SERVIZIO SANITARIO REGIONALE

Dipartimento Tutela della Salute e Politiche Sanitarie

AZIENDA OSPEDALIERA
"Pugliese Ciaccio"
Catanzaro

REGIONE CALABRIA

GESTIONE DATA BREACH

indice

Modifiche..... **1**

Scopo..... **2**

Campo di Applicazione..... **2**

Definizioni..... **2**

Documenti di Riferimento..... **3**

Contenuti..... **4**

premessa..... 4
Gestione del data breach interno alla struttura..... 5
Home page intranet aziendale- sezione privacy.....6
Modalità e profilo all'autorità del Garante.....
Gestione del data breach esterno della Struttura 6
Modalità e profili all'Autorità al Garante Privacy.....6
Modalità di comunicazione agli interessati..... 7
Registro delle violazioni..... 7
Schema di valutazione scenario Data breach..... 7

Allegati..... **9**

VERIFICA	Approvazione	
Data Protection Officer Dr.ssa Sarah Yacoubi	Direttore Generale AOPC Dr. Giuseppe Panella	Data di emissione 12/12/2018

SCOPO

Il presente documento ha lo scopo di indicare a tutto il personale operante presso l'Azienda Pugliese Ciaccio di Catanzaro la modalità della gestione di un Data Breach, ovvero di un episodio di violazioni di dati personali nel rispetto dei principi e delle disposizioni contenuti nel Regolamento (UE) 679/2016 sulla protezione dei Dati Personali (GDPR).

In questo documento si sintetizzano le regole per garantire la realizzabilità tecnica e la sostenibilità organizzativa nella gestione del Data Breach, sotto i diversi aspetti relativi a:

-modalità e comunicazione al titolare tramite il dpo

-valutazione dell'evento accaduto

-modalità e profilo di segnalazione all'autorità del Garante

-eventuale comunicazione all'interessato

Campo di Applicazione

La procedura si applica a tutto l'ambito aziendale e a tutti i soggetti, che a vari titolo, svolgono attività presso l'Azienda Ospedaliera Pugliese Ciaccio di Catanzaro. La procedura si applica inoltre in presenza di possibili violazioni di dati personali, siano essi contenuti in banche informatiche o cartaceo.

Definizioni:

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 (art. 4, punto 1).

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4, punto 2).

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia digitalizzato o meno, centralizzato, decentralizzato o ripartito in modo funzionale o geografico (art. 4, punto 6).

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 la 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 (art. 4, punto 7). In questo contesto, è titolare del trattamento AOPC CATANZARO

Data Protection Officer: la persona fisica individuata dal titolare del trattamento (Vedi delibera n 225/2018 del 22/5/2018) come Responsabile della protezione dei dati personali cosi come previsto per tutte le pubbliche amministrazioni dal GDPR (in particolare artt. 37, 38, 39).

Autorizzato al trattamento: la persona fisica, espressamente designata, che opera sotto l'autorità del titolare del trattamento, con specifici compiti e funzioni connessi al trattamento dei dati personali (art. 4, punto 10).
Responsabile del trattamento: la persona fisica che, secondo l'organizzazione aziendale, ricopre un ruolo gestionale e di responsabilità all'interno di AOPC che determina specifiche modalità organizzative rispetto ad uno o più trattamenti

Violazione dei dati personali: ***(c.d. Data breach):***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 (art. 4, punto 12)

Documenti di riferimento

- *Regolamento UE 679/2016, considerando n. 85, 86, 87, 88 artt. 33, 34*
- *Guidelines on Personal data breach notification under Regulation 2016/679 – article 29 data protection working party (Adopted on 3 October 2017 – as last Revised and Adopted on 6 February 2018)*

D.lgs. 196/2003e s.m.i
Delibera N.308del 12/07/2018 con riguardo al trattamento dei dati personali (GDPR)-ricognizione delle principali azioni di adeguamento dell'Azienda Ospedaliera Pugliese Ciaccio.

