PROCEDURA PER LA GESTIONE DI DATA BREACH AI SENSI DEL REGOLAMENTO EUROPEO 679/2016

Sommario

1.PREMESSA

I dati personali possono essere soggetti al rischio di perdita, distruzione o diffusione indebita (ad esempio a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi), determinandosi, in tali casi, una possibile violazione dei medesimi dati (cd. Data Breach).

Con l'entrata in vigore del Reg. UE 2016/679 (GDPR), è stato introdotto l'obbligo per ogni organizzazione di gestire i Data Breach, annotarli in un apposito registro e, ove necessario, notificarli all'Autorità Garante e comunicarli alle persone fisiche interessate. Il mancato rispetto delle disposizioni in materia di Data Breach può portare l'organizzazione a subire importanti sanzioni.

Poiché l'eliminazione totale del rischio è per definizione impossibile, anche l'organizzazione più attenta può subire un Data Breach. Pertanto, le violazioni o potenziali violazioni non vanno mai nascoste o trascurate ma comunicate ai soggetti incaricati della loro gestione. Infatti, ogni violazione è utile all'organizzazione per individuare le proprie vulnerabilità e migliorarsi.

Con la presente procedura, vengono individuati i criteri per riconoscere un Data Breach e le regole per gestirlo. Tutti i dipendenti e/o collaboratori di Azienda Zero saranno informati in merito alla presente procedura mediante idonea delibera e/o circolare.

2.SCOPO DEL DOCUMENTO E AMBITO DI APPLICAZIONE

Questa procedura si prefigge lo scopo di definire le opportune modalità operative da attuare in caso di Data Breach, nel rispetto della normativa in materia di trattamento dei dati personali, garantendo l'aderenza ai principi e alle disposizioni contenute nel GDPR.

La presente procedura si applica a tutti i dati raccolti, conservati ed elaborati dall'Azienda Zero, i quali devono essere gestiti in conformità con le politiche di protezione dei dati stabilite, e mettendo in atto idonee procedure per l'individuazione, l'investigazione e la segnalazione di violazioni. In particolare, si applica a tutte le violazioni dei dati, siano esse sospette o confermate, ed è concepita per indicare ai soggetti implicati la corretta gestione di tali violazioni, a partire dalla valutazione dell'evento accaduto al fine di determinare se e come devono essere segnalate:

- al Titolare (nel caso di trattamenti effettuali sia all'interno dell'Azienda sia da parte dei Responsabili del trattamento);

– all'Autorità competente (Garante per la Protezione dei Dati Personali);

– agli interessati del trattamento. Per quanto non previsto in questo documento, si richiamano nel loro complesso le norme di legge ed in particolare il Regolamento UE 679/2016.

3. DEFINIZIONI

DATI PERSONALI: qualsiasi informazione riguardante una persona fisica identificata o identificabile; 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. 4.1 GDPR).

Rientrano nella categoria di dato personale, ad esempio, documenti di identità, rubriche e-mail, numeri di telefono, coordinate bancarie ecc. Vanno considerati dati personali anche quei dati che, pur non identificando automaticamente una persona, permettono l'identificazione attraverso confronto con altre fonti di dati, come targhe automobilistiche, indirizzi IP, MAC-address di dispositivi informatici ecc.

PSEUDONIMIZZAZIONE: tecnica che consente il trattamento dei dati personali in modo che non siano associabili a un soggetto specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali Dati Personali non siano attribuiti a una persona fisica identificata o identificabile.

CATEGORIE PARTICOLARI DI DATI PERSONALI: dati personali idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (Art. 9 del GDPR). Rientra nelle categorie particolari di dati personali, ad esempio, qualsiasi dato riferito ad un soggetto da cui si possa evincere: lo stato di gravidanza, infortuni, l'iscrizione a un sindacato, l'assenza dal lavoro per motivi religiosi, l'autenticazione tramite riconoscimenti delle impronte digitali, la firma grafometrica ecc.

DATI GIUDIZIARI: dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza (Art. 10 GDPR). Sono qualificabili come dati giudiziari, ad esempio, penali di condanna

definitivi concernenti le pene accessorie, le informazioni riportate sul casellario giudiziale, misure alternative alla detenzione che hanno prosciolto l'imputato, DASPO ecc.

In termini di precauzioni nei trattamenti, i dati giudiziari devono essere trattati analogamente alle categorie particolari di dati personali.

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. 4.2 GDPR).

Quindi qualunque operazione effettuata sul dato si configura come trattamento.

INTERESSATO: la persona fisica cui si riferiscono i dati personali.

Esempi di interessati: clienti, potenziali clienti, dipendenti, candidati all'assunzione, pazienti, scolari o studenti, utenti di un sito web, soggetti iscritti a un servizio (ad es. newsletter) ecc.

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 (Art 4.7 GDPR).

Quindi, con Titolare del trattamento si fa riferimento all'Azienda Sanitaria Zero complessivamente intesa.

