DOCUMENTO	**PODB.01– PROCEDURA DA ADOTTARE IN CASO DI VIOLAZIONE DEI DATI PERSONALI**
RIFERIMENTI	Art. 4, 33, 34 del Regolamento UE 679/2016
	Ufficio Privacy
	REV. 0 del 28/02/2020

ART. 1 - INTRODUZIONE

Il presente documento è redatto in adempimento a quanto previsto dal Regolamento UE 679/2016 (di seguito GDPR) in materia di violazione dei dati personali.

ART. 2 – TERMINI E DEFINIZIONI

Si riportano le definizioni degli acronimi utilizzati nella presente Procedura:

- ✓ GDPR General Data Protection Regulation
- ✓ RPD / DPO Responsabile della Protezione dei Dati / Data Protection Officer
- ✓ UE Unione Europea
- ✓ WP Working Party

Per eventuali altre definizioni si rimanda allo standard 27001 "*Information technology — Security techniques Information security management systems — Overview and vocabulary*".

Per «dato personale», ai sensi dell'art. 4 p. 1 del GDPR, si intende "*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".*

Per "*Data Breach*" si intende un evento in conseguenza del quale si verifica una violazione dei dati personali. Ai sensi dell'art. 4 p.12 del GPDR 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*".
Le Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679 precisano la nozione di violazione come di seguito riportata:
Nel parere 03/2014 sulla notifica delle violazioni, il Gruppo di lavoro ha spiegato che le violazioni possono essere classificate in base ai seguenti tre principi ben noti della sicurezza delle informazioni:

- *"violazione della riservatezza", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;*
- *"violazione dell'integrità", in caso di modifica non autorizzata o accidentale dei dati personali;*
- *"violazione della disponibilità", in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.*

Va altresì osservato che, a seconda dei casi, una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse. Ci si potrebbe chiedere se una perdita temporanea della disponibilità dei dati personali costituisca una violazione e, in tal caso, se si tratti di una violazione che richiede la notifica. L'articolo 32 del regolamento ("Sicurezza del trattamento") spiega che nell'attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, si dovrebbe prendere in considerazione, tra le altre cose, "la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento" e "la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico". Di conseguenza, un incidente di sicurezza che

determina l'indisponibilità dei dati personali per un certo periodo di tempo costituisce una violazione, in quanto la mancanza di accesso ai dati può avere un impatto significativo sui diritti e sulle libertà delle persone fisiche. Va precisato che l'indisponibilità dei dati personali dovuta allo svolgimento di un intervento di manutenzione programmata del sistema non costituisce una "violazione della sicurezza" ai sensi dell'articolo 4, punto 12.
Come nel caso della perdita o distruzione permanente dei dati personali (o comunque di qualsiasi altro tipo di violazione), una violazione che implichi la perdita temporanea di disponibilità dovrebbe essere documentata in conformità all'articolo 33, paragrafo 5. Ciò aiuta il titolare del trattamento a dimostrare l'assunzione di responsabilità all'autorità di controllo, che potrebbe chiedere di consultare tali registrazioni16. Tuttavia, a seconda delle circostanze in cui si verifica, la violazione può richiedere o meno la notifica all'autorità di controllo e la comunicazione alle persone fisiche coinvolte. Il titolare del trattamento dovrà valutare la probabilità e la gravità dell'impatto dell'indisponibilità dei dati personali sui diritti e sulle libertà delle persone fisiche. Conformemente all'articolo 33, il titolare del trattamento dovrà effettuare la notifica a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Questo punto dovrà chiaramente essere valutato caso per caso. Va notato che, sebbene una perdita di disponibilità dei sistemi del titolare del trattamento possa essere solo temporanea e non avere un impatto sulle persone fisiche, è importante che il titolare del trattamento consideri tutte le possibili conseguenze della violazione, poiché quest'ultima potrebbe comunque dover essere segnalata per altri motivi.

ART. 3 - RIFERIMENTI NORMATIVI

- ✓ D.Lgs. 196/2003 Codice per la protezione dei dati personali così come modificato dal Decreto Legislativo 10 agosto 2018 n, 101 "*Disposizioni per l'adeguamento della Normativa Nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)*"
- ✓ Regolamento (UE) 2016/679 del Parlamento Europeo del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), in particolare gli articoli 33 (Notifica all'Autorità di Controllo), 34 (notifica agli interessati) e 28 (Responsabile del trattamento)
- ✓ Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679.
- ✓ Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche – Provvedimento del Garante della privacy del 2 luglio 2015
- ✓ D.Lgs. 82/2005 Codice dell'Amministrazione Digitale (CAD)
- ✓ artt. 331 e 361 del Codice di Procedura Penale (obbligo di denuncia da parte del pubblico ufficiale)
- ✓ Decreto 9 gennaio 2008 del Ministero degli interni in attuazione della Legge 155/2005 sulle infrastrutture critiche
- ✓ Decreto del Presidente del Consiglio dei Ministri 1 aprile 2008 "Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettività" previste dall'articolo

71, comma 1-bis del decreto legislativo 7 marzo 2005, n. 82, recante il «Codice dell'amministrazione digitale» G.U. 21 giugno 2008, n. 144.

