C O M U N E D I R I V O L I V E R O N E S E
Provincia di Verona
C.A.P. 37010 - Piazza Napoleone I° , n 3

Istruzione per la gestione del Data Breach (Allegato A)

Revisione	Data di emissione	Motivo della revisione	Visto preparazione	Visto approvazione	Estremi di approvazione
00	22/02/2023	Prima emissione			

Sommario

1 PREMESSA

Una violazione dei dati personali (c.d. *data breach*) può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, quali ad esempio la perdita del controllo dei dati personali che li riguardano o la 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 per la persona fisica interessata.

2 SCOPO DEL DOCUMENTO ED AMBITO DI APPLICAZIONE

Il presente documento si prefigge lo scopo di indicare all'Organizzazione le modalità più opportune per la gestione del data breach, nel rispetto della normativa specifica in materia di trattamento dei dati personali, secondo quanto disposto dall'artt. 33 e 34 del Regolamento (UE) 2016/679.

Nel presente documento, quindi, si indicano gli step tecnici ed organizzativi necessari ad una corretta gestione del data breach, secondo lo schema seguente:

- Segnalazione al Privacy Manager.
- Segnalazione dal Privacy Manager al Titolare del trattamento e primo contatto con il DPO laddove individuato.
- Valutazione dell'evento accaduto.
- Notifica all'Autorità di Controllo.

- Eventuale comunicazione agli interessati coinvolti.
- Tenuta del registro delle violazioni.
- Monitoraggio continuo.

Per tali ragioni, il presente documento deve essere condiviso con tutti gli operatori dell'Organizzazione, affinché ricevano idonee istruzioni relative alla gestione della presente procedura.

3 DEFINIZIONI

- **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 (art. 4 punto 1 Regolamento (UE) 2016/679).
- **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 (art. 4 punto 2 Regolamento (UE) 2016/679).
- **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 (art. 4 punto 5 Regolamento (UE) 2016/679)**.**
- **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 (art. 4 punto 7, cons. 74 Regolamento (UE) 2016/679).
- **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 (art. 4 punto 8 Regolamento (UE) 2016/679).
- **Responsabile della protezione dei dati, DPO/RPD:** soggetto, persona fisica o giuridica, interno o esterno all'Organizzazione, individuata e nominata Responsabile della protezione dei dati, ai sensi del Regolamento (UE) 2016/679 (si vedano in particolare artt. 37, 38 e 39 Regolamento (UE) 2016/679).
- **Delegato al trattamento:** soggetto, persona fisica sottoposta all'autorità del titolare del trattamento, che, nell'ambito dell'assetto organizzativo di quest'ultimo, esercita specifici compiti e funzioni connesse al trattamento dei dati personali (art. 2 – quaterdecies c. 1 D.lgs. 196/2003).
- **Privacy manager:** persona fisica delegata dal titolare del trattamento che operativamente si occupa di valutare e tenere monitorato lo stato di avanzamento dei lavori di adeguamento al GDPR 2016/679 nonché al D.lgs. 196/2003 così come modificato e integrato dal D.lgs. 101/2018, e curando i rapporti con il DPO incaricato, nonché con l'Autorità di Controllo.
- **Autorizzato al trattamento:** persona fisica espressamente autorizzata, che opera sotto l'autorità diretta del titolare del trattamento, con specifici compiti e funzioni relative al trattamento dei dati personali (art. 2 – quaterdecies c. 2 D.lgs. 196/2003).

- **"Data Breach", 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 (art. 4 punto 12 Regolamento (UE) 2016/679).

4 IDENTIFICAZIONE DELLE RESPONSABILITÀ

L'identificazione dei ruoli e delle responsabilità dei soggetti coinvolti è un elemento indispensabile per assicurare il corretto governo della procedura da attuare nel caso di violazione dei dati personali e permettere un'efficace operatività, intesa come attuazione di quanto in seguito esposto.
Si ritiene fondamentale che tutto il personale sia consapevole dei ruoli e delle responsabilità in tale ambito, correlate allo svolgimento della attività lavorative. In particolare, ai vertici dell'organizzazione, che di fatto sono i responsabili ultimi nel caso di violazione dei dati personali all'interno dell'Organizzazione.

Titolare del trattamento (Process Owner)

- Notifica la violazione all'Autorità di Controllo competente a norma dell'articolo 33 Regolamento (UE) 2016/679, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza.
- 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.
- Monitora ogni evento che riguardi la possibile violazione dei dati personali.

Responsabile del trattamento

- Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
- Assiste e supporta il titolare del trattamento, tenendo conto della natura del trattamento e delle informazioni a sua disposizione.
- Monitora ogni evento che riguardi la possibile violazione dei dati personali.

