



I.S.R.A.A.
**ISTITUTO PER SERVIZI DI RICOVERO
E ASSISTENZA AGLI ANZIANI**
ENTE PUBBLICO - I.P.A.B. - Decreto Regione Veneto
n. 43 del 09/01/1991

| | | |
|-------------|------------|----------|
| Presidente | Luigi | CALDATO |
| Consiglieri | Walter | FRANDOLI |
| | Gianfranco | PIVATO |
| | Maurizio | VANIN |
| | Paolo | ZORZI |

| P | A |
|-------------------------------------|-------------------------------------|
| <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> |

Segretario Giorgio PAVAN

DELIBERAZIONE DEL CONSIGLIO DI AMMINISTRAZIONE

N. 01 del 10.01.2020

**OGGETTO: ADEGUAMENTO AL GDPR - ARTICOLI 33 e 34 DEL
REGOLAMENTO (UE) 679/2016. ADOZIONE DELLA PROCEDURA
PER LA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI
(DATA BREACH)**

RELATORE il Presidente

Premesso che in data 25.05.2018 è entrato in vigore il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati). Premesso inoltre che in data 19.09.2018 è entrato in vigore il D.lg. 10.08.2018 n. 101, di armonizzazione al Regolamento (UE) 2016/679.

Evidenziato come il Regolamento (UE) 2016/679 – denominato “Regolamento generale sulla protezione dei dati”, in sigla RGPD – detti una nuova disciplina in materia di trattamento dei dati personali, prevedendo tra gli elementi caratterizzanti e innovativi il “principio di responsabilizzazione” (c.d. accountability) e ponendo al centro del nuovo quadro normativo la figura del “Responsabile della protezione dei dati”, in sigla RPD.

Sottolineato come l’Ente sia tenuto, a seguito dell’entrata in vigore del Regolamento (UE) 2016/679, ad una serie di adempimenti conseguenti;

Ricordato che ISRAA ha proceduto alla nomina del RPD, nella persona della dr.ssa Silvia Mastrangelo;

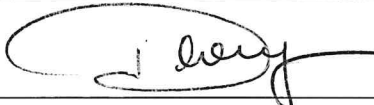
Accertato che tra gli adempimenti obbligatori ai sensi della normativa comunitaria in esame rientri quello previsto dagli artt. 33 e 34 del Regolamento (UE) 2016/679, e segnatamente quello

relativo all'adozione di una specifica procedura disciplinante la gestione delle violazioni dei dati personali ("data breach");

ciò premesso;

IL CONSIGLIO DI AMMINISTRAZIONE

- Preso atto che a far data dal 19 febbraio u.s. il Consiglio di Amministrazione dell'Ente agisce in regime di prorogatio ai sensi dell'art. 6 dello Statuto e ai sensi della Circolare n. 2 della Giunta Regionale del Veneto del 13/05/1996 avente ad oggetto: "IPAB, modificazioni statutarie, indicazioni istruttorie"
- Preso atto di quanto esposto dal relatore;
- preso atto dei pareri:
 - in ordine alla regolarità tecnica;

| | | |
|-------------------|---------------------------|---|
| Parere favorevole | IL DIRETTORE COORDINATORE |  |
|-------------------|---------------------------|---|

Ad unanimità di voti espressi in forma palese;

DELIBERA

1. di adottare, per le motivazioni esposte in premessa, la procedura disciplinante la gestione delle violazioni dei dati personali ("data breach") di cui agli artt. 33 e 34 del Regolamento (UE) 2016/679, allegata alla presente deliberazione per formarne parte integrante e sostanziale;
2. di pubblicare la documentazione allegata nella Sezione Amministrazione Trasparente – Disposizioni Generali, nonché nella "Sezione Protezione dati personali" della home page del sito istituzionale www.israa.it;
3. di dare atto che il presente provvedimento è esecutivo dalla data della sua adozione, ai sensi dell'art. 20 del vigente Statuto, approvato con deliberazioni nn. 206 del 26.7.1999 e 249 del 30.08.1999 (Coreco n. 3999 del 9.9.99)

gp/ms

P:\PRIVACY3_DATA BREACH\DELIBERA APPROVAZIONE DATA BREACH\DELIBERAadozione procedura data breach .docx

DATA BREACH E PROCEDURA PER LA GESTIONE DEGLI EVENTI

I Premessa

Con il termine data breach, ai sensi degli artt. 33 e 34 del Reg. UE 679/2016, s'intende la violazione dei dati personali dell'interessato persona fisica, che può consistere, a titolo esemplificativo e non esaustivo (Considerando 85 del Regolamento), in:

- perdita del controllo dei dati personali che riguardano gli interessati o limitazione dei loro diritti;
- discriminazione, furto o usurpazione d'identità;
- perdite finanziarie, decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale;
- qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

II Le tipologie di violazione dei dati personali

In linea con la definizione di violazione di dati personali, ex art. 4 p.12 Reg. UE, possiamo distinguere 3 tipi di violazione, che possono tuttavia combinarsi tra loro:

- 1) violazione di riservatezza, quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale.
- 2) Violazione di integrità, quando si verifica un'alterazione di dati personali non autorizzata o accidentale.
- 3) Violazione di disponibilità, quando si verifica perdita, inaccessibilità, o distruzione, accidentali o non autorizzate, di dati personali.

III Cosa prescrive a riguardo il Regolamento UE?

A. Art. 33: Notifica al Garante.

Il Regolamento UE prescrive che il **titolare**, non appena viene a conoscenza di un'avvenuta violazione dei dati personali del trattamento, dovrebbe notificare la violazione al Garante della Privacy, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui è venuto a conoscenza del Data breach. Se non effettuata entro 72 ore, deve essere fornita una giustificazione per il ritardo.

La notifica

A norma dell'art. 33 *la notifica deve almeno:*



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 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.*

Resta fermo che *qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.*

La notifica va trasmessa al Garante per la protezione dei dati personali, inviandola all'indirizzo: protocollo@pec.gpdp.it, utilizzando il modello messo a disposizione del Garante e seguendo le istruzioni per la compilazione, scaricabile al seguente url: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9128501>.

La notifica, inviata al Garante tramite posta elettronica all'indirizzo pec di cui sopra, deve essere sottoscritta digitalmente (con firma elettronica qualificata/firma digitale) ovvero con firma autografa. In quest'ultimo caso la notifica deve essere presentata unitamente alla copia del documento d'identità del firmatario.

L'oggetto del messaggio deve contenere obbligatoriamente la dicitura "NOTIFICA VIOLAZIONE DATI PERSONALI" e opzionalmente la denominazione del titolare del trattamento.

La notifica non è dovuta se risulti improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Tale evenienza si verifica, per esempio, allorché siano state efficacemente attuate misure tecnologiche di cifratura o pseudonimizzazione che rendano improbabile ricostruire l'origine del dato, oppure quando il dato è inidoneo a rivelare alcunché di pregiudizievole o comunque riservato circa l'interessato.

B. Art. 34: Comunicazione all'interessato.

In aggiunta all'obbligo di notifica all'autorità di controllo, è previsto l'obbligo di comunicare, in un linguaggio semplice e chiaro, la violazione dei dati personali allo stesso interessato allorché tale violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

La Comunicazione all'interessato

A norma dell'art. 34 la comunicazione, la cui forma è libera, deve obbligatoriamente:

- *rappresentare 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.*

Anche ove sussistessero tali condizioni, l'art. 34 esonera il titolare dall'obbligo di comunicazione allorché sia soddisfatta almeno 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;*
- 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 analogo efficacia.*

IV Obblighi generali in capo al titolare del trattamento dei dati

Oltre alle specifiche richiamate dal Regolamento in ordine alle tecnologie che devono essere adottate per trattare i dati personali in sicurezza, l'art. 32 all'ultimo comma dispone che *il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali (ovvero gli incaricati) non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.*

E' opportuno che il titolare predisponga lettere di incarico precise ai responsabili ed agli incaricati, e fornisca loro adeguata formazione circa gli obblighi derivanti da *Data breach*.

Parimenti (art. 32.5) è fatto obbligo per **il titolare di documentare qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio**. Tale documentazione consente all'autorità di controllo di verificare il rispetto delle disposizioni di legge (cd. inventario delle violazioni).

Si ricorda che l'obbligo di notifica spetta al titolare, che pertanto è chiamato a verificare preventivamente l'idoneità del responsabile del trattamento, specie se trattasi di un fornitore di servizi esterno all'azienda, a gestire tempestivamente ed adeguatamente un data breach, anche prevedendo, a norma dell'art. 28 del Regolamento, idonei accordi che regolino il rapporto di fornitura in modo da garantire il rispetto del Regolamento.

