Sanitaservice ASL BT s.r.l.

con sede in Via Fornaci n. 201 – 76123 Andria BT www.sanitaserviceaslbat.it e-mail:

segreteria@sanitaserviceaslbat.it.

PROCEDURA OPERATIVA

PER LA GESTIONE DELLE VIOLAZIONI DELLA SICUREZZA

DEI DATI PERSONALI

"DATA BREACH"

INDICE

*1. Introduzione……..……..……..

1. INTRODUZIONE

La normativa contenuta nel Regolamento UE 2016/679 si propone di tutelare la riservatezza dei dati personali, per evitare che un uso non corretto degli stessi possa danneggiare o ledere le libertà fondamentali e la dignità personale di ognuno. Ciò è ancora più evidente in quelle realtà che trattano quotidianamente una pluralità di dati di estrema delicatezza, riguardanti il più delle volte la salute delle persone.

La Sanitaservice ASL BT s.r.l.[1], nella sua qualità di titolare del trattamento e/o responsabile del trattamento dati ex articolo 28 del Regolamento UE 2016/679 (per attività di gestione dei servizi di Ausiliariato/Pulizia, di Emergenza Urgenza, Logistica e Accoglienza, Supporto ai Sistemi Informativi) si impegna a mantenere protetti i dati personali trattati nell'ambito delle proprie attività e ad agire senza ingiustificato ritardo in caso di violazione dei dati stessi (incluse eventuali notifiche all'Autorità Garante competente ed eventuali comunicazioni agli interessati).

Per questo motivo la società ha redatto la presente procedura al fine di garantire, secondo un processo standardizzato, le azioni da attuare nell'eventualità in cui si presentino violazioni concrete, potenziali o sospette di dati personali e per poter riscontrare nei tempi e nei modi previsti dal Regolamento (UE) 2016/679 l'Autorità Garante e/o gli interessati.

Infine, il presente documento individua il soggetto coordinatore dell'intera procedura, individuato all'interno della compagine aziendale nella persona del Data Protection Officer designato.

2. SCOPO

Questo documento descrive le modalità operative adottate dalla Sanitaservice ASL BT s.r.l., nella sua qualità di titolare del trattamento e/o responsabile del trattamento dati, al fine di garantire la gestione, in maniera standardizzata e nel rispetto di quanto previsto dall'articolo 33 del Regolamento UE 2016/679, delle violazioni di dati personali.

In particolare, vengono definite le modalità e le responsabilità per effettuare:

- la notifica di una violazione dei dati personali all'autorità di controllo;
- la comunicazione di una violazione dei dati personali all'interessato;

garantendo altresì:

- l'identificazione della violazione;
- l'analisi delle cause della violazione;
- la definizione delle misure da adottare per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi;
- la registrazione delle informazioni relative alla violazione, delle misure identificate e dell'efficacia delle stesse.

3. CAMPO DI APPLICAZIONE

La procedura è applicabile a tutte le attività di trattamento dati svolte dalla Sanitaservice ASL BT s.r.l., (di seguito il titolare del trattamento e/o responsabile del trattamento dati), con particolare riferimento alla:

- gestione ordinaria delle tipiche attività di trattamento dati in qualità di titolare del trattamento, quali ad esempio: gestione del personale societario, gestione amministrativa, gestione contabile e finanziaria ecc. ecc.;
- gestione ordinaria delle tipiche attività di trattamento dati in qualità di responsabile del trattamento, quali ad esempio: gestione dei servizi di Ausiliariato/Pulizia, di Emergenza Urgenza, Logistica e Accoglienza, Supporto ai Sistemi Informativi;

1 SANITASERVICE ASL BT S.r.l. è una Società di servizi interamente partecipata dalla ASL BT (Azienda Sanitaria Locale della Provincia di Andria-Barletta-Trani) con sede ad Andria.

4. DEFINIZIONI

Amministratore di sistema (ADS): professionista che generalmente in ambito informatico, gestisce e manutiene un impianto di elaborazione o di sue componenti ad esempio, gestore delle password, amministratore di database e di reti;

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

Consenso dell'interessato: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

Data breach (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;

Data Protection Officer o Responsabile dei dati personali (DPO-RDP): professionista generalmente appartenente all'organico della società, che il titolare nomina al fine di avere al suo interno un punto di riferimento, esperto di privacy e di facilitare l'osservanza della predetta materia;

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

Dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

Dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

Dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

Informativa: documento o insieme di informazioni contenente le informazioni che il titolare deve fornire all'interessato per chiarire se quest'ultimo è obbligato o meno a rilasciare i dati personali;

Interessato: persona fisica a cui si riferiscono i dati;

Misure di sicurezza: complesso di misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione;

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

Soggetto autorizzato: la persona fisica, espressamente designata e specificatamente istruita, che opera sotto l'autorità del titolare del trattamento, con specifici compiti e funzioni connessi al trattamento dei dati personali;

Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

5. RIFERIMENTI NORMATIVI

Articolo 33

Notifica di una violazione dei dati personali all'autorità di controllo

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

3. La notifica di cui al paragrafo 1 deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

4. 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.

5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

Articolo 34

Comunicazione di una violazione dei dati personali all'interessato

1. 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.