ART. 4 - SCOPO E CAMPO DI APPLICAZIONE DEL DOCUMENTO

4.1 SCOPO

Questa Procedura è redatta al fine di tutelare le persone, i dati e le informazioni e documentare i flussi per la gestione delle violazioni dei dati personali trattati da ASP SpA sia nei casi in cui essa si configura quale Titolare del trattamento sia nei casi in cui risulta Responsabile esterno di altri Titolari (in particolare del Comune di Asti).

ASP SpA ad integrazione delle procedure già adottate in materia di protezione dei dati personali ai sensi della legislazione vigente, ha predisposto azioni da attuare nell'eventualità in cui si presentino violazioni concrete, potenziali o sospette di dati personali trattati al fine di:

- ✓ evitare rischi per i diritti e le libertà degli interessati
- ✓ evitare danni economici alla Società
- ✓ notificare la violazione (data breach) al Garante e/o agli interessati, nei tempi e nei modi previsti dalla normativa europea
- ✓ non incorrere nelle sanzioni previste dal GDPR per omessa notifica
- ✓ minimizzare l'impatto della violazione e prevenire che si ripeta.

4.2 CAMPO DI APPLICAZIONE

Questa Procedura si applica a qualunque attività svolta da ASP SpA con particolare riferimento a tutti gli archivi e/o documenti cartacei e a tutti i sistemi informativi attraverso cui sono trattati dati personali, anche con il supporto di fornitori esterni.
Questa Procedura è rivolta a tutti i soggetti che a qualsiasi titolo trattano dati personali per conto di ASP SpA, in qualsiasi formato e con qualsiasi mezzo, quali:

- ✓ i dipendenti,
- ✓ i collaboratori che, a prescindere dal tipo di rapporto intercorrente, nel corso del proprio impiego presso ASP SpA, abbiano accesso a dati personali;
- ✓ qualsiasi soggetto (persona fisica o persona giuridica) che, in ragione del rapporto contrattuale in essere con ASP SpA abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento ex art. 28 GDPR o di autonomo Titolare.

Il rispetto della presente Procedura è obbligatorio per tutti i soggetti coinvolti. La mancata conformità alla presente Procedura potrà comportare l'irrogazione di provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere.

ART. 5 - PROCEDURA DI GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

5.1 VIOLAZIONE IN CASO DI TRATTAMENTO EFFETTUATO DA ASP SPA

Nel caso in cui uno dei soggetti di cui all'art. 4.2 della presente Procedura venga a conoscenza di una concreta, potenziale o sospetta violazione di dati personali, dovrà essere attivato il flusso di adempimenti di seguito descritti e schematizzati:

A. Rilevazione e segnalazione della violazione dei dati personali
B. Raccolta delle informazioni sulla violazione ed eventuale comunicazione della violazione
C. Valutazione del rischio e individuazione delle azioni correttive
D. Analisi delle valutazioni effettuate e delle azioni da intraprendere
E. Nei casi in cui ASP SpA è titolare del trattamento: notifica della violazione al Garante della privacy
F. Nei casi in cui ASP SpA è titolare del trattamento: comunicazione agli interessati (se necessaria)
G. Documentazione delle violazioni (Registro dei data breach)

Per una pronta e corretta attuazione delle attività sopra descritte ASP spa applica la seguente procedura operativa:

A) Rilevazione e segnalazione della violazione dei dati personali

Qualora si sia verificato un evento (es. incendio, attacco informatico, furto) che anche solo potenzialmente possa comportare una violazione di dati personali (es. perdita di integrità, di disponibilità, di riservatezza) colui che lo rileva:

a) se appartenente al personale di Staff deve comunicarlo immediatamente al proprio Responsabile di funzione attraverso l'invio di una e-mail all'indirizzo di posta aziendale e all'Ufficio Privacy all'indirizzo privacy@asp.asti.it;

b) se appartenente al personale di una Business Unit deve comunicarlo immediatamente al proprio Dirigente attraverso l'invio di una e-mail all'indirizzo di posta aziendale e all'Ufficio Privacy all'indirizzo privacy@asp.asti.it;

c) se trattasi di Responsabile esterno del Trattamento, ex art 28 GDPR, deve comunicarlo immediatamente, a mezzo mail al Direttore Esecutivo del Contratto/Referente Aziendale e all'Ufficio Privacy all'indirizzo privacy@asp.asti.it;

Qualora Asp SpA si configuri come Responsabile del Trattamento di altro Titolare del Trattamento ex art. 28 GDPR, l'Ufficio Privacy, ricevuta la segnalazione, provvederà a dare notizia circa la supposta violazione al Titolare del Trattamento dei Dati a mezzo pec.

