A.S.P.
DELIA REPETTO
azienda pubblica per i servizi alla persona
Via Circondaria Nord, 39
41013 Castelfranco Emilia (MO)

Determinazione n. 391 del 9.12.2019

Oggetto: Approvazione schema di procedura per la gestione della violazione dei dati personali (DATA BREACH).

IL DIRETTORE

Premesso che:

- la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale;

- l'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione Europea ("Carta") e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione Europea ("TFUE") stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano;

- il Parlamento Europeo e il consiglio dell'Unione Europea hanno approvato il 27 aprile 2016 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, abrogando la Direttiva 95/46/CE (di seguito solo "GDPR");

- il 24 maggio 2016 è entrato ufficialmente in vigore il GDPR, applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018;

- il Regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi;

- in esecuzione del GDPR ed al fine di attuare un quadro più solido e coerente in materia di protezione dei dati, affiancato da efficaci misure di adeguamento, è richiesto alle aziende e alle Pubbliche Amministrazioni di approntare un piano di protezione dei dati personali che,

partendo dalla mappatura e dall'analisi dei trattamenti, effettui la valutazione del rischio di violazione ed individui infine le misure volte ad eliminare o almeno ridurre il rischio stesso;

- dato atto che permane comunque la possibilità che i dati personali vengano violati da parte di soggetti terzi, e che si rende quindi necessario prevedere una procedura da attuare nel caso si verificasse l'evento in questione.

Visto lo schema di procedura per la gestione della violazione dei dati personali (DATA BREACH) predisposto dal DPO dell'Ente, in qualità di Responsabile della Protezione dei dati, che contiene le indicazioni, le responsabilità e le azioni da attuare per la gestione della procedura da attivare in caso di possibile violazione dei dati personali, in osservanza agli obblighi relativi alla notifica all'Autorità Garante per la protezione dei dati personali e alla comunicazione all'interessato, in ossequio alle previsioni di cui agli articoli 33 e 34 del Regolamento europeo n. 679 del 2016;
Visti gli allegati allo schema di cui sopra;

DETERMINA

1. Di approvare lo schema di procedura per la gestione della violazione dei dati personali (DATA BREACH), così come predisposto dal DPO dell'Ente, che contiene le indicazioni, le responsabilità e le azioni da attuare per la gestione della procedura da attivare in caso di possibile violazione dei dati personali, in osservanza agli obblighi relativi alla notifica all'Autorità Garante per la protezione dei dati personali e alla comunicazione all'interessato, in ossequio alle previsioni di cui agli articoli 33 e 34 del Regolamento europeo n. 679 del 2016, allegati alla presente deliberazione quale parte integrante e sostanziale.

2. Di disporre che tutti i soggetti (Amministratori, Dipendenti, Collaboratori, ecc.) che trattano dati personali dell'Ente vengano informati del presente provvedimento e osservino la presente Procedura.

ASP "Delia Repetto" CASTELFRANCO EMILIA

Il Direttore
Dott.ssa Elena Zini

Allegato a)

MANUALE OPERATIVO PER LA GESTIONE, LA SEGNALAZIONE DI EVENTUALI VIOLAZIONI DEI DATI PERSONALI E LA TENUTA DEL RELATIVO REGISTRO

Introduzione

Il 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 - RGDP) definisce **la "violazione dei dati personali" come 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 (c.d. "data breach").**

Il presente documento si prefigge l'obiettivo di rappresentare una Guida nel riconoscimento e nella gestione di eventuali e non auspicabili violazioni a beneficio di:

- Lavoratori dipendenti nonché coloro che, a qualsiasi titolo – e quindi a prescindere dal rapporto contrattuale intercorrente – abbiano accesso ai dati personali trattati nel corso delle prestazioni richieste per conto del titolare del trattamento
- Qualsiasi soggetto (persona fisica o persona giuridica) che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento abbia accesso ai suddetti dati e agisca in qualità di responsabile del Trattamento (art. 28 GDPR) o di autonomo titolare o di contitolare

Il rispetto della procedura contenuta nel presente documento è obbligatoria per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste dalla stessa potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempimenti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia.

Nella redazione del presente documento si è tenuto conto delle indicazioni e delle disposizioni:

- del 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 - RGDP);

- del Decreto legislativo 30 giugno 2003, numero 196, recante il "Codice in materia di protezione dei dati personali", come modificato, da ultimo, dal Decreto legislativo 10 agosto 2018, numero 101;

- del Gruppo WP "Articolo 29" all'interno delle Linee-guida in materia di notifica delle violazioni di dati personali, approvate, in via definitiva, il 6 febbraio 2018;

- del Garante per la protezione dei dati personali nella "Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali" e nelle altre linee guida afferenti.

Il presente documento è soggetto a integrazioni e modifiche alla luce dell'evoluzione normativa italiana ed europea nonché delle prassi che saranno, di volta in volta, riscontrate all'interno dell'ASP

Premesse

Le procedure esplicitate nel presente documento di riferiscono a:

- dati personali trattati "da" e "per conto" del titolare del trattamento, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo;
- dati personali conservati o trattati a mezzo di qualsiasi altro Sistema in uso presso l'ASP Delia Repetto.

Cosa si intende per "dato personale"?

Il Regolamento (UE) 2016/679 definisce il "dato personale" come "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 on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".

Il concetto di "dato personale" appare oggi sempre più dilatato, fino a ricomprendervi qualunque contenuto informativo, dalla classica espressione alfabetica sino all'immagine o al suono: in tal senso, un "dato personale" non è necessariamente un dato testuale, ma anche un'immagine, una videoripresa od una registrazione della voce. Ne discende che anche un suono o un fotogramma sono informazioni comprese nella definizione di "dato personale"; inoltre, soddisfano la definizione anche l'informazione irrilevante, quella positiva, l'informazione minima o la meta-informazione, ossia l'informazione sull'informazione, non rilevando, ai fini della nozione di "dato personale", nemmeno la verità o la falsità del l'informazione: del resto, un'informazione falsa o imprecisa produce tendenzialmente effetti pregiudizievoli ancor più che un'informazione corretta. Si può pertanto affermare che, per precisa scelta del legislatore europeo, la nozione di "dato personale" è particolarmente ampia, anche sul piano applicativo, e non è un concetto facilmente limitabile.

Il nome, il cognome, la data di nascita sono tutti "dati" che consentono l'identificazione diretta dell'interessato e sono riconducibili alla nozione di dati identificativi, ossia dati che non comportano particolari operazioni di ricostruzione per identificare in maniera diretta l'interessato. Ma anche un indirizzo IP si configura come dato personale.

Allo stesso modo, è opportuno sottolineare che la definizione di dato personale non fa riferimento, né direttamente né indirettamente, alla riservatezza: il dato personale non è necessariamente un dato riservato. Sono dati personali, ad esempio, il numero di matricola, il numero di telefono, l'indirizzo di posta elettronica: il dato personale può anche essere un dato conosciuto dai più.

Che cos'è una violazione dei dati personali?

Per poter porre rimedio a una violazione occorre innanzitutto essere in grado di riconoscerla. All'articolo 4, punto 12, il Regolamento definisce la "violazione dei dati personali" come "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". In tal senso, si ha:

- "distruzione" dei dati, ogni qual volta gli stessi non esistono più o non esistono più in una forma che sia di qualche utilità per il titolare del trattamento;

- "danno" quando i dati personali sono stati modificati, corrotti o non sono più completi;

- "perdita" dei dati personali nel caso in cui i dati potrebbero comunque esistere, ma il titolare del trattamento potrebbe averne perso il controllo o l'accesso, oppure non averli più in possesso. Un esempio di perdita di dati personali può essere la perdita o il furto di un dispositivo contenente una copia della banca dati dei dipendenti o degli ospiti del titolare del trattamento; oppure il caso in cui l'unica copia di un insieme di dati personali sia stata crittografata da un ransomware (malware del riscatto) oppure dal titolare del trattamento mediante una chiave non più in suo possesso;

- "trattamento non autorizzato o illecito" quando viene effettuata una divulgazione di dati personali a (o l'accesso da parte di) destinatari non autorizzati a ricevere (o ad accedere) ai dati oppure quando viene svolta qualsiasi altra forma di trattamento in violazione del regolamento. E' chiaro, comunque, che una violazione è un tipo di incidente di sicurezza. Tuttavia, come indicato all'articolo 4, punto 12, il regolamento si applica soltanto in caso di violazione di dati personali. La conseguenza di tale violazione è che il titolare del trattamento non è più in grado di garantire l'osservanza dei principi relativi al trattamento dei dati personali di cui all'articolo 5 del Regolamento.