2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo 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).

3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati

personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

6. DESCRIZIONE DELLE ATTIVITA'

Nel presente paragrafo sono descritte le modalità operative adottate dal titolare del trattamento e/o responsabile del trattamento e le relative attività da compiere, allorché venga segnalata una presunta violazione o si attesti l'avvenuta violazione (data breach).

6.1. Individuazione e segnalazione della violazione

Le violazioni dei dati personali sono una tipologia di incidente per la sicurezza delle informazioni nel quale sia coinvolto qualsiasi genere di dato di natura personale (anagrafici, numeri di carte personali, codici identificativi, dati sanitari, dati biometrici, dati relativi a conti correnti, ecc.).

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

- Violazione della riservatezza – in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali;
- Violazione dell'integrità – in caso di alterazione non autorizzata o accidentale dei dati personali;
- Violazione della disponibilità – in caso di accidentale o non autorizzata perdita di accesso o distruzione di dati personali.

A seconda delle circostanze, una violazione può riguardare tutti gli aspetti sopra indicati o una combinazione di essi. Tutti possono rilevare violazioni dei dati personali.

L'individuazione di potenziali violazioni dei dati personali avviene:

- per **segnalazione diretta** da parte degli attori coinvolti (interessati, personale interno, Data Protection Officer, responsabili esterni del trattamento o sub responsabili del trattamento dati, soggetti terzi ecc. ecc.);
- anche a seguito di **attività di monitoraggio** degli eventi che possono arrecare violazioni dei dati, sia digitale ed automatizzata che cartacea.

Nel caso in cui uno degli attori coinvolti si accorga di una concreta, potenziale o sospetta violazione dei dati personali, deve immediatamente informare del possibile incidente il Titolare del trattamento e/o responsabile del trattamento dati (utilizzando ad esempio la seguente e-mail segreteria@sanitaserviceaslbat.it), nonché il referente privacy aziendale, nonché il Data Protection Officer all'indirizzo e-mail rdp@sanitaserviceaslbat.it, mediante la compilazione dell'Allegato A – Modulo di comunicazione interna di Data Breach - da inviare anche a mezzo e-mail. Qualora un soggetto esterno, comunichi una possibile violazione dati senza l'utilizzo del modello sopra menzionato, si dovrà, ove possibile, immediatamente richiedere la compilazione dello stesso al fine di ottenere una risposta corrispondente alla presente procedura.

Le attività di monitoraggio invece, si possono suddividere in due tipologie:

- Il monitoraggio degli eventi di natura Software e ICT - tale monitoraggio include l'insieme delle attività di controllo finalizzate al rilevamento degli eventi tracciati dai sistemi informatici e dai sistemi di security ICT aziendale. Tali eventi relativi ai sistemi ICT sono monitorati e gestiti dall'Amministratore di Sistema esterno e da eventuali responsabili esterni del trattamento deputati alla sicurezza informatica interna;
  In caso di rilievo di concreta, sospetta e/o avvenuta violazione dei dati personali relativi ai sistemi ICT aziendali, l'Amministratore di Sistema deve immediatamente informare il Titolare del trattamento, mediante la compilazione dell'Allegato A – Modulo di comunicazione interna di Data Breach - da inviare anche a mezzo e-mail.

- Il monitoraggio dei luoghi fisici del trattamento e dell'archiviazione di dati personali - I luoghi fisici preposti al trattamento di informazioni personali e sensibili, con particolare riferimento agli eventuali archivi cartacei, devono essere controllati periodicamente dal personale interno. In caso di rilievo di concreta, sospetta e/o avvenuta violazione dei dati personali in particolare relativamente agli archivi cartacei ma anche digitali (ad esempio smarrimento o furto di documenti cartacei o digitali e personal computer, ovvero tentativi di forzatura alle porte di accesso a alle serrature dei armadi e cassettiere, presenza di personale non autorizzato in locali interdetti al pubblico), il soggetto che rileva la sospetta violazione, deve immediatamente informare il Titolare del trattamento e/o responsabile del trattamento dati, mediante la compilazione dell'Allegato A – Modulo di comunicazione interna di Data Breach - da inviare anche a mezzo e-mail.

7. MODALITA' OPERATIVA DI GESTIONE DELLE VIOLAZIONI DATI

La gestione di una violazione dei dati personali è stata standardizzata in un processo suddiviso nelle seguenti quattro fasi:

1. Identificazione e indagine preliminare;
2. Risk assesment e individuazione misure;
3. Notifica della violazione dei dati personali all'autorità di controllo;
4. Comunicazione della violazione dei dati personali a interessato/i;

7.1 Identificazione e indagine preliminare

A seguito di ricezione della segnalazione, sempre compilata tramite l'Allegato A, da parte di uno degli attori, il Data Protection Officer, con l'ausilio del referente privacy aziendale come designato, effettua la registrazione della segnalazione, e quindi, con il supporto dell'Amministratore di sistema e del titolare del trattamento (nella persona dell'amministratore unico), effettuerà una valutazione preliminare riguardante la possibile violazione occorsa, ciò al fine di stabilire se si sia effettivamente verificata un'ipotesi di Data Breach (violazione) e se sia necessaria un'indagine più approfondita dell'accaduto, richiedendo il coinvolgimento diretto di altri soggetti (aziende specializzate in cyber security, consulenti esterni privacy ecc. ecc.) con i quali avviare la fase di risk assesment (par. 7.2).