Dal momento della rilevazione dell'evento da parte del segnalante decorre il termine di 72 h entro cui notificare all'Autorità Garante la violazione, secondo i casi e le modalità descritte al punto 5.1 lett. E.

B) Raccolta delle informazioni sulla violazione

Il Dirigente/Responsabile di Funzione, informato della supposta violazione dal sottoposto con l'ausilio del segnalante e dell'Ufficio privacy, raccoglie tempestivamente le informazioni sulla potenziale violazione utilizzando il modello di rilevazione allegato alla presente Procedura (Allegato 1).

Il Dirigente/Responsabile di funzione di concerto con l'Ufficio Privacy, se verifica che l'evento sia qualificabile anche solo potenzialmente come Data Breach, deve dare notizia della supposta violazione all'Amministratore Delegato, al Responsabile Sistemi Informativi e al DPO e procede secondo il successivo punto C.

Qualora ASP SpA sia Responsabile esterno di altro Titolare del trattamento dei dati (es: Comune di Asti) l'Ufficio Privacy deve tempestivamente trasmettere a mezzo pec il modello di rilevazione compilato al Titolare del trattamento dei dati personali.

C) Valutazione del rischio e individuazione delle azioni correttive

Sentito l'Amministratore Delegato se reperibile, il Dirigente/Responsabile di Funzione convoca tempestivamente l'Unità di crisi composta oltreché da lui, dal Responsabile Sistemi Informativi, DPO, Coordinatore Ufficio Privacy; nel caso in cui ASP SpA agisca quale Responsabile esterno di altro Titolare del trattamento (es: del Comune di Asti), anche il DPO (ovvero, in sua mancanza, il legale rappresentante o soggetto da lui delegato) del Titolare stesso.

Tutti i componenti dell'unità di crisi diversi dal DPO devono essere adeguatamente formati sul contenuto degli artt. 4, 33 e 34 del Reg (UE) 679/2016

L'unità di crisi viene convocata presso la sede legale di ASP spa.

Nel corso della riunione viene effettuata, seguendo la metodologia di valutazione del rischio di cui all'Allegato 2, una valutazione del rischio approfondita che determini:

- natura della violazione,
- categoria/e e numero di interessati,
- probabili conseguenze delle violazioni,
- misure adottate.

D) Analisi delle valutazioni effettuate e delle azioni da intraprendere

L'Unità di crisi provvede poi ad individuare le azioni correttive (urgenti e strutturali) da attuare.

E) Nei casi in cui ASP SpA è titolare del trattamento: notifica della violazione al Garante della Privacy

Esclusivamente nei casi in cui la violazione dei dati attiene ad un trattamento per il quale ASP spa si configura quale Titolare, qualora l'Unità di crisi reputi probabile che l'incidente presenti un rischio per i diritti e le libertà degli interessati, l'Ufficio Privacy, con il supporto del DPO, dopo aver consultato le informazioni contenute all'indirizzo https://www.garanteprivacy.it/regolamentoue/databreach, sentito l'Amministratore Delegato, procede alla Notifica della violazione al Garante utilizzando il modello di cui all'Allegato 3.

La notifica deve avvenire, ove possibile, entro 72 ore dal momento in cui è stata rilevata la violazione dei dati personali. Se, dopo la notifica iniziale, una successiva indagine dimostra che l'incidente di sicurezza è stato contenuto e che non si è verificata alcuna violazione il Titolare del trattamento può informarne l'autorità di controllo. Tali informazioni possono quindi essere aggiunte

alle informazioni già fornite all'autorità di controllo e l'incidente può essere quindi registrato come un evento che non costituisce una violazione.

F) Nei casi in cui è ASP SpA è Titolare del trattamento: comunicazione agli interessati (se necessaria)

Qualora l'Unità di crisi abbia reputato che l'incidente rappresenti un ELEVATO rischio per i diritti e le libertà degli interessati, oltre alla notifica al Garante, sentito l'Amministratore Delegato, il Titolare del Trattamento procede alla comunicazione dell'incidente agli interessati utilizzando il modello di cui all'Allegato 4 ed in ogni caso senza ingiustificato ritardo.