  Questo punto mette in luce la differenza tra un incidente di sicurezza e una violazione dei dati personali: **mentre tutte le violazioni dei dati personali sono incidenti di sicurezza, non tutti gli incidenti di sicurezza sono necessariamente violazioni dei dati personali.**

Tipologia di violazioni dei dati personali

Nel parere 03/2014 sulla notifica delle violazioni, il Gruppo di lavoro articolo 29 ha spiegato che le violazioni possono essere classificate in base ai seguenti tre principi ben noti della sicurezza delle informazioni:

- "violazione della riservatezza", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;

- "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.

Va altresì osservato che, a seconda dei casi, una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse. Mentre stabilire se vi sia stata una violazione della riservatezza o dell'integrità è relativamente evidente, può essere meno ovvio determinare se vi è stata una violazione della disponibilità. Una violazione sarà sempre considerata una violazione della disponibilità se si è verificata una perdita o una distruzione permanente dei dati personali.

Esempi di perdita di disponibilità possono aversi quando i dati vengono cancellati accidentalmente o da una persona non autorizzata, oppure, in caso di dati crittografati in maniera sicura, quando la chiave di decifratura viene persa. Se il titolare del trattamento non è in grado di ripristinare l'accesso ai dati, ad esempio ricorrendo a unbackup, la perdita di disponibilità sarà considerata permanente. Può verificarsi perdita di disponibilità anche in caso di interruzione significativa del servizio abituale di un'organizzazione, ad esempio un'interruzione di corrente o attacco da "blocco di servizio" (denial of service) che rende i dati personali indisponibili.

L'articolo 32 del Regolamento ("Sicurezza del trattamento") spiega che, nell'attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, si dovrebbe prendere in considerazione, tra le altre cose, "la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento" e "la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico". Di conseguenza, un incidente di sicurezza che determina l'indisponibilità dei dati personali per un certo periodo di tempo costituisce una violazione, in quanto la mancanza di accesso ai dati può avere un impatto significativo sui diritti e sulle libertà delle persone fisiche. Come nel caso della perdita o distruzione permanente dei dati personali (o comunque di qualsiasi altro tipo di violazione), una violazione che implichi la perdita temporanea di disponibilità dovrebbe essere documentata in conformità all'articolo 33, paragrafo 5. Ciò aiuta il titolare del trattamento a dimostrare l'assunzione di responsabilità all'autorità di controllo, che potrebbe chiedere di consultare tali

registrazioni. Tuttavia, a seconda delle circostanze in cui si verifica, la violazione può richiedere o meno la notifica all'autorità di controllo e la comunicazione alle persone fisiche coinvolte. Il titolare del trattamento dovrà valutare la probabilità e la gravità dell'impatto dell'indisponibilità dei dati personali sui diritti e sulle libertà delle persone fisiche. Conformemente all'articolo 33, il titolare del trattamento dovrà effettuare la notifica a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Questo punto dovrà chiaramente essere valutato caso per caso. Va notato che, sebbene una perdita di disponibilità dei sistemi del titolare del trattamento possa essere solo temporanea e non avere un impatto sulle persone fisiche, è importante che il titolare del trattamento consideri tutte le possibili conseguenze della violazione, poiché quest'ultima potrebbe comunque dover essere segnalata per altri motivi.

Le violazioni quindi, possono accadere per un ampio numero di ragioni che possono includere a titolo esemplificativo e non esaustivo:

- Divulgazioni di dati personali a soggetti non autorizzati;
- Perdita o furto fi dati o di strumenti nei quali i dati sono memorizzati;
- Perdita o furto di documenti cartacei;
- Infedeltà aziendale (es. data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia per distribuirla a terzi)
- Accesso abusivo (es. data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite)
- Casi di pirateria informatica (usurpazione delle credenziali d'accesso- fishing)
- Banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo "owner"
- Virus o altri attacchi al sistema informatico o alla rete aziendale
- Violazione di misure di sicurezza fisica (forzatura di porte o finestre di stanze di sicurezza o armadi contenenti archivi con informazioni riservate)
- Smarrimento di pc portatili, devices o attrezzature informatiche aziendali
- Invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario

Gestione e notifica di una violazione di dati personali:

Le violazioni di dati personali sono gestite dal titolare del trattamento o da un suo delegato, con la collaborazione degli uffici e dei servizi interessati, sotto la supervisione del RDP

La comunicazione all'Autorità di controllo ai sensi dell'articolo 33 del RGPD

Il Regolamento UE 2016/679 afferma che una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, 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.

Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali 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 non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Questo solleva la questione relativa al momento in cui il titolare del trattamento può considerarsi "a conoscenza" di una violazione.

Il Gruppo di lavoro articolo 29 ritiene che il titolare del trattamento debba considerarsi "a conoscenza" nel momento in cui è ragionevolmente certo che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali.

Il titolare del trattamento è quindi tenuto a prendere le misure necessarie per assicurarsi di venire "a conoscenza" di eventuali violazioni in maniera tempestiva in modo da poter adottare le misure appropriate. Il momento esatto in cui il titolare del trattamento può considerarsi "a conoscenza" di una particolare violazione dipenderà dalle circostanze della violazione: in alcuni casi sarà relativamente evidente, fin dall'inizio, che c'è stata una violazione, mentre in altri potrebbe occorrere del tempo per stabilire se i dati personali sono stati compromessi. Tuttavia, l'accento dovrebbe essere posto sulla tempestività dell'azione per indagare su un incidente per stabilire se i dati personali

sono stati effettivamente violati e, in caso affermativo, prendere misure correttive ed effettuare la notifica, se necessario.

Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo. Inoltre, è espressamente previsto un onere informativo anche in capo al Responsabile del trattamento: questi, infatti, è tenuto ad informare il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione. L'articolo 33 del Regolamento specifica altresì il "contenuto minimo" della notifica del Titolare del trattamento all'Autorità di controllo competente; la predetta notifica deve:

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. 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.

Il paragrafo 5 dell'articolo 35 del RGPD impone altresì al titolare del trattamento di documentare qualsiasi violazione dei dati personali, comprese le circostanze ad esse relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio, al fine di consentire all'Autorità di controllo di verificare il rispetto della disposizione in esame. Il Gruppo di lavoro articolo 29 ritiene che il nuovo obbligo di notifica presenti una serie di vantaggi: all'atto della notifica all'autorità di controllo, infatti, il titolare del trattamento può ottenere consulenza sull'eventuale necessità di informare le persone fisiche interessate. La comunicazione della violazione alle persone fisiche interessate consente al titolare del trattamento di fornire loro informazioni sui rischi derivanti dalla violazione e sui provvedimenti che esse possono prendere per proteggersi dalle potenziali conseguenze della violazione.

Qualsiasi piano di risposta alle violazioni dovrebbe mirare a proteggere le persone fisiche e i loro dati personali. Di conseguenza, la notifica della violazione dovrebbe essere vista come uno strumento per migliorare la conformità in materia di protezione dei dati personali.

Allo stesso tempo, va osservato che la mancata segnalazione di una violazione a una persona fisica o all'autorità di controllo può comportare l'imposizione di una sanzione al titolare del trattamento ai sensi dell'articolo 83.

La notifica per fasi

A seconda della natura della violazione, il titolare del trattamento può avere la necessità di effettuare ulteriori accertamenti per stabilire tutti i fatti pertinenti relativi all'incidente.

L'articolo 33, paragrafo 4, afferma pertanto 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*".

Ciò significa che il Regolamento prende atto del fatto che il titolare del trattamento non sempre dispone di tutte le informazioni necessarie su una violazione entro 72 ore dal momento in cui ne è venuto a conoscenza, dato che non sempre sono disponibili entro tale termine dettagli completi ed esaustivi su un incidente.