Nel caso in cui si individuasse una possibile violazione di dati contenuti in un sistema informatico (ICT), il Data Protection Officer inoltrerà la segnalazione, oltre che al titolare del trattamento e/o responsabile del trattamento anche all'Amministratore di Sistema per effettuare una istruttoria e le valutazioni di competenza in merito all'accaduto.

Utile supporto, per tutti i soggetti coinvolti nella presente procedura, al fine di individuare preliminarmente la possibile violazione è il modulo "scenari di Data Breach" (allegato B) il quale attraverso numerosi esempi illustra quando una possibile violazione diviene un data breach e le eventuali contromisure da attuare.

7.2. Risk assesment e individuazione delle misure

A termine della fase di valutazione preliminare, nel caso si stabilisca che una possibile violazione è effettivamente avvenuta, il coordinatore Data Protection Officer informerà tempestivamente il titolare del trattamento e/o responsabile del trattamento dati e, in caso di violazioni informatiche l'Amministratore di sistema, al fine di stabilire congiuntamente:

1. le opportune misure correttive e di protezione **preliminari** che possano limitare i danni che la violazione potrebbe causare (i.e. riparazione fisica di strumentazione; utilizzo dei file di back up per recuperare dati persi o danneggiati; isolamento/chiusura di un settore compromesso della rete; cambio dei codici di accesso…ecc.);

2. le modalità e le tempistiche di suddette misure, individuando gli attori e i compiti per limitare la violazione;
3. la valutazione del rischio, come di seguito indicata:

Il livello di rischio è definito sulla base di due parametri, gravità e probabilità:

- gravità: rilevanza degli effetti pregiudizievoli che la violazione è in grado di produrre sui diritti e le libertà delle persone coinvolte (es. impedendo il controllo da parte dell'interessato sulla diffusione dei propri dati);
- probabilità: grado di possibilità che si verifichino uno o più eventi temuti (es. la perdita di ogni traccia dei dati).

Ai fini della identificazione dei valori da attribuire ai due parametri per la valutazione del rischio, è possibile considerare i seguenti fattori:

- tipo di violazione;
- natura, sensibilità e volume dei dati personali;
- facilità nella identificazione degli interessati;
- gravità delle conseguenze per gli interessati;
- particolarità degli interessati (es. bambini);
- particolarità dei responsabili del trattamento (es. personale sanitario);
- numero degli interessati.

Gravità	Impatto della violazione sui diritti e le libertà delle persone coinvolte: - Basso: nessun impatto - Medio: impatto poco significativo, reversibile - Alto: impatto significativo, irreversibile
Probabilità	Possibilità che si verifichino uno o più eventi temuti: - Basso: l'evento temuto non si manifesta - Medio: l'evento temuto potrebbe manifestarsi - Alto: l'evento temuto si è manifestato

	GRAVITÀ			
P		**A**	**M**	**B**
R	**A**			
O				
B	**M**			
A				
B				

I L I T A'	**B**			

	DESCRIZIONE	**NOTIFICA ALL'AUTORITA'**	**COMUNICAZIONE AGLI INTERESSATI**
R I S C H I O	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 le libertà degli interessati e sulla sicurezza dei dati personali coinvolti	SI	SI

Sulla base degli elementi di cui sopra:

1. Il titolare del trattamento, con l'eventuale supporto del Data Protection Officer, stima la gravità e la probabilità della violazione e classifica il rischio.[2]

2. Il Data Protection Officer, previa condivisione della valutazione con l'amministratore di sistema e il referente privacy aziendale e il titolare del trattamento dati, documenta la decisione presa a seguito della valutazione del rischio nel "Registro delle violazioni" (allegato C). **Prevale la scelta del titolare del trattamento ove ci sia disaccordo sulla valutazione e stima del Data Protection Officer.**

- Nel caso in cui il rischio sia considerato **non elevato** e non si ritenga necessario procedere con la notificazione, il titolare del trattamento specifica la giustificazione per tale scelta.
- Nel caso il rischio lo richieda, il titolare del trattamento con l'eventuale ausilio del Data Protection Officer prepara la notifica della violazione (par 7.3)

3. Gli elementi a supporto del procedimento e degli esiti della valutazione del rischio sono documentati e tale documentazione è conservata come da par. 8.

4. se la violazione ricade nei casi in cui è necessario notificare all'Autorità Garante per la Protezione dei dati personali (ove sia probabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche);

[2] La valutazione del rischio deve essere compiuta secondo quanto previsto dalle "*raccomandazioni per una metodologia di valutazione della gravità delle violazioni dei dati personali*" emanate da Enisa nel documento di lavoro v. 1.0

5. se l'entità della violazione necessiti di comunicare l'accadimento agli interessati (ove la violazione presenti un elevato rischio per i diritti e le libertà delle persone fisiche).