Contenuti

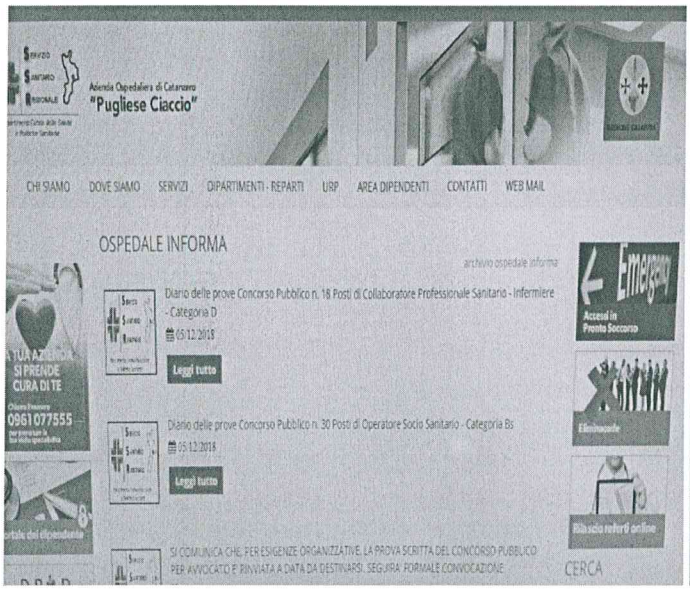
Premessa

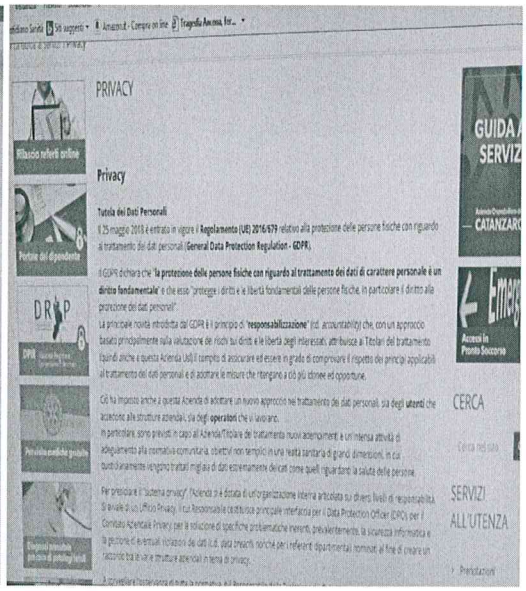
Una violazione dei dati personali (c.d data breach)può, se non affronta in modo adeguato tempestivo, provoca danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione di 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 interessata.

Gestione del *data breach All'interno della struttura*

Ogni operatore aziendale autorizzato a trattare dati personali, qualora venga a conoscenza di un potenziale data breach, avvisa tempestivamente il delegato al trattamento a cui afferisce (di norma il Direttore o il Responsabile della struttura presso cui presta servizio).
Il soggetto delegato a trattare dati personali, valuta l'evento, se ritiene confermate le valutazioni di un potenziale data breach lo segnala tempestivamente inviando una mail al DPO utilizzando il modulo allegato (All.1)reperibile alla sezione privacy-intranet aziendale.

Intranet home page aziendale-sezione privacy





Il responsabile privacy effettua a sua volta una valutazione dell'evento avvalendosi nel caso di eventuali altre professionalità necessarie per la corretta analisi della situazione del Dpo per eventuali funzioni consulenziali.

Ai fini di una corretta classificazione dell'episodio, il responsabile del trattamento utilizzerà lo schema del scenario di Data Breach allegato alla presente procedura.

Pertanto, sulla scorta delle determinazioni raggiunte e solo qualora ritenga che la violazione dei dati personali presenti un rischio per i diritti e liberta delle persone fisiche

Il **DPO** predispone un eventuale notificazione all'autorità del Garante. A firma del titolare del trattamento d inviare senza ingiustificato ritardo e , ove, possibile, entro 72 ore, da determinarsi

dal momento in cui il titolare ne e venuto a conoscenza cioè quando abbia un ragionevole di grado di certezza della verificazione di un incidente di sicurezza che riguardi dati personali .
Oltre il termine delle 72 ore la notifica deve essere corredata delle ragione del ritardo.

E comunque fatta salva la possibilità di fornire successivamente alla autorità del garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il titolare venga a conoscenza, a seguito della effettuazione di ulteriori indagini e attività di follow up 8c.d. notifica in fase).