Pertanto, il regolamento consente una notifica per fasi.

Ciò è consentito a condizione che il titolare del trattamento indichi i motivi del ritardo, in conformità all'articolo 33, paragrafo 1.

Il Gruppo di lavoro raccomanda che, all'atto della prima notifica all'autorità di controllo, il titolare del trattamento informi quest'ultima del fatto che non dispone ancora di tutte le informazioni richieste e che fornirà ulteriori dettagli in un momento successivo. L'obiettivo dell'obbligo di notifica consiste nell'incoraggiare il titolare del trattamento ad agire prontamente in caso di violazione, a contenerla e, se possibile, a recuperare i dati personali compromessi e a chiedere un parere pertinente all'autorità di controllo.

La notifica all'autorità di controllo entro le prime 72 ore può consentire al titolare del trattamento di assicurarsi che le decisioni in merito alla notifica o alla mancata notifica alle persone fisiche siano corrette. Tuttavia, lo scopo della notifica

all'autorità di controllo non è solo di ottenere orientamenti sull'opportunità di effettuare o meno la notifica alle persone fisiche interessate. In certi casi sarà evidente che, a causa della natura della violazione e della gravità del rischio, il titolare del trattamento dovrà effettuare la notifica alle persone fisiche coinvolte senza indugio. Ad esempio, se esiste una minaccia immediata di usurpazione d'identità oppure se categorie particolari di dati personali vengono divulgate online, il titolare del trattamento deve agire senza ingiustificato ritardo per contenere la violazione e comunicarla alle persone fisiche coinvolte. In circostanze eccezionali, ciò potrebbe persino aver luogo prima della notifica all'autorità di controllo. Più in generale, la notifica all'autorità di controllo non può fungere da giustificazione per la mancata comunicazione della violazione all'interessato laddove la comunicazione sia richiesta. È opportuno inoltre precisare che se, dopo la notifica iniziale, una successiva indagine dimostra che l'incidente di sicurezza è stato contenuto e che non si è verificata alcuna violazione il titolare del trattamento può informarne l'autorità di controllo. Tali informazioni possono quindi essere aggiunte alle informazioni già fornite all'autorità di controllo e l'incidente può essere quindi registrato come un evento che non costituisce una violazione. Non si incorre in alcuna sanzione se si segnala un incidente che alla fine si rivela non essere una violazione.

Circostanze nelle quali non è richiesta una notifica

L'articolo 33, paragrafo 1, chiarisce che se è ***"improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche"*** **tale violazione non è soggetta a notifica all'autorità di controllo.**

Un esempio potrebbe essere quello di dati personali già disponibili pubblicamente, la cui divulgazione non costituirebbe un rischio probabile per la persona fisica.

Nel parere 03/2014 sulla notifica delle violazioni, il Gruppo di lavoro ha spiegato che:

- una violazione della riservatezza di dati personali crittografati con un algoritmo all'avanguardia costituisce in ogni caso una violazione dei dati personali e deve essere notificata. Se però la riservatezza della chiave rimane intatta (ossia se la chiave non è stata compromessa nell'ambito di una violazione della sicurezza ed è stata generata in maniera tale da non poter essere individuata con i mezzi tecnici disponibili da qualcuno che non è autorizzato ad accedervi), in linea di principio i

dati risultano incomprensibili. Di conseguenza è improbabile che la violazione possa influire negativamente sulle persone fisiche e quindi non dovrebbe essere loro comunicata. Tuttavia, anche se i dati sono crittografati, una perdita o alterazione può avere effetti negativi per gli interessati ove il responsabile del trattamento non disponga delle necessarie copie di riserva. In tal caso, la notifica agli interessati dovrebbe essere necessaria anche se sono state adottate misure di protezione mediante crittografia. Viceversa, se i dati personali sono stati resi sostanzialmente incomprensibili ai soggetti non autorizzati e se esiste una copia o un backup, una violazione della riservatezza che coinvolga dati personali correttamente crittografati potrebbe non dover essere notificata all'autorità di controllo, poiché è improbabile che tale violazione possa presentare un rischio per i diritti e le libertà delle persone fisiche. Di conseguenza, potrebbe non essere necessario nemmeno informare la persona interessata, dato che è improbabile che vi siano rischi elevati. Tuttavia, si dovrebbe tenere presente che, sebbene inizialmente la notifica possa non essere richiesta se non esiste un rischio probabile per i diritti e le libertà delle persone fisiche, la situazione può cambiare nel corso del tempo e il rischio dovrebbe essere rivalutato. Ad esempio, se la chiave risulta successivamente essere stata compromessa o essere stata esposta a una vulnerabilità nel software di cifratura, è possibile che sia ancora necessario procedere alla notifica. Inoltre, va osservato che se si verifica una violazione in assenza di backup dei dati personali crittografati si è in presenza di una violazione della disponibilità che potrebbe presentare rischi per le persone fisiche e pertanto potrebbe richiedere la notifica. Analogamente, laddove si verifichi una violazione che implichi la perdita di dati crittografati, anche se esiste una copia di backup dei dati personali si potrebbe comunque trattare di una violazione soggetta a segnalazione, a seconda del periodo di tempo necessario per ripristinare i dati dal backup e dell'effetto che la mancanza di disponibilità ha sulle persone fisiche.

Come afferma l'articolo 32, paragrafo 1, lettera c), un importante fattore di sicurezza è "la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico"

Esempio: Una violazione che non richiederebbe la notifica all'autorità di controllo sarebbe la perdita di un dispositivo mobile crittografato in maniera sicura, utilizzato dal titolare del trattamento e dal suo personale. Se la chiave di cifratura rimane in possesso del titolare del trattamento e non si tratta dell'unica copia dei dati personali,

questi ultimi sarebbero inaccessibili a qualsiasi pirata informatico. Ciò significa che è improbabile che la violazione presenti un rischio per i diritti e le libertà degli interessati in questione. Se in seguito diventa evidente che la chiave di cifratura è stata compromessa o che il software o l'algoritmo di cifratura è vulnerabile, il rischio per i diritti e le libertà delle persone fisiche cambia e potrebbe quindi essere necessaria la notifica. Tuttavia, si avrà mancato rispetto dell'articolo 33 se il titolare del trattamento non effettua la notifica all'autorità di controllo nel caso in cui i dati non siano stati effettivamente crittografati in maniera sicura. Di conseguenza, nel selezionare il software di cifratura, il titolare del trattamento deve valutare attentamente la qualità e la corretta attuazione della cifratura offerta, capire il livello di protezione effettivamente offerto e se quest'ultimo è appropriato in ragione dei rischi presentati. Il titolare del trattamento dovrebbe altresì avere familiarità con le specifiche modalità di funzionamento del prodotto di cifratura.

Ad esempio, un dispositivo può essere crittografato una volta spento, ma non mentre è in modalità stand-by. Alcuni prodotti che utilizzano la cifratura dispongono di "chiavi predefinite" che devono essere modificate da ciascun cliente per essere efficaci. La cifratura potrebbe essere considerata adeguata dagli esperti di sicurezza al momento della sua messa in atto, ma diventare obsoleta nel giro di pochi anni, il che significa che può essere messo in discussione il fatto che i dati siano sufficientemente crittografati dal prodotto in questione e che quest'ultimo fornisca un livello appropriato di protezione.

La notifica di una violazione di dati personali: la comunicazione agli interessati ai sensi dell'articolo 34 del RGPD

In alcuni casi, oltre a effettuare la notifica all'autorità di controllo, il titolare del trattamento è tenuto a comunicare la violazione alle persone fisiche interessate. L'articolo 34, paragrafo 1, afferma che "Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo". Il titolare del trattamento dovrebbe tenere a mente che la notifica all'autorità di controllo è obbligatoria a meno che sia improbabile che dalla violazione possano derivare rischi per i diritti e le libertà delle persone fisiche. Inoltre, laddove la violazione presenti un rischio elevato per i diritti e le libertà delle persone fisiche occorre informare anche queste ultime. La soglia per la

comunicazione delle violazioni alle persone fisiche è quindi più elevata rispetto a quella della notifica alle autorità di controllo, pertanto non tutte le violazioni dovranno essere comunicate agli interessati, il che li protegge da inutili disturbi arrecati dalla notifica. Il regolamento afferma che la comunicazione di una violazione agli interessati dovrebbe avvenire "senza ingiustificato ritardo", il che significa il prima possibile. L'obiettivo principale della comunicazione agli interessati consiste nel fornire loro informazioni specifiche sulle misure che questi possono prendere per proteggersi.

