ASL RIETI

REGIONE LAZIO

**AZIENDA SANITARIA LOCALE RIETI**

Via del Terminillo, 42 - 02100 – Rieti - C.F. e P.I. 00821180577

Tel. 0746-2781- PEC:asl.rieti@pec.it – www.asl.rieti.it

***Commissario Straordinario: Dott. ssa Marinella D'Innocenzo***

**Decreto Presidente Regione Lazio n. T00051 del 17.03.2017**

**Deliberazione n.1/C.S. del 20.03.2017**

# DELIBERAZIONE DEL COMMISSARIO STRAORDINARIO n. 598 del 03.11.2017

STRUTTURA PROPONENTE: Ufficio Prevenzione della Corruzione, Trasparenza e Privacy

Oggetto: Regolamento Europeo UE679/2016: Adozione Regolamento aziendale in materia di c.d. "Data Breach".

Estensore: Dott.ssa Annamaria Di Rico Firma Annamaria Di Rico

Il Dirigente sottoscrivendo il presente provvedimento, attesta che lo stesso, a seguito dell'istruttoria effettuata, nella forma e nella sostanza, è totalmente legittimo, ai sensi dell'art.1 della L. n° 20/1994 e ss.mm.ii., assumendone di conseguenza la relativa responsabilità, ex art.4, comma2, L.165/2001, nonché garantendo l'osservanza dei criteri di economicità, di efficacia, di pubblicità, di imparzialità e trasparenza di cui all'art.1, comma 1°, L. n.° 241/1990, come modificato dalla L. n° 15/2005. Il dirigente attesta altresì che il presente provvedimento è coerente con gli obiettivi dell'Azienda ed assolutamente utile per il servizio pubblico ai sensi dell'art.1, L. n° 20/1994 e ss.mm.ii.

Responsabile del Procedimento: Dott.ssa Annamaria Di Rico Firma Annamaria Di Rico

Data 27/10/2017

Il Dirigente: Dott.ssa Barbara Proietti

Data 30-10-2017 Firma

~~Il Direttore~~ della U.O.C. Economico Finanziaria con la sottoscrizione del presente atto attesta che lo stesso non comporta scostamenti sfavorevoli rispetto al budget economico.

Voce del conto economico ~~su cui~~ imputare la spesa: _____

Autorizzazione: _____

Data _____ Dott.ssa Barbara Proietti Firma _____

Parere del Direttore Amministrativo Dott. ssa Anna Petti

favorevole ☒ non favorevole (con motivazioni allegate al presente atto) ☐

Data 02/11/2017 Firma

Parere del Direttore Sanitario Dott. Paolo Anibaldi

favorevole ☒ non favorevole (con motivazioni allegate al presente atto) ☐

Data 02/11/2017 Firma

**IL RESPONSABILE DELL' UFFICIO PREVENZIONE DELLA CORRUZIONE, TRASPARENZA E PRIVACY**

**PREMESSO che:**

- con il D.Lgs. n.196 del 30.06.2003 è stato emanato il codice in materia di protezione dei dati personali denominato "Codice della privacy";
- il legislatore ha voluto uniformare nei paesi appartenenti alla Comunità Europea la normativa in materia con l'emanazione di un Regolamento Europeo, pubblicato il 4 maggio 2016 sulla Gazzetta Ufficiale Europea, che introduce delle innovazioni ed abroga la Direttiva 95/46/CE attuata in Italia prima con la Legge 675/96 e successivamente con il Codice Privacy del 2003, finalizzato a sviluppare il mercato unico digitale attraverso la creazione e la promozione di nuovi servizi, applicazioni, piattaforme e software.
- Il succitato Regolamento Europeo Privacy UE/2016/679, entrato in vigore il 25 Maggio 2016 fissa il termine ultimo per adeguarsi ai nuovi obblighi in materia di protezione dei dati personali al 25 Maggio 2018;

**VISTO che** il succitato Regolamento:
- all'art.4, c.12 definisce la violazione dei dati personali il c.d. "Data Breach";
- agli artt. 33 e 34 prevede la tempistica e modalità di notifica all'Autorità di controllo ed all'interessato per i casi più gravi;

**CONSIDERATO** prioritario tra i vari nuovi adempimenti imposti dal Regolamento UE proporre un regolamento che disciplini le modalità procedurali aziendali per la notifica delle violazioni dei dati personali- "data breach";

**VISTO** quanto disposto dalla normativa in parola si è formulato un Regolamento aziendale in materia di c.d. Data Breach, allegato al presente atto e parte integrante dello stesso;

