Sistema Socio Sanitario
Regione Lombardia
ATS Brescia

Agenzia di Tutela della Salute di Brescia
Sede Legale: viale Duca degli Abruzzi, 15 – 25124 Brescia
Tel. 030.38381 Fax 030.3838233 - www.ats-brescia.it
Posta certificata: protocollo@pec.ats-brescia.it
Codice Fiscale e Partita IVA: 03775430980

DECRETO n. 300 del 23/05/2022

Cl.: 1.1.02

OGGETTO: Procedura da seguire in caso di violazione di Dati Personali (Data Breach) ai sensi degli articoli 33 e 34 del Regolamento UE 2016/679.

Il DIRETTORE GENERALE – Dott. Claudio Vito Sileo
nominato con D.G.R. XI/1058 del 17.12.2018

Acquisiti i ***pareri*** del	
DIRETTORE SANITARIO	Dott.ssa Laura Emilia Lanfredini
del	
DIRETTORE SOCIOSANITARIO	Dott.ssa Jolanda Bisceglia
e del	
DIRETTORE AMMINISTRATIVO	Dott.ssa Sara Cagliani

Sistema Socio Sanitario
Regione Lombardia
ATS Brescia

IL DIRETTORE GENERALE

Premesso che il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016 (di seguito GDPR), disciplina la protezione delle persone fisiche con riguardo al trattamento dei dati personali;
Atteso che detto Regolamento, entrato in vigore il 24 maggio 2016 e direttamente applicabile agli Stati dell'UE dal 25 maggio 2018, ha abrogato la direttiva 95/46/CE; non ha abrogato, invece, né il D.Lgs. n. 196/2003 (codice della privacy) né i provvedimenti del Garante privacy rimasti in vigore, nei limiti della compatibilità e sino ad eventuali differenti e specifichi interventi normativi;
Visto il D.Lgs. n. 101 del 10 agosto 2018 (entrato in vigore il 19 settembre 2018) che ha introdotto specifiche disposizioni finalizzate ad armonizzare le norme di cui al codice privacy nazionale con quelle introdotte dal GDPR;
Rilevato che:

- l'art. 33 del suddetto GDPR 2016/679 dispone che *"in caso di violazione di dati personali, il Titolare del Trattamento notifica la violazione all'autorità di controllo competente a norma dell'art. 55, senza ingiustificato ritardo e, ove possibile, entro le 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro le 72 ore, è corredata dai motivi del ritardo*";
- le Linee Guida del Gruppo di Lavoro art. 29 per la protezione dei dati del 03/10/2017 emendate in data 06/02/2018 dettagliano le iniziative che i soggetti tenuti debbono adottare con riguardo agli obblighi di notifica e di comunicazione delle violazioni sanciti dal GDPR, prevedendo altresì alcune misure che i titolari e i responsabili del trattamento possono intraprendere per soddisfare i nuovi obblighi;

Dato atto che per "Data Breach" si intende un evento in conseguenza del quale si verifica una "violazione dei dati personali" e cioè, come disposto dall'articolo 4 par. 1 punto 12 del GPDR "*una 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*", in conseguenza del quale il Titolare del trattamento non è più in grado di garantire l'osservanza dei principi relativi al trattamento di dati personali;
Ritenuto necessario adottare una procedura da seguire in caso di Data Breach che individui le azioni da porre in essere qualora si verifichi un evento sussumibile nella definizione sopra esplicitata;
Rammentato che:

- con Determinazione dirigenziale n. 473 del 09/07/2020 è stata formalizzata l'aggiudicazione del servizio di Responsabile della Protezione dei dati Personali (DPO) alla ditta Liguria Digitale SpA per il periodo dal 24/07/2020 al 23/07/2022;
- con Decreto D.G. n. 135 del 29/03/2019 è stata affidata alla Dottoressa Francesca Brun la "Funzione di gestione adempimenti in materia di protezione dei dati personali" e il coordinamento del Tavolo Tecnico Privacy, la cui composizione è stata di recente aggiornata in forza del Decreto D.G. n. 288 del 17/05/2022;