Come osservato in precedenza, a seconda della natura della violazione e del rischio presentato, la comunicazione tempestiva aiuterà le persone a prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione. L'articolo 34, paragrafo 2, del Regolamento precisa che "La comunicazione all'interessato (...) descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d)"; in sostanza, il titolare del trattamento deve fornire, secondo tale disposizione, almeno le seguenti informazioni:

- una descrizione della natura della violazione;
- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto;
- una descrizione delle probabili conseguenze della violazione;
- una descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

In linea di principio, la violazione dovrebbe essere comunicata direttamente agli interessati coinvolti, a meno che ciò richieda uno sforzo sproporzionato; in tal caso si procede a una comunicazione pubblica o a una misura simile che permetta di informare gli interessati con analoga efficacia (articolo 34, paragrafo 3, lettera c). Esempi di metodi trasparenti di comunicazione sono: la messaggistica diretta (ad esempio messaggi di posta elettronica, SMS, messaggio diretto), banner o notifiche su siti web di primo piano, comunicazioni postali e pubblicità di rilievo sulla stampa. Una semplice comunicazione all'interno di un comunicato stampa o di un blog aziendale non costituirebbe un mezzo efficace per comunicare una violazione

all'interessato. **Il Gruppo di lavoro raccomanda al titolare del trattamento di scegliere un mezzo che massimizzi la possibilità di comunicare correttamente le informazioni a tutte le persone interessate.** A seconda delle circostanze, ciò potrebbe significare che il titolare del trattamento dovrebbe utilizzare diversi metodi di comunicazione, anziché un singolo canale di contatto. Inoltre, il titolare del trattamento potrebbe dover garantire che la comunicazione sia accessibile in formati alternativi appropriati e lingue pertinenti al fine di assicurarsi che le persone fisiche siano in grado di comprendere le informazioni fornite loro.

Ad esempio, nel comunicare una violazione a una persona, sarà di norma appropriata la lingua utilizzata durante il precedente normale corso degli scambi di comunicazioni con il destinatario. Tuttavia, se la violazione riguarda interessati con i quali il titolare del trattamento non ha precedentemente interagito o, in particolare, interessati che risiedono in un altro Stato membro o in un altro paese non UE diverso da quello nel quale è stabilito il titolare del trattamento, la comunicazione nella lingua nazionale locale potrebbe essere accettabile, tenendo conto della risorsa richiesta. L'obiettivo principale è aiutare gli interessati a comprendere la natura della violazione e le misure che possono adottare per proteggersi. Il considerando 86 spiega che "Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge. Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione". Il titolare del trattamento potrebbe quindi contattare e consultare l'autorità di controllo non soltanto per chiedere consiglio sull'opportunità di informare gli interessati in merito a una violazione ai sensi dell'articolo 34, ma anche sui messaggi appropriati da inviare loro e sul modo più opportuno per contattarli. Parallelamente, il considerando 88 indica che la notifica di una violazione dovrebbe tenere "conto dei 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". Ciò può significare che in determinate circostanze, ove giustificato e su consiglio delle autorità incaricate dell'applicazione della legge, il

titolare del trattamento può ritardare la comunicazione della violazione agli interessati fino a quando la comunicazione non pregiudica più tale indagine. Tuttavia, passato tale arco di tempo, gli interessati dovrebbero comunque essere tempestivamente informati. Se non ha la possibilità di comunicare una violazione all'interessato perché non dispone di dati sufficienti per contattarlo, il titolare del trattamento dovrebbe informarlo non appena sia ragionevolmente possibile farlo (ad esempio quando l'interessato esercita il proprio diritto ai sensi dell'articolo 15 di accedere ai dati personali e fornisce al titolare del trattamento le informazioni supplementari necessarie per essere contattato). Circostanze nelle quali non è richiesta una notifica L'articolo 34, paragrafo 3, stabilisce tre condizioni che, se soddisfatte, non richiedono la comunicazione agli interessati in caso di violazione, ossia:

- il titolare del trattamento ha applicato misure tecniche e organizzative adeguate per proteggere i dati personali prima della violazione, in particolare misure atte a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi;

- immediatamente dopo una violazione, il titolare del trattamento ha adottato misure destinate a garantire che non sia più probabile che si concretizzi l'elevato rischio posto ai diritti e alle libertà delle persone fisiche;

contattare gli interessati richiederebbe uno sforzo sproporzionato, ad esempio nel caso in cui i dati di contatto siano stati persi a causa della violazione o non siano mai stati noti.

Conformemente al principio di responsabilizzazione, il titolare del trattamento dovrebbe essere in grado di dimostrare all'autorità di controllo di soddisfare una o più di queste condizioni. Va tenuto presente che, sebbene la comunicazione possa inizialmente non essere richiesta se non vi è alcun rischio per i diritti e le libertà delle persone fisiche, la situazione potrebbe cambiare nel corso del tempo e il rischio dovrebbe essere rivalutato. Se il titolare del trattamento decide di non comunicare una violazione all'interessato, l'articolo 34, paragrafo 4, spiega che l'autorità di controllo può richiedere che lo faccia, qualora ritenga che la violazione possa presentare un rischio elevato per l'interessato. In alternativa, può ritenere che siano state soddisfatte le condizioni di cui all'articolo 34, paragrafo 3, nel qual caso la comunicazione all'interessato non è richiesta. Qualora stabilisca che la decisione di non effettuare la comunicazione all'interessato non sia fondata, l'autorità di

controllo può prendere in considerazione l'esercizio dei poteri e delle sanzioni a sua disposizione.

Gestione di un data breach: procedura e misure specifiche.

Il presente documento ha lo scopo di indicare agli uffici dell'Asp le opportune modalità di gestione di un data breach, nel rispetto della normativa in materia di trattamento dei dati personali, garantendo in particolare l'aderenza ai principi e alle disposizioni contenute nel Regolamento UE 679/2016 e nel D. Lgs 196/03 sm.i

In questo documento si schematizzano le regole per garantire il rispetto dei principi esposti, nella gestione di un data breach, sotto i diversi aspetti relativi a:

- raccolta delle informazioni, identificazione ed indagine preliminare (Fase 1);
- analisi delle segnalazioni e valutazione dell'evento accaduto (Fase 2);
- modalità e profili di segnalazione all'Autorità Garante e agli interessati (Fase 3);
- registrazione e segnalazione nel registro dei data breach;
- analisi post violazione (Fase 5).

È necessario che tutti i dipendenti, collaboratori, e tutti coloro che trattano dati, anche "per conto" del titolare siano edotti in merito alla presente procedura.

Fase 1: raccolta delle informazioni

La raccolta delle informazioni rispetto ad eventi anomali possono pervenire da:

- Fonti interne tali intendendosi il personale dipendente o somministrato .
- Fonti esterne o anche dall'analisi di informazioni presenti sul Web, ovvero dai Responsabili esterni delle attività di trattamento.
- Ogni Interessato può segnalare, anche solo in caso di sospetto, che i propri Dati Personali siano stati utilizzati abusivamente o fraudolentemente da un terzo; in tal caso, l'Interessato può richiedere all'Asp la verifica dell'eventuale violazione.

Le segnalazioni, a qualunque soggetto/servizio dell'Asp pervengano, devono essere tempestivamente comunicate, comunque non oltre 12 ore dalla conoscenza della violazione, alla Direzione all'indirizzo direzione@aspdeliarepetto.it ed al

Responsabile della Protezione dei Dati all'indirizzo rdp@aspdeliarepetto.it, o ancora preferibilmente, a mezzo PEC all'indirizzo del titolare del trattamento aspdeliarepetto@legalmail.it

La presa in carico di tutte le segnalazioni è di responsabilità del Titolare che provvederà a gestirle coinvolgendo la Direzione e le altre funzioni interessate secondo quanto specificato nella presente procedura.