L'uso dei servizi Cloud di archiviazione dati, infine, richiede una particolare attenzione da parte del titolare del trattamento, giacché il *Cloud* generalmente spoglia il titolare del trattamento della possibilità di ingerirsi nella gestione del sistema informatico. In tal caso il titolare del trattamento, oltre a verificare preventivamente che il servizio in *Cloud* abbia specifiche conformi al Regolamento Ue, *in primis* circa l'ubicazione dei server e le condizioni generali di contratto, dovrà anche



monitorare sistematicamente il registro dei log e degli eventi, per verificare eventuali violazioni dei dati personali, specie in punto accessi non autorizzati di terzi.

V Criteri per determinare l'opportunità della notifica

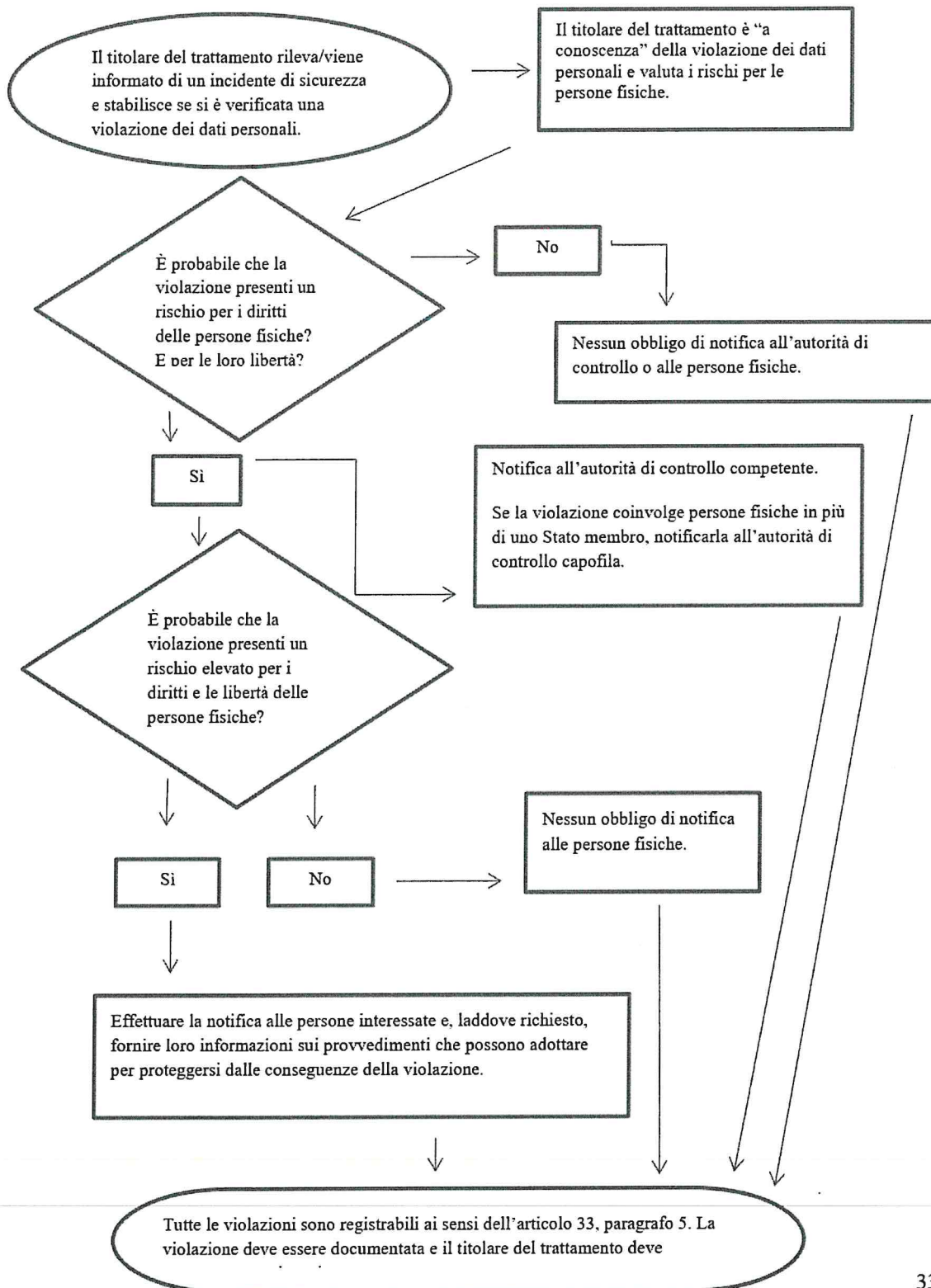
La qualificazione della violazione del Data breach è rimessa sostanzialmente al Titolare, sulla base della valutazione tanto della qualità del dato, quanto dei sistemi tecnologici a presidio dello stesso. Ed invero, a fronte della perdita di dati estremamente sensibili, un efficace sistema di anonimizzazione potrebbe rendere superfluo procedere alla notifica. Nel dubbio, tuttavia, è opportuno adottare la soluzione maggiormente in linea con le esigenze di tutela richiamate dal Regolamento.