Responsabile per la Protezione del Dato (DPO/RPD)

- Deve sempre essere informato di tutte le fasi inerenti alla violazione, gli accertamenti e le notifiche obbligatorie.

Privacy Manager

- Deve ricevere le segnalazioni di eventi che possono riguardare violazioni di dati personali, gestire operativamente la procedura di data breach, provvedere a redigere ed inoltrare la notifica di violazione all'Autorità di Controllo competente nonché coordinare le verifiche ed occuparsi di fungere da punto di contatto con il DPO e con l'Autorità di Controllo (una volta effettuata la notifica).

Amministratore di Sistema

- Coadiuva il titolare o il responsabile per documentare qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Il titolare o il responsabile seguono le istruzioni impartite dall'Amministratore di sistema.

Delegati, autorizzati al trattamento ed interessati

- Procedono a segnalare al Privacy Manager ogni evento che possa riguardare una violazione dei dati personali.
- Coadiuvano il titolare o il responsabile per le attività richieste a contenimento delle violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.
- Seguono le istruzioni impartite.

5 NORMATIVA DI RIFERIMENTO

- Regolamento (UE) 2016/679, e nello specifico i considerando n. 85, 86, 87, 88 e artt. 33 e 34.
- Guidelines on Personal data breach notification under Regulation 2016/679 – article 29 data protection working party (Adopted on 3 October 2017 – as last Revised and Adopted on 6 February 2018).
- D.lgs. 196/2003 come modificato ed integrato dal D.lgs. 101/2018.

6.1. IDENTIFICAZIONE DELLA VIOLAZIONE DI DATI PERSONALI

Un data breach, dunque, si configura come un incidente di sicurezza che colpisce la riservatezza, l'integrità o la disponibilità del dato personale. In breve, si ravviserà un data breach ogni qual volta che un dato personale sia perso, distrutto, corrotto o rivelato: ad esempio nel caso in cui un soggetto, in assenza di autorizzazione, acceda o diffonda il dato, o nel caso in cui questo sia reso indisponibile, ad esempio quando sia stato "bloccato" da un ransomware, o accidentalmente perso o distrutto.

Per una corretta gestione delle violazioni dei dati personali è necessario preliminarmente aver provveduto ad una corretta mappatura dei dati contenenti informazioni personali, al fine di poter identificare, in ogni momento:

- Il nome e i dati di contatto del titolare del trattamento e, se presente, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati.
- Le finalità del trattamento.
- L'identificazione delle categorie di interessati e delle categorie di dati personali.
- L'identificazione delle categorie di destinatari a cui i dati personali siano stati o saranno comunicati, compresi i destinatari di paesi terzi.
- L'identificazione, se presenti, dei trasferimenti di dati personali verso paesi terzi e la loro identificazione.
- L'identificazione dei termini ultimi previsti per la cancellazione delle diverse categorie di dati.
- Una descrizione delle misure di sicurezza tecniche e organizzative identificate per i vari trattamenti.
- L'identificazione degli autorizzati ai vari trattamenti.
- Una Valutazione d'impatto sulla protezione dei dati.

Una volta in possesso di tutte le informazioni elencate è possibile procedere alla fase successiva.

6.2. AVVIO DELLA GESTIONE DELLA VIOLAZIONE

Il presente documento descrive, qui di seguito, la procedura che deve essere adottata al fine di una corretta gestione di ogni evento che possa anche solo potenzialmente essere definito data breach.

- Ogni soggetto autorizzato al trattamento, qualora venga a conoscenza di un potenziale caso di data breach, avvisa tempestivamente, laddove presente, il delegato al

trattamento di riferimento, secondo quanto previsto dall'organigramma privacy di cui si è dotata l'Organizzazione.

- Il delegato al trattamento, o l'autorizzato al trattamento lì dove il delegato al trattamento non sia presente, procedono a segnalare tempestivamente l'evento che possa potenzialmente costituire un data breach, al privacy manager.
- La segnalazione perviene al privacy manager tramite le consuete modalità di gestione degli eventi, utilizzando il "Rapporto di Violazione all'interno del portale X-GDPR".
- Il privacy manager informa dell'accaduto il titolare del trattamento, mantenendolo informato per ogni singola fase della procedura.
- Il privacy manager procede subito con la comunicazione dell'accaduto al DPO designato dall'Organizzazione, che viene mantenuto informato relativamente a tutte le fasi di indagine e gestione relativamente all'evento malevolo.
- Lo stesso privacy manager contatta il responsabile del trattamento eventualmente coinvolto nel trattamento dei dati colpiti dall'evento, e raccoglie tutte le informazioni messe da quest'ultimo a disposizione.
- Il privacy manager, supportato se del caso dal gruppo privacy, effettua una valutazione dell'evento, avvalendosi anche, laddove necessario, di altre specifiche professionalità necessarie per la corretta analisi dell'accaduto.
- Una volta correttamente classificato l'episodio, nel caso in cui si ritenga necessario o utile, il privacy manager predispone l'eventuale notifica all'Autorità di Controllo individuata quale competente (si veda punto 6.3. del presente documento), sulla base del modello "Modello di notifica data breach" (allegato alla presente procedura), a firma del titolare del trattamento, da inoltrare senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui il titolare ne sia 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. Oltre il termine delle 72 ore la notifica all'Autorità di Controllo deve essere corredata dalla descrizione delle ragioni del ritardo.
- Il privacy manager, di concerto con il titolare del trattamento, stabilisce le azioni immediate da eseguirsi, le priorità, le responsabilità e le tempistiche. Con specifico riferimento alla definizione delle priorità, dovrà essere considerata la seguente scala:

- Priorità Alta: **dove si riscontri un rischio per i diritti e le libertà degli interessati elevato** è necessario provvedere a correzioni da attuare immediatamente per impedire ulteriori rischi.
- Priorità Media: **dove si riscontra rischio per i diritti e le libertà degli interessati medi** è necessario provvedere a correzioni da attuare velocemente perché possono evitare un aumento dei rischi.
- Priorità Bassa: **dove si riscontra rischio per i diritti e le libertà degli interessati basse,** l'azione di contrasto va eseguita dopo aver posto in essere le correzioni con priorità alta e media.
- Priorità nulla: **dove si riscontra rischio trascurabile per i diritti e le libertà dell'interessato**, non è necessaria alcuna azione.

- La scelta e le motivazioni che hanno portato, eventualmente, a non notificare l'evento al Garante per la Protezione dei Dati Personali, deve essere documentata a cura del privacy manager, con nota che deve necessariamente essere condivisa con titolare del trattamento e DPO.

Inoltre, qualora il titolare del trattamento sospetti che la violazione relativa alla sicurezza delle informazioni sia attribuibile ad un atto fraudolento da parte di una persona (sia fisica che giuridica), lo stesso deve interpellare l'Autorità Giudiziaria competente – Polizia Postale – e deve interrompere qualsiasi attività che possa contaminare in qualsiasi modo gli elementi che potrebbero essere oggetto di indagini. Inoltre, le evidenze oggettive (testimonianze, documenti, ecc.) atte a dimostrare la responsabilità della persona devono essere raccolte quanto prima e conservate a cura dello stesso titolare del trattamento, al fine di poter intraprendere un'eventuale azione legale (civile o penale) se necessario.

6.3. NOTIFICA DELLA VIOLAZIONE ALL'AUTORITÀ DI CONTROLLO

Come sopra evidenziato, il privacy manager procede a notificare l'evento all'Autorità di Controllo ritenuta competente, utilizzando la procedura indicata dal Garante per la Protezione dei Dati Personali, raggiungibile all'indirizzo: https://servizi.gpdp.it/databreach/s/

A norma dell'art. 34, la notifica della violazione all'Autorità di Controllo competente – il Garante per la Protezione dei Dati Personali ex art. 153 D.lgs. 196/2003, deve riportare almeno, in un linguaggio semplice e diretto:

a) una descrizione della 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 dei dati personali coinvolti.

b) la comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) la descrizione delle probabili conseguenze della violazione dei dati personali;

d) la descrizione delle 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.

Il Regolamento (UE) 2016/679 riconosce l'eventualità che non sempre sia possibile raccogliere tutte le informazioni necessarie in sole 72 ore al fine di comprendere esattamente cosa sia successo e che su cosa sia necessario intervenire. Per tale ragione l'art. 33 permette al titolare del trattamento di riportare le informazioni richieste per fasi successive, senza ulteriore ingiustificato ritardo. In ogni caso, è necessario che il privacy manager dia una priorità all'indagine, procedendo con risorse adeguate e con la dovuta urgenza. Si richiede, infatti, che il titolare del trattamento notifichi comunque la violazione nel momento in cui egli ne venga a conoscenza, e che inoltri le successive informazioni il prima possibile: si evidenzia che nel caso in cui vi sia già coscienza dell'impossibilità di comunicare le informazioni dettagliate come sopra evidenziate, è in ogni caso consigliabile spiegare all'Autorità di Controllo i motivi del ritardo, individuando un termine entro il quale si ritiene possibile poter comunicare le ulteriori informazioni.

Il privacy manager, inoltre, 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 della normativa in materia di protezione del dato personale.