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 (Art. 4.8 GDPR). I trattamenti da parte di un Responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico che vincola il Responsabile al Titolare del trattamento, determinandone l'oggetto e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento (Art. 28.3 GDPR). Ad ogni Responsabile del trattamento deve essere comunicato il contatto del Gruppo Privacy al quale effettuare l'eventuale segnalazione di potenziale Data Breach.

Si tratta principalmente delle aziende fornitrici che trattano dati necessari a fornire specifici servizi all'Azienda, come società informatiche (che abbiano accesso ai dati personali presenti sul sistema informatico), consulenti del lavoro (che trattano dati personali dei dipendenti), altre società coinvolte nell'attività dell'Azienda.

DESIGNATO: Direttore/responsabile di struttura o altra figura, individuata secondo quanto previsto nel Regolamento aziendale privacy, ai sensi dell'art. 2 – quaterdecies, comma 1, del Codice Privacy dal Titolare del trattamento, per la capacità, l'esperienza e la formazione in funzione dell'incarico ricoperto, con l'attribuzione dei compiti e delle funzioni specificatamente previste nell'atto di nomina;

AUTORIZZATO: la persona fisica che ha accesso a dati personali e agisce sotto l'autorità del Titolare o del Responsabile del trattamento, ed è stato istruito a trattarli (Art. 29 GDPR).

Quindi, tutti i dipendenti o collaboratori che trattano dati per l'Azienda Zero.

DATA PROTECTION OFFICER (c.d. DPO): la persona fisica individuata come Responsabile della protezione dei dati personali ai sensi del GDPR (in particolare artt. 37, 38, 39).

GRUPPO PRIVACY: il Gruppo aziendale preposto a coordinare le attività amministrative necessarie per il rispetto degli obblighi normativi in materia di protezione dei dati.

REFERENTE PRIVACY è la figura individuata dal Responsabile, interno della propria Struttura, che fornisce supporto allo stesso in tutte le attività relative al trattamento dei dati personali.

4. DESCRIZIONE ATTIVITA' E RESPONSABILITA'

4.1 Matrice delle Responsabilità

	Designato al trattamento	Responsabile ex art.28	Gruppo Privacy	DPO	Referente Privacy	Altre Strutture aziendali competenti	Direzione aziendale
Invio Segnalazione Data Breach		R			R		
Presa in carico segnalazione Data Breach			R	I	I		
Contenimento del danno e valutazioni iniziali	C	C	R	I	C	C	I
Comunicazione alla Direzione Aziendale degli esiti delle valutazioni			R	I			I
Determinazioni in merito alla notifica all'autorità di Controllo sulla base delle risultanze del Gruppo Privacy			C	C			R
Notifica all'Autorità di Controllo			C	R			
Valutazione notifica agli interessati			R	C			I
Eventuale comunicazione agli interessati	I	I	R	C			I
Aggiornamento del Registro delle violazioni			R	C			

R= Responsabile C= Collabora I = Informato

5. VIOLAZIONI DI DATI PERSONALI (DATA BREACH)

Rappresenta un Data Breach o violazione di sicurezza qualsiasi evento in conseguenza del quale si verifica una violazione di dati personali. Più precisamente, qualsiasi evento 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, secondo l'articolo 4, punto 12 del Regolamento Ue 679/2016.

Si ha un Data Breach ogniqualvolta si verifica una:

1) violazione della riservatezza dei dati (in caso di divulgazione di dati personali o accesso agli stessi non autorizzati o accidentali);

2) violazione dell'integrità dei dati (in caso di modifica non autorizzata o accidentale di dati personali);

3) violazione della disponibilità dei dati (in caso di perdita, impossibilità assoluta di accesso o distruzione accidentali o non autorizzate di dati personali).

Sono Data Breach le violazioni che riguardano dati personali, ovvero: 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.

I Data Breach possono avere sia natura informatica (es. un malware o un attacco hacker) che analogica (es. lo smarrimento di documentazione cartacea contenente dati personali).

Per aiutare il personale a riconoscerli, vengono forniti di seguito alcuni esempi di Data Breach più comuni, elencati più dettagliatamente nell' Allegato C. In caso di dubbio, è sempre necessario rivolgersi immediatamente al Gruppo Privacy, databreach@aziendazero.piemonte.it:

• smarrimento o furto di un dispositivo informatico contenente dati personali (laptop, tablet, smartphone, chiavi USB, Hard Disk esterni etc.) (perdita di disponibilità e riservatezza);

• guasto o non corretto funzionamento di un dispositivo informatico contenente dati personali (perdita di disponibilità);

• azione di un virus informatico o malware (perdita di riservatezza, disponibilità ed integrità);

• accesso non autorizzato ad un database o ad un dispositivo informatico (perdita di riservatezza e potenzialmente integrità);

• accesso non autorizzato a locali aziendali riservati o ad un archivio cartaceo (perdita di riservatezza, potenziale integrità e disponibilità);

• compromissione di una password utilizzata per accedere a dati aziendali (perdita di riservatezza, potenziale integrità e disponibilità);

• distruzione o perdita di un archivio cartaceo, schede o formulari contenenti dati personali (perdita di riservatezza e disponibilità);

• divulgazione su Internet di informazioni, dati, immagini senza autorizzazione (perdita di riservatezza);

• cancellazione accidentale di dati personali non recuperabili (perdita di disponibilità);

• invio di dati personali riservati ad un destinatario sbagliato (perdita di riservatezza);

• impossibilità di rispondere ad una richiesta di accesso ai propri dati personali formulata da un interessato (perdita di disponibilità).