In via preliminare si rimanda alle **linee guida WP 29 aggiornate al 6 febbraio 2018**, che forniscono una casistica di situazioni tipo che un Titolare del trattamento può essere chiamato ad affrontare in presenza di una Data Breach. Ove il caso concreto sfugga alla casistica elencata, criteri per potere compiere tale scelta consapevolmente sono stati individuati dall'European Union Agency for Network and Information Security (ENISA), nel documento chiamato "Recommendations for a methodology of the assessment of severity of personal data breaches".



WORKFLOW PROCEDURA DATA BREACH

A. Diagramma di flusso che illustra gli obblighi di notifica



VI Procedura per la gestione degli eventi in azienda

1. L'autorizzato al trattamento ravvisa un incidente nella gestione dei dati che astrattamente può determinare un data breach ai sensi del regolamento.
2. Viene senza indugio informato il titolare/responsabile, che di concerto con l'amministratore di sistema, nel caso il data breach si riferisca al trattamento dati effettuato con strumenti informatici, procedono alla valutazione d'impatto dell'incidente in relazione ai diritti degli interessati, utilizzando nell'ordine: la casistica offerta dal WP 29, la procedura ENISA.
Nel caso l'incidente sia ravvisato direttamente dall'amministratore di sistema, egli deve senza indugio notiziare il titolare e procedere di concerto alla valutazione d'impatto.
Se nominato, il DPO deve essere informato e messo nelle condizioni di partecipare.
3. In base all'esito della verifica:
 - a) se il data breach non risulta presentare alcun rischio per gli interessati, non si provvede ad alcuna notifica né all'autorità di controllo né agli interessati. Si procede comunque ad annotare nell'apposito registro l'incidente. Nel caso di responsabile esterno, il report deve essere trasmesso anche al titolare. Parimenti nel caso di contitolarità del trattamento, tutti devono essere notiziati dell'evento.
 - b) Se il data breach risulta presentare rischi per gli interessati, si procede conformemente allo schema del WP 29 allegato, oppure in base alla procedura ENISA, così da stimare la gravità del rischio per procedere alla notifica alla sola autorità garante (o all'autorità capofila nel caso l'incidente coinvolga interessati di diversi stati membri), financo ai singoli individui, utilizzando il modulo allegato.
4. In ogni caso tutti gli incidenti devono confluire in un registro conservato a cura del titolare a mezzo di ristretti autorizzati conformemente alla lettera di nomina.



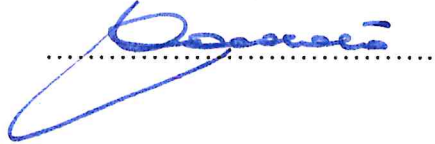
Si richiamano espressamente le:

- 1) Linee guida WP 29 Data Breach;
- 2) Casistica WP 29 in Italiano;
- 3) Procedura ENISA valutazione di impatto degli incidenti;
- 4) Excel con formule per applicazione della procedura ENISA;
- 5) Registro delle violazioni in formato Excel;
- 6) Modello di notifica Data-breach dal sito Garante;
- 7) Modello di comunicazione agli interessati.




Letto, approvato, viene sottoscritto

IL PRESIDENTE



I CONSIGLIERI



IL DIRETTORE



Il sottoscritto Direttore Coordinatore dell'Istituto per Servizi di Ricovero e Assistenza agli Anziani di Treviso certifica che copia informatica del presente atto, ai sensi dell'art. 20 del vigente Statuto dell'Ente e dell'art. 1 del Regolamento adottato con Deliberazione del Consiglio di Amministrazione I.S.R.A.A. nr. 14 del 04.03.2011, venne pubblicata all'Albo Telematico il giorno di 17.01.2020 e che non venne presentato alcun reclamo.

IL DIRETTORE

.....