In tale sede, si ricorda che, nel caso si verifichi una data breach che colpisca interessati ubicati in Paesi Europei diversi, il Garante per la Protezione dei Dati Personali potrebbe non essere l'Autorità di Controllo capofila. Ciò significa, dunque, che parte della procedura di risposta ad un data breach deve essere finalizzata necessariamente a individuare quale delle Autorità di Controllo Europee sia quella capofila e competente a ricevere la notifica di data breach. A tal fine, per una guida completa finalizzata a determinare quale sia l'Autorità di Controllo capofila, si rinvia alle "Linee guida per l'individuazione dell'autorità di controllo capofila in relazione a uno specifico titolare del trattamento o responsabile del trattamento", emanate dal Working Party art. 29 Regolamento (UE) 2016/679.

6.4. COMUNICAZIONE DELLA VIOLAZIONE ALL'INTERESSATO

Nel caso in cui sia probabile che la violazione possa comportare dei rischi elevati per i diritti degli interessati, anche questi devono essere informati senza ingiustificato ritardo, al fine di consentire loro di prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione.

Se, infatti, la notifica all'Autorità di Controllo è obbligatoria ogni qual volta si verifichi un evento che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, la comunicazione all'interessato necessita, per la sua verificazione, l'identificazione di un rischio ulteriormente più alto di danno

per i diritti e le libertà degli interessati. Per tali ragioni, il titolare del trattamento dovrà valutare la gravità, sia potenziale che reale, dell'impatto sugli individui quale risultanza della violazione, e la probabilità della sua verificazione. Nel caso in cui le conseguenze dell'impatto della violazione siano particolarmente gravose, il rischio è alto: in tali casi, il titolare del trattamento dovrà informare prontamente gli interessati coinvolti e colpiti dalla violazione, e ciò in modo particolare laddove vi sia la necessità di mitigare un rischio immediato di danno. Uno dei motivi principali, infatti, che determinano la necessità di provvedere alla comunicazione nei confronti degli interessati è quello di proteggerli dagli effetti del data breach.

Il privacy manager, dunque, predispone l'eventuale comunicazione all'interessato/agli interessati, a firma del titolare del trattamento, da inviarsi nei tempi e nei modi che lo stesso, anche attraverso la funzione consulenziale del DPO, individuerà come più opportuna come specificato dall'art. 34 del Regolamento (UE) e tenendo conto delle eventuali indicazioni fornite dall'Autorità di Controllo.

7 REGISTRO DELLE VIOLAZIONI

Il privacy manager cura l'aggiornamento del registro delle violazioni, ai sensi dell'art. 33 c. 5 Regolamento (UE) 2016/679 (indicazioni di dove viene tenuto il registro?).

8 MONITORAGGIO CONTINUO

Al fine di provvedere ad una corretta gestione della procedura per far fronte ad una violazione dei dati personali si ricorda che è necessaria la verifica costante delle condizioni di sicurezza per la protezione delle informazioni personali. Tale verifica deve essere effettuata sulle misure tecniche organizzative identificate per i vari trattamenti, al fine non solo di definire nel più breve tempo possibile la causa che ha portato alle violazioni dei dati personali ma anche allertarsi immediatamente di fronte ad una possibile violazione dei dati personali.

9 RISPOSTA ALLA VIOLAZIONE DI DATI PERSONALI

Oltre alle attività di identificazione, notifica della violazione e monitoraggio, è necessario inoltre:

1. Che le attività di risposta siano coordinate con le parti interne ed esterne al trattamento, per includere eventuale supporto da parte degli organi di legge o dalle forze dell'ordine.
2. Che vengano condotte approfondite analisi per assicurare un'adeguata riposta e supporto alle eventuali attività di ripristino o compartimentazione della violazione.
3. Che vengano eseguite azioni per prevenire l'espansione di un evento di sicurezza, per mitigare i suoi effetti e per rimuovere le cause della violazione. L'evento che ha determinato la violazione del dato personale, inoltre, dovrà essere necessariamente tenuto conto nella successiva valutazione di impatto sulla protezione dei dati personali ai sensi dell'art. 35 Regolamento (UE) 2016/679.

10 ELENCO DEI DOCUMENTI ALLEGATI ALLA PROCEDURA E MODALITÀ DI CONSERVAZIONE

Documento	Responsabile conservazione	Luogo di conservazione	Tempo conservazione
Rapporto di Violazione all'interno del portale X-GDPR	Privacy manager	Archivi specifici	10 anni
Modello di notifica data breach	Privacy manager	Archivi specifici	10 anni

C O M U N E D I R I V O L I V E R O N E S E

P r o v i n c i a d i V e r o n a

C.A.P. 37010 - Piazza Napoleone I° , n 3

Procedura per la gestione dei diritti degli interessati (Allegato B)

Revisione	Data di emissione	Motivo della revisione	Visto preparazione	Visto approvazione	Estremi di approvazione
00	_____	Prima emissione	Privacy Manager	Delibera di Giunta	Delibera numero ___ del _____

Sommario

1 PREMESSA

Il Regolamento (UE) 2016/679 si propone di tutelare la riservatezza dei dati personali, al fine di evitare che un trattamento non corretto degli stessi possa comportare un danno ai diritti ed alle libertà degli interessati, persone fisiche. A tal scopo, l'Ente ha redatto la presente procedura, per garantire, secondo un sistema di gestione standardizzato, la tutela dei diritti dell'interessato e la gestione delle richieste di esercizio degli stessi.