**VISTO** il D.L.vo 502/92 e successive modificazioni ed integrazioni;

**DATO ATTO** che la proposta è coerente con il vigente Piano Triennale Aziendale della Prevenzione della Corruzione e del Programma Triennale per la Trasparenza e l'Integrità;

**PROPONE**

**DI** adottare il Regolamento aziendale in materia di c.d. "Data Breach" allegato, parte integrante del presente atto, formulato ai sensi dell'art.33 del Regolamento Europeo UE 2016/679;

**DI DISPORRE** che il presente atto venga pubblicato nell'albo pretorio on-line aziendale ai sensi dell'art.32, comma1, della legge 18.09.2009, n.69 e del D.Lgs. 14.03.2013 n.33

in oggetto ☐ per esteso ☒

## IL COMMISSARIO STRAORDINARIO

Preso atto:

- Il Dirigente sottoscrivendo il presente provvedimento, attesta che lo stesso, a seguito dell'istruttoria effettuata, nella forma e nella sostanza, è totalmente legittimo, ai sensi dell'art.1 della L. n° 20/1994 e ss.mm.ii., assumendone di conseguenza la relativa responsabilità, ex art.4, comma2, L.165/2001, nonché garantendo l'osservanza dei criteri di economicità, di efficacia, di pubblicità, di imparzialità e trasparenza di cui all'art.1, comma 1°, L. n.° 241/1990, come modificato dalla L. n° 15/2005. Il dirigente attesta altresì che il presente provvedimento è coerente con gli obiettivi dell'Azienda ed assolutamente utile per il servizio pubblico ai sensi dell'art.1, L. n° 20/1994 e ss.mm.ii.;

- Che il Direttore Amministrativo ed il Direttore Sanitario hanno espresso parere positivo con la sottoscrizione dello stesso;

## DELIBERA

- Di approvare e far propria la proposta di cui trattasi che qui si intende integralmente riportata;

- Di dichiarare il presente provvedimento immediatamente esecutivo non essendo sottoposto al controllo regionale, ai sensi del combinato disposto dell'art.30 della L.R. n. 18/94 e successive modificazioni ed integrazioni e degli artt.21 e 22 della L.R. 45/96.

Il Commissario Straordinario
Dott.ssa Marinella D'Innocenzo

La presente Deliberazione è inviata al Collegio Sindacale

in data 03 NOV. 2017

La presente Deliberazione è esecutiva ai sensi di legge

dal 03 NOV. 2017

La presente Deliberazione viene pubblicata all'Albo Pretorio on-line aziendale
ai sensi dell'art.32, comma 1, L.18.09.2009, n.69 e del D.Lgs. 14.03.2013 n.33

in oggetto ☐ per esteso ☒

in data 03 NOV. 2017

Rieti lì 03 NOV. 2017

IL FUNZIONARIO

SISTEMA SANITARIO REGIONALE
ASL
RIETI

REGIONE
LAZIO

# ASL RIETI
# REGOLAMENTO AZIENDALE
# IN MATERIA DI C.D. *DATA BREACH*

1. Cosa s'intende per *"Data Breach"*;
2. Notificazione del *Data Breach;*
3. Modalità di notifica;
4. Notifica all'Autorità di controllo e suoi contenuti;
5. Comunicazione agli Interessati e suoi contenuti;
6. Condizioni per la mancata comunicazione agli Interessati;
7. Possibili determinazioni dell'Autorità di controllo;
8. Valutazione preliminare del rischio;
9. Esiti della valutazione del rischio
10. Modalità della valutazione del rischio
11. Registro cronologico del DPO;
12. Sanzioni e responsabilità;
13. Modalità di Notificazione;
14. Norma finale;
15. Modello allegato per la notificazione Data Breach al Garante.

ALL. 1
Pag. 1 di 14

**Articolo 1**

***(Cosa s'intende per "Data Breach")***

Il Regolamento UE 679/2016, 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 del 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 D*ata breach*, tutti i Titolari del Trattamento devono effettuare la notificazione della violazione dati personali al Garante per la Protezione dei Dati.

Il Regolamento 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 violazioni di dati all'Autorità nazionale di protezione dei 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 Regolamento Eu, l'Asl di Rieti, 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:

a) 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;
b) comunicare il nome e i dati di contatto del Responsabile della protezione dei dati, del Responsabile del trattamento dei dati, 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 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 Regolamento Eu, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, l'Asl di Rieti, in qualità di titolare del trattamento, comunicherà, senza ingiustificato ritardo, la violazione all'interessato, anche al fine di consentigli l'adozione di idonee precauzioni volte a ridurre al minimo il potenziale danno derivante dalla violazione dei suoi dati personali.