Considerato che la competenza in ordine alla notifica della violazione al Garante Privacy e della Comunicazione agli interessati è in capo al Direttore Generale, quale Titolare del trattamento e può essere da questi delegata con atto formale al Responsabile della Funzione di gestione degli adempimenti in materia di protezione dei dati personali (di seguito Responsabile Funzione Privacy) e, in caso di sua assenza e/o impedimento, ad uno dei componenti del Tavolo Tecnico Privacy sopra indicato, fra le cui funzioni si annovera l'assolvimento di ogni adempimento imposto

dalla normativa in materia di protezione dei dati personali, anche in accordo con le altre strutture dell'amministrazione di volta in volta interessate, al fine di garantire adeguata sicurezza e protezione al trattamento dei dati personali;
Vista la proposta della Dott.ssa Francesca Brun, quale titolare della "Funzione di gestione adempimenti in materia di protezione dei dati personali", che attesta, in qualità di Responsabile del procedimento, la regolarità tecnica del presente provvedimento;
Dato atto che dal presente provvedimento non discendono oneri per l'Agenzia;
Acquisiti i pareri del Direttore Sanitario, Dott.ssa Laura Emilia Lanfredini, del Direttore Sociosanitario, Dott.ssa Jolanda Bisceglia e del Direttore Amministrativo, Dott.ssa Sara Cagliani, che attesta, altresì, la legittimità del presente atto;

D E C R E T A

a) di approvare per le motivazioni di cui in premessa e che si intendono qui integralmente riportate, la "Procedura da seguire in caso di violazione di Dati Personali (Data Breach) - ai sensi degli articoli 33 e 34 del Regolamento UE 2016/679", allegata al presente atto quale parte integrante (composto da n. 12 pagine), comprensiva degli allegati - Allegato 1 "Segnalazione incidente di sicurezza" (composto di n. 3 pagine) e Allegato 2 "Modello di comunicazione del Data Breach all'interessato" (composto da n. 1 pagina);
b) di stabilire che la suddetta Procedura entra in vigore dalla data di approvazione del presente atto;
c) di dare atto che dal presente provvedimento non discendono oneri per l'Agenzia;
d) di demandare alla Funzione di gestione adempimenti in materia di protezione dei dati personali il compito di informare le articolazioni dell'Agenzia dell'approvazione della Procedura di che trattasi;
e) di pubblicare a cura della "Funzione di gestione delle relazioni interne ed esterne" il presente provvedimento nella sezione Privacy del sito web istituzionale;
f) di dare atto che il presente provvedimento è sottoposto al controllo del Collegio Sindacale, in conformità ai contenuti dell'art. 3-ter del D.Lgs. n. 502/1992 e ss.mm.ii. e dell'art. 12, comma 14, della L.R. n. 33/2009;
g) di disporre, a cura del Servizio Affari Generali e Legali, la pubblicazione all'Albo on-line – sezione Pubblicità legale - ai sensi dell'art. 17, comma 6, della L.R. n. 33/2009, e dell'art. 32 della L. n. 69/2009, ed in conformità alle disposizioni ed ai provvedimenti nazionali e comunitari in materia di protezione dei dati personali.

Firmato digitalmente dal Direttore Generale
Dott. Claudio Vito Sileo

Sistema Socio Sanitario
Regione Lombardia
ATS Brescia

PROCEDURA DA SEGUIRE IN CASO DI VIOLAZIONE DI DATI PERSONALI (*DATA BREACH*)

(ai sensi degli artt. 33 e 34 Regolamento UE 2016/679)

INDICE

1. PREMESSA e PRECISAZIONE DELLO SCOPO

La presente procedura è adottata da ATS Brescia con sede a Brescia (BS) viale Duca degli Abruzzi n. 15 e in forza del presente documento ATS Brescia si prefigge lo scopo di fornire indicazioni sulle opportune modalità di gestione delle eventuali violazioni di dati personali (c.d. data breach), nel rispetto della normativa in materia di trattamento dei dati personali, garantendo in particolare, l'aderenza ai principi e alle disposizioni contenute nel Regolamento UE 679/2016.

In particolare il documento individua le specifiche attività e le connesse responsabilità e competenze nel caso in cui si verifichino episodi che possono integrare un'ipotesi di violazione di dati personali trattati da ATS Brescia.

Per quanto non espressamente previsto nel presente Regolamento, si richiamano le norme vigenti che disciplinano la materia.

