Istituzione scolastica CPIA MATERA
via B. Matrazzo s.n.c.
75100 MATERA (MT)

P. IVA 93057380771

LINEA GUIDA VIOLAZIONE DATI PERSONALI

INDICE

1. INTRODUZIONE

1.1 SCOPO ED OBIETTIVI

Il presente documento ha lo scopo di definire le Linee Guida per gestire gli eventuali casi di Violazione Dati Personali (Violazione Dati Personali), che istituzione scolastica adotta ed applica al fine di rispettare le prescrizioni introdotte dalla normativa europea in materia di protezione dati personali, ed in particolare dagli artt 33 e 34 del Regolamento europeo n.2016/679 (nel seguito anche "Regolamento" o "GDPR").

1.2 AMBITO DI APPLICAZIONE

Il presente documento si applica a istituzione scolastica ed interessa tutti gli ambiti operativi, incluse anche le attività realizzate dai Fornitori che operano accedendo ai dati ed ai sistemi informativi di istituzione scolastica, ovvero effettuano i trattamenti nella titolarità di istituzione scolastica sui propri sistemi, nei termini e nei limiti indicati nei successivi paragrafi.

1.3 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 (regolamento generale sulla protezione dei dati) [GDPR]:**

  articolo 4 Definizioni - punto 12)

  «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;

  A titolo esemplificativo e non esaustivo, gli eventi di possibile ***Violazione dei dati personali*** possono essere costituiti da:

  - **distruzione di dati informatici o documenti cartacei** (intesa come indisponibilità irreversibile di dati con accertata impossibilità di ripristino degli stessi), conseguente ad eliminazione logica (es. errata cancellazione dei dati nel corso di un intervento manuale o automatizzato o fisica (es. rottura di dispositivi di memorizzazione informatica, incendio/allagamento locali dove sono archiviati i contratti ed altri documenti dei clienti)

  - **perdita di dati,** conseguente a smarrimento/furto di supporti informatici (es. laptop, HD, memory card) o di documentazione contrattuale o altri documenti cartacei (in originale o in copia)

- **accesso non autorizzato o intrusione a sistemi** informatici (es. sistemi di contact management gestiti dai call center), tramite lo sfruttamento di vulnerabilità dei sistemi interni e delle reti di comunicazione oppure attraverso la compromissione o rilevazione abusiva di credenziali di autenticazione (es. userid e password) per l'accesso ai sistemi

- **modifica non autorizzata di dati**, derivante ad esempio da un'erronea esecuzione di interventi sui sistemi informatici o intervento umano

- **rivelazione di dati e documenti a soggetti terzi non legittimati**, anche non identificati, conseguenti ad esempio alla fornitura di informazioni, anche verbali, a persone diverse dal soggetto legittimato (in assenza di delega formale di quest'ultimo), all'invio di fatture o altri documenti di valore contrattuale o esecutivo a soggetti diversi dall'effettivo destinatario o errata gestione di supporti informatici

art. 33 Notifica di una violazione dei dati personali all'autorità di controllo,

art. 34 Comunicazione di una violazione dei dati personali all'interessato

A livello nazionale, il Garante per la protezione dati personali (Garante Privacy) ha emesso una Guida all'applicazione al GDPR (http://www.garanteprivacy.it/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali) che fornisce indicazioni e raccomandazioni di carattere generale: relativamente alla Violazione Dati Personali queste sono riportate nella sezione "Approccio basato sul rischio e misure di accountability (responsabilizzazione) di titolari e responsabili".

2. LINEE GUIDA

2.1 DIAGRAMMA DEL PROCESSO DI GESTIONE VIOLAZIONE DATI PERSONALI

Nel diagramma di Fig. 1 sono indicati i passi fondamentali richiesti dalla normativa per la corretta gestione di eventi di Violazione Dati Personali, mentre il successivo schema di Fig. 2 fornisce indicazioni circa il contenuto informativo delle notifiche e delle comunicazioni che occorre effettuare verso il Garante Privacy e verso gli Interessati nonchè dei casi nei quali la comunicazione di Violazione Dati Personali agli Interessati può essere omessa, salvo diverso avviso del Garante Privacy.

