PROCEDURA DATA BREACH

ALLEGATO N.1)

AL C.E.ed C. DI TE.RI. SRL – SEZIONE 5 – ART. 5.4 – SEZ. *Principi Generali* – compiti part. del Resp. – *lett. a)*

Articolo 1

(Cosa s'intende per "Data Breach")

Il GDPR 2016/679, all'art. 4, c. 12 definisce la violazione dei dati personali: "*Qualsiasi violazione di sicurezza che comporta anche 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*".

Si tratta di una definizione molto ampia, in quanto comprende qualunque evento che metta a rischio i dati personali trattati (indipendentemente dalla causa che l'ha generata, (i c.d. incidenti informatici, anche accidentali).

Articolo 2

(Notificazione de Data Breach)

Ai sensi e per gli effetti dell'art. 33 del Regolamento EU, in caso di violazione dei dati personali, il **Titolare** del Trattamento ha l'obbligo di notificare la violazione all'Autorità di controllo competente **senza ingiustificato ritardo** e, ove possibile, **entro 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 72 ore, devono essere esplicitati chiaramente i motivi del ritardo.

Al riguardo, il considerando 86 del GDPR chiarisce ulteriormente che l'obbligo di notifica interviene qualora la violazione dei dati personali sia suscettibile di presentare un rischio per i diritti e le libertà della persona fisica.

Articolo 3

(Modalità di notifica)

In caso di *Data Breach*, tutti i **Titolari** del Trattamento devono effettuare la notificazione della violazione dei dati personali al Garante per la Protezione dei Dati. Il GDPR distingue due modalità di notifica, a seconda della gravità di rischio per i diritti e le libertà delle persone fisiche, associato alla violazione:

1) la notificazione dell'avvenuta violazione di dati all'Autorità nazionale di protezione dati personali (prevista dall'art. 33 del Regolamento UE);
2) la comunicazione ai soggetti a cui si riferiscono i dati, nei casi più gravi (c.d. soggetti "interessati"), prevista dall'art. 34 del Regolamento UE.

Articolo 4

(Notifica all'Autorità di controllo e suoi contenuti)

In ossequio a quanto prescritto dall'art. 33 del GDPR 2016/679, l'**Azienda**, in qualità di **Titolare** del trattamento, procederà alla notifica all'Autorità di controllo, "*senza ingiustificato ritardo*" e, ove possibile, entro 72 ore da quando ne è venuto a conoscenza, ove risulti probabile che dalla violazione possano derivare rischi per i diritti e le libertà degli interessati.

Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, dovranno essere esplicitati e documentati i motivi del ritardo, anche al fine di non incorrere nelle sanzioni previste dal Regolamento Europeo.

La notifica all'Autorità di controllo deve contenere almeno le seguenti informazioni minime:

1) descrivere la 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 di registrazioni dei dati personali in questione;

2) comunicare il nome e i dati di contatto del Responsabile della Protezione dei Dati (DPO), del Responsabile del Trattamento dei dati o di altro contatto presso cui ottenere più informazioni;
3) descrivere le probabili conseguenze della violazione dei dati personali;
4) descrivere le 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.

Qualora non sia possibile fornire tutte le suddette informazioni contestualmente alla notifica, quest'ultima dovrà essere integrata, anche in fasi successive, con i dati e le notizie mancanti, senza ulteriore ingiustificato ritardo.

Articolo 5

(Comunicazione agli interessati e suoi contenuti)

In ossequio a quanto prescritto dall'art. 34 del GDPR 2016/679, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, l'**Azienda**, in qualità di **Titolare** del Trattamento, comunicherà, senza ingiustificato ritardo, la violazione all'interessato, anche al fine di consentirgli l'adozione di idonee precauzioni volte a ridurre al minimo il potenziale danno derivante dalla violazione dei suoi dati personali.

La comunicazione all'interessato si dovrà descrivere con un linguaggio semplice e chiaro:

a) la natura della violazione dei dati personali;
b) comunicare il nome e i dati di contatto del Responsabile della Protezione dei Dati (DPO) o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;

d) descrivere le 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 nel caso, per attenuarne i possibili effetti negativi.

Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

1) 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;
2) 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;
3) detta 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.

Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personal, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni è soddisfatta.

Articolo 6

(Condizioni per la mancata comunicazione agli Interessati)

In attuazione dell'art. 34, comma 3 del GDPR 2016/679, l'Azienda, in qualità di Titolare del Trattamento, non darà luogo alla comunicazione all'interessato, ove risulti comprova e soddisfatta una delle seguenti condizioni:

1) 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 ad es. la cifratura;
2) 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;
3) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Articolo 7

(Possibili determinazioni dell'Autorità di Controllo)

Nel caso in cui il titolare non abbia ancora comunicato all'interessato la violazione dei dati personali, l'Autorità di controllo può comunque richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al punto 1, 2 o 3 dell'articolo risulti soddisfatta.

Articolo 8

(Valutazione preliminare del rischio)

Una violazione dei dati personali può, se non affrontata in modo tempestivo, provocare danni fisici, materiali o immateriali, oltre che reputazionali alle persone fisiche.

In presenza di un'avvenuta accertata violazione dei stai personali, l'Azienda, in qualità di Titolare del Trattamento, procederà subito ad effettuare con riguardo alla natura, all'ambito di applicazione, al contesto ed alle finalità del trattamento,

una preliminare valutazione oggettiva sulle probabilità e gravità dei rischi, per i diritti e le libertà delle persone fisiche che possono derivare da trattamenti di dati personali oggetto di violazione con particolare riguardo ai seguenti aspetti:

1) limitazione o privazione dei diritti delle persone fisiche;
2) perdita dell'esercizio del controllo dei propri dati personali;
3) discriminazione;
4) furto o usurpazione d'identità;
5) perdite finanziarie;
6) decifratura non autorizzata della pseudonimizzazione;
7) pregiudizio alla reputazione;
8) perdita di riservatezza dei dati protetti dal segreto professionale;
9) qualsiasi danno economico o sociale significativo alla persona fisica interessata;
10) se sono trattati dei dati personali che rivelano l'origine raziale o etnica, le opinioni politiche, le convenzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;
11) in caso di valutazione di aspetti personali, mediante l'analisi o la previsione di spetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;
12) se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori;
13) se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

Inoltre, in sede di valutazione oggettiva dell'effettiva sussistenza del rischio e della

sua gravità, ai fini dell'eventuale assolvimento dell'obbligo di notifica delle violazioni di dati personali, si terrà debitamente conto anche delle circostanze di tale violazione, quali ad esempio:

a) se i dati personali fossero o meno protetti con misure tecniche adeguate di protezione atte a limitare efficacemente il rischio di furto d'identità o altre forme di abuso;

b) se esistono legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali.

Articolo 9

(Esiti della valutazione del rischio)

In relazione ai diversi esiti che possono derivare dalla valutazione preliminare del rischio, si potranno verificare le seguenti conseguenze:

1) ove risulti probabile che dalla violazione possano derivare rischi per i diritti e le libertà degli interessati, il Titolare del trattamento provvederà a:

1.1) notificare il data breach all'Autorità di controllo (art. 33 GDPR), secondo le previsioni di cui all'art. 4 del presente Regolamento;

2) ove risulti probabile che dalla violazione possano derivare elevati rischi per i diritti e le libertà degli interessati, il Titolare del trattamento provvederà a :

2.2) notificare il data brach all'Autorità di controllo (art. 33 GDPR), secondo le previsioni di cui all'art. 4 del presente Regolamento;

2.3) a comunicare il data breach ai soggetti cui si riferiscono i dati (c.d. "interessati"(art. 34 GDPR), secondo le previsioni di cui all'art. 4 del presente Regolamento;

3) ove, invece, risulti improbabile che dalla violazione possano derivare rischi per i diritti e le libertà degli interessati, il titolare del trattamento non procederà con le notifiche e le comunicazioni di cui ai precedenti n. 1 e 2.