La competenza in ordine alla notifica della violazione al Garante Privacy e della Comunicazione agli interessati è in capo al Direttore Generale, quale Titolare del trattamento e può essere da questi delegata con atto formale al Responsabile della Funzione di gestione degli adempimenti in materia di protezione dei dati personali (di seguito Responsabile Funzione Privacy) e, in caso di sua assenza e/o impedimento, ad uno dei componenti del Tavolo tecnico in materia di privacy già istituito con atto del Direttore Generale e composto da differenti professionalità.

2. RIFERIMENTI NORMATIVI

- *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 – RGPD o, in inglese, GDPR): in particolare gli articoli 33 (Notifica all'Autorità di Controllo), 34 (notifica agli interessati) e 28 (Responsabile del trattamento)*

- *D.Lgs. 196/2003 "Codice per la protezione dei dati personali"*
- *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 Autorità Garante del 2 luglio 2015*

- *Artt. 331 e 361 del Codice di Procedura Penale (obbligo di denuncia da parte del pubblico ufficiale)*

- *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. 13 del Decreto del Presidente del Consiglio dei Ministri 24 ottobre 2014 "Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese. (14A09376) (G.U. 9 dicembre 2014, n. 285)*

3. DEFINIZIONE DATA BREACH

Per "Data Breach" si intende un evento in conseguenza del quale si verifica una "violazione dei dati personali"

Nello specifico, l'articolo 4 par. 1 punto 12 del GPDR definisce la violazione dei dati personali come "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".

La violazione dei dati personali è un tipo di incidente di sicurezza in conseguenza del quale il Titolare del trattamento non è più in grado di garantire l'osservanza dei principi relativi al trattamento di dati personali.

4. ALTRE DEFINIZIONI

"Dato personale": è «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» (cfr.art. 4 del Regolamento (UE) 2016/679 e art. 2, comma 1, lett. a), del D.Lgs 51/2018).

Specialmente delicati sono **dati appartenenti a categorie particolari (già denominati dati sensibili e supersensibili)**, e cioè dati personali idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale; dati genetici; dati biometrici intesi ad identificare in modo univoco una persona fisica; dati relativi alla salute o alla vita sessuale o all'orientamento sessuale e i **dati personali relativi a condanne penali e reati (già denominati dati giudiziari)** (cfr. artt. 9-10 del Regolamento (UE) 2016/679).

"**Incidente di sicurezza**" è un evento (o una serie di eventi) di origine dolosa o accidentale, esterno o interno all'organizzazione, che può comportare la compromissione dei dati detenuti da un'organizzazione, mettendo a rischio uno o più dei tre principi della sicurezza delle informazioni: riservatezza, integrità e disponibilità. Un incidente di sicurezza può riguardare contemporaneamente la riservatezza, l'integrità o la disponibilità di dati e informazioni o consistere in una qualsiasi combinazione di esse.

"**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. 2 lettera b) D. Lgs. 51/2018).

"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» (cfr. art. 4 punto 7), del Regolamento (UE) 2016/679 e art. 2, comma 1, lett. h), del D.Lgs 51/2018).

"**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» (cfr. art. 4, punto 8), del Regolamento (UE) 2016/679 e art. 2, comma 1, lett. i), del D.Lgs 51/2018).

"**Data Protection Officer"** (DPO): la persona fisica individuata come Responsabile del trattamento come individuato dalla Sezione 4 (artt. 367-39) del Regolamento (UE) n. 2016/679.

"**Delegato**": la persona cui il Titolare, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, attribuisce specifici compiti e funzioni connessi al trattamento di dati personali; la persona che viene in tal modo designata opera sotto l'autorità del Titolare che individua le modalità più opportune per l'espletamento delle funzioni delegate (Art. 2 quaterdecies D. Lgs. 196/2003).