L'unità di crisi determinerà anche, considerando i sistemi utilizzati di solito e il rapporto che intercorre con gli interessati, quale è il metodo più idoneo ad effettuare la comunicazione. Ad esempio, se la violazione ha ad oggetto la diffusione di indirizzi mail, andrà individuato uno strumento alternativo che permetta una comunicazione efficace, ossia che giunga direttamente all'interessato e non intercettabile da un ipotetico "violatore", anche chiedendo consiglio all'Autorità Garante stessa[1].

In ogni caso la comunicazione agli interessati deve essere:

a) tempestiva: ("senza ingiustificato ritardo", Art. 34 GDPR).

b) realistica: La finalità della comunicazione non è quella di "rassicurare" l'interessato, ma di portarlo a conoscenza dell'effettivo rischio che sta correndo; omettere la reale entità della violazione che è stata subita, per non ledere l'immagine pubblica o la fiducia degli interessati, rischia di compromettere maggiormente la situazione.

c) utile: Il titolare "dovrebbe anche fornire consulenza specifica alle persone fisiche sul modo in cui proteggersi dalle possibili conseguenze negative della violazione".[2]

G) Documentazione delle violazioni (Registro dei data breach)

In ogni caso, anche in assenza di notifica e/o comunicazione agli interessati, il Dirigente/Responsabile di funzione deve documentare qualsiasi violazione dei dati personali dei trattamenti che gli competono compilando la sezione appositamente dedicata nel Registro dei trattamenti; l'Ufficio Privacy detiene il Registro delle Violazioni di tutti i Trattamenti seguendo lo schema di cui all'All. 5.

5.2 VIOLAZIONE IN CASO DI TRATTAMENTI ESTERNALIZZATI

Nei casi in cui ASP Spa si avvale di soggetti esterni per il trattamento dei dati personali li nomina Responsabili esterni del trattamento di dati (ex art 28 GDPR). Qualora nei contratti con i

[1] Cfr. Garante Privacy, Provvedimento 30 aprile 2019 sul Data Breach;
[2] Cfr. "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679" del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati del 3 ottobre 2017, come modificate e adottate in ultimo il 6 febbraio 2018 e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018;

Responsabili esterni o in qualunque altro atto tra le parti non siano previste specifiche modalità di gestione dei data breach deve essere applicata la seguente procedura.
Il Responsabile esterno del trattamento è tenuto a comunicare ad ASP Spa (utilizzando l'allegato 1 – Modulo per la raccolta delle informazioni sulla violazione dei dati), l'avvenuta violazione entro e non oltre 24 ore dalla scoperta al fine di consentire ad ASP Spa (laddove questa sia Titolare del trattamento dei dati), la notifica al Garante e la eventuale comunicazione agli interessati entro i termini stabiliti dal Regolamento UE 679/2016.
Chiunque riceva segnalazioni di avvenute violazioni da parte di soggetti esterni, compresi i Responsabili esterni del trattamento, deve comunicarlo immediatamente al Direttore Esecutivo del Contratto/Referente Aziendale e all'Ufficio Privacy nelle modalità previste dall'art. 5.1 lett. A) punto c).

5.3 MODALITA' DI DIFFUSIONE DELLA PROCEDURA AL PERSONALE DIPENDENTE

La presente procedura sarà disponibile a tutti i dipendenti attraverso portale web nella propria Area Riservata del sito aziendale www.asp.asti.it nella sezione "Documenti vari".

5.4 TRASMISSIONE DELLA PROCEDURA AI RESPONSABILI ESTERNI DEL TRATTAMENTO

In caso di affidamento di lavori, servizi o forniture o di incarico consulenziale, che comporti trattamento di dati personali, a un soggetto esterno, nominato pertanto Responsabile del Trattamento ex art. 28 GDPR, sarà cura dell'Ufficio Approvvigionamenti inoltrare la presente Procedura allo stesso Fornitore o Consulente.

ALLEGATI

Fanno parte integrante della presente procedura i seguenti documenti:

- ✓ Allegato 1 - Modulo per la raccolta di informazioni sulla violazione dei dati
- ✓ Allegato 2 - Metodologia di valutazione del rischio connesso alla violazione
- ✓ Allegato 3 - Modello di notifica al Garante
- ✓ Allegato 4 - Comunicazione della violazione all'interessato
- ✓ Allegato 5 - Registro delle violazioni
- ✓ Allegato 6 - Esempi di violazioni di dati