Ulteriore supporto al fine di individuare preliminarmente la possibile violazione nonché la necessità di notificazione all'Autorità Garante e di comunicazione agli interessati, è il modulo "Risk Assessement – violazione dati personali" (allegato D), che dovrà essere compilato in ogni sua parte dal titolare del trattamento, con l'ausilio del Data Protection Officer del referente privacy aziendale e dall'Amministratore di sistema secondo le indicazioni di cui all'art. 33 del Regolamento UE 2016/679.

Si precisa che in caso di divergenza di pareri tra il Data Protection Officer e il titolare del trattamento e/o responsabile del trattamento in merito ad un effettivo data breach e quindi al conseguente obbligo di notifica all'Autorità Garante e alla comunicazione agli interessati, il DPO documenterà per iscritto ogni sua scelta, restando in capo al titolare del trattamento non accogliere la scelta del DPO e quindi non procedere con la notifica e comunicazione, con ogni responsabilità conseguente.

7.3. Notifica della violazione dei dati personali all'autorità di controllo

Il regolamento (UE) 2016/679 prevede che, non appena si viene a conoscenza di una violazione dei dati personali che presenti un rischio di qualsiasi livello superiore al livello "basso" per i diritti e le libertà delle persone coinvolte, è obbligatorio effettuare la notifica all'Autorità.

Per le violazioni così identificate, il titolare del trattamento con il supporto del Data Protection Officer, dell'amministratore di sistema e del referente privacy aziendale, come previsto a partire dal 1° luglio 2021, dovranno procedere alla notifica di una violazione di dati personali al Garante Privacy tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/ (*cfr. Provvedimento del 27 maggio 2021 - Procedura telematica per la notifica di violazioni di dati personali (data breach) [9667201*].

Il modello di cui all'allegato E della presente procedura è divenuto un facsimile, da NON utilizzare più per la notifica al Garante ma utile per vedere in anteprima i contenuti che andranno comunicati al Garante.

Per semplificare gli adempimenti previsti, il Garante ha ideato e messo disposizione un apposito strumento di autovalutazione (self assessment) Self Assessment - Notifica di una violazione dei dati personali (data breach) (gpdp.it) che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza.

N.B.: l'invio della notifica all'Autorità di controllo tramite posta elettronica certificata (PEC), non è più prevista ma sostituita da quanto sopra previsto.

L'invio avviene **entro 72 ore** dal momento in cui il titolare del trattamento è venuto a conoscenza della violazione.

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

Il documento di notifica contiene almeno i seguenti elementi:

- 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;
- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- le probabili conseguenze della violazione dei dati personali;
- le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione;

- i motivi del ritardo, qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore;
- eventualmente, una dichiarazione sulla mancanza di alcune delle informazioni necessarie e un impegno a fornire, il prima possibile, le informazioni aggiuntive, in una o più fasi successive.

7.4. Comunicazione della violazione dei dati personali a interessato/i

Nel caso di accertamento di una violazione dei dati personali che sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, come valutato secondo quanto indicato al par. 7.2, il titolare del trattamento dati con il supporto del Data Protection Officer redige la bozza di comunicazione di violazione dati personali dell'interessato. Sarà compito del titolare del trattamento (anche per il tramite del referente privacy aziendale) procedere al materiale invio della predetta comunicazione.

La comunicazione non è richiesta se è soddisfatta una delle seguenti condizioni:

- il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- 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;
- 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.

La comunicazione contiene almeno i seguenti elementi:

- la natura della violazione dei dati personali, descritta con linguaggio semplice e chiaro;
- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- le probabili conseguenze della violazione dei dati personali;
- le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione.

Il modulo di “comunicazione di violazione all’interessato” è riportato in Allegato F.

Per la comunicazione, è possibile identificare uno o più canali di comunicazione, a seconda delle circostanze, quali e-mail, SMS, posta, comunicati pubblicitari, banner o notifiche su siti web, scegliendo il canale che massimizza la probabilità che tutti gli interessati siano raggiunti dal messaggio.

8. DOCUMENTAZIONE DELLA VIOLAZIONE E REGISTRO

Indipendentemente dalla valutazione circa la necessità di procedere a notificazione e/o comunicazione della violazione di Data Breach, ogniqualvolta si verifichi un incidente comunicato dagli attori che partecipano al trattamento attraverso l’Allegato A, il titolare del trattamento e/o responsabile del trattamento dati, con l’ausilio del Data Protection Officer sarà tenuto a documentarlo.
Tale documentazione sarà affidata al titolare del trattamento con l’ausilio del Data Protection Officer e dell'Amministratore di sistema (qualora la violazione riguardi dati contenuti in sistemi informatici).
Il titolare del trattamento provvederà alla tenuta di un apposito “Registro delle violazioni” (allegato C), in cui saranno riportate le seguenti informazioni:

1. numerazione progressiva;
2. data di rilevazione;
3. area/processo interessato dalla violazione;
4. descrizione della violazione;
5. tipo di violazione;
6. cause della violazione;

7. conseguenze della violazione;
8. numero e categorie di interessati coinvolti;
9. tipologia di dati violati;
10. elementi a supporto della valutazione del rischio: livello di gravità, livello di probabilità, livello di rischio derivante;
11. misure per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi, con indicazione dei tempi per l'attuazione delle misure;
12. necessità della notifica alla Autorità e data/ora della stessa, ove applicabile;
13. necessità della comunicazione all'interessato e data/ora della stessa, ove applicabile;
14. esito violazione e riscontri garante.