5. CLASSIFICAZIONE DELLE VIOLAZIONI DI DATI PERSONALI (DATA BREACH)

La violazione dei dati personali, come sopra definita, può incidere sulla:

- Riservatezza, in caso di divulgazione o accesso a dati non autorizzato o accidentale;
- L'integrità, in caso di modifica non autorizzata o accidentale di dati personali;
- La disponibilità, in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.
  Le Linee Guida adottate dal Gruppo di Lavoro Articolo 29 ed approvate nella versione emendata il 6 febbraio 2018 (di seguito "Linee Guida") forniscono i seguenti esempi di perdita di disponibilità:
  • i dati sono stati cancellati accidentalmente o da una persona non autorizzata;
  • i dati sono stati crittografati in modo sicuro, ma la chiave per decrittografarli è stata persa ed il Titolare non può ripristinare l'accesso ai dati, ad esempio da un backup: in tal caso si avrà una perdita permanente di disponibilità;
  • vi è un'interruzione significativa del servizio regolare di un'organizzazione, ad esempio in caso di interruzione di corrente o attacco di tipo DoS che rende i dati personali non disponibili.

Una violazione può riguardare contemporaneamente le tre casistiche, nonché qualsiasi combinazioni delle stesse.

Tutti gli episodi di data breach sono da considerarsi tali a prescindere dalla gravità delle conseguenze. Determinati incidenti o violazioni potrebbero non avere particolari impatti sui diritti o sulle libertà degli interessati, ma è ugualmente importante riconoscerli e averne consapevolezza, affinché l'Agenzia e i Responsabili che gestiscono la sicurezza dei dati possano mettere in atto adeguate contromisure o implementare nuove misure preventive.

Il Regolamento sottolinea come una violazione può potenzialmente avere una serie di effetti avversi significativi sugli interessati che possono causare "danni fisici, materiali o immateriali". Ciò può includere la perdita del controllo sui propri dati personali, la limitazione dei loro diritti, discriminazione, il furto di identità o frode, una perdita finanziaria, una decifratura non autorizzata di pseudonimizzazione, un danno alla reputazione e la perdita di riservatezza dei dati personali protetti del segreto professionale, così come anche includere qualsiasi altro significativo svantaggio economico o sociale per gli individui

6. GESTIONE DELL'EVENTO

La procedura tecnica di gestione degli incidenti che comportano una violazione dei

dati personali si articola nelle seguenti fasi:

1. Acquisizione della notizia da parte dei soggetti "Riceventi" che provvederanno ad attivare i passi successivi;
2. Analisi dell'evento per determinare se vi è stata violazione;
3. Contenimento del danno;
4. Valutazione della gravità dell'evento;
5. Notifica al Garante Privacy, ove necessario;
6. Altre segnalazioni dovute, ove necessarie;
7. Comunicazione agli interessati, ove necessario;
8. Inserimento dell'evento nel Registro delle Violazioni;
9. Azioni correttive specifiche e per analogia.

7. ACQUISIZIONE DELLA NOTIZIA

La segnalazione di un data breach può essere effettuata da chiunque – sia esso dipendente da ATS o collaboratore a vario titolo (consulente, tirocinante, ecc) sia esterno all'organizzazione dell'Agenzia (DPO, fornitori, ecc) – ne abbia avuto notizia.

A tal fine è fatto obbligo ad ogni dipendente di segnalare, per il tramite del relativo Responsabile, qualsiasi incidente di sicurezza. La segnalazione deve essere accompagnata da una sintetica descrizione dell'incidente.

La segnalazione deve essere inoltrata, immediatamente, al Titolare e/o al Responsabile della Funzione Privacy mediante:

- posta elettronica – privacy@ats-brescia.it
- posta elettronica certificata – protocollo@pec.ats-brescia.it

Il Titolare o il Responsabile della Funzione Privacy qualora sussistano le condizioni per classificare il segnalato incidente di sicurezza come data breach ha a disposizione 72 ore per la successiva notifica al Garante.
Detto termine decorre da quando il Titolare o il Responsabile ha "*ragionevole grado di certezza*", previo completamento dell'istruttoria, che si è verificato un incidente di sicurezza che ha determinato la compromissione di dati personali

Eventuali notifiche effettuate oltre il termine delle 72 ore devono essere accompagnate dai motivi del ritardo.