La scelta e le motivazioni che hanno portato a non notificare l'evento devono essere documentate a cura del DPO

Gestione del *data breach* esterno alla struttura

Ogniqualvolta l'AOPC/ Titolare del trattamento si trovi ad affidare il trattamento di dati ad un soggetto Terzo/ Responsabile del trattamento, è tenuta a stipulare con tale soggetto uno specifico contratto che lo vincoli al rispetto delle istruzioni impartitegli dal titolare in materia di protezione dati: è necessario che la presente procedura di segnalazione di *Data Breach* sia inclusa nel suddetto contratto o comunque venga inoltrata al fornitore. Ciò al fine di obbligare il responsabile ad informare il titolare del trattamento senza ingiustificato ritardo, di ogni potenziale evento di *Data Breach*

Modalità e profili di notifica all'Autorità Garante Privacy

Ogni responsabile del trattamento, qualora venga a conoscenza di un potenziale *Data Breach* che riguardi dati di cui l'azienda sia titolare, ne dà avviso senza ingiustificato ritardo al referente privacy tramite il modulo allegato (All.2)
Per "ingiustificato ritardo" si considera la notizia pervenuta al titolare al più tardi entro 12 ore dalla presa di conoscenza iniziale da parte del responsabile.
Ai fini di una corretta classificazione dell'episodio il responsabile privacy utilizzerà lo schema Di scenario di *Data Breach* allegato al presente schema di procedura.
Pertanto, sulla scorta delle determinazioni raggiunte, il DPO predispone l'eventuale comunicazione all'Autorità Garante, a firma del titolare, da inviare senza ingiustificato ritardo e, ove possibile, entro **72 ore**, da determinarsi dal momento in cui il titolare ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza della verificazione di un incidente di sicurezza che riguardi dati personali.
Oltre il termine delle **72 ore**, la notifica deve essere corredata delle ragioni del ritardo.

E' comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il titolare venga a conoscenza, a seguito della effettuazione di ulteriori indagini e attività di follow-up (c.d. notifica in fasi)
La scelta e le motivazioni che hanno portato a non notificare l'evento deve essere documentata a cura del DPO.

Modalità di comunicazione agli interessati

Nel caso in cui dal *Data Breach* possa derivare un rischio elevato per i diritti e le libertà delle persone, anche queste devono essere informate senza ingiustificato ritardo, al fine di consentire loro di prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione.
Il responsabile privacy predispone l'eventuale comunicazione all'interessato/agli interessati, a firma del titolare, da inviarsi nei tempi e nei modi che lo stesso, anche attraverso la funzione consulenziale del DPO, individuerà come più opportuna come specificato nell'art. 34 del GDPR e tenendo conto di eventuali indicazioni fornite dall'Autorità Garante[1]

[1] [1] INB: Rimane salva la possibilità che sia il responsabile del trattamento ad effettuare una notifica per conto del titolare del trattamento, se il Titolare del Trattamento ha rilasciato specifica autorizzazione al Responsabile del trattamento, all'interno del suddetto contratto. Tale notifica deve essere fatta in conformità con gli articoli 33 e 34 del GDPR. La responsabilità legale della notifica rimane in capo al titolare del trattamento. In questa procedura si esamina la responsabilità legale della notifica rimane in capo al titolare del trattamento. In questa procedura si esamina solamente il caso d'uso ordinario in cui la notifica venga effettuata dal titolare del trattamento

Registro delle violazioni

Presso l'ufficio privacy e istituito il registro delle violazioni in cui sono documentati tutti gli episodi di data breach verificarsi dall'entrata in vigore de GDPR e il cui l'aggiornamento e a cura del DPO.

Schema di valutazione scenari – *data breach*

Di seguito sono illustrati alcuni esempi, non esaustivi, di possibili violazioni di dati personali, allo scopo di supportare i soggetti coinvolti nella procedura, nella valutazione in merito alla necessità di effettuare o meno la notifica di *data breach* all'Autorità Garante

Distruzione	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del titolare, né di altri. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo.	Caratteristiche: • Dati non recuperabili o provenienti da procedure non ripetibili Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione	• Rottura dell'ecografo prima di inviare al sistema centrale l'immagine. • Guasto non riparabile dell'hard disk contenente uno o più referti che, in violazione al regolamento, erano salvati localmente • Incendio di archivio cartaceo delle cartelle cliniche. • Distruzione di campioni biologici	Rottura di una chiavetta USB che non contiene dati personali originali (in unica copia) • Rottura di un PC che non contiene dati personali originali (in unica copia) • Distruzione di un documento, ad esempio a causa di un guasto di sistema, durante la sua stesura nell'apposito applicativo
Perdita	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del titolare, ma potrebbe essere nella disponibilità di terzi (lecitamente o illecitamente). In caso di richiesta di dato da parte dell'interessato non sarebbe possibile produrlo, ed è possibile che terzi possano avere impropriamente accesso al dato.	Caratteristiche: • Dati non recuperabili o provenienti da procedure non ripetibili • Dati relativi a più assistiti, relativi a interi episodi o relativi a tipologie di dato la cui indisponibilità lede i diritti fondamentali dell'interessato o relativi a tipologie di dato la cui divulgazione conseguente alla perdita possa ledere i diritti fondamentali dell'interessato Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione	• Smarrimento di chiavetta USB contenente dati originali • Smarrimento di fascicolo cartaceo personale dipendente	• Smarrimento di un documento, ad esempio a causa di un guasto di sistema, appena avvenuta la stampa