Fase 2: analisi delle segnalazioni e valutazione del rischio - compilazione della scheda evento

- Il titolare, ricevuta la segnalazione, avvia un'analisi finalizzata alla raccolta dei dati concernenti l'anomalia e alla compilazione della Scheda Evento (Allegato A), contenente tutte le informazioni raccolte: data evento anomalo, data presunta di avvenuta violazione, data e ora in cui si è avuto conoscenza della violazione; fonte segnalazione; tipologia violazione e di informazioni coinvolte; descrizione evento anomalo, numero reale o anche solo potenziale di interessati coinvolti; categoria e numerosità di Dati Personali di cui si presume una violazione; indicazione del luogo in cui è avvenuta la violazione dei dati, specificando altresì se essa sia avvenuta a seguito di smarrimento di device mobili; sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione ecc.. Obiettivo dell'analisi è quella di verificare che la segnalazione non sia un cd. "falso positivo". Nel caso la violazione su dati personali venga accertata, la Direzione, con la collaborazione degli Uffici/Servizi coinvolti dalla violazione, recupera le informazioni di dettaglio sull'evento e le riporta nella Scheda Evento, secondo la seguente classificazione:

- distruzione di dati illecita;
- perdita di dati illecita;
- modifica di dati illecita;
- distruzione di dati accidentale;
- perdita di dati accidentale;
- modifica di dati accidentale;

- divulgazione non autorizzata;
- accesso ai dati personali illecito.

La violazione deve essere valutata secondo i livelli di rischio:

Nullo

Basso

Medio

Alto

Il rischio va riferito alla probabilità che si verifichi una delle seguenti condizioni a danno di persone fisiche anche diverse dall'Interessato a cui si riferiscono i dati, a causa della violazione dei Dati Personali:

1. discriminazioni;
2. furto o usurpazione d'identità;
3. perdite finanziarie;
4. pregiudizio alla reputazione;
5. perdita di riservatezza dei dati personali protetti da segreto professionale;
6. decifratura non autorizzata della pseudonimizzazione;
7. danno economico o sociale significativo;
8. privazione o limitazione di diritti o libertà;
9. impedito controllo sui dati personali all'interessato;
10. danni fisici, materiali o immateriali alle persone fisiche.

Saranno inoltre valutate, come variabili qualitative dell'impatto temuto, le seguenti eventuali condizioni:

a) che si tratti di dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché di dati genetici, dati relativi alla salute o dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; b) che si tratti di dati relativi a valutazione di aspetti personali, in particolare 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;

c) che si tratti di dati di persone fisiche vulnerabili, in particolare gli ospiti dell'ASp;

d) che il trattamento riguardi una notevole quantità di Dati Personali;

e) che il trattamento riguardi un vasto numero di Interessati.

Il titolare del trattamento deve provvedere affinché vengano tempestivamente adottate misure che consentano di minimizzare le conseguenze negative della violazione.

Nel caso in cui l'evento segnalato risulti essere un falso positivo, si chiude l'incidente; l'evento viene comunque inserito a cura della Direzione nel Registro dei Data Breach (Allegato B)

Di seguito al fine di agevolare l'individuazione del livello di rischio, che è definito sulla base di due parametri, gravità e probabilità, si riporta di seguito una schema esemplificativo:

GRAVITA'	Impatto della violazione sui diritti e le libertà fondamentali delle persone coinvolte. - Nullo o Basso: nessun impatto - Medio: impatto poco significativo, reversibile - Alto: impatto significativo, irreversibile
PROBABILITA'	Possibilità che si verifichino uno o più eventi temuti - Nulla o bassa: l'evento temuto non si manifesta - Media: l'evento temuto potrebbe manifestarsi - Alta: l'evento temuto si è manifestato

La combinazione di questi due parametri,secondo i livelli sopra descritti darà luogo ad una valutazione di rischio:

- Alto  Medio  nullo/basso 

		GRAVITA'		
PROBABILITA'		A	M	N/B
	A			
	M			
	N/B			

RISCHIO	DESCRIZIONE	NOTIFICA ALL'AUTORITA ,,	COMUNICAZIONE AGLI INTERESSATI
	NULLO/BASSO: Nessun pregiudizio sui diritti e sulle libertà degli interessati né sulla sicurezza dei dati personali coinvolti	NO	NO
	MEDIO: possibile pregiudizio sui diritti e sulle libertà degli interessati e sulla sicurezza dei dati personali coinvolti	SI	NO
	ALTO: pregiudizio certo sui diritti e sulle libertà degli interessati e sulla sicurezza dei dati personali coinvolti	SI	SI

Fase 3: notifica e comunicazione

La presente fase prevede due sottofasi:

3.A: Notifica all'Autorità Garante

Redatta la Scheda Evento, il titolare del trattamento, sulla base dei parametri sopra descritti deve valutare le azioni da intraprendere ed avviare la notificazione verso

l'Autorità di controllo e, ove necessario, la comunicazione agli interessati, verificando e validando la documentazione pervenuta dalle precedenti fasi di lavoro.

Il Titolare del trattamento notifica 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 e dunque sia stato dallo stesso classificato "NULLO/BASSO".

Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, va corredata dei motivi del ritardo.

La notifica all'Autorità di controllo deve:

a) descrivere, ove possibile:

- la natura della violazione dei dati personali;

- le categorie e il numero approssimativo di Interessati;

- le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del RPD 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 dell'ASp per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi. 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.

B: Comunicazione della violazione all'interessato

Il titolare del trattamento, sentito il Responsabile della Protezione dei Dati, deve informare gli interessati dell'evento anomalo, in tutti i casi in cui, a norma degli articoli 33 e 34 del Regolamento, venga valutato che la violazione risulta presentare rischi classificati come "ALTI" nella Scheda Evento (Allegato A) per i diritti e le libertà delle persone fisiche. La comunicazione deve essere rivolta all'interessato

senza ingiustificato ritardo dall'avvenuta conoscenza e valutazione della violazione, attraverso il canale di comunicazione ritenuto più idoneo; deve essere intellegibile, concisa, trasparente, e facilmente accessibile; deve essere utilizzato un linguaggio semplice e chiaro adottando, se possibile, la stessa lingua parlata dall'interessato. Rispetto alle modalità della comunicazione si applicano quelle ritenute più idonee dal Titolare.

La comunicazione di Data Breach all'interessato deve contenere le seguenti informazioni:

a) data e ora della violazione, anche solo presunta, e data e ora in cui si è avuto conoscenza della stessa;

b) natura della violazione dei dati personali;

c) nome e i dati di contatto del Responsabile della Protezione dei Dati o di altro punto di contatto presso cui ottenere più informazioni;

d) le probabili conseguenze della violazione dei dati personali;

e) una descrizione sintetica delle misure adottate o di cui si propone l'adozione da parte dell'Asp per porre rimedio alla violazione 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) sono state messe 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 incomprensibili a chiunque non sia autorizzato ad accedervi (sono fatti salvi i casi in cui la violazione della sicurezza ha comportato la distruzione o la perdita dei dati personali degli interessati);

b) sono state successivamente adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà delle persone fisiche (in tal caso è necessario documentare le misure nella scheda di violazione);

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.

In allegato al presente documento (Allegato C) è disponibile un Fac-simile di comunicazione all'interessato della violazione dei dati personali.

Fase 4: registrazione e segnalazione nel registro dei data breach

Nel Registro dei Data Breach (Allegato B), il Titolare documenta ogni singolo evento, sia esso, "Falso", "Irrilevante" ovvero "Rilevante"; in quest'ultimi due casi, devono essere indicate nel registro:

- le conseguenze del Data Breach;
- i provvedimenti adottati per porvi rimedio o attenuarne le conseguenze;
- l'eventuale notificazione all'Autorità di Controllo;
- l'eventuale comunicazione all'interessato. Tale documentazione consente all'Autorità di Controllo di verificare il rispetto delle norme in materia di notificazione delle violazioni di dati personali.

Responsabile della tenuta del Registro dei Data Breach è il titolare del trattamento.