8. ANALISI DELL'EVENTO E CONTENIMENTO DEL DANNO

A seguito della rilevazione e o segnalazione il Responsabile della Funzione Privacy anche mediante i componenti del Tavolo tecnico effettua una prima valutazione al fine di verificare che nell'incidente siano stati violati dati trattati dall'Agenzia.
L'analisi è finalizzata alla raccolta delle informazioni riguardanti:
- le categorie di interessati i cui dati sono stati violati (utenti, dipendenti, fornitori …);
- le categorie di dati personali compromesse (es, dati personali, dati sensibili, dati giudiziari …);
- la tipologia di incidente: violazione della riservatezza, disponibilità o integrità (es. accesso non autorizzato, perdita, alterazione, furto, disclosure, distruzione …)
- ogni altra informazione ritenuta necessaria

a tal fine può essere utilizzato il modello di cui all'allegato 1. (All. 1)

Il Responsabile della Funzione Privacy anche mediante i componenti del Tavolo tecnico mette in atto le opportune azioni, tempestivamente per il contenimento o annullamento del danno.

9. VALUTAZIONE DELLA GRAVITÀ DELL'EVENTO

Nella fase di valutazione occorre innanzitutto stabilire se nell'incidente sono coinvolti i dati personali.
In caso di risposta positiva occorre valutare l'impatto sugli interessati.
Se si tratta di una violazione di riservatezza occorre verificare che le misure di sicurezza in vigore (es.: cifratura dei dati) rendano improbabile l'identificazione degli interessati (non compromissione della chiave, algoritmo di cifratura o impronta senza vulnerabilità note). In caso di perdita di integrità o disponibilità di dati occorre valutare se è possibile il recupero degli stessi in tempi compatibili con i diritti degli interessati.
Se in tale modo i rischi per gli interessati sono trascurabili, la procedura può terminare, dopo aver documentato il processo e le scelte operate.

Nel caso in cui i rischi per l'interessato non siano trascurabili occorre procedere alla notifica al Garante.

Il Responsabile della Funzione Privacy anche mediante i componenti del Tavolo tecnico deve, con l'eventuale supporto di altre competenti Strutture dell'Agenzia, accertare la probabilità o meno che l'evento abbia comportato dei rischi per i diritti e la libertà delle persone; conseguentemente deve appurare se l'evento merita di essere notificato al Garante della Privacy e con quali modalità (notifica unica o per fasi)
In ogni caso dovrà:
- informare tempestivamente il DPO che dovrà fornire ogni necessario supporto;
- informare tempestivamente il Titolare al trattamento;
- effettuare una comunicazione all'Autorità giudiziaria competente, se necessaria e se non ancora effettuata dal segnalante.

In conformità a quanto disposto dall'art. 33 paragrafo n. 1 del Regolamento non vi è obbligo di notifica della violazione quando è "improbabile" che questa comporti un rischio per i diritti e le libertà delle persone fisiche.

Nella fase di valutazione del rischio si devono prendere in considerazione tanto la probabilità quanto la gravità del rischio per i diritti e le libertà fondamentali, sulla scorta di una valutazione oggettiva. La valutazione deve tenere conto dei seguenti criteri:
- Tipo di violazione;
- Natura, carattere sensibile e volume dei dati personali;
- Facilità di identificazione delle persone fisiche;
- Gravità delle conseguenze per le persone fisiche;
- Caratteristiche particolari dell'interessato;
- Caratteristiche particolari del titolare del trattamento di dati;
- Numero di persone fisiche interessate.

10. NOTIFICA AL GARANTE DELLA PRIVACY

Dopo avere effettuato l'analisi dell'evento con la raccolta delle informazioni descritte nei paragrafi che precedono ed aver valutato la gravità del danno (ossia se la violazione abbia comportato rischi non trascurabili per i diritti e le libertà delle persone) il Titolare del trattamento o suo Delegato deve effettuare la notifica al Garante Privacy.
Non appena il Titolare ha un ragionevole grado di certezza che si è verificata una violazione, se ricorrono i presupposti dell'art. 33 par. 1 del Regolamento, deve provvedere alla notifica all'Autorità di Controllo entro le 72 ore. Qualora il Titolare non riesca ad effettuare la notifica entro 72 ore, deve indicare i motivi del ritardo. Inoltre nella misura in cui non sia possibile fornire tutte le informazioni contestualmente, le informazioni possono essere fornite in fasi successive (così detta "notifica per fasi", "notifica preliminare" e "notifica integrativa"), senza ulteriore ingiustificato ritardo e con conseguente motivazione del ritardo medesimo.

La notifica è effettuata tramite apposita procedura telematica adottata per la notifica delle

violazioni dei dati personali con il provvedimento n. 209 del 27/05/2021 e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/.
La procedura telematica costituisce l'unica e ordinaria modalità mediante la quale la notifica può essere validamente eseguita e accolta dall'Autorità.