Modifica	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, è stato irreversibilmente modificato, senza possibilità di ripristinare lo stato originale. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo con certezza che non sia stato alterato	Caratteristiche: Modifiche sistematiche su più casi Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	• Guasto tecnico che altera parte dei contenuti di un sistema clinico, compromettendo anche i backup • Azione involontaria, o fraudolente, di un utente che porta alla alterazione di dati sanitari in modo non tracciato e irreversibile	Guasto tecnico che altera parte dei contenuti di un sistema clinico, rilevato e sanato tramite operazioni di recovery • Azione involontaria di un utente che porta alla alterazione di dati tracciata e reversibile • Modifica di un documento non ancora validato dal proprio autore.
Divulgazione non Autorizzata	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente), a seguito di incidente o azione fraudolenta, viene trasmesso a terze parti senza il consenso dell'interessato o in violazione del regolamento dell'organizzazione	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	• Malfunzionamento del sistema di oscuramento del sistema dipartimentale che invia a SOLE • Consegna di un CD con dati dei pazienti ad altra struttura senza autorizzazione	• Il medico sul proprio sistema dipartimentale seleziona il paziente Mario Rossi ma visita il paziente Luca Bianchi. Inserisce anamnesi e gli altri valori di refertazione ed invia a SOLE. • Infezione virale di un PC con un virus che dalla scheda tecnica non trasmette dati su internet • Trasmissione non autorizzata di un documento non ancora validato dal proprio

Accesso non Autorizzato	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente) sono stati resi disponibili per un intervallo di tempo a persone (anche incaricati dal titolare) non titolati ad accedere al dato secondo principio di pertinenza e non eccedenza, o secondo i regolamenti dell'organizzazione	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione. Indisponibilità dei dati personali oltre i tempi definiti a livello aziendale	• Accesso alla rete aziendale da persone esterne all'organizzazione che sfruttano vulnerabilità di sistemi • Accesso da parte di un utente a dati non di sua pertinenza a seguito di configurazione errata dei permessi di accesso ad un sistema clinico	• Accesso da parte di un utente a dati di sua pertinenza, a cui segue un uso improprio degli stessi • Accesso non autorizzata di un documento non ancora validato dal proprio autore. • Indisponibilità dei dati personali a causa della manutenzione programmata del sistema in corso
Indisponibilità temporanea del dato	Un insieme di dati personali, a seguito di incidente, azione fraudolenta o involontaria, è non disponibile per un periodo di tempo che lede il diritto dell'interessato	Indisponibilità dei dati personali oltre i tempi definiti a livello aziendale	• Infezione da ransomware che comporta la temporanea perdita di disponibilità dei dati e questi non possono essere ripristinati dal backup • perdita della chiave di de crittografia di dati crittografati in modo sicuro • irraggiungibilità di un sito di stoccaggio delle cartelle cliniche poste in montagna per isolamento neve • cancellazione accidentale dei dati da parte di una persona non autorizzata	• Indisponibilità dei dati personali a causa della manutenzione programmata del sistema in corso

Un *Data Breach*, quindi, non è solo un attacco informatico, ma può consistere anche in un accesso abusivo, un incidente (es. un incendio o una calamità naturale), nella semplice perdita di un dispositivo mobile di archiviazione (es. chiavetta USB, disco esterno), nella sottrazione di documenti con dati personali (es. furto di un cellulare di un dipendente).
I casi di *Data Breach* per le casistiche già descritte si estendono ai documenti cartacei o su supporti analogici.
La comunicazione involontaria di documenti, o in generale di dati, che non abbiano vero senso compiuto/riconducibilità verso l'interessato non è considerato *Data Breach,* ma è considerato un normale errore procedurale. Questo poiché:

- chi riceve non può sapere a quale paziente fisico è riferito il testo;
- il paziente fisico non è danneggiato poiché nessuno riferimento alla sua persona è stato diffuso.

