PROCEDURA OPERATIVA PER LA GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

INDICE

Realizzata da:	Verifica	Approvazione
Dott.ssa Marianna Catalini	(RSGQI) Dr. Roberto Papa	Direttore Generale Dott. Michele Caporossi Direttore Amministrativo Dott. Antonello Maraldo Direttore Sanitario Dr. Arturo Pasqualucci

Rev.	Data	Natura della revisione	Pag.
00	18/10/2018	Emissione (con determina)	Tutte
01	13/07/2022	Aggiornamento e nuovo layout	Tutte

1. OGGETTO

Con la presente procedura operativa si intende regolamentare la gestione delle violazioni di dati personali nell'ambito dei trattamenti effettuati dall'Azienda in qualità di titolare del trattamento.

Infatti il Reg. UE 2016/679 agli artt. 33 e 34 prevede l'obbligo per il titolare di adottare misure tecniche ed organizzative in caso di violazione di dati personali in modo tale da accertare se si sia effettivamente verificata una violazione di dati personali e, in tal caso, valutare se la stessa possa presentare un rischio (probabilità) per i diritti e le libertà degli interessati, nonché la gravità per gli stessi.

Con la procedura in esame vengono adottate le misure organizzative per la gestione delle violazioni di dati personali nel rispetto delle prescrizioni di cui al Reg. UE 2016/679, affinché l'Azienda possa agire tempestivamente a tutela dei diritti e delle libertà degli interessati.

2. SCOPO E CAMPO DI APPLICAZIONE

Lo scopo della procedura è quello di provvedere tempestivamente agli adempimenti necessari nel caso in cui si verifichi una presunta violazione di dati personali e, conseguentemente, di dare istruzioni a tutto il personale circa le modalità di gestione di un episodio di violazione di dati personali, attribuendo responsabilità, funzioni e compiti ai diversi soggetti direttamente coinvolti nella gestione delle violazioni.

La presente procedura si applica, quindi, a tutto il personale dell'Azienda, nonché a tutti i soggetti che a diverso titolo svolgono attività di trattamento di dati personali per l'Azienda con qualsiasi modalità (informatica o cartacea) le stesse vengano condotte.

Al fine di meglio definire l'ambito di applicazione della procedura in questione si richiamano le definizioni di cui all'art. 4 del Reg. UE 2016/679[1] e di seguito si specifica che per violazione dei dati personali si intende la

[1] Ai fini dell'art. 4 Regolamento UE 2016/679 s'intende per: «dato personale»: 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; «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; «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile; «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico; «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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri; «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; «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento; «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile; «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento; «violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati; «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione; «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle

violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati, o comunque trattati.

Le violazioni di dati personali possono essere classificate in base ai tre principi della sicurezza delle informazioni:

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

Di seguito alcuni esempi di violazioni.

A) Distruzione: un insieme di dati personali che a seguito di incidente o azione fraudolenta non è più nella disponibilità del titolare, né di altri, e qualora tali dati siano richiesti dall'interessato non possano essere forniti.

1. Incendio di archivi cartacei contenenti documentazione relativa a dati personali.
2. Guasto non riparabile dell'hard disk contenente documenti che, in violazione al Reg. UE 2016/679, erano salvati solo localmente.
3. Distruzione di campioni biologici.

B) Perdita: un insieme di dati personali che a seguito di un incidente o azione fraudolenta non è più nella disponibilità del titolare, ma di terzi non autorizzati e quindi, qualora tali dati siano richiesti dall'interessato, non è possibile produrli ed il terzo potrebbe essere in possesso del dato in modo illegittimo.

1. Smarrimento supporto di memoria rimovibile.
2. Smarrimento documentazione contenente dati personali.

C) Modifica: un insieme di dati personali che, a seguito di un incidente o azione fraudolenta, è stato irreversibilmente modificato senza possibilità di ripristinare lo stato originale e in caso di richiesta da parte dell'interessato non sarebbe possibile produrlo in quanto alterato.

1. Guasto tecnico che altera parte di contenuti di un sistema informativo compromettendo anche i backup.
2. Azione involontaria o fraudolenta di chiunque che porti all'alterazione del dato in modo non tracciato e irreversibile.

D) Divulgazione/comunicazione non autorizzata: un insieme di dati personali che, a seguito di un incidente o azione fraudolenta, viene trasmesso a terzi senza il consenso dell'interessato o senza che ciò sia possibile sulla base delle disposizioni di legge e regolamentari.