Ad integrazione di quanto riportato nel registro, il Data Protection Officer, fornisce ausilio nella raccolta e conservazione di tutti i documenti relativi ad ogni violazione, compresi quelli inerenti alle circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione è resa disponibile all'Autorità di controllo per le verifiche di competenza.

9. CONTROLLI

Qualora siano identificati più titolari del trattamento (caso di responsabili esterni del trattamento o di titolari autonomi), ruoli e responsabilità tra le parti sono stati definiti preliminarmente con la "Nomina di responsabile esterno del trattamento", per la gestione degli obblighi di notifica e di comunicazione in caso di violazione dei dati personali.
In questi casi, il titolare del trattamento con il supporto del Data Protection Officer concorda con i responsabili esterni del trattamento o titolari autonomi le modalità per la gestione degli obblighi di notifica e di comunicazione in caso di violazione dei dati personali, al fine di garantire il rispetto dei termini di notifica e di comunicazione, di cui il titolare del trattamento resta legalmente responsabile.

10. VIOLAZIONI DATI PERSONALI IN QUALITA' DI RESPONSABILE DEL TRATTAMENTO

In riferimento alla gestione dei servizi di Ausiliariato/Pulizia, di Emergenza Urgenza, Logistica e Accoglienza, Supporto ai Sistemi Informativi, la Sanitaservice ASL BT s.r.l. svolge tale ruolo in qualità di responsabile del trattamento dati ex articolo 28 del Regolamento UE 2016/679, in quanto tratta dati personali "per conto" del titolare del trattamento Asl Bat.

Con la presente procedura si elencano dettagliatamente i ruoli e le responsabilità del personale aziendale e quali attività dovranno essere compiute dalla Sanitaservice ASL BT s.r.l., quando si verifichi una violazione dati personali.

Al fine di comprendere al meglio i soggetti e i termini successivamente utilizzati, si precisa quanto segue:

- *per titolare del trattamento dati s'intende*: ASL BT l'azienda sanitaria locale della provincia di Barletta – Andria – Trani;
- *per responsabile del trattamento dati s'intende*: Sanitaservice ASL BT s.r.l. Società di servizi interamente partecipata dalla ASL BT;

Segnalazione di data breach effettuata dal Titolare del Trattamento ASL BT.

Ove la segnalazione di probabile "data breach" avvenga direttamente dal titolare del trattamento (affidante servizio), il responsabile del trattamento Sanitaservice ASL BT s.r.l. dovrà immediatamente informare dell'accaduto il Data Protection Officer, il referente privacy aziendale e l'amministratore di sistema, affinché entro poche ore venga riunito il "team data breach". I già menzionati soggetti in ossequio a quanto previsto nel contratto di designazione forniranno ogni necessaria collaborazione al titolare del trattamento per comprendere le cause, le eventuali contromisure da attuare nonché ove siano presenti dei sub-responsabili del trattamento, informeranno immediatamente tramite pec quest'ultimi.

Essendo la titolarità dei dati dell'affidante commessa, il responsabile del trattamento Sanitaservice ASL BT s.r.l., salvo specifico caso e approvazione, non dovrà intraprendere nessuna attività di notifica all'Autorità Garante e/o agli interessati, in quanto è il titolare del trattamento che governa l'intera procedura ed effettua ogni valutazione, azione ed attività. Il responsabile dovrà quindi fornire unicamente l'assistenza ed eseguire i compiti richiesti dal titolare mentre, solo ove il data breach riguardi, ad esempio, sistemi informatici della Sanitaservice ASL BT s.r.l. questa dovrà attuare le proprie politiche di data breach.

Segnalazione di data breach effettuata dal responsabile del trattamento dati Sanitaservice ASL BT s.r.l.

Ove il responsabile del trattamento Sanitaservice ASL BT s.r.l. per segnalazione diretta da parte di personale interno e/o esterno, oppure anche a seguito di attività di monitoraggio degli eventi anche di natura informatica, rilevi internamente un probabile data breach, dovrà immediatamente riunire il "team data breach"[3], e come previsto all'interno della designazione a responsabile del trattamento dovrà immediatamente (e comunque non oltre 12 ore dal probabile evento), informare tramite pec e/o e-mail il titolare del trattamento dati (ASL BT). Il team data breach in ossequio a quanto previsto nel contratto di designazione fornirà ogni necessaria collaborazione al titolare del trattamento per comprendere le cause, le eventuali contromisure da attuare nonché ove siano presenti dei sub-responsabili del trattamento, informerà immediatamente tramite pec quest'ultimi.

Essendo la titolarità dei dati dell'affidante commessa, il responsabile del trattamento Sanitaservice ASL BT s.r.l., salvo specifico caso e approvazione, non dovrà intraprendere nessuna attività di notifica all'Autorità Garante e/o agli interessati, in quanto è il titolare del trattamento che governa l'intera procedura ed effettua ogni valutazione, azione ed attività. Il responsabile dovrà quindi fornire unicamente l'assistenza ed eseguire i compiti richiesti dal titolare mentre, solo ove il data breach riguardi, ad esempio, sistemi informatici della Sanitaservice ASL BT s.r.l. questa dovrà attuare le proprie politiche di data breach.