Allegati
Allegato 1 modello per la segnalazione di un sospetto caso del Data Breach
Allegato 2 segnalazione da parte di Ditta Esterna di un sospetto caso del Data Breach

Allegato 1

MODULO PER LA SEGNALAZIONE DI UN SOSPETTO CASO DEL DATA BREACH

Data

Al dpo
dpo@aocz.it

NOME COGNOME RECAPITO TELEFONICO DELLA PERSONA CHE HA RILEVATO L'EPISODIO

NOME COGNOME DEL DELEGATO CHE HA TRASMESSO L'EPISODIO

DENOMINAZIONE DELLA E BANCA / BANCHE DATI OGGETTO DI DATA BREACH E BREVE DESCRIZIONE DELLA VIOLAZIONE DEI DATI PERSONALI IVI TRATTATI

Quando si e verificata la violazione dei dati personali trattati nell'ambito della banca dati ?

- Il----------
- Tra il----------il----------
- In un tempo che non e stato possibile ancora determinare

E possibile che sia ancora in corso
Dove e avvenuta la violazione dei dati (specificare se avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

---

modalità di esposizione al rischio (compilare solo se a conoscenza):

Distruzione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione
Perdita

Modifica
Divulgazione non autorizzata

Accesso non autorizzato
Altro

Dispositivo oggetto della violazione:
Computer
Rete
Dispositivo mobile
File o parte di un file
Strumento di backup
Documento cartaceo
Campione
Altro

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione (compilare solo se a conoscenza):

Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati?

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

Che tipo di dati sono oggetto di violazione?

- Dati anagrafici/codice fiscale
- Dati di accesso e di identificazione (username, password, custode ID, altro)
- Dati relativi ai minori
- Dati personali idonei a rivelare l'origine razziale o etnica, le convinzioni religiose o filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
- Dati personali relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona
- Dati giudiziari
- Copia per immagine su supporto informatico
- Ancora sconosciuto
- Altro;

Livello di gravità della violazione dei dati personali trattati nell'ambito della banca dati (secondo le valutazioni del delegato)?

- Basso/trascurabile
- Medio

- Alto
- Molto alto

Misure tecniche e organizzative applicate ai dati oggetto di violazione (compilare solo se a conoscenza):

Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future (compilare solo se a conoscenza)?

Allegato 2

SEGNALAZIONE DA PARTE DI DITTA ESTERNA DI UN SOSPETTO CASO DI DATA BREACH

Data:

All' Azienda Ospedaliera
Pugliese Ciaccio Catanzaro

DPO

Ditta

_____

NOME COGNOME RECAPITO TELEFONICO DELLA PERSONA CHE HA RILEVATO L'EPISODIO

NOME COGNOME DEL DELEGATO CHE HA TRASMESSO L'EPISODIO

DENOMINAZIONE DELLA E BANCA / BANCHE DATI OGGETTO DI DATA BREACH E BREVE DESCRIZIONE DELLA VIOLAZIONE DEI DATI PERSONALI IVI TRATTATI

_____

Quando si e verificata la violazione dei dati personali trattati nell'ambito della banca dati ?

- Il----------
- Tra il----------il----------
- In un tempo che non e stato possibile ancora determinare

E possibile che sia ancora in corso
Dove e avvenuta la violazione dei dati (specificare se avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

_____

_____

modalità di esposizione al rischio (compilare solo se a conoscenza):

Distruzione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione
Perdita
Modifica
Divulgazione non autorizzata
Accesso non autorizzato
Altro

Dispositivo oggetto della violazione:
Computer
Rete
Dispositivo mobile
File o parte di un file
Strumento di backup
Documento cartaceo
Campione
Altro

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione (compilare solo se a conoscenza):

Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati?

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

Che tipo di dati sono oggetto di violazione?

- Dati anagrafici/codice fiscale
- Dati di accesso e di identificazione (username, password, custode ID, altro)
- Dati relativi ai minori
- Dati personali idonei a rivelare l'origine razziale o etnica, le convinzioni religiose o filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
- Dati personali relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona
- Dati giudiziari

- Copia per immagine su supporto informatico
- Ancora sconosciuto
- Altro;

Livello di gravità della violazione dei dati personali trattati nell'ambito della banca dati (secondo le valutazioni del delegato)?

- Basso/trascurabile
- Medio
- Alto
- Molto alto

Misure tecniche e organizzative applicate ai dati oggetto di violazione (compilare solo se a conoscenza):

Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future (compilare solo se a conoscenza)?