---

caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici; «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute; «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51; «autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto: a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; c) un reclamo è stato proposto a tale autorità di controllo.

1. Trasmissione di dati personali ad opera del personale incaricato al trattamento a soggetti terzi non autorizzati a trattare il dato come, ad esempio, l'invio di documenti a soggetto diverso dall'interessato.

E) Accesso non autorizzato: un insieme di dati personali che sono messi a disposizione per un intervallo di tempo a persone non titolate a compiere quel trattamento specifico.
1. Accesso alla rete aziendale ad opera di terzi.
2. Accesso a dati personali di altro soggetto rispetto all'interessato per errore di profilazione.
3. Accesso a dati personali per i quali non si ha l'autorizzazione al trattamento.

F) Indisponibilità temporanea del dato: un insieme di dati personali che a seguito di un incidente o azione fraudolenta è non disponibile per un periodo di tempo così da ledere i diritti dell'interessato.
1. Cancellazione accidentale di dati che non possono essere immediatamente ripristinati.

La casistica sopra descritta è riportata a titolo esemplificativo e non esaustivo, pertanto, in caso di dubbio circa il fatto se si sia in presenza di una violazione o meno bisogna, comunque, seguire la presente procedura.

3. RIFERIMENTI NORMATIVI

- 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.
- D. Lgs. 30 giugno 2003 n. 196 (Codice in materia di protezione dei dati personali) così come novellato dal D.Lgs. 10 agosto 2018 n. 101.
- Linee Guida EDPB 01/2021 "Linee Guida in materia di notifica della violazione di dati personali wp 250".
- Parere 03/2014 sulla notifica delle violazioni dei dati personali adottato il 25 marzo 2014.
- Manuale RPD: "Linee guida destinate ai responsabili della protezione dei dati nei settori pubblici e para pubblici per il rispetto del Regolamento Generale sulla protezione dei dati dell'Unione Europea", approvato dalla Commissione luglio 2019.

4. COMPOSIZIONE DEL GRUPPO PER LA GESTIONE DI VIOLAZIONI DI DATI PERSONALI

Nell'ambito della presente procedura è stabilmente costituito un gruppo per la gestione di violazioni di dati personali che è deputato a verificare se ci sia stata una violazione e, conseguentemente, in caso di riscontro positivo, la natura, la gravità e, quindi, la probabilità di essa di incidere sui diritti e le libertà fondamentali degli interessati.
Il gruppo è così costituito:

- Referente aziendale privacy o, in sostituzione, suo delegato;
- Responsabile sistemi informativi o, in sostituzione, suo delegato;

- Responsabile Transizione Digitale o, in sostituzione, suo delegato (se diverso dal Responsabile sistemi informativi);
- Componente SO Qualità, rischio clinico, innovazione gestionale e tecnologica o, in sostituzione, suo delegato;
- DPO o, in sostituzione, suo delegato (con funzione di supporto/consulenza/informazione).

Il Coordinatore del "Gruppo per la gestione delle violazioni" è individuato nella figura del Referente aziendale per la privacy il quale è tenuto a svolgere i compiti spettanti al titolare del trattamento, ai sensi degli art. 33 e 34 Reg. UE 2016/679, quale figura a tal fine designata, resta inteso che l'attività conclusiva del Gruppo deve essere comunicata dal Referente aziendale Privacy al titolare per la sua validazione.

Il DPO, come previsto dal manuale RPD del luglio 2019 e dal Reg. UE 2016/679, svolge funzioni di consulenza, di informazione, di sorveglianza sull'osservanza del medesimo Regolamento europeo; in particolare nel caso si verifichi una violazione di dati, oltre ai compiti appena indicati, funge anche da punto di contatto per l'autorità di controllo e per gli interessati e supporta il titolare nella redazione dei documenti fornendo parere in merito alla struttura, amministrazione e impostazione della relativa documentazione.

Il DPO supporta, altresì, il titolare e per esso il Referente Aziendale Privacy nel processo di notifica all'autorità di controllo e durante qualsiasi successiva indagine da parte della medesima autorità, rimanendo sempre in capo al titolare (per esso il Referente Aziendale Privacy), nel rispetto della differenziazione dei ruoli e al fine di evitare situazioni di conflitto di interessi e incompatibilità, il compimento dei conseguenti adempimenti prescritti dalle disposizioni di legge in materia in capo al titolare.

L'individuazione dei "sostituti" deve avvenire sin dall'approvazione della presente procedura al fine di consentire l'individuazione dei soggetti che dovranno obbligatoriamente partecipare al gruppo per gli adempimenti dalla legge previsti in capo al titolare del trattamento.