Fase 5: analisi post violazione

L'ultima fase del processo di gestione delle violazioni di dati personali prevede la raccolta finale delle evidenze, l'analisi delle informazioni giunte sul contesto di violazione osservato, e la valutazione delle stesse al fine di effettuare un'analisi post-incidente, per verificare l'efficacia e l'efficienza delle azioni intraprese durante la gestione dell'evento ed identificare possibili aree di miglioramento. Tale attività prevede il coinvolgimento dei soggetti che gestiscono a vario titolo i servizi informatici dell'ASP, del RPD, della Direzione, con eventuale supporto da parte di altri Uffici/Servizi.

Data breach presso un Responsabile esterno del trattamento

Quando un terzo agisce in qualità di Responsabile esterno della attività di trattamento svolte per conto e nell'interesse dell'ASP, in caso di violazione dei dati personali, deve informare l'ASP stessa (che agisce in qualità di Titolare), senza ingiustificato ritardo e non al più tardi di 24 ore dal momento in cui ha conoscenza della violazione, inviando una comunicazione ai seguenti recapiti: alla Direzione

all'indirizzo direzione@aspdeliarepetto.it ed al Responsabile della Protezione dei Dati all'indirizzo rdp@aspdeliarepetto.it, o ancora preferibilmente, a mezzo PEC all'indirizzo del titolare del trattamento aspdeliarepetto@legalmail.it Successivamente il responsabile esterno del trattamento dovrà collaborare con l'ASP per consentirgli di adempiere agli obblighi previsti dalla normativa agli articoli 33 e 34 del Regolamento.

La procedura che segue è riportata come allegato nel Contratto per il Trattamento dei Dati Personali, salvo diversamente concordata con il Responsabile. [quanto segue è consigliabile ma ci si aspetta che responsabili strutturati abbiano già procedure interne che rifletteranno gli obblighi di legge, e che quindi in pratica la procedura si concluderà qui. Ove invece il responsabile sia destrutturato e non abbia procedure per il caso di data breach, si consiglia di proseguire come segue] Il Responsabile deve assistere l'ASp avviando un'analisi preliminare finalizzata alla raccolta dei dati concernenti l'anomalia e alla compilazione della Scheda Evento utilizzando il modello allegato alla presente documento, contenente tutte le informazioni raccolte: data evento, anche la data presunta di avvenuta violazione (in tal caso va specificato); data e ora in cui si è avuto conoscenza della violazione; fonte della segnalazione; tipologia di violazione e di informazioni coinvolte; descrizione evento anomalo; numero di interessati coinvolti; numerosità di dati personali di cui si presume una violazione; indicazione della data, anche presunta, della violazione e del momento in cui se ne è avuta conoscenza; indicazione del luogo in cui è avvenuta la violazione dei dati, specificando altresì se essa sia avvenuta a seguito di smarrimento di device mobili; sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione. Una volta condotta l'analisi preliminare, il Responsabile esterno deve condurre un'analisi di primo livello per verificare che la segnalazione non tratti un falso positivo; all'esito dell'accertamento, qualora si tratti di un falso positivo il Responsabile esterno deve comunicarlo immediatamente all'ASP agli stessi indirizzi di cui sopra, al fine di consentirgli di inserire l'evento nella sezione "eventi falsi positivi" del Registro dei Data Breach (Allegato B). In caso contrario, il Responsabile recupera le informazioni di dettaglio sull'evento necessarie alle analisi di secondo livello, e le riporta nella Scheda Evento che deve essere inviata, possibilmente via PEC, tempestivamente e non oltre 24 ore dalla conoscenza della violazione, al Responsabile dell'essere inserito dall'Asp in un apposito Registro

dei Data Breach, il cui modello è allegato alla presente documento, e, una volta ricevuta la Scheda Evento, l'ASP deve procedere secondo le prescrizioni di cui alla lettera C della "Fase 2", alla "Fase 3", alla "Fase 4" e alla "Fase 5" di cui al Paragrafo 6.

ALLEGATO A

– SCHEDA EVENTO N. _____–

RACCOLTA DELLE INFORMAZIONI E VALUTAZIONE DEL RISCHIO CONNESSO AL DATA BREACH

A cura del titolare del trattamento dei dati insieme al personale dell'ufficio coinvolto della violazione e con la supervisione del Responsabile per la protezione dei dati

DATA EVENTO E ORA DELLA VIOLAZIONE ANCHE SOLO PRESUNTA (SPECIFICANDO SE E' PRESUNTA)
DATA E ORA IN CUI SI E'AVUTO COOSCENZA DELLA VIOLAZIONE
FONTE DELLA SEGNALAZIONE E DATI DI CONTATTO
TIPOLOGIA EVENTO ANOMALO
DESCRIZIONE EVENTO ANOMALO

CATEGORIA DI DATI COINVOLTI NELLA VIOLAZIONE, ANCHE SOLO POTENZIALE (SPECIFICANDO SE E' POTENZIALE)	
DATI PERSONALI GENERICI	
DATI PARTICOLARI (origine razziale ed etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati genetici, dati biometrici, dati giudiziari, dati relativi alla salute o all'orientamento sessuale della persona)	
Informazioni che possono essere utilizzate per commettere furti d'identità (dati di accesso ed identificazione, Cf, copie di carta d'identità, passaporto o carte di credito)	
Informazioni personali relative a soggetti fragili (anziani, disabili...)	
Profili individuali che includono informazioni relative a performance lavorative, salario o stato di famiglia, sanzioni disciplinari che potrebbero causare danni significativi alle persone	
ALTRO	

NUMEROSITA' DEI DATI PERSONALI VIOLATI DI CUI SI E' CERTI O DI CUI SI PRESUME LA VIOLAZIONE

LUOGO IN CUI E' AVVENUTA LA VIOLAZIONE DEI DATI E DISPOSTIVI OGGETTO DELLA STESSA (es. computer, rete, dispositivo mobile, file o parte di file, strumento di back up -server, documento cartaceo, altro....)

DESCRIZIONE DEI SISTEMI DI ELABORAZIONE E/O MEMORIZZAZIONE DEI DATI COINVOLTI, CON INDICAZIONE DELLA LORO UBUCAZIONE

LA VIOLAZIONE PUO' COMPORTARE PREGIUDIZIO ALLA REPUTAZIONE, PERDITA DI RISERVATEZZA DI DATI PROTETTI DA SEGRETO PROFESSIONALE, DECIFRATURA NON AUTORIZZATA DELLA PSEUDONIMIZZAZIONE, O QUALSIASI ALTRO DATO ECONOMICO O SOCIALE SIGNIFICATIVO?

SI	QUALE	NO

GLI INTERESSATI RISCHIANO DI ESSERE PRIVATI DELL'ESERCIZIO DEL CONTROLLO SUI DATI PERSONALI CHE LI RIGUARDANO?

QUALI MISURE TECNICHE ED ORGANIZZATIVE SONO ADOTTATE AI DATI OGGETTO DI VIOLAZIONE (es. pseudonimizzazione e cifratura dei dati)

CLASSIFICAZIONE	RISCHIO			
	NULLO	BASSO	MEDIO	ALTO
DISTRUZIONE DI DATI ILLECITA				

PERDITA DI DATI ILLECITA				
MODIFICA DI DATI ILLECITA				
DISTRUZIONE DI DATI ACCIDENTALE				
PERDITA DI DATI ACCIDENTALE				
MODIFICA DI DATI ACCIDENTALE				
DIVULGAZIONE DI DATI NON AUTORIZZATA				
ACCESSO AI DATI PERSONALI NON AUTORIZZATO				
ALTRO_____				

CONCLUSIONI SULL'EVENTO			
IRRILEVANTE			
FALSO POSITIVO			
RILEVANTE			
NOTIFICAZIONE DEL DATA BREACH AL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI	SI	IN CHE DATA	NO
COMUNICAZIONE DEL DATA BREACH AGLI INTERESSATI	SI	IN CHE DATA	NO
COMUNICAZIONE DEL DATA BREACH AD ALTRI SOGGETTI	SI	IN CHE DATA	NO

LUOGO E DATA_____

FIRMA_____

Allegato B

REGISTRO
DELLE VIOLAZIONI DEI DATI PERSONALI
O DATA BREACH

Approvato con Deliberazione dell'Amministratore unico n. _____del_____

EVENTO				CONSEGUENZE	PROVVEDIMENTI ADOTTATI	NOTIFICA AL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI		COMUNICAZIONI ALL'INTERESSATO	
Scheda n°	Irrilevante	Falso Positivo	Rilevante			SI/NO	DATA	SI/NO	DATA

EVENTO				CONSEGUENZE	PROVVEDIMENTI ADOTTATI	NOTIFICA AL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI		COMUNICAZIONI ALL'INTERESSATO	
Scheda n°	Irrilevante	Falso Positivo	Rilevante			SI/NO	DATA	SI/NO	DATA

Allegato c

VIOLAZIONE DI DATI PERSONALI – MODELLO DI NOTIFICA AL GARANTE

I titolari di trattamento di dati personali sono tenuti a notificare al Garante le violazioni dei dati personali (*data breach*) che comportano accidentalmente o in modo illecito la distruzione, la perdita, la modificazione, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, anche nell'ambito delle comunicazioni elettroniche, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà degli interessati.