Il responsabile del trattamento dati Sanitaservice ASL BT s.r.l. dovrà prevedere, successivamente all'avvenuta violazione, una revisione delle proprie politiche di sicurezza affinché tali eventi non possano ripetersi in futuro.

Si precisa che in caso di divergenza di pareri tra il Data Protection Officer e il responsabile del trattamento in merito ad un effettivo data breach e quindi al conseguente obbligo di notifica al titolare del trattamento affidante commessa, il DPO documenterà per iscritto ogni sua scelta, restando in capo al titolare del trattamento non accogliere la scelta del DPO e quindi non procedere con la notifica e comunicazione, con ogni responsabilità conseguente.

11. 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)
- Decreto Legislativo 30 giugno 2003 n. 196 come modificato dal D.lgs. n. 101/2018, recante il Codice in materia di protezione dei dati personali e provvedimenti adottati dall'Autorità Garante per la protezione dei dati personali;
- Linee guida sulla notifica delle violazioni di dati personali ai sensi del Regolamento 679/2016 (WP250), adottate dal Gruppo di lavoro Articolo 29 ("WP29"), in via definitiva, il 6 febbraio 2018;
- Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del Regolamento 2016/679 (WP248), adottate dal WP29, in via definitiva, il 4 ottobre 2017;
- Provvedimento del 27 maggio 2021 - Procedura telematica per la notifica di violazioni di dati personali (data breach) [9667201];
- Linee guida 01/2021 sugli esempi relativi alla notifica di violazione dei dati, adottate da EDPB il 14 gennaio 2021 e sottoposte a consultazione pubblica;

[3] "team data breach" composto da Data Protection Officer, referente privacy aziendale e Amministratore di Sistema;

12. ALLEGATI

Allegato A – “Modulo di Comunicazione interna di Data Breach”;
Allegato B – “Scenari di data breach”;
Allegato C – “Registro delle violazioni”;
Allegato D - “Risk Assesment – violazione dati personali”;
Allegato E - “Notifica violazione autorità di controllo”;
Allegato F - “Modulo di “comunicazione di violazione all’interessato”;

Andria, _____

IL TITOLARE E/O RESPONSABILE DEL TRATTAMENTO
Sanitaservice ASL BT s.r.l.

_____

ALLEGATO A - MODULO DI COMUNICAZIONE INTERNA DI DATA BREACH

1. **Breve descrizione della violazione di dati personali**

……

……

……

2. **Quando si è verificata la violazione di dati personali?**

Il ……

Tra il e il ……

In un tempo non ancora determinato ……

È possibile che sia ancora in corso ……

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

……

……

……

4. **Modalità di esposizione al rischio?**

……

……

……

5. ***Tipo di violazione***

- Lettura (presumibilmente i dati non sono stati copiati);
- Copia (i dati sono ancora presenti sui sistemi del titolare);
- Alterazione (i dati sono presenti sui sistemi ma sono stati alterati);
- Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione);
- Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione);
- Altro:

……

……

……

6. ***Dispositivo oggetto della violazione***

- Computer;
- Dispositivo mobile;
- Documento cartaceo;
- File o parte di un file;
- Strumento di backup;
- Rete;

7. **Sintetica *descrizione* dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:**

……

……

……

8. **Quante *persone* sono state colpite dalla violazione di dati personali?**

- N. di persone……
- Circa ……. Persone ……
- Un numero (ancora) sconosciuto di persone;

9. **Che tipo di *dati* sono coinvolti nella violazione?**

- Dati anagrafici;
- Numero di telefono (fisso o mobile);
- Indirizzo di posta elettronica;
- Dati di accesso e di identificazione (user name, password, customer ID, altro);
- Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro);
- Altro: ……
- Altri dati di personali (sesso, data di nascità, età, ...), dati sensibili e giudiziari;
- Ancora sconosciuto;

10. **Livello di gravità della violazione dei dati personali (secondo le valutazioni del' Area/Ufficio)?**

- Basso/trascurabile
- Medio
- Alto
- Molto alto

11. Misure tecniche e organizzative applicate ai dati colpiti dalla violazione

……

……

……

……, ……

Firma

_____

ALLEGATO – B "SCENARI DI DATA BREACH"