Conformemente al principio di responsabilizzazione, dunque, l'Azienda è esentata dall'effettuare la notifica solo se è in grado di dimostrare al Garante che la violazione dei dati personali non presenta rischi per i diritti e per le libertà fondamentali delle persone fisiche interessate.

Articolo 10

(Modalità della Valutazione preliminare del rischio)

Ogni Autorizzato (già incaricato) o Responsabile del Trattamento ha l'obbligo di segnalare immediatamente con la più ampia libertà di forme e procedure (anche per le vie brevi e/o oralmente), la violazione dei dati personali, procedendo poi ala formale comunicazione entro massimo 24 ore ai soggetti di seguito indicati:

a) Titolare del Trattamento, in persona del Legale Rappresentante pro tempore;
b) DPO

Ai fini del rispetto dei tempi prescritti dalla normativa, d'intesa con il Titolare del Trattamento, unitamente alla Direzione Sanitaria ed Amministrativa, il DPO provvederà immediatamente e comunque non oltre le 24 ore successive alla ricezione della comunicazione, inviata anche per posta elettronica all'indirizzo dedicato a convocare, riunire e presiedere un tavolo tecnico, nella composizione minima di seguito indicata, per effettuare la valutazione preliminare sule probabilità e gravità dei rischi, per i diritti e le libertà degli interessati che possono derivare da trattamenti dei dati personali oggetto di violazione:

a) DPO
b) il Responsabile del Trattamento al quale si riferisce il data breach

Il DPO ha piena facoltà di convocare altri soggetti che ritiene utili alle necessità del caso.

Il DPO dovrà quindi curare e documentare l'attività istruttoria, acquisendo tutti gli elementi probatori alla base della valutazione.

All'esito delle attività dovrà essere redatto sintetico verbale con possibile documentazione di supporto, ricognitivo delle analisi e degli esiti della valutazione effettuata, nonché delle conseguenti proposte operative da sottoporre al Titolare del Trattamento per la decisione finale.

Detto verbale, sottoscritto da tutti i convenuti, sarà inoltrato al Titolare del Trattamento e per conoscenza alla direzione aziendale.

Ricevuto il verbale e l'allegata documentazione, in relazione all'esito della valutazione di cui all'art. precedente, il Titolare del Trattamento procederà come indicato nell'art. 9.

Gli eventuali atti di notifica all'Autorità di controllo e la possibile comunicazione a/agli interessato/i, saranno quindi predisposti e redatti da DPO e presentati al Titolare del Trattamento per la sottoscrizione.

Il DPO dovrà garantire che la notificazione, in via telematica tramite posta elettronica certificata sia effettuata dall'Autorità di controllo (anche se in forma generica e con riserva di integrazione) entro i termini prescritti dal GDPR 2016/679.

La comunicazione deve essere redatta con cura e attenzione in quanto può dar luogo a un intervento dell'Autorità di controllo nell'ambito dei suoi compiti e poteri previsti dal GDPR.

Articolo 11

(Registro cronologico)

Il Titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Atteso che tale documentazione consente all'Autorità di controllo di verificare, in qualsiasi momento, il rispetto del GDPR in materia di data breach, la stessa sarà custodita, con la massima cura e diligenza dal Titolare che dovrà tenere altresì apposito registro cronologico, elaborato secondo variabili di interesse dei casi di violazione dei dati.

Articolo 12

(Soluzioni e responsabilità)

Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi il GDPR 2016/679, ha il diritto di proporre reclamo ad un'Autorità di controllo, la quale può infliggere, a seconda dei casi, sanzioni amministrative pecuniarie effettive, proporzionate e dissuasive, ai sensi dell'art. 83.

Inoltre, in caso di data breach, l'interessato, ex art. 82, che subisce un danno materiale o immateriale causato da una violazione dei dati personali, ha anche il diritto di ottenere il risarcimento del danno dal Titolare del Trattamento o dal Responsabile del Trattamento, a meno che il Titolare del Trattamento non riesca a dimostrare di avere adottato tutte le misure di sicurezza previste dal Regolamento Europeo che l'evento dannoso non gli è in alcun modo imputabile.