La notifica non deve includere i dati personali oggetto di violazione (es. non fornire i nomi dei soggetti interessati dalla violazione).
Si ricorda che chiunque, in un procedimento dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi ne risponde ai sensi dell'art. 168 del Codice in materia di protezione dei dati personali (Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante), salvo che il fatto non costituisca più grave reato.

Notifica di una violazione dei dati personali

(art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del d.lgs. 51/2018)

Tipo di notifica

○ Preliminare[1] ○ Completa ◉ Integrativa [2] rif.

Effettuata ai sensi del ◉ art. 33 RGPD ○ art. 26 d.lgs 51/2018

Sez. A - Dati del soggetto che effettua la notifica

Cognome Nome
E-mail:
Recapito telefonico per eventuali comunicazioni:
Funzione rivestita:

Sez. B - Titolare del trattamento

Denominazione[3]:
Codice Fiscale/P.IVA: Soggetto privo di C.F./P.IVA ☐
Stato:
Indirizzo:
CAP : Città: Provincia:
Telefono:
E-mail:
PEC:

1 Il titolare del trattamento avvia il processo di notifica pur in assenza di un quadro completo della violazione con riserva di effettuare una successiva notifica integrativa. E' obbligatoria la compilazione delle sezioni A, B, B1 e C.

2 Il titolare del trattamento integra una precedente notifica (inserire il numero di fascicolo assegnato alla precedente notifica, se noto)

3 Indicare nome e cognome nel caso di persona fisica

Sez. B1- Dati di contatto per informazioni relative alla violazione

Indicare i riferimenti del soggetto da contattare per ottenere maggiori informazioni circa la violazione

◉ Responsabile della protezione dei dati[4] - prot. n.

○ Altro soggetto[5]

Cognome Nome
E-mail:
Recapito telefonico per eventuali comunicazioni:
Funzione rivestita:

Sez. B2- Ulteriori soggetti coinvolti nel trattamento

Indicare i riferimenti di ulteriori soggetti coinvolti ed il ruolo svolto (contitolare o responsabile del trattamento[6], rappresentante del titolare non stabilito nell'Ue)

Denominazione[7] *:
Codice Fiscale/P.IVA: Soggetto privo di C.F./P.IVA ☐
Ruolo: ○ Contitolare ○ Responsabile ○ Rappresentante

Denominazione *: .....
Codice Fiscale/P.IVA: ..... Soggetto privo di C.F./P.IVA ☐
Ruolo: ○ Contitolare ○ Responsabile

Denominazione *: .....
Codice Fiscale/P.IVA: ..... Soggetto privo di C.F./P.IVA ☐
Ruolo: ○ Contitolare ○ Responsabile

Denominazione *: .....
Codice Fiscale/P.IVA: ..... Soggetto privo di C.F./P.IVA ☐
Ruolo: ○ Contitolare ○ Responsabile

[4] Qualora designato, indicare il numero di protocollo assegnato alla comunicazione dei dati di contatto del RPD
[5] In assenza di un RPD, indicare i riferimenti di un punto di contatto designato per la notifica in questione
[6] In tale tipologia rientra anche il Responsabile individuato ai sensi art. 28, par. 4
[7] Indicare nome e cognome nel caso di persona fisica

Sez. C - Informazioni di sintesi sulla violazione

1. **Indicare quando è avvenuta la violazione**

- (•) Il
- ( ) Dal (la violazione è ancora in corso)
- ( ) Dal al
- ( ) In un tempo non ancora determinato

Ulteriori informazioni circa le date in cui è avvenuta la violazione

2. **Momento in cui il titolare del trattamento è venuto a conoscenza della violazione**

Data: Ora:

3. **Modalità con la quale il titolare del trattamento è venuto a conoscenza della violazione**

- ( ) Il titolare è stato informato dal responsabile del trattamento
- ( ) Altro[8]

4. **In caso di notifica oltre le 72 ore, quali sono i motivi del ritardo?[9]**

5. **Breve descrizione della violazione**

[8] Ad esempio: Segnalazione da parte di un interessato, comunicazione da parte di terzi, ecc.

[9] Da compilare solo per notifiche tardive.

6. **Natura della violazione**
   - ☐ a) Perdita di confidenzialità[10]
   - ☐ b) Perdita di integrità[11]
   - ☐ c) Perdita di disponibilità[12]

7. **Causa della violazione**
   - ☐ Azione intenzionale interna
   - ☐ Azione accidentale interna
   - ☐ Azione intenzionale esterna
   - ☐ Azione accidentale esterna
   - ☐ Sconosciuta
   - ☐ Altro (specificare)

8. **Categorie di dati personali oggetto di violazione**
   - ☐ Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale, altro...)
   - ☐ Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
   - ☐ Dati di accesso e di identificazione (username, password, customer ID, altro…)
   - ☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…)
   - ☐ Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro…)
   - ☐ Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza o di prevenzion
   - ☐ Dati di profilazione
   - ☐ Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…)
   - ☐ Dati di localizzazione
   - ☐ Dati che rivelino l'origine razziale o etnica
   - ☐ Dati che rivelino opinioni politiche
   - ☐ Dati che rivelino convinzioni religiose o filosofiche
   - ☐ Dati che rivelino l'appartenenza sindacale
   - ☐ Dati relativi alla vita sessuale o all'orientamento sessuale
   - ☐ Dati relativi alla salute
   - ☐ Dati genetici
   - ☐ Dati biometrici
   - ☐ Categorie ancora non determinate
   - ☐ Altro

[10] Diffusione/ accesso non autorizzato o accidentale
[11] Modifica non autorizzata o accidentale
[12] Impossibilità di accesso,perdita, distruzione non autorizzata o accidentale

9. Indicare il volume (anche approssimativo) dei dati personali oggetto di violazione[13]

- ◯ N.
- ◯ Circa n.
- ◯ Un numero (ancora) non definito di dati

10. Categorie di interessati coinvolti nella violazione

- ☐ Dipendenti/Consulenti
- ☐ Utenti/Contraenti/Abbonati/Clienti (attuali o potenziali)
- ☐ Associati,soci, aderenti, simpatizzanti, sostenitori
- ☐ Soggetti che ricoprono cariche sociali
- ☐ Beneficiari o assistiti
- ☐ Pazienti
- ☐ Minori
- ☐ Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
- ☐ Categorie ancora non determinate
- ☐ Altro (specificare)

☐ Ulteriori dettagli circa le categorie di interessati

11. Numero (anche approssimativo) di interessati coinvolti nella violazione

- ◯ N. interessati
- ◯ Circa n. interessati
- ◯ Un numero (ancora) sconosciuto di interessati

[13] Ad esempio numero di referti, numero di record di un database, numero di transazioni registrate.