Se la notifica viene effettuata da un Delegato è necessario previamente informare il titolare del trattamento.

11. COMUNICAZIONE AGLI INTERESSATI

Se la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare o il suo Delegato deve comunicare la violazione anche all'interessato senza ingiustificato ritardo, al fine di fornire con tempestività, informazioni specifiche sulle misure da adottare per proteggersi.
La comunicazione agli interessati, secondo quanto previsto dal paragrafo n. 3 dell'art. 34 del Regolamento, non è richiesta quando:

- 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;
- 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 dell'articolo 3 del GDPR;
- la comunicazione richiederebbe sforzi sproporzionati; in tal caso, si procede invece ad una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

da predisporre secondo il modello allegato 2 (All. 2)

La comunicazione deve contenere, ai sensi dell'art. 34 del paragrafo 2 del Regolamento, le seguenti informazioni:
- una descrizione della natura della violazione;
- il nome e dati di contatto del responsabile dei dati (DPO) o di altro punto di contatto presso cui ottenere più informazioni;
- una descrizione delle probabili conseguenze delle violazioni 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 Garante può comunque richiedere al Titolare di comunicare la violazione anche agli interessati se ritiene che la violazione di dati personali presenti un rischio elevato.

La comunicazione dovrebbe avvenire considerando quanto segue:

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

Anche di queste fasi deve essere prodotta e conservata appropriata documentazione.

12. INSERIMENTO DELL'EVENTO NEL REGISTRO DELLE VIOLAZIONI

L'art. 33 paragrafo n. 5 del GDPR, prescrive al Titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all'Autorità di controllo di verificare il rispetto della norma.
Pertanto, il Titolare e/o il Responsabile della Funzione Privacy dovranno inserire nel Registro delle violazioni l'evento che sarà documentato e tracciabile e in grado di fornire evidenza nelle sedi competenti.

A tal fine viene istituito il Registro delle violazioni che dovrà riportare le seguenti informazioni:

- data segnalazione violazione
- soggetto segnalante
- tipo di violazione
- descrizione attività istruttoria
- riferimenti della notifica al Garante Privacy
- riferimenti della comunicazione agli interessati
- motivazione/i della mancata notifica al Garante Privacy
- motivazione/i della mancata comunicazione agli interessati
- note aggiuntive

La responsabilità della corretta gestione del Registro è affidata al Responsabile della Funzione Privacy che alla fine di ogni anno solare lo sottoscrive e lo inserisce nel sistema di gestione documentale mediante apposizione di un numero di protocollo.

13. MIGLIORAMENTO

Potranno essere previste in base alla violazione verificatasi, azioni di miglioramento come di seguito individuate, in maniera non esaustiva:

- analisi dell'incidente con figure tecniche-professionali competenti per individuare le vulnerabilità;
- adozione di nuovi sistemi tecnici di prevenzione/protezione e/o di sistemi di controllo/monitoraggio/allarme;
- individuazione di controlli e misure di sicurezza che diminuiscano la probabilità di reiterazione dell'incidente o i relativi impatti sul sistema colpito e su sistemi analoghi;
- valutazione su possibilità di copertura assicurativa;
- azioni informative e formative rivolte ai dipendenti;
- revisione delle relazioni con Clienti e Fornitori;
- pianificare dei test periodici per verificare la validità della presente procedura;
- revisione della procedura, se necessario, e di eventuali altri documenti collegati.

Tali azioni verranno definite dal Titolare o suo delegato.