La comunicazione all'interessato di dovrà descrive, con un linguaggio semplice e chiaro:

- la natura della violazione dei dati personali;
- comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;
- 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.

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

a) 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;

b) 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;
c) 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.

Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, 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, l'Asl di Rieti, in qualità di titolare del trattamento, non darà luogo alla comunicazione all'interessato, ove risulti comprova e soddisfatta una delle seguenti condizioni:

a) 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;
b) 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;
c) 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 del trattamento 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 alle lett. a), b) o c) dell'articolo risulti soddisfatta.

## Articolo 8

*(Valutazione preliminare del rischio)*

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

In presenza di una avvenuta, accertata violazione dei dati personali, l'Asl Rieti, 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 speudonimizzazione;
7. pregiudizio alla reputazione;
8. perdita di riservatezza dei dati protetti dal segreto professionale;
9. qualsiasi altro danno economico o sociale significativo alla persona fisica interessata;
10. se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni 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 aspetti 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 l'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:
   a. 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:
   a. notificare il *data breach* all'Autorità di controllo (art.33 GDPR), secondo le previsioni di cui all'art 4 del presente Regolamento;
   b. 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 comunicazioni di cui ai precedenti n.1) e 2).

Conformemente al principio di responsabilizzazione, dunque, l'Asl di Rieti 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.

All. 1
Prop. 7 del 14

## Articolo 10

*(Modalità della Valutazione preliminare del rischio)*

Ogni Responsabile di Unità Operativa complessa (UOC) o Semplice Dipartimentale (UOSd), in quanto Responsabile del trattamento di pertinenza del proprio settore 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 alla formale comunicazione entro massimo 24 ore ai soggetti di seguito indicati:

- Titolare del trattamento, in personale del Legale Rappresentante pro-tempore;
- DPO;
- Direzione sanitaria aziendale;
- Direzione amministrativa aziendale.

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 sulle probabilità e gravità dei rischi, per i diritti e le libertà degli interessati, che possono derivare da trattamenti dei dati personali oggetto di violazione

- DPO;
- il Responsabile del trattamento presso il cui servizio si è verificato il data breach;
- il Responsabile dell'UOC Informatica aziendale.

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 e protocollato, sarà inoltrato al Titolare del trattamento e per conoscenza alla direzione aziendale.

ALL. 2
Pag. 8 di 14

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 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 all'Autorità di controllo (anche se in forma generica, e con riserva di integrazione) – entro i termini prescritti dal Regolamento UE.
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 Regolamento Ue.

**Articolo 11**

***(Registro cronologico del DPO)***

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 DPO il quale, all'uopo, dovrà tenere altresì apposito registro cronologico, elaborato secondo variabili di interesse, dei casi di violazione dei dati.

**Articolo 12**

***(Sanzioni e responsabilità)***

Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi il Regolamento Eu., 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

All. 1
Pag. 3 di 14

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)***, pubblicato sul sito istituzionale Asl Rieti, 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 rinvio alla vigente normativa legislativa e regolamentare.
L'Asl Rieti 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.n1).***

Allegato 1 al Provvedimento del 2 luglio 2015

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

# VIOLAZIONE DI DATI PERSONALI

## MODELLO DI COMUNICAZIONE AL GARANTE

Secondo quanto prescritto dal **Provvedimento del 2 luglio 2015**, le amministrazioni pubbliche 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 persona fisica addetta alla comunicazione** _____

**Funzione rivestita** _____

**Indirizzo PEC e/o EMAIL per eventuali comunicazioni** _____

**Recapito telefonico per eventuali comunicazioni** _____

**Eventuali Contatti (altre informazioni)** _____

Allegato 1

**Denominazione della/e banca/banche dati oggetto di data breach e breve descrizione della violazione dei dati personali ivi trattati**

**Quando si è verificata la violazione dei dati personali trattati nell'ambito della banca dati?**

- ☐ Il _____
- ☐ Tra il _____ e il _____
- ☐ In un tempo non ancora determinato
- ☐ E' possibile che sia ancora in corso

**Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)**

**Modalità di esposizione al rischio**

**Tipo di violazione**

- ☐ Lettura (presumibilmente i dati non sono stati copiati)
- ☐ Copia (i dati sono ancora presenti sui sistemi del titolare)
- ☐ Alterazione (i dati sono presenti sui sistemi ma sono stati 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 :

All. 1
Pag. 13 di 14

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/codice fiscale
- ☐ Dati di accesso e di identificazione (*user name*, *password*, *customer ID*, altro)
- ☐ Dati relativi a minori
- ☐ Dati personali idonei a rivelare l'origine razziale ed etnica, 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 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?**

☐ Sì, 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?**

| |
|---|
| |