Esempio	Notifica all'Autorità	Comunicazione agli interessati	Note
Il Titolare conserva il backup di un archivio di dati personali criptati su una chiave USB	NO	NO	Per tutto il tempo in cui i dati sono criptati con uno stato di algoritmi sempre aggiornati, i backup dei dati esistono in un'unica chiave che non è compromessa, e i dati possono essere conservati periodo di tempo corretto questo non può essere considerato violazione da riportare
Il titolare gestisce un servizio on line (sito internet). A seguito di un attacco informatico su quel servizio, i dati personali dei suoi utenti sono stati trafugati. Il Titolare ha utenti in un singolo stato membro	Sì, riferire all'autorità di controllo se c'è una probabile conseguenza per gli individui	Sì, riferire agli interessati, in base alla natura dei dati personali coinvolti, se la gravità delle probabili conseguenze per gli interessati è alta	
Una breve interruzione di corrente di qualche minuto di durata presso il call center del Titolare che comporta che gli utenti non sono in grado di contattare il Titolare e accedere alla loro documentazione	NO	NO	Questa non è una violazione da notificare, tuttavia è un incidente registrabile secondo l'art. 33(5). Appropriata documentazione sull'evento dovrebbe essere mantenuta dal Titolare
Un Titolare subisce un attacco informatico ransomware per cui tutti i dati sono decriptati. Non sono disponibili backup e i dati non posso essere recuperati. In fase di investigazione, risulta chiaramente che l'unica caratteristica del ransomware era di decriptare i dati e che non c'era altro malware presente nel sistema.	Sì, riferire all'autorità di controllo, se ci sono probabili conseguenze per gli individui poiché in questo caso c'è perdita di disponibilità.	Sì, riferire agli individui, in base alla natura dei dati interessati e alla possibile conseguenza della mancanza di disponibilità dei dati, quali possono essere le possibili conseguenze.	Se c'è un backup disponibile e i dati possono essere conservati per un tempo limitato, questo potrebbe non essere riferito all'autorità di controllo o agli individui poiché non ci sarebbe mancanza definitiva di disponibilità o confidenzialità. Comunque, se l'autorità di controllo viene a conoscenza di un incidente per altre vie, può considerare un'indagine per valutare la bontà l'adempimento rispetto ai più ampi requisiti di sicurezza in base all'art. 32

ALLEGATO – B "SCENARI DI DATA BREACH"

Esempio	Notifica all'Autorità	Comunicazione agli interessati	Note
Un individuo contatta il call center di una banca per riferire di una violazione di dati. L'individuo ha ricevuto l'estratto conto mensile di qualcun altro. Il titolare intraprende una piccola indagine (es. che si risolve in 24 ore) e ritiene con ragionevole sicurezza che c'è stata violazione dei dati e che il problema sul sistema può o potrà coinvolgere altri individui.	SÌ	Solo agli individui interessati viene notificato se c'è alto rischio ed è chiaro che non riguarda altri.	Se, dopo un'ulteriore indagine si riscontra che l'evento riguarda più interessati, si deve aggiornare l'Autorità di controllo e il Titolare notifica l'evento anche agli altri interessati coinvolti se c'è alto rischio per loro.
Una mail di direct marketing viene inviata a destinatari nei campi "a" o "cc", consentendo così ad ogni destinatario di vedere l'indirizzo mail di altri destinatari.	Sì, la notifica all'autorità di controllo può essere obbligatoria se sono coinvolti un gran numero di individui e se sono rivelati dati sensibili (es. nella mailing list di uno psicoterapeuta) o se altri fattori presentano alti rischi (es. la mail contiene le password, ecc.).	Sì, riferire agli individui in base allo scopo ed al tipo di dati personali coinvolti ed alla gravità delle possibili conseguenze.	La notifica può non essere necessaria se nessun dato sensibile viene rivelato e se viene rivelato solo un minimo numero di indirizzi mail.
Hardware Utilizzo di chiavette o dischi USB inappropriati per la sensibilità delle informazioni, uso o trasporto di hardware sensibile per scopi personali, il disco rigido contenente le informazioni viene utilizzato per uno scopo non previsto (ad esempio per trasportare altri dati ad un fornitore, per trasferire altri dati da un database all'altro, ecc.)	Sì, riferire all'autorità di controllo se c'è una probabile conseguenza per gli individui	Sì, riferire agli interessati, in base alla natura dei dati personali coinvolti, se la gravità delle probabili conseguenze per gli interessati è alta	La notifica può non essere necessaria se nessun dato sensibile viene rivelato e se viene rivelato solo un minimo numero di indirizzi mail.

ALLEGATO – B "SCENARI DI DATA BREACH"

Esempio	Notifica all'Autorità	Comunicazione agli interessati	Note
Una società di hosting di siti Web (responsabile del trattamento) identifica un errore nel codice che controlla l'autorizzazione dell'utente. Ciò implica che ogni utente può accedere ai dettagli dell'account di qualsiasi altro utente.	Come responsabile del trattamento, la società di hosting di siti Web deve informare i suoi clienti interessati (i titolari del trattamento) prontamente. Supponendo che la società di hosting abbia condotto la propria indagine, i titolari del trattamento interessati dovrebbero essere ragionevolmente fiduciosi sul fatto che tutti abbia subito una violazione e quindi è vengono considerati come "informati" una volta che sono stati notificati dalla società di hosting (responsabile del trattamento). I titolari del trattamento devono quindi informare l'autorità di vigilanza.	Se non ci sono alti rischi per i singoli interessati, essi non devono essere notificati.	La società di hosting del sito web (titolare del trattamento) deve prendere in considerazione qualsiasi altro obbligo di notifica (ad esempio ai sensi della direttiva NIS). Se non vi è alcuna prova che questa vulnerabilità sia sfruttata con questo particolare responsabile del trattamento, una violazione notificabile potrebbe non essersi verificata ma potrebbe essere registrabile o essere oggetto di non conformità ai sensi dell'articolo 32.
Le cartelle cliniche di un ospedale non sono disponibili per un periodo di 30 ore a causa di un attacco informatico.	Sì, l'ospedale è obbligato a notificare già che ci possono essere gravi conseguenze per il benessere del paziente e la sua privacy.	Sì, notificare alle persone colpite	