Entrambi gli schemi forniscono una vista d'insieme del processo e delle attività che costituiscono la base delle linee guida descritte dal presente documento.

Nella figura che segue:

DPA= Data Protection Authority, ossia il Garante Privacy;

Data Breach= Violazione Dati Personali

Controller= Titolare di trattamento dati personali

Istituzione scolastica CPIA MATERA
via B. Matrazzo s.n.c.
75100 MATERA (MT)

P. IVA 93057380771

Processor= Responsabile di trattamento dati personali

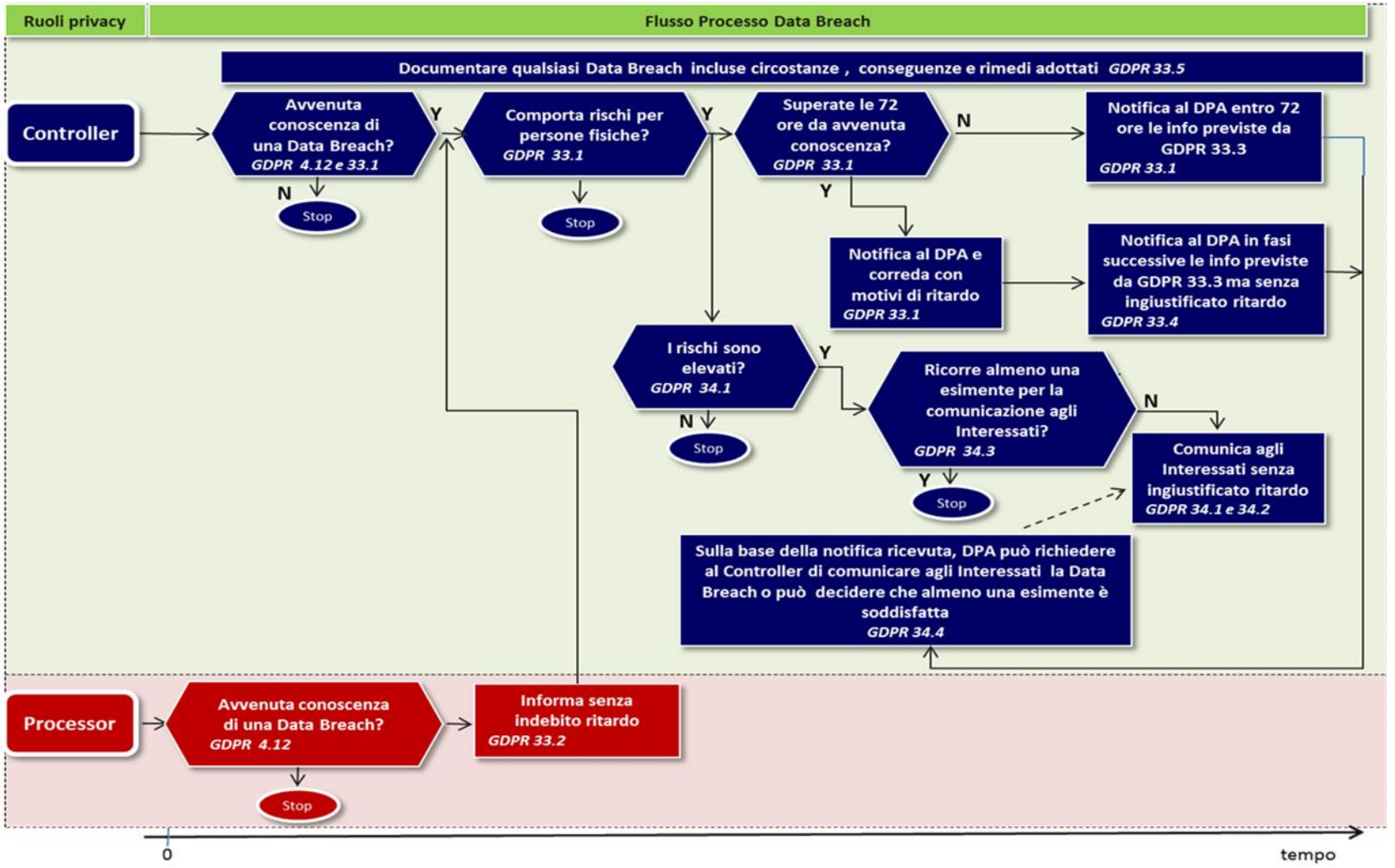
Ruoli privacy
Flusso Processo Data Breach
Documentare qualsiasi Data Breach incluse circostanze , conseguenze e rimedi adottati GDPR 33.5
Controller
Avvenuta conoscenza di una Data Breach? GDPR 4.12 e 33.1
Y
N
Stop
Comporta rischi per persone fisiche? GDPR 33.1
Y
Stop
Superate le 72 ore da avvenuta conoscenza? GDPR 33.1
N
Y
Notifica al DPA entro 72 ore le info previste da GDPR 33.3 GDPR 33.1
Notifica al DPA e correda con motivi di ritardo GDPR 33.1
Notifica al DPA in fasi successive le info previste da GDPR 33.3 ma senza ingiustificato ritardo GDPR 33.4
I rischi sono elevati? GDPR 34.1
Y
N
Stop
Ricorre almeno una esimente per la comunicazione agli Interessati? GDPR 34.3
N
Y
Stop
Comunica agli Interessati senza ingiustificato ritardo GDPR 34.1 e 34.2
Sulla base della notifica ricevuta, DPA può richiedere al Controller di comunicare agli Interessati la Data Breach o può decidere che almeno una esimente è soddisfatta GDPR 34.4
Processor
Avvenuta conoscenza di una Data Breach? GDPR 4.12
Stop
Informa senza indebito ritardo GDPR 33.2
0
tempo

