica.
4. **Pagina informativa** - Violazione dei dati personali (data breach): la pagina predisposta dal Garante contiene link alla normativa e a documenti interpretativi, schede informative e pagine tematiche in tema di violazione dei dati personali.
5. Fac-simile del modello di **Notifica di una violazione dei dati personali** predisposto dal Garante: il fac-simile è costituito da un documento che è possibile scaricare e gestire in locale (non sulla rete) per verificare, al di fuori della procedura informatica, la tipologia di dati richiesti dal Garante per compilare la notifica. Il fac-simile è fornito sul sito solo a titolo dimostrativo e non è direttamente utilizzabile per l'invio della notifica al Garante (la compilazione va, infatti, eseguita come indicato al precedente punto 2.)



Schermata della pagina del Garante dedicata al data breach, https://servizi.gpdp.it/databreach/s/

Si consiglia caldamente ai Titolari del trattamento della PCM di far riferimento a questi 5 tool/documenti per l'analisi delle violazioni in PCM.

4 Registro dei data breach

Secondo quanto previsto dall'art. 33 del GDPR, 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, anche al fine di rendere disponibile tale documentazione all'Autorità di controllo in caso di eventuali verifiche di competenza.

Pertanto, una volta terminate le fasi illustrate nei paragrafi precedenti, il Titolare del trattamento, con il supporto del Referente privacy della struttura, procede all'aggiornamento di un apposito **Registro dei data breach**.

Nell'attesa della predisposizione di uno strumento unico e centralizzato, il Titolare del trattamento potrà utilizzare il modello in formato Excel allegato alle presenti Linee guida (Allegato 1 – "Registro dei data breach") e scaricabile nell'apposita sezione del portale *intranet* della Presidenza del Consiglio dei ministri, tramite il percorso "Approfondimenti tematici" > "Trattamento dei dati personali" > "Data breach – Violazione dei dati personali".

Come riportato nel modello in Excel, il Registro dovrà contenere le seguenti informazioni di base:

- Numero identificativo della violazione
- La data in cui è avvenuta la violazione (anno, mese, giorno)
- Nominativo del Titolare del trattamento
- Tipo di violazione (riservatezza, integrità e/o disponibilità dei dati)
- Valutazione della gravità (nulla, bassa, media, alta o molto alta)
- Necessità della notifica al Garante
- Necessità della comunicazione agli interessati

Ad integrazione di tali informazioni, il Titolare del trattamento avrà cura di redigere un apposito *Verbale di dettaglio della violazione*, utilizzando il modello allegato alle presenti Linee guida (Allegato 2 – "Verbale di dettaglio della violazione" scaricabile nella predetta sezione del portale *intranet*), ove andranno riportate le seguenti informazioni:

1. <u>Anagrafica</u>

- Struttura PCM (acronimo)
- Num. d'ordine Registro dei data breach
- Data (aaaa-mm-gg)
- ID Scheda Trattamento del processo
- Titolare del trattamento
- Responsabile del Trattamento

2. <u>Tempistiche e tipologia della violazione</u>

- Data e ora evento (anche presunta)
- Data e ora in cui si è avuta contezza della violazione
- Fonte della segnalazione della violazione
- Tipologia di evento (sintetico)
- Luogo fisico/virtuale dell'incidente

3. <u>Descrizione evento</u>

- Tipo di incidente e contesto in cui si è riscontrata la violazione

- Descrizione del servizio/portale/database/processo impattato
- Tipo di impatto specifico sugli aspetti di Riservatezza, Integrità e Disponibilità dei dati
- Eventuali altri elementi utili per la descrizione dell'evento

4. <u>Caratterizzazione dei dati violati</u>

- Natura generale delle informazioni
- Categorie degli interessati
- Categorie dei dati
- Volume generale dei dati violati
- Numero di interessati (anche approssimativo) coinvolti nella violazione
- Facilità di identificazione delle persone fisiche interessate alla violazione

5. <u>Misure tecniche/organizzative</u>

- Vulnerabilità utilizzate per violare i dati
- Misure tecniche e organizzative attivate per il contenimento dei danni a valle della violazione e tempistiche di attivazione delle misure

6. <u>Valutazione della gravità della violazione</u>

- Metodologia usata per la valutazione
- Livello di gravità

7. <u>Decisione sulla comunicazione al Garante</u>

- La violazione è stata comunicata al Garante entro le 72 ore previste dalla norma?
- Motivazioni a riguardo della decisione adottata
- Data e ora di comunicazione al Garante

8. <u>Decisioni sulla comunicazione agli interessati</u>

- La violazione è stata comunicata agli interessati?
- Motivazioni a riguardo della decisione adottata
- Dettagli eventuali sulle modalità e sulle tempistiche di realizzazione della comunicazione
- Eventuale data e ora di avvio della comunicazione gli interessati

Il Verbale di dettaglio della violazione, contenente le informazioni sopra riportate, formerà parte integrante del file Excel del Registro dei data breach e dovrà essere allegato al suo interno, nell'apposita cella, tramite collegamento ipertestuale.

Una volta compilato, **il Titolare del trattamento dovrà trasmettere al RPD il Registro con le informazioni sulla violazione e il relativo verbale di dettaglio**.

Inoltre, come già anticipato, sarà cura del Titolare del trattamento conservare copia del Registro, del Verbale di dettaglio e di tutta la documentazione prodotta nell'ambito della procedura di data breach per un periodo appropriato, preferibilmente non inferiore a 10 anni, al fine di fornire prove all'Autorità di controllo in merito al rispetto delle previsioni del Regolamento.