Sez. D - Informazioni di dettaglio sulla violazione

1. **Descrizione dell'incidente di sicurezza alla base della violazione**[14]

2. **Descrizione delle categorie di dati personali oggetto della violazione**[15]

3. **Descrizione dei sistemi e delle infrastrutture IT coinvolti nell'incidente, con indicazione della loro ubicazione**

4. **Misure di sicurezza tecniche e organizzative adottate per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture IT coinvolti**[16]

[14] Segue punto 5, 6 e 7 della sez. C
[15] Segue punto 8 della sez. C
[16] Indicare le misure in essere al momento della violazione

Sez. E - Possibili conseguenze e gravità della violazione

1. Possibili conseguenze della violazione sugli interessati

a) In caso di perdita di confidenzialità: [17]

☐ I dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento
☐ I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati
☐ I dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito
☐ Altro (specificare)

b) In caso di perdita di integrità:[18]

☐ I dati sono stati modificati e resi inconsistenti
☐ I dati sono stati modificati mantenendo la consistenza
☐ Altro (specificare)

c) In caso di perdita di disponibilità:[19]

☐ Mancato accesso a servizi
☐ Malfunzionamento e difficoltà nell'utilizzo di servizi
☐ Altro (specificare)

Ulteriori considerazioni sulle possibili conseguenze

[17] Da compilare solo nel caso in cui è stata selezionata l'opzione a) del punto 6, Sez. C
[18] Da compilare solo nel caso in cui è stata selezionata l'opzione b) del punto 6, Sez. C
[19] Da compilare solo nel caso in cui è stata selezionata l'opzione c) del punto 6, Sez. C

2. Potenziali effetti negativi per gli interessati

- ☐ Perdita del controllo dei dati personali
- ☐ Limitazione dei diritti
- ☐ Discriminazione
- ☐ Furto o usurpazione d'identità
- ☐ Frodi
- ☐ Perdite finanziarie
- ☐ Decifratura non autorizzata della pseudonimizzazione
- ☐ Pregiudizio alla reputazione
- ☐ Perdita di riservatezza dei dati personali protetti da segreto professionale
- ☐ Conoscenza da parte di terzi non autorizzati

Qualsiasi altro danno economico o sociale significativo (specificare)

3. Stima della gravità della violazione

- ○ Trascurabile
- ○ Basso
- ○ Medio
- ○ Alto

Indicare le motivazioni

Sez. F – Misure adottate a seguito della violazione

1. **Misure tecniche e organizzative adottate (o di cui si propone l'adozione[20]) per porre rimedio alla violazione e ridurne gli effetti negativi per gli interessati**

2. **Misure tecniche e organizzative adottate (o di cui si propone l'adozione) per prevenire simili violazioni future**

[20] Nella descrizione distinguere le misure adottate da quelle in corso di adozione

Sez. G - Comunicazione agli interessati

1. La violazione è stata comunicata agli interessati?

- ○ Sì, è stata comunicata il
- ○ No, sarà comunicata il in una data da definire
- ○ No, sono tuttora in corso le dovute valutazioni[21]
- ◉ No e non sarà comunicata perché:

a) il titolare del trattamento ritiene che la violazione dei dati personali non presenti un rischio elevato per i diritti e le libertà delle persone fisiche;
Spiegare le motivazioni

b) 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;

Descrivere le misure applicate

■ c) 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;

Descrivere le misure adottate

d) detta comunicazione richiederebbe sforzi sproporzionati.
Descrivere la modalità (comunicazione pubblica o misura simile) tramite la quale gli interessati sono stati informati

[21] Selezionando questa opzione, il titolare del trattamento si impegna a effettuare una integrazione alla presente notifica

2. **Numero di interessati a cui è stata comunicata la violazione**[22]

   N. interessati

3. **Contenuto della comunicazione agli interessati**

4. **Canale utilizzato per la comunicazione agli interessati**
   - ☐ SMS
   - ☐ Posta cartacea
   - ☐ Posta elettronica
   - ☐ Altro (specificare)

[22] Da compilare solo nel caso in cui al punto 1 venga scelta una delle prime due opzioni.

Sez. H - Altre informazioni

1. **La violazione coinvolge interessati di altri Paesi dello Spazio Economico Europeo[23]?**

   ◉ SI (indicare quali):

   ○ NO

2. **La violazione coinvolge interessati di Paesi non appartenenti allo Spazio Economico Europeo?**

   ○ SI (indicare quali):

   ○ NO

3. **La violazione è stata notificata ad altre autorità di controllo[24]?**

   ○ SI (indicare quali):

   ○ NO

4. **La violazione è stata notificata ad altri organismi di vigilanza o di controllo in virtù di ulteriori disposizioni normative[25]?**

   ○ SI (indicare quali):

   ○ NO

5. **E' stata effettuata una segnalazione all'autorità giudiziaria o di polizia?**

   ○ SI
   ○ NO

[23] Fanno parte dello Spazio Economico Europeo tutti gli Stati membri della Unione Europea, nonchè l'Islanda, il Liechtenstein e la Norvegia

[24] Autorità di controllo così come definite ex art. 51 del Regolamento (UE) 2016/679

[25] Ad esempio: Regolamento (UE) 910/2014 (eIDAS), d.lgs. 65/2018 attuativo della Direttiva (UE) 2016/1148 (NIS)

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI

Ai sensi dell'articolo 13 del Regolamento (UE) 2016/679 si rappresenta che il Garante per la protezione dei dati personali, in qualità di titolare del trattamento (con sede in Piazza Venezia 11, IT-00187, Roma; Email: garante@gpdp.it; PEC: protocollo@pec.gpdp.it; Centralino: +39 06696771), tratterà i dati personali conferiti con il presente modulo, con modalità prevalentemente informatiche e telematiche, per le finalità previste dal Regolamento (UE) 2016/679 e dal Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196 e s.m.i.), in particolare per l'esecuzione dei propri compiti di interesse pubblico o comunque connessi all'esercizio dei propri pubblici poteri attribuiti al Garante dalla disciplina vigente.

Il conferimento dei dati, fermo restando quanto previsto dall'art. 33, par. 4, del Regolamento (UE) 2016/679, è obbligatorio e la loro mancata indicazione non consente di ritenere adempiuto il dovere di notificazione della violazione all'autorità di controllo. I dati acquisiti nell'ambito della procedura saranno conservati in conformità alle norme sulla conservazione della documentazione amministrativa.

I dati saranno trattati esclusivamente dal personale e da collaboratori del Garante o delle imprese espressamente designate come responsabili del trattamento. Al di fuori di queste ipotesi, i dati non saranno diffusi, né saranno comunicati a terzi, fatti salvi i casi in cui si renda necessario comunicarli ad altri soggetti coinvolti nell'attività istruttoria e nei casi specificamente previsti dal diritto nazionale o dell'Unione europea.

Gli interessati hanno il diritto di ottenere dal Garante, nei casi previsti, l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt. 15 e ss. del Regolamento UE 2016/679). L'apposita istanza è presentata contattando il Responsabile della protezione dei dati presso il Garante (Garante per la protezione dei personali - Responsabile della Protezione dei dati personali, Piazza Venezia 11, 00187, Roma, email: rpd@gpdp.it).

Gli interessati che ritengono che il trattamento dei dati personali a loro riferiti avvenga in violazione di quanto previsto dalla disciplina in materia di protezione dei dati personali hanno il diritto di proporre reclamo al Garante, come previsto dall'art. 77 del Regolamento (UE) 2016/679, o di adire le opportune sedi giudiziarie ai sensi dell'art. art. 79 del Regolamento citato.

Allegato D

Gentile Sig._____

Via_____

Città_____

Oggetto: comunicazione all'interessato

La informiamo che in data _____siamo venuti a conoscenza di un evento che potrebbe aver coinvolto e violato i Suoi dati personali.

Siamo venuti a conoscenza della violazione nel seguente modo:_____

_____

Presumiamo che in data _____ ore_____sia accaduto quanto segue: (descrivere natura della violazione)_____

_____

_____

_____

_____

Le possibili conseguenze dell'evento sono_____

_____

_____

_____

In risposta all'evento, abbiamo adottato le seguenti misure di sicurezza:

_____

_____

_____

Per maggiore garanzia, La invitiamo a:

_____

_____

Per qualsiasi informazione o chiarimento, può contattare il titolare del trattamento Asp Delia Repetto, ai seguenti recapiti:

Tel._____

mail

Pec._____

Email del Responsabile per la protezione dei dati personali: rdp@aspdeliarepetto.it

Cordiali saluti