2 SCOPO DEL DOCUMENTO ED AMBITO DI APPLICAZIONE

Il presente documento si prefigge lo scopo di indicare all'Organizzazione le modalità più opportune per la gestione, nel rispetto di quanto previsto dal Regolamento Comunitario, delle richieste di esercizio dei diritti dell'interessato.

Nel presente documento, quindi, si indicano gli step organizzativi necessari ad una corretta gestione delle richieste di esercizio dei diritti degli interessati, secondo lo schema che segue:

- Segnalazione al Privacy Manager.
- Segnalazione dal Privacy Manager al Titolare del trattamento e primo contatto con il DPO laddove individuato.
- Valutazione della richiesta.
- Notifica della risposta all'interessato e tenuta del registro delle richieste di esercizio dei diritti.

3 DEFINIZIONI

- **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 (art. 4 punto 1 Regolamento (UE) 2016/679).
- **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 (art. 4 punto 2 Regolamento (UE) 2016/679).
- **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 (art. 4 punto 5 Regolamento (UE) 2016/679).

- **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 (art. 4 punto 7, cons. 74 Regolamento (UE) 2016/679).
- **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 (art. 4 punto 8 Regolamento (UE) 2016/679).
- **Responsabile della protezione dei dati, DPO/RPD:** soggetto, persona fisica o giuridica, interno o esterno all'Organizzazione, individuata e nominata Responsabile della protezione dei dati, ai sensi del Regolamento (UE) 2016/679 (si vedano in particolare artt. 37, 38 e 39 Regolamento (UE) 2016/679).
- **Delegato al trattamento:** soggetto, persona fisica sottoposta all'autorità del titolare del trattamento, che, nell'ambito dell'assetto organizzativo di quest'ultimo, esercita specifici compiti e funzioni connesse al trattamento dei dati personali (art. 2 – quaterdecies c. 1 D.lgs. 196/2003).
- **Privacy manager:** persona fisica delegata dal titolare del trattamento che operativamente si occupa di valutare e tenere monitorato lo stato di avanzamento dei lavori di adeguamento al GDPR 2016/679 nonché al D.lgs. 196/2003 così come modificato e integrato dal D.lgs. 101/2018, e curando i rapporti con il DPO incaricato, nonché con l'Autorità di Controllo. Tale figura è specificamente definita dalla norma UNI 11697:2017.
- **Autorizzato al trattamento:** persona fisica espressamente autorizzata, che opera sotto l'autorità diretta del titolare del trattamento, con specifici compiti e funzioni relative al trattamento dei dati personali (art. 2 – quaterdecies c. 2 D.lgs. 196/2003).
- **"Data Breach", 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 (art. 4 punto 12 Regolamento (UE) 2016/679).

4 IDENTIFICAZIONE DELLE RESPONSABILITÀ

L'identificazione dei ruoli e delle responsabilità dei soggetti coinvolti è un elemento indispensabile per assicurare il corretto governo della procedura da attuare nel caso di esercizio dei diritti dell'interessato, e permette un'efficace operatività, intesa come attuazione di quanto in seguito esposto.

Si ritiene fondamentale che tutto il personale sia consapevole dei ruoli e delle responsabilità in tale ambito, correlate allo svolgimento delle attività lavorative. In particolare, ai vertici dell'organizzazione, che di fatto sono i responsabili ultimi all'interno dell'Organizzazione.

Titolare del trattamento (Process Qwner)

- È il soggetto responsabile del rilascio delle informazioni richieste dall'interessato, ed è il soggetto obbligato all'adempimento delle istanze proposte dall'interessato stesso nell'ambito dell'esercizio dei diritti.
- Il Titolare del trattamento provvede alla gestione ed all'espletamento delle richieste di esercizio dei diritti, secondo quanto previsto dalla presente procedura e nel rispetto delle prescrizioni normative di cui al Regolamento (UE) 2016/679.
- Monitora ogni evento che riguardi la possibile violazione dei dati personali.

Responsabile del trattamento

- Deve informare l'interessato, che ponga una richiesta presso di lui, in merito alle sedi opportune, presso il Titolare del trattamento, dove porre le proprie istanze.
- Deve informare senza ritardo il Titolare del trattamento, in merito a richieste di esercizio dei diritti degli interessati, poste presso di lui.