I soggetti sopra individuati fanno parte stabilmente del "Gruppo per la gestione di violazioni di dati personali", il DPO nella funzione sopra indicata è previsto, nei suddetti termini, dalle disposizioni di legge in materia.

Il "Gruppo per la gestione violazioni di dati personali" deve essere implementato di volta in volta da ulteriori professionalità qualora, avuto riguardo alla tipologia ed alla natura della violazione riscontrata, l'eventuale violazioni veda coinvolte altre strutture a cui è affidata la gestione del processo che ha originato l'eventuale violazione o, comunque, qualora siano richieste specifiche competenze.

Si riporta di seguito una tabella riepilogativa della composizione del Gruppo per la gestione di violazioni di dati personali stabilmente costituito e di una possibile composizione allargata (quest'ultima indicata a titolo esemplificativo).

Tabella n. 1

	GRUPPO STABILE	GRUPPO ALLARGATO ipotesi 1	GRUPPO ALLARGATO ipotesi 1
Referente aziendale privacy/sostituto	X	X	x
Responsabile sistemi informativi/sostituto	X	X	x
Componente SO Qualità, rischio clinico, innovazione gestionale e tecnologica/sostituto	X	X	X
Responsabile per la transizione digitale/sostituto	X	X	X
DPO/sostituto	X	X	X
Direttore SO/SOSD/SO	-	X	-
Responsabile gestione conservazione documentazione sanitaria	-	-	-
Responsabile esterno al trattamento di dati personali	-	X	
Contitolare del trattamento di dati personali	-	-	X
Referente scientifico studi clinici - progetti ricerca/sostituto	-	-	X

5. FUNZIONAMENTO DEL GRUPPO PER LA GESTIONE DI VIOLAZIONI DI DATI PERSONALI

Il titolare del trattamento deve documentare qualsiasi violazione di dati personali, comprese le circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio, anche per le violazioni di dati personali che non sono soggette all'obbligo di notifica all'Autorità di Controllo. Le fasi di seguito descritte hanno lo scopo di documentare le attività poste in essere dal titolare mediante la predisposizione di appositi format che registrano le attività e le valutazioni compiute dal titolare del trattamento e che verranno inserite in apposito registro denominato "registro delle violazioni".

Il Gruppo per la gestione di violazioni di dati personali deve essere attivato dal Coordinatore ogniqualvolta venga effettuata una segnalazione.

La segnalazione circa una possibile violazione di dati personali può essere sia interna all'Azienda sia esterna, quindi, avvenire ad opera di soggetti terzi.

L'attivazione del Gruppo deve avvenire tempestivamente e, comunque, in un termine breve idoneo a stabilire se la segnalazione effettivamente configuri una possibile violazione di dati personali.

Il "termine breve" deve essere inteso quale quello strettamente necessario ad effettuare una preliminare istruttoria, sufficiente ad avere conoscenza del verificarsi di una possibile violazione di dati, da cui far decorrere il termine per le eventuali comunicazioni previste dagli art. 33 e 34 del Reg. UE 2016/679, fissato in 72 ore dalla conoscenza della violazione dei dati personali da parte del titolare del trattamento.

Il titolare del trattamento può dirsi a conoscenza della violazione di dati personali (direttamente o su segnalazione) solo quando al termine dell'istruttoria iniziale che deve essere tempestivamente effettuata, indicata al paragrafo 6.2 si è stabilito che la segnalazione configuri effettivamente una violazione di dati personali (cfr. linee guida sulla notifica delle violazioni dei dati personali ai sensi del Reg. UE 2016/679 del 6 febbraio 2018).
In considerazione di tale termine perentorio le attività relative alla gestione della violazione di dati dovranno, pertanto, essere organizzate in modo tale da rispettare il termine ultimo indicato dall'art. 33 del Reg UE 2016/679 secondo le modalità che di seguito vengono descritte.

6. MODALITA' DI SEGNALAZIONE E RILEVAZIONE DI UNA POSSIBILE VIOLAZIONE DI DATI PERSONALI (DATA BREACH)

Di seguito vengono descritte le modalità di segnalazione e rilevazione di una possibile violazione di dati.