Figura 1 - Diagramma

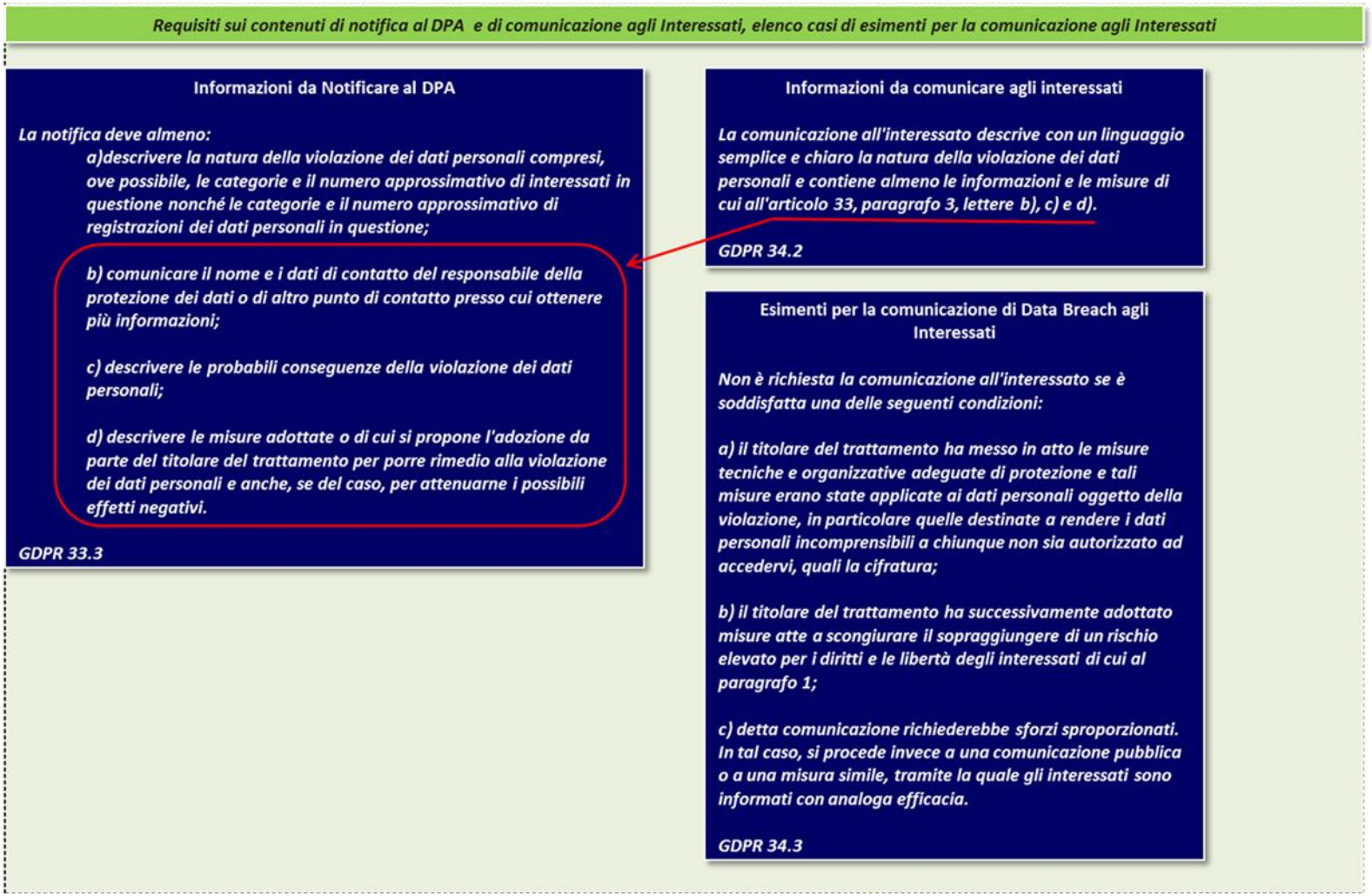

Figura 2 - Contenuti informativi ed esimenti

2.2 ASPETTI GENERALI

2.2.1 OBIETTIVI

Avendo a riferimento gli obiettivi perseguiti dal Regolamento in termini di protezione dei dati personali da accessi illegittimi, perdita, modifica, etc. è di fondamentale importanza che istituzione scolastica, quale Titolare del trattamento, definisca ed implementi un processo di **gestione della violazione -Violazione Dati Personali**, che sia in grado di assicurare di:

I) rilevare situazioni di Violazione Dati Personali, anche avvenute nell'ambito dei trattamenti di dati personali affidati a Responsabili –Processor, esterni in modo tempestivo e puntuale
II) valutare correttamente se un evento di Violazione Dati Personali comporti rischi per i diritti e le libertà fondamentali degli Interessati al fine di attivare il relativo processo di gestione della violazione procedendo negli step previsti a partire dalla Notifica al Garante Privacy
III) esaminare se la gravità dell'evento o la tipologia dei dati violati connoti le caratteristiche di "**rischio elevato**" procedendo, in caso affermativo, a dare corso anche alla Comunicazione agli Interessati, salvo che non esistano le condizioni per evitare di dover procedere in tal senso (condizioni esimenti di cui all'art. 34 c. 3 del Regolamento)
IV) gestire l'evento di Violazione Dati Personali fino alla sua risoluzione documentandolo come richiesto dalla norma
V) apprendere da quanto emerso con l'evento di Violazione Dati Personali per migliorare i processi e le procedure individuando ed applicando le opportune soluzioni volte a mitigare i rischi di nuova occorrenza di simili casi (Lesson Learnt).