ALLEGATO – B “SCENARI DI DATA BREACH”

I dati personali di 5000 studenti . vengono erroneamente inviati alla mailing list sbagliata con oltre 1000 destinatari.	Sì, riferire all'autorità di vigilanza.	Sì, notificare gli interessati in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze	

ALLEGATO C – REGISTRO DELLE VIOLAZIONI

N.	DATA DI RILEVAZIONE	AREA/PROCESSO	DESCRIZIONE DELLA VIOLAZIONE	CATEGORIE DI INTERESSATI E NUMERO APPROSSIMATIVO DI INTERESSATI PER CATEGORIA	CATEGORIE DI REGISTRAZIONI DEI DATI PERSONALI E NUMERO APPROSSIMATIVO DI REGISTRAZIONI PER CATEGORIA	CAUSE DELLA VIOLAZIONE	CONSEGUENZE DELLA VIOLAZIONE	MISURE, RESPONSABILITÀ E DATA DI ATTUAZIONE	GRAVITÀ	PROBABILITÀ	RISCHIO	NECESSITÀ DI NOTIFICA E DATA	NECESSITÀ DI COMUNICAZIONE E DATA	VERIFICA ATTUAZIONE MISURE E DATA DI ATTUAZIONE	VERIFICA EFFICACIA MISURE E DATA DI VERIFICA

ALLEGATO D – RISK ASSESSMENT – VIOLAZIONE DATI PERSONALI

RISK ASSESSMENt	DESCRIZIONI E NOTE
Dispositivi oggetto del Data Breach (computer, rete dispositivo mobile, file o parte di un file, strumento di back up, documento cartaceo, altro).	
Modalità di esposizione al rischio (tipo di violazione): - lettura (presumibilmente i dati non sono stati copiati); - copia (i dati sono ancora presenti sui sistemi ma del titolare); - alterazione (i dati sono presenti sui sistemi ma sono stati alterati); - cancellazione (i dati non sono più presenti e non li ha neppure l'autore della violazione); - furto (i dati non sono più sui sistemi el titolare e li ha l'autore della violazione); - altro.	
Breve descrizione dei sistemi di elaborazione o di memorizzazione dati coinvolti, con indicazione della loro ubicazione.	
Se laptop è stato perso/rubato: quando è stata l'ultima volta in cui il laptop è stato sincronizzato con il sistema IT centrale?	
Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati violata?	
La violazione può avere conseguenze negative in uno dei seguenti settori aziendali: - ……	

ALLEGATO D – RISK ASSESSMENT – VIOLAZIONE DATI PERSONALI

RISK ASSESSMENt	DESCRIZIONI E NOTE
Quali dati particolari sono coinvolti: - origine razziale o etnica; - opinion politiche, convinzioni religiose o filosofiche; - appartenenza sindacale; - dati genetici; - dati biometrici; - dati giudiziari; - relative alla salute o all'orientamento sessuale di una persona.	
Informazioni che possono essere utilizzate per commettere furti d'identità (i.e. dati di accesso e di identificazione, codice fiscale e copie di carta d'identità, passaporto o carte di credito).	
Informazioni personali relative a soggetti fragili (i.e. anziani, disabili, minori).	
Profili individuali che includono informazioni relative a performance lavorative, salario o stato di famiglia, sanzioni disciplinari, che potrebbero causare danni significativi alle persone	
La violazione può comportare pregiudizio alla reputazione, perdita di riservatezza di dati protetti da segreto professionale, decifratura non autorizzata, o qualsiasi altro dato economico o sociale significativo?	
Gli interessati rischiano di essere privati dell'esercizio del controllo sui dati personali che li riguardano?	
Quali misure tecniche e organizzative sono adottate ai dati oggetto di violazione? (i.e. La pseudonimizzazione e la cifratura dei dati personali)	
Il Titolare del trattamento ha adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati successivamente alla violazione?	

ALLEGATO D – RISK ASSESSMENT – VIOLAZIONE DATI PERSONALI

RISK ASSESSMENt	DESCRIZIONI E NOTE
Classificazione gravità della violazione (1, 2 o 3) e motivazioni:	
Notificazione del Data Breach all'Autorità Garante	
Comunicazione del Data Breach agli interessati	
Comunicazione del Data Breach ad altri soggetti	

……, ……

Firma

_____

ALLEGATO – F MODULO DI COMUNICAZIONE DI VIOLAZIONE ALL'INTERESSATO

Gentile .....

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

Presumiamo che in data ....., ore....., una terza parte non autorizzata abbiamo acquisito i seguenti dati personali relativi alla Sua posizione:

.....

.....

.....

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 <.....>, <.....>, ai seguenti recapiti:

ALLEGATO – F MODULO DI COMUNICAZIONE DI VIOLAZIONE ALL'INTERESSATO

- Tel……
- Email……

……, ……

Il titolare del trattamento

_____