CONSIGLIO di BACINO
LAGUNA DI VENEZIA
Ambito Territoriale Ottimale per il servizio idrico integrato

Istruzione per la gestione del Data Breach

Revisione	Data di emissione	Motivo della revisione	Visto preparazione	Visto approvazione	Estremi di approvazione
00	06/07/2023	Prima emissione			Del. CI n. 23 del 28/09/2023

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 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;
- 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'Ente, 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;
- l'eventuale 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 il 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 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 medio** 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 basso,** 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 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. Il registro delle violazioni è presente all'interno del portale X-GDPR ed è costituito dalle sezioni "Gestione eventi", "Gestione Incidenti" e "Gestione Data breach" nel menu "Relazioni con il DPO".

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	Privacy manager	portale X-GDPR	10 anni
Modello di notifica data breach	Privacy manager	Protocollo informatico	10 anni