2.2.2 AMBITO DI APPLICAZIONE

Tutti i dati personali dei quali istituzione scolastica è Titolare del trattamento devono essere protetti da adeguate misure di sicurezza e la loro violazione, in qualunque situazione si realizzi, deve attivare il processo di gestione della Violazione Dati Personali.
Anche nel caso in cui istituzione scolastica svolga il ruolo di Responsabile per trattamenti di titolarità di altre aziende, il processo di gestione Violazione Dati Personali dovrà esser attivato ma, in questo caso, limitatamente agli aspetti di rilevazione e di comunicazione senza indebito ritardo prevista dalla relazione Processor a Controller (Art. 33.2 del GDPR)

2.2.3 CRITERI DI INNESCO

Il processo di gestione di Violazione Dati Personali deve essere applicato per tutti i casi in cui istituzione scolastica, direttamente o indirettamente sia posta in condizione di avere il ragionevole dubbio ovvero l'evidenza del verificarsi di una violazione e ciò indipendentemente dal ruolo di Titolare o di Responsabile del trattamento in quanto, come previsto dall'art. 33 c. 1 e 2 del GDPR entrambi hanno l'obbligo di attivarsi per contrastare una tale evenienza.

2.2.4 RESPONSABILITÀ

2.2.4.1 Predisposizione

In istituzione scolastica è definito un Comitato Violazione Dati Personali (Comitato, o il Titolare) il quale:

- deve essere prontamente informato in caso di un presunto evento di Violazione Dati Personali
- devono essergli prontamente riportati eventuali problemi nel corso di gestione dell'evento
- ha compiti decisionali per la definizione delle azioni per la gestione dell'evento una volta che lo stesso sia catalogato come Violazione Dati Personali
- ha il compito di evidenziare le azioni di Lesson Learnt, a seguito della conclusione di un evento di Violazione Dati Personali, per mitigare i rischi di occorrenza di incidenti simili

Al fine di assicurare la corretta e tempestiva gestione di un evento di violazione, è necessario che:

A. per tutti i trattamenti dati nella titolarità di istituzione scolastica sia stata effettuata l'analisi dei rischi di base (Privacy Risk Analysis) in quanto adempimento propedeutico per effettuare la valutazione in ordine alla esigenza di notificare un evento di Violazione Dati Personali al Garante Privacy ed eventualmente anche agli Interessati
B. per tutti i contratti con fornitori operanti nel ruolo di Responsabili trattamento dati personali - siano presenti le opportune clausole che riportano l'obbligo di legge, per essi, di comunicare al Titolare prestare la propria collaborazione in caso di Violazione Dati Personali
C. sia definito un indirizzo email ove ricevere le segnalazioni di possibili casi di evento di Violazione Dati Personali sia dall'interno dell'azienda che dall'esterno, (fornitori, partner, ma anche clienti).

2.2.4.2 Responsabilità di gestione operativa di evento Violazione Dati Personali

Le attività di gestione operativa in caso di evento di Violazione Dati Personali prevedono:

1) la responsabilità operativa della struttura organizzativa competente per il trattamento dati personali nell'ambito del quale si è originato l'evento di Violazione Dati Personali, che cura anche il necessario collegamento con i suoi Responsabili trattamento dati personali e Terze Parti ed Interessati eventualmente coinvolti nell'evento.
A tale scopo le strutture organizzative aziendali individuano ciascuna un proprio punto di contatto per gli aspetti relativi a situazioni di potenziale Violazione Dati Personali (nel seguito: Referente Privacy).

2) il supporto operativo del Responsabile IT

3) ll supporto operativo del Responsabile legale per:

- la redazione dei testo di Notifica al Garante Privacy e relativo invio all'Autorità
- la redazione del testo di Comunicazione eventuale agli Interessati. La modalità ed il canale da impiegare per inoltrare la Comunicazione agli Interessati è individuata e resa operativa caso per caso.