Si ha un Data Breach anche quando la violazione riguarda un fornitore che tratta dati personali per conto di Azienda Zero (ad esempio un fornitore di servizi informatici, un partner in un progetto, un'agenzia etc.).

5.1 SEGNALAZIONE DEL DATA BREACH

Quando si riconosce o si sospetta che si sia verificato un Data Breach, questo deve essere comunicato senza ingiustificato ritardo al Titolare che dovrà avviare le procedure previste dagli articoli 33 e 34 del Regolamento Ue 679/2016.

La comunicazione di un Data Breach può arrivare dai seguenti soggetti:

INTERNAMENTE:

- da personale dipendente;
- da operatore aziendale autorizzato;
- da personale convenzionato/consulenti/stagisti/tirocinanti/ etc.;

ESTERNAMENTE:

- da parte degli interessati;
- da parte degli organi pubblici (Agid, Polizia, giornalisti etc.);

- da parte dei responsabili del trattamento (fornitori);
- da parte di altri soggetti;

Nell'eventualità in cui si constati o si sospetti un evento di data breach è necessario inviare tempestivamente una notifica all'indirizzo databreach@aziendazero.piemonte.it (collegato agli indirizzi mail dei componenti del Gruppo Privacy) nel quale si indicano gli elementi utili ad avviare gli approfondimenti del caso. Compilando ALLEGATO A) – Modulo di comunicazione del Data Breach.

Il Data Breach deve essere notificato all'Autorità Garante da parte del titolare del trattamento entro il termine massimo di 72 ore.

I soggetti esterni all'organizzazione possono segnalare all'Azienda eventi che comportino una violazione della privacy con qualsiasi mezzo a loro disposizione (ad esempio telefono, PEC, posta elettronica, di persona) indicando le proprie generalità e i propri dati di contatto. Successivamente a tale segnalazione, al fine di acquisire tutte le informazioni utili per la relativa verifica, il Gruppo Privacy deve inviare a tale soggetto l'Allegato A per la compilazione.

Possono essere valutate anche le segnalazioni anonime se sufficientemente circostanziate.

In questi casi sarà il Gruppo Privacy a compilare il modulo di comunicazione.

Il Gruppo Privacy effettua una prima valutazione dell'evento per accertarsi che l'incidente di sicurezza si sia effettivamente verificato, acquisendo ulteriori elementi dal Designato e dal Referente Privacy della Struttura interessata, che, dal momento della segnalazione, devono rendersi disponibili al fine di fornire chiarimenti, avvalendosi eventualmente di altri contributi secondo le varie competenze aziendali. Al fine di analizzare la segnalazione il GP può utilizzare la procedura di autovalutazione disponibile sul sito del Garante per la protezione dei dati personali e può anche richiedere la consulenza del DPO.

Se uno dei componenti del GP viene direttamente a conoscenza anche informalmente del potenziale caso di Data Breach deve far attivare la procedura indicata a inizio paragrafo.

La comunicazione, oltre che tempestiva, deve includere tutti i dettagli noti sull'incidente.

A titolo esemplificativo, ma non esaustivo, si indicano:

- l'ora e la data della violazione;
- l'ora e la data in cui è stata scoperta la violazione;
- una descrizione del tipo di violazione accertata (sulla riservatezza, l'integrità o la disponibilità dei dati) o degli elementi per cui si sospetta una violazione;
- le tipologie di dati coinvolti nella violazione (avendo cura di evidenziare eventuali violazioni su categorie particolari di dati personali, o su dati giudiziari);
- le categorie di interessati a cui i dati personali si riferiscono
- se noto, il numero di interessati coinvolti;
- se note, le modalità con cui è avvenuta la violazione, avendo cura di evidenziare se la violazione è ancora in corso;
- soggetti terzi (ad es. fornitori) qualora coinvolti o direttamente interessati alla violazione;
- le azioni già intraprese per porre rimedio alla violazione.

Qualora l'istruttoria abbia esito positivo, il GP la condividerà con il Titolare del Trattamento e con il DPO per le successive decisioni.

Al fine di stabilire le tempistiche per la gestione del Data Breach, si precisa che, nelle Linee Guida 9/2022 (versione 2.0 del 28/03/2023) sulla notifica delle violazioni dei dati personali è indicato dal Gruppo di lavoro europeo che il Titolare del trattamento può dirsi "a conoscenza" di una violazione quando abbia un "ragionevole grado di certezza che la violazione