Allegato 1

SEGNALAZIONE INCIDENTE DI SICUREZZA

DATI DEL SEGNALANTE	
Nome, cognome, qualifica	
Recapito telefonico, mail	
Struttura di appartenenza	
DATA DELL'INCIDENTE	
Quando si è verificata la violazione dei dati personali?	[] Il ___/___/_____ [] Tra il ___/___/____e il [] In un tempo non ancora determinato [] E' possibile che sia ancora in corso
LUOGO DELL'INCIDENTE	
Dove si è verificata la violazione dei dati personali?	
DESCRIZIONE DELL'INCIDENTE	
Classificazione dell'incidente	[ ] Violazione della riservatezza [ ] Violazione dell'integrità [ ] Violazione della disponibilità
Tipo di violazione	[ ] **Lettura** (presumibilmente i dati sono stati consultati, ma non sono stati copiati) [ ] **Copia** (I dati sono ancora presenti sul sistema/device, ma sono stati anche copiati altrove) [ ] **Alterazione** (I dati sono presenti sul sistema/device, ma sono stati alterati) [ ] **Cancellazione** (I dati non sono più sul sistema/device e non li ha più l'autore della violazione) [ ] **Furto di dati** (I dati non sono più sul sistema/device e li ha l'autore della violazione) [ ] **Furto di device o supporto di memorizzazione o materiale cartaceo** (es. computer, chiavetta USB, documenti cartacei contenenti particolari categorie di dati) - Specificare quale device, supporto di memorizzazione _____ [ ] **Furto di materiale cartaceo contenente categorie particolari di dati (es. cartelle ciniche, referti, etc.)** - Specificare la tipologia di documentazione_____ [[ ] **Furto di credenziali di accesso a** (es. account personale, password, applicazioni: AREAS, Concerto, etc.) [ ] **Accesso abusivo al sistema informatico:** - Denominazione del sistema _____ - Collocazione fisica del sistema (se interno o esterno all'Azienda) [ ] **Divulgazione non autorizzata o non voluta di dati personali** [ ] Altro _____

Oggetto della violazione	[ ] PC [ ] Rete [ ] Dispositivo mobile [ ] File o parte di un file [ ] Strumento di Backup [ ] Materiale cartaceo [ ] Altro
Quali categorie di soggetti interessati sono coinvolti dalla violazione?	[ ] Dipendenti [ ] Utenti [ ] Altro
Tipo di dato oggetto della violazione	[ ] Dati personali (es. dati anagrafici/codice fiscale/indirizzo di posta elettronica) [ ] Dati di accesso e di identificazione (username, password) [ ] Dati relativi a minori [ ] Dati personali idonei a rivelare l'origine razziale ed etnica [ ] Dati personali idonei a rivelare le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale [ ] Dati genetici [ ] Dati biometrici [ ] Dati relativi alla salute [ ] Dati relativi alla vita sessuale o all'orientamento sessuale [ ] Dati giudiziari [ ] Dati sanitari relativi a persone sieropositive, a persone che fanno uso di sostanze stupefacenti, di sostanze psicotrope e di alcool [ ] Altro :
Numero approssimativo degli interessati coinvolti nella violazione	[ ] numero certo di persone ____ [ ] numero presunto di persone____ [ ] numero sconosciuto di persone _____
Livello di gravità della violazione dei dati	[ ] Basso/trascurabile [ ] Medio [ ] Alto [ ] Molto alto
Effetti e conseguenze della violazione:	
Quali misure tecniche ed organizzative sono state adottate per contenere la violazione dei dati e prevenire violazioni future	

Allegato 2

MODELLO DI COMUNICAZIONE DEL DATA BREACH ALL'INTERESSATO

Modello da intestare/datare e protocollare

Gentile (*nome e cognome dell'interessato*),

Con la presente si comunica che *Nome del Titolare*, Titolare del trattamento in data è venuta a conoscenza di un evento che potrebbe aver coinvolto i Suoi dati personali.

In particolare, è accaduto quanto di seguito descritto.

Inserire breve descrizione dell'incidente in relazione al quale si ritiene necessaria la comunicazione all'interessato ed indicazione dei dati personali violate.

Dall'analisi dei fatti sopra riportati, in considerazione della natura della violazione e della tipologia di dati personali coinvolti, si comunicano le possibili conseguenze dell'evento:

Inserire descrizione delle probabili conseguenze del data breach

L'Agenzia, venuta a conoscenza dell'incidente, ha tempestivamente posto in essere le seguenti misure tecniche ed organizzative:

Descrizione delle azioni già poste in essere o di cui si propone l'adozione per porre rimedio o attenuare gli effetti del data breach

Come previsto dall'art. 33 del Regolamento UE 2016/679 l'Agenzia ha provveduto a notificare questa violazione al Garante Privacy (*se fatta notifica al Garante*).

Per ricevere ulteriori conformazioni, può contattare:

Email PEC *TEL.*

Distinti saluti

Il Titolare del Trattamento
o suo Delegato