Il Comitato ha la responsabilità di mantenere aggiornato il repository con le Informazioni relative ai casi di Violazione Dati Personali, che dovrà essere reso disponibile per essere consultato dal Garante Privacy.

Le responsabilità sono ulteriormente rappresentate in modo schematico nei successivi paragrafi.

2.3 REGOLE GENERALI

2.3.1 Step del processo di gestione evento di Violazione Dati Personali

2.3.1.1 Rilevazione, raccolta delle informazioni ed analisi

Tutte le persone che operano presso le organizzazioni aziendali, ciascuno in base al proprio ambito di competenza e responsabilità, in caso di sospetto di possibile evento di Violazione Dati Personali (vedasi definizione ed esempi riportati nel paragrafo "Riferimenti Normativi") invia senza indugio una comunicazione email all'indirizzo stabilito (vedasi quanto riportato nel precedente paragrafo "Responsabilità di Predisposizione") e al suo responsabile gerarchico in azienda. Quest'ultimo dovrà attivarsi per fornire il suo contributo alle attività di analisi che saranno svolte dal Comitato.

Queste mail rimangono archiviate nella mail box in oggetto per: 1 anno.

Il contenuto della mail box in oggetto è parte integrante del Repository di informazioni di cui al art. 33.5 del GDPR.

2.3.1.2 Valutazione delle evento

Il Comitato effettua una prima valutazione al fine di stabilire se si tratta o meno di Violazione Dati Personali:

I) sulla base della definizione di Violazione Dati Personali e degli esempi forniti nel precedente paragrafo di "Riferimenti Normativi"
II) sulla base del caso specifico e relative caratteristiche e contingenze
III) tenendo conto del risultato della più recente Privacy Risk Analysis effettuata sul trattamento di dati personali relativo al caso di possibile violazione all'esame, in particolare se presenta un livello di rischio superiore al minimo L (LOW)
IV) tenendo conto in particolare della natura e della gravità del caso specifico e delle sue conseguenze e effetti negativi per l'interessato, quali:
    - provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano 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 o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Inoltre il Comitato:

I) se il livello di rischio evidenziato dalla più recente Privacy Risk Analysis è maggiore di M (Medium) e
II) qualora non siano in essere le misure esimenti per la comunicazione agli interessati di cui alle lettere a) o b) dell'art 34.3 del GDPR.

valuta se ricorrono le condizioni per procedere anche con la comunicazione agli Interessati, a meno che non rilevi che, per il caso in esame, risulti essere applicabile la condizione prevista dall'art 34.3 lettera c) del GDPR per cui " *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.*"

Le decisioni assunte in questo step sono archiviate nel Repository di informazioni di cui all'art. 33.5 del GDPR.

2.3.1.3 Raccolta di ulteriori informazioni

Qualora necessario il Comitato richiede ai Referenti privacy ed ai Fornitori anch'essi eventualmente coinvolti nel caso di Violazione Dati Personali, di rendere al più presto disponibile ogni altra indicazione necessaria a circoscrivere meglio il caso e ad indirizzare la sua pronta risoluzione.
In particolare il Responsabile IT mantiene i rapporti con tutte le parti esterne, per la componente sistemi informatici, coinvolte lato Fornitori ai fini di una efficiente ed efficace comunicazione di informazioni ed indicazioni, coinvolgendo il competente Referente privacy aziendale.

Queste mail rimangono archiviate nella mail box per 1 anno e devono essere considerate parte integrante del Repository di informazioni di cui all'art. 33.5 del GDPR.

2.3.1.4 Notifica al Garante Privacy

Sulla base delle informazioni raccolte, e tenendo presenti le condizioni e le tempistiche di cui all'33.1e 33.3 del GDPR, il Responsabile legale provvede alla comunicazione verso il Garante Privacy, utilizzando modalità e forme indicate dalla stessa Autorità.

Queste comunicazioni sono archiviate nel Repository di informazioni di cui all'art. 33.5 del GDPR.