6.1. SEGNALAZIONE

SEGNALAZIONE	
Chi	Chiunque ne venga a conoscenza (personale dell'Azienda, Responsabile del trattamento dati personali, soggetti terzi all'Azienda)
A chi	Al Titolare del Trattamento/Referente Aziendale Privacy/DPO o al Gruppo per la gestione di violazioni di dati personali o al direttore SO/SOSD/SOD che dovrà segnalarlo al Gruppo
Come	Preferibilmente mediante comunicazione scritta trasmessa anche via mail o, comunque, laddove non sia possibile procedere immediatamente, anche telefonicamente o di persona
Quando	Immediatamente, non oltre le 12 ore, da quando si è avuta conoscenza dell'evento che potrebbe dar luogo ad una violazione di dati personali

Il soggetto che effettua la segnalazione, qualora interno, dovrà fornire una breve descrizione degli eventi occorsi indicando cosa/dove/come/quando è successo, quali e quanti interessati sono stati coinvolti e le categorie e quantità dei dati oggetto della presunta violazione **(allegato n. 1)**.

Nel caso in cui la segnalazione sia avvenuta telefonicamente o di persona il segnalante interno dovrà, comunque, fornire successivamente ed in un tempo breve, entro poche ore da quando ha effettuato la comunicazione di persona o telefonicamente, una segnalazione scritta nei termini appena indicati.

Nel caso in cui la segnalazione pervenga da un soggetto esterno, al fine di avere una descrizione degli eventi occorsi, se non specificamente indicati nella segnalazione, il Gruppo potrà contattare il segnalante nell'immediatezza per acquisire le informazioni, non altrimenti acquisibili, utili alla corretta gestione della segnalazione e a compiere l'istruttoria necessaria per l'effettiva conoscenza dell'eventuale violazione. Anche in questo caso potrà, pertanto, essere acquisita una relazione scritta sugli accadimenti.

6.1. VALUTAZIONE DELLA SEGNALAZIONE

Il Gruppo per la gestione di violazioni di dati personali, una volta convocato, deve provvedere preliminarmente a verificare se la segnalazione possa o meno considerarsi una violazione di dati personali secondo quanto previsto dall'art. 4, comma 12, del Reg. UE 2016/679.

La valutazione circa l'effettiva configurazione di una violazione di dati personali viene effettuata dal Gruppo sulla base dei seguenti elementi come da modello per la valutazione della segnalazione **(allegato n. 2)**:

La segnalazione è riferita ad un fatto (possibile violazione) effettivamente accaduto
Il fatto che è segnalato è relativo a trattamenti di competenza del titolare del trattamento
La segnalazione ha comportato una perdita di riservatezza, integrità o disponibilità di dati di natura personale

6.2. VALUTAZIONE IN ORDINE ALLA GRAVITA' DELLA VIOLAZIONE ED ALLA PROBABILITA' CHE LA VIOLAZIONE DETERMINI UN RISCHIO PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI

Il Gruppo per la gestione di violazione di dati personali, una volta rilevato che la segnalazione configura una violazione, secondo quanto indicato al precedente paragrafo 6.1, effettua una valutazione in ordine:

1) alla probabilità che la violazione dei dati personali presenti un rischio per i diritti e le libertà degli interessati

2) al rischio elevato per i diritti e le libertà degli interessati

Tale valutazione viene effettuata sulla base del modello per la valutazione della violazione di dati personali **(allegato n. 3)** e viene compilata e sottoscritta dal Gruppo. Si precisa che il DPO, in quanto previsto dalla legge come figura autonoma ed indipendente rispetto al titolare del trattamento, sottoscrive il modello nella sua funzione di consulente e di supporto al titolare.

In particolare il modello tiene conto delle indicazioni e dei modelli messi a disposizione dell'Autorità Garante per la protezione dei dati personali.

Per quanto concerne la valutazione di cui al punto 1) del presente paragrafo "Probabilità che la violazione dei dati personali presenti un rischio per i diritti e le libertà degli interessati" si tiene conto dei seguenti criteri:

A) Categoria dei dati personali (ad esempio dati personali comuni e dati sensibili appartenenti alla particolare categoria di dati di cui all'art. 9 del Reg. UE 2016/679)

B) Tipologia del dato personale (ad esempio nome, cognome, indirizzo, data di nascita, residenza o domicilio, dati economici/finanziari, numero di tessera sanitaria, matricola, identità digitale) in relazione ad una specifica informazione (tipologia di dato personale come sopra indicato a titolo esemplificativo unitamente ad una condizione di salute specifica - malattia/patologia - o ad una condizione sociale - beneficiario di contributi o di esenzioni)

C) Numerosità dei dati per singolo interessato

D) Facilità di identificazione dell'interessato

E) Natura della violazione e in conseguenza della natura dell'incidenza della violazione sulla riservatezza e/o integrità e/o disponibilità valutare, a titolo esemplificativo il numero dei soggetti che sono venuti a conoscenza del dato personale, la durata dell'indisponibilità, la temporanea o definitiva perdita dell'integrità

Possono essere valutati ulteriori criteri in relazione alla specificità della violazione dei dati personali e peculiarità del trattamento di dati personali posto in essere.