Infine, l'art. 83 stabilisce espressamente che la violazione degli obblighi del Titolare del Trattamento e del Responsabile del Trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43 è soggetta a sanzioni.

Articolo 13

(Modalità di notificazione)

La notificazione della violazione dei dati deve essere redatta secondo il modello di cui all'art. 11, allegato al presente Regolamento (All.1) ed inviato telematicamente, tramite posta elettronica certificata, all'indirizzo: databreach.pa@pec.gpdp.it

Articolo 14

(Norma finale)

Per tutto quanto non espressamente previsto nel presente Regolamento si fa riferimento alla vigente normativa legislativa e regolamentare.

L'Azienda si riserva di apportare al presente Regolamento le modifiche, rettifiche e/o integrazioni che si renderanno necessarie, anche alla luce di eventuali innovazioni normative intervenute in materia o pronunciamenti dell'Autorità Garante per la protezione dei dati.

Articolo 15

(Modello allegato per la notifica data breach al Garante)

In allegato al presente Regolamento, il modello di notifica data breach al Garante (All.1)

Il Responsabile del Trattamento _____

L'Amministratore di Sistema Gestionale _____

All.1

VIOLAZIONE DI DAITI PERSONALI

MODELLO DI COMUNICAZIONE AL GARANTE

Secondo quanto prescritto dal Provvedimento del 2 luglio 2015, le amministrazioni pubbliche ed oggi anche le aziende private sono tenute a comunicare al Garante all'indirizzo: databreach.pa@pec.gpdp.it le violazioni dei dati personali (data breach) che si verificano nell'ambito delle banche dati (qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti, art. 4, comma 1, lett. P del Codice) di cui sono titolari.
La comunicazione deve essere effettuata entro 48 ore dalla conoscenza del fatto, compilando il modulo che segue.

Amministrazione titolare del trattamento:

Denominazione o ragione sociale:

Provincia: Comune:

CAP: Indirizzo:

Nome persona fisica addetta alla comunicazione:

Cognome della persona fisica addetta alla comunicazione:

Funzione rivestita:

Indirizzo PEC o MAIL per eventuali comunicazioni:

Recapito telefonico per eventuali comunicazioni:

Eventuali contatti:

Denominazione della/e banca/e dati oggetto di data breach e breve descrizione della violazione dei dati:

Quando si è verificata la violazione dei dati?:

- il
- tra il e il
- in un tempo non ancora determinato
- è possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati?:

Modalità di esposizione al rischio

Tipo di violazione:

- lettura (presumibilmente i dati non sono stati copiati)
- copia (i dati sono ancora presenti sul sistema del titolare)
- alterazione (i dati sono presenti sui sistemi ma sono alterati)
- cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
- furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
- altro:

Dispositivo oggetto della violazione:

- computer
- rete
- dispositivo mobile
- file o parte di un file
- strumento di backup
- documento cartaceo
- altro:

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti con indicazione della loro ubicazione:

Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati?

- n. persone
- circa persone
- un numero ancora sconosciuto di persone

Che tipo di dati sono oggetto di violazione?

- dati anagrafici
- dati di acceso e identificazione (user name, password, altro)
- dati relativi a minori

- dati personali idonei a rivelare l'origine raziale ed etnica, orientamento religioso, filosofico o di altro genere, opinioni politiche, adesione a partiti, sindacati organizzazioni o associazioni
- dati personali idonei a rivelare lo stato di salute e la vita sessuale
- dati giudiziari
- copia per immagine su supporto informatico di documenti analogici
- ancora sconosciuto
- altro

Livello di gravità della violazione dei dati personali trattati nell'ambito della banca dati (secondo le valutazioni del titolare):

- basso/trascurabile
- medio
- alto
- molto alto

Misure tecniche e organizzative applicate ai dati oggetto di violazione:

La violazione è stata comunicata anche agli interessati?

- si è stata comunicata il
- no, perché

Qual è il contenuto della comunicazione resa agli interessati?

Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?