2.3.1.5 Comunicazione agli Interessati

Sulla base delle informazioni raccolte, e tenendo presenti le condizioni e le tempistiche di cui all'art. 34.1e 34.2 del GDPR viene effettuata la eventuale comunicazione verso gli Interessati. La modalità di veicolo della Comunicazione agli Interessati è di volta in volta individuata a cura del Comitato e resa operativa anche avendo a riferimento criteri di opportunità, impatti sul business, immediatezza ed efficacia del messaggio da veicolare.

Queste comunicazioni sono archiviate nel Repository di informazioni di cui all'art. 33.5 del GDPR.

2.3.1.6 Risoluzione dell'evento di Violazione Dati Personali

Le parti attivate dal Comitato, inclusi anche specifici fornitori/partner se opportuno/necessario, provvedono alle attività di competenza per la risoluzione dell'evento.

2.3.1.7 Chiusura evento di Violazione Dati Personali ed Archiviazione dati

Spetta al Comitato stabilire l'avvenuta risoluzione della problematica e, quindi, dichiarare concluso l'evento di Violazione Dati Personali.
Il Comitato redige un report descrittivo delle azioni svolte, le contromisure applicate e gli enti interni ed esterni coinvolti.

Questo report è archiviato nel Repository di informazioni di cui all'art. 33.5 del GDPR.

2.3.2 Step del processo di Lesson Learnt

Il Comitato in base a tutte le informazioni raccolte sul caso di Violazione Dati Personali provvede alla redazione di un report che illustri gli eventuali elementi da tenere in considerazione per migliorare la capacità di reazione dell'Azienda e/o per evitare o mitigare il ripresentarsi di simili rischi.

Istituzione scolastica CPIA MATERA
via B. Matrazzo s.n.c.
75100 MATERA (MT)

P. IVA 93057380771

Questo report è archiviato nel Repository di informazioni di cui all'art. 33.5 del GDPR.

Appendice - Modello di informazioni relative ad eventi di Violazione Dati Personali ai sensi dell'art. 33.5 del GDPR

La tabella che segue riporta il contenuto informativo considerato minimo per descrivere un evento di Violazione Dati Personali in modo strutturato, sono segnalati in sfondo grigio i campi che devono essere compilati solo se l'evento è stato effettivamente riconosciuto come una Violazione Dati Personali.

Identificatore univoco dell'evento:_____
Indicare se l'evento è: non considerato Violazione Dati Personali considerato Violazione Dati Personali ma non tale da comportare rischi per i diritti e le libertà fondamentali degli individui considerato Violazione Dati Personali e come tale notificato alla Autorità considerato Violazione Dati Personali, tale da comportare rischi elevati per i diritti e le libertà fondamentali per gli individui e da comunicare anche agli interessati considerato Violazione Dati Personali e tale da comportare rischi elevati per i diritti e le libertà fondamentali per gli individui ma da non comunicare agli interessati in quanto in essere le misure di cui al comma 3 dell'art 34 del GDPR
Fonte che ha segnalato l'evento ,anche più di un voce: internamente all'Azienda, via email ad apposito indirizzo email aziendale per Violazione Dati Personali, in data:_____ internamente all'Azienda, con altra modalità di comunicazione, indicare quale:_____, in data:_____ Da Fornitore, ed in tale caso indicare quale/i_____ e con quale modalità è stata fatta la segnalazione:_____, in data:_____ Da Clienti, ed in tale caso indicare se possibile quale/i_____ e con quale modalità è stata fatta la segnalazione:_____, in data:_____ Da Prospect, ed in tale caso indicare quale/i_____ e con quale modalità è stata fatta la segnalazione:_____, in data:_____

Istituzione scolastica CPIA MATERA
via B. Matrazzo s.n.c.
75100 MATERA (MT)

P. IVA 93057380771

Da Terza parte, ed in tale caso indicare se possibile quale/i_____ e con quale modalità è stata fatta la segnalazione:_____, in data:_____