Per quanto concerne la valutazione di cui al punto 2) del presente paragrafo "Il rischio per i diritti e le libertà degli interessati sia elevato" si tiene conto, oltre che dei criteri indicati appena sopra, anche di tali ulteriori criteri:

a) Categoria di interessati coinvolti con particolare riferimento alla loro fragilità

b) Numerosità degli interessati coinvolti

c) In caso di violazione della riservatezza, l'affidabilità del soggetto/soggetti che è/sono venuti a conoscenza del dato personale

Possono essere valutati ulteriori criteri in relazione alla specificità della violazione dei dati personali e peculiarità del trattamento di dati personali posto in essere.

Il Gruppo per la gestione di violazione di dati deve indicare le azioni di mitigazione da attuare nell'immediatezza, nonché quelle correttive da porre in essere in termini di prevenzione del rischio la cui implementazione dovrà essere monitorata dal DPO.

Il Gruppo, effettuate le valutazioni in ordine alla probabilità/improbabilità che la violazione possa comportare un rischio per i diritti e le libertà degli interessati e se tale rischio sia elevato, provvede, solo qualora sia accertata la probabilità del rischio per i diritti e le libertà degli interessati, alla notifica all'Autorità Garante per la protezione dei dati personali e, se il rischio sia ritenuto elevato, anche alla comunicazione agli interessati.

La notifica all'Autorità Garante per la protezione dei dati personali deve essere effettuata obbligatoriamente online sul sito istituzionale messo a disposizione dall'Autorità Garante medesima, non sono, infatti, accettate dall'Autorità altre modalità con cui procedere alla notifica.

Alla compilazione della notifica provvede materialmente il Referente aziendale per la privacy, quale soggetto designato dal titolare del trattamento, sulla base del modello messo a disposizione a titolo di fac – simile dall'Autorità Garante per la protezione dei dati personali **(allegato n. 4)**, compilato e sottoscritto dal Gruppo per la gestione di violazione dati personali. Si precisa che il DPO, in quanto previsto dalla legge come figura autonoma ed indipendente rispetto al titolare del trattamento, sottoscrive il modello esclusivamente nella sua funzione di consulente e di supporto al titolare del trattamento.

Si evidenzia che qualora non si disponga di tutte le informazioni necessarie ad effettuare la notifica completa all'Autorità di controllo nei termini previsti dal Reg. UE 2016/679 (72 ore da quando il titolare è a conoscenza della violazione), si dovrà procedere ad una notifica parziale che dovrà essere integrata dal Gruppo e materialmente effettuata dal Referente aziendale per la privacy non appena saranno state acquisite tutte le informazioni necessarie al suo completamento.

Nel caso in cui il Gruppo per la gestione di violazione dati personali ritenga di non dover procedere alle comunicazioni di cui sopra la violazione deve essere, comunque, iscritta nel Registro delle violazioni detenuto dall'Azienda **(doc. n. 5)** con i relativi documenti predisposti ed eventualmente acquisiti e rubricata con numerazione progressiva per anno; allo stesso modo deve essere iscritta la violazione di dati personali comunicata all'Autorità Garante per la protezione dei dati personali.

L'eventuale comunicazione all'interessato deve contenere la descrizione della natura della violazione e le probabili conseguenze, deve, inoltre, indicare i dati di contatto del DPO presso cui ottenere maggiori informazioni, nonché le misure adottate o che si intende adottare ai fini di mitigare l'occorso.

Tale comunicazione deve essere effettuata per conto del Titolare del trattamento dal Referente aziendale per la privacy.

7. ALLEGATI

Allegato n. 1: Modello segnalazione evento

Allegato n. 2: Modello per verifica natura segnalazione

Allegato n. 3: Modello analisi violazione

Allegato n. 4: Modello notifica all'Autorità di controllo[2]

Allegato n. 5: Schema registro violazioni

[2] La notifica dovrà essere effettuata esclusivamente online, non è infatti consentita una modalità di notifica differente: il modello ha solo la funzione di predisporre gli elementi e le informazioni necessarie alla notifica online.