Responsabile per la Protezione del Dato (DPO/RPD)

- Esprime parere di competenza sulla "ricusabilità" delle richieste di esercizio dei diritti degli interessati.
- Fornisce supporto ai Delegati al trattamento per l'espletamento delle attività necessarie ad adempiere alle richieste di esercizio dei diritti degli interessati.
- Coadiuva il Privacy Manager nella gestione delle richieste, e nella predisposizione delle risposte rivolte agli interessati istanti.
- Effettua l'istruttoria e la verifica di sussistenza di richieste e segnalazioni.
- Nel caso in cui si riscontrino delle non conformità nel trattamento o una immotivata inottemperanza delle richieste di esercizio dei diritti degli interessati, comunica al Titolare del trattamento ed al Privacy Manager le azioni corretti e/o migliorative da adottare, nonché la relativa tempistica, al fine di assicurare la tutela dei diritti degli interessati.
- Nel caso in cui si riscontri una violazione dei dati personali, si rimanda alle specifiche istruzioni "Istruzioni per la gestione del Data Breach".
- Riceve ed identifica univocamente le segnalazioni formali di presunta violazione dei dati o di immotivata inottemperanza alle richieste di esercizio dei diritti.
- Coopera con il Privacy Manager per la revisione, l'adeguamento, miglioramento dei processi e delle attività afferenti alla tutela dei diritti degli interessati.

Privacy Manager

- Deve ricevere ed identificare univocamente le richieste di esercizio dei diritti. Deve inoltre verificare la completezza delle richieste nonché la presenza di idoneo documento identificativo dell'interessato.

- Deve valutare in via preliminare la congruità o la ricusabilità della richiesta, eventualmente chiedendo il parere di competenza del Responsabile per la Protezione del Dato (DPO/RPD).
- Nel caso in cui, al termine della valutazione preliminare, la richiesta di esercizio sia da ritenersi "ricusabile", deve fornire tempestiva comunicazione all'interessato ai riferimenti indicati nella richiesta.
- Nel caso in cui, al termine della valutazione preliminare, la richiesta di esercizio sia da ritenersi "non ricusabile", deve inoltrare la richiesta al Delegato al trattamento competente, al fine di ottemperare a quanto richiesto dall'interessato indicando i tempi massimi di risposta.
- Riceve la comunicazione di adempimento da parte del Delegato al trattamento, nei termini indicati.
- Deve comunicare all'interessato tutte le informazioni relative alla richiesta entro 30 giorni (trenta) dal ricevimento della stessa.
- Deve comunicare all'interessato le motivazioni dell'eventuale inottemperanza entro i 30 (trenta) giorni dal ricevimento della richiesta, nel caso in cui il Delegato al trattamento via via competente segnali a sua volta l'impossibilità di adempiere.
- Deve custodire ed aggiornare il registro delle richieste di esercizio.
- Deve comunicare al Titolare del trattamento ed al Responsabile per la Protezione dei Dati ogni criticità rilevata nello svolgimento delle attività, segnalando eventuali violazioni dei dati riscontrate (secondo la prescritta specifica istruzione), al fine di consentire il rapido espletamento degli obblighi di comunicazione al Garante per la Protezione dei Dati Personali.

Amministratore di Sistema

- Coadiuva il titolare nel reperire le informazioni necessarie ad adempiere alle richieste di esercizio dei diritti degli interessati.

Delegati al trattamento

- Procedono a segnalare al Privacy Manager ogni richiesta ricevuta di esercizio dei diritti da parte degli interessati.
- Ricevono le richieste di esercizio dei diritti, pervenute dal Privacy Manager e ritenute "non ricusabili".
- Analizzano le richieste e mette in atto tutte le azioni necessarie ad ottemperare alle stesse nelle tempistiche indicate dal Privacy Manager e comunque non oltre il termine di 30 (trenta) giorni.
- Nel caso in cui, nell'esecuzione delle attività richieste, riscontrassero la necessità di supporto circa le indicazioni del Regolamento (UE) 2016/679, devono inoltrare la richiesta di supporto al Responsabile per la Protezione dei Dati laddove individuato.
- Nel caso in cui, nell'esecuzione delle attività richieste, riscontrassero l'impossibilità oggettiva ad ottemperare alla richiesta o la necessità di tempi di risoluzione maggiori, ne comunicano le motivazioni e le eventuali tempistiche al Privacy Manager, che provvederà ad informare l'interessato.
- Devono comunicare al Titolare del trattamento ed al Responsabile per la Protezione dei Dati ogni criticità rilevata nello svolgimento delle attività, segnalando eventuali violazioni dei dati riscontrate (secondo la prescritta specifica istruzione), al fine di consentire il

rapido espletamento degli obblighi di comunicazione al Garante per la Protezione dei Dati Personali.

- Coadiuvano il titolare o il responsabile per le attività richieste ai fini dell'adempimento alle richieste degli interessati, comprese le circostanze a esse relative, e le loro conseguenze.
- Seguono le istruzioni impartite.

Autorizzati al trattamento e interessati

- Coadiuvano il titolare o il responsabile per le attività richieste ai fini dell'adempimento alle richieste degli interessati, comprese le circostanze a esse relative, e le loro conseguenze.
- Seguono le istruzioni impartite.

5 NORMATIVA DI RIFERIMENTO

- Regolamento (UE) 2016/679, e nello specifico i considerando n. 31, 58, 60, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72 e artt. 12, 13, 14, 15, 16, 17, 18, 19, 20, 21 e 22.
- Guidelines on the right of "data portability" (Adopted on 13 December 2016 – as last Revised and Adopted on 5 April 2017).
- D.lgs. 196/2003 come modificato ed integrato dal D.lgs. 101/2018.

6 GESTIONE DELLE RICHIESTE DI ESERCIZIO DEI DIRITTI

L'interessato potrà inoltrare la propria richiesta di esercizio dei diritti oppure una segnalazione di presunta inottemperanza o violazione utilizzando anche il modello (allegato A), predisposto dall'Organizzazione, tramite i seguenti canali di comunicazione:

- Pec o mail dell'interessato indirizzata ai seguenti recapiti: mail _____, pec _____.
- Pec o mail del Responsabile per la Protezione dei Dati Personali, su impulso scaturito da una richiesta dell'interessato.
- Richiesta inoltrata dall'interessato a mezzo posta all'indirizzo _____.
- Richiesta presentata di persona dall'interessato alla sportello, utilizzando il modulo allegato alla presente procedura (allegato A).

Si precisa che l'interessato potrà presentare alcune delle sue richieste anche telefonicamente, come segue:

- Contattando il numero telefonico _____, l'interessato potrà richiedere e ricevere chiarimenti verbali limitati, potendo ottenere solamente informazioni generiche sulle modalità di trattamento del dato personale adottate dall'Organizzazione, nonché sulle modalità di esercizio dei diritti degli interessati, con esclusione tassativa di ulteriori informazioni telefoniche aventi ad oggetto ogni altra

tipologia di informazione. L'interessato che intenda esercitare i propri diritti telefonicamente dovrà essere ricondotto, conseguentemente, ai canali tipici di comunicazione come sopra elencati.

Il Titolare del trattamento provvede alla gestione ed all'espletamento delle richieste di esercizio dei diritti, secondo quanto previsto dalla presente procedura e nel rispetto delle prescrizioni normative di cui al Regolamento (UE) 2016/679, per il tramite del Privacy Manager, al quale sono affidati i compiti di supervisione e coordinamento di tutte le attività poste in atto dall'Organizzazione ed, in particolare, il monitoraggio delle tempistiche e dell'espletamento delle azioni necessarie ad adempiere alle richieste dell'interessato.

6.1 IDENTIFICAZIONE DELL'ISTANTE E VALUTAZIONE DI FONDATEZZA

In seguito alla richiesta dell'interessato, che può avvenire tramite i canali sopra descritti, è necessario preliminarmente procedere con l'identificazione certa del soggetto istante, e nel caso in cui non sia possibile espletare tale controllo oppure nel caso in cui tale controllo di esito negativo, la richiesta dovrà essere rigettata con notifica all'interessato attestante le motivazioni del diniego.

In primo luogo, inoltre, è necessario verificare in via pregiudiziale la fondatezza di quanto richiesto (e dunque se la richiesta sia attinente al trattamento dei dati personali): laddove tale prima valutazione rilevi la non fondatezza della domanda, essa andrà rigettata con notifica all'interessato attestante le motivazioni del diniego.

6.2 ATTIVITÀ PER LA CLASSIFICAZIONE DELLE RICHIESTE DELL'INTERESSATO

In riferimento a quanto richiesto dall'interessato ed ai tempi di esecuzione possibili, di cui si dirà qui di seguito, è quindi necessario classificare la richiesta ricevuta come segue:

- **Diritto di accesso dell'interessato** (art. 15 Regolamento (UE) 2016/679) – l'interessato chiede conferma che sia o meno in corso un trattamento dei dati personali che lo riguardano. Lo stesso interessato può eventualmente chiedere di ottenere l'accesso a tali dati, nonché una copia degli stessi, e tutte le informazioni di cui alle lettere da a) ad h) dell'art. 15, par. 1, Regolamento (UE) 2016/679.
- **Diritto di rettifica** (art. 16 Regolamento (UE) 2016/679) – l'interessato chiede la rettificazione e/o l'aggiornamento dei dati personali che lo riguardano.
- **Diritto alla cancellazione** (art. 17 Regolamento (UE) 2016/679) – l'interessato chiede la cancellazione dei propri dati personali.
- **Diritto di limitazione di trattamento** (art. 18 Regolamento (UE) 2016/679) – l'interessato chiede la limitazione del trattamento dei dati personali che lo riguardano, in quanto contesta l'esattezza dei dati personali, oppure ritiene che il trattamento dei dati sia illecito, oppure i dati personali siano necessari all'istante stesso per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
- **Diritto alla portabilità dei dati** (art. 20 Regolamento (UE) 2016/679) – l'interessato chiede di ricevere i dati personali che lo riguardano in un formato strutturato, oppure che questi siano trasmessi direttamente ad altro titolare del trattamento.
- **Diritto di opposizione** (art. 21 Regolamento (UE) 2016/679) – l'interessato si oppone al trattamento dei suoi dati personali.

6.3 ATTIVITÀ PER L'ESERCIZIO DELLE RICHIESTE DELL'INTERESSATO

Una volta classificate le richieste dell'interessato, i soggetti coinvolti, come specificato al punto 4, devono agire come prescritto dalla presente proceduta affinché quanto specificatamente richiesto dall'interessato venga soddisfatto.

Nell'ambito di tali attività è necessario ricordare che:

- Il termine per ottemperare alla richiesta dell'interessato è di giorni 30 (trenta) dalla data di ricevimento della richiesta, e può essere prolungato di ulteriori giorni 60 (sessanta), se necessario, tenuto conto della complessità e del numero delle richieste pervenute. Nel caso di dilatazione del termine di risposta, il Privacy Manager informa l'interessato di tale proroga nonché contestualmente, dei motivi del ritardo, entro 30 (trenta) giorni dal ricevimento della richiesta.
- Le informazioni fornite dall'interessato ed eventuali comunicazioni e azioni intraprese sono gratuite.
- Nel caso in cui le richieste dell'interessato siano manifestamente infondate o eccessive per il Titolare del trattamento, in particolare per la loro natura ripetitiva, il Titolare del trattamento può:

  a) Addebitare un contributo spese ragionevole, tenendo conto i costi amministrativi sostenuti per fornire le informazioni richieste; oppure

  b) Rifiutare di soddisfare la richiesta.

6.4 NOTIFICA DELLA CONCLUSIONE DELLE ATTIVITÀ RICHIESTE DALL'INTERESSATO E REGISTRO DELLE RICHIESTE DI ESERCIZIO DEI DIRITTI

Una volta concluse le attività necessarie per adempiere alla richiesta dei diritti, queste devono essere verbalizzate e notificate all'interessato al contatto da questi comunicato al momento della richiesta, con un riscontro puntuale rispetto alle istanze dello stesso.

Tutte le richieste di esercizio dei diritti dell'interessato vengono protocollate, individuate univocamente, registrate ed archiviate all'interno del "Registro delle richieste di esercizio dei diritti". Il Privacy Manager custodisce tale registro, che dovrà riportare le seguenti indicazioni:

- Identificativo univoco della richiesta;
- Descrizione sintetica dell'oggetto della domanda;
- Esito della richiesta;
- Data di registrazione della richiesta;
- Data di comunicazione all'interessato circa gli esiti della richiesta;
- Eventuali Note e Segnalazioni (ad esempio pareri integrativi del DPO).

7 INDICATORI DI MONITORAGGIO PROCESSO DESCRITTO

	Attività	Caratteristica da misurare	Oggetto del controllo	Note
Efficienza	Attività di gestione delle richieste dell'interessato	TEMPO TRASCORSO DALLA RICHIESTA DI UN INTERESSATO E LA NOTIFICA DI CONCLUSIONE DELL'ATTIVITÀ RICHIESTA	TEMPO TRASCORSO DALLA RICHIESTA DI UN INTERESSATO E LA NOTIFICA DI CONCLUSIONE DELL'ATTIVITÀ RICHIESTA	
Efficacia	Attività di gestione delle richieste dell'interessato	NUMERO DELLE RICHIESTE DELL'INTERESSATO EVASE ENTRO I 30 GIORNI	NUMERO DELLE RICHIESTE DELL'INTERESSATO EVASE ENTRO I 30 GIORNI	

8 ELENCO DEI DOCUMENTI ALLEGATI ALLA PROCEDURA E MODALITÀ DI CONSERVAZIONE

Documento	Responsabile conservazione	Luogo di conservazione	Tempo conservazione
Richiesta dell'interessato	Titolare del trattamento	Archivi specifici	10 anni
Notifiche all'interessato	Titolare del trattamento	Archivi specifici	10 anni
Registro delle richieste di esercizio dei diritti	Titolare del trattamento	Archivi specifici	10 anni