Da altra fonte, ed in tale caso indicare se possibile quale/i_____ e con quale modalità è stata fatta la segnalazione:_____, in data:_____

Sintetica descrizione dell'evento e delle circostanze in cui è accaduto:_____

Giorno e Data stimati dell'evento:_____

Dove è avvenuto l'evento:_____

Tipo di evento,anche più di una voce:

- Lettura dei dati (i dati potrebbero essere stati copiati)
- Copia (i dati, seppur copiati, sono ancora presenti in Azienda)
- Alterazione (i dati, seppure ancora presenti in Azienda, sono stati modificati)
- Cancellazione (i dati non sono più presenti in Azienda nè sono in possesso dei trasgressori)
- Furto (i dati non sono più presenti in Azienda e sono in possesso del trasgressore)
- Altro: specificare_____

Dispositivo oggetto della violazione (uno o più dei seguenti casi)

- Workstation
- Laptop
- Smart device/Mobile device (smartphone,...)
- DataBase
- Sistema Informativo
- Documenti cartacei
- File
- Strumenti/sistemi di Back up
- Elementi di rete
- Altro: specificare_____

Sintetica descrizione dei sistemi usati per trattare/conservare i dati oggetti di violazione, indicando anche le relative dislocazioni

Stima del numero di persone i cui dati sono stati violati

- Numero esatto:_____

o

- Numero ipotetico:_____

o Numero non ancora noto
Quali tipi di dati sono stati coinvolti nella violazione (indicare uno o più): Dati personali Dati sensibili Dati giudiziari Dati riferiti allo stato di salute Numeri telefonici Indirizzo email Dati accesso a risorse (es. userid e passwrd) Dati relativi a conti bancari e simili (es. numeri di carte di credito,...) Non ancora noti Altro: specificare:_____ Dati considerati NON dati personali: specificare_____
Criticità ipotizzata della violazione L Basso M Medio H Alto VH Molto alto
<u>Misure tecniche ed organizzative applicate ai dati anteriormente all'evento</u> • Descrizione sintetica • link/riferimenti a documentazione di dettaglio
<u>Misure tecniche organizzative individuate per limitare/prevenire il ripetersi di simili casi di violazione</u> • Descrizione sintetica • link/riferimenti a documentazione di dettaglio
<u>Rilevazione, raccolta delle informazioni ed analisi</u> Set delle: • Mail di cui al paragrafo 2.3.1.1Rilevazione, raccolta delle informazioni ed analisi • Mail/altre forme di comunicazione adottate da chi ha segnalato l'evento
<u>Valutazione dell' evento</u> • Mail/report di decisione in merito alla classificazione dell'evento (di cui al paragrafo 2.3.1.2
<u>Raccolta di ulteriori informazioni sulla Violazione Dati Personali</u> • Mail di cui al paragrafo 2.3.1.3

Notifica all'Autorità • scambi di mail/comunicazioni con l'Autorità di cui al paragrafo 2.3.1.4 • Report di Violazione Dati Personali all'Autorità
Comunicazione agli Interessati (se effettuata) • scambi di eventuali mail/comunicazioni con l'Autorità o altri soggetti in merito alla preparazione della comunicazione agli Interessai, di cui al paragrafo 2.3.1.5 • Testo e descrizione delle modalità di veicolazione della comunicazione agli Interessati
Chiusura evento di Violazione Dati Personali • Report di cui al paragrafo 2.3.1.7
Successiva fase di Lesson Learnt • Report di cui al paragrafo 2.3.2

Se non indicato diversamente nei precedenti paragrafi, e fatti salvi gli eventuali tempi di conservazione espressamente indicati dalla normativa italiana applicabile al Repository di Violazione Dati Personali, i dati relativi a ciascun evento saranno conservati per 1 anno a partire dalla data di ricevuta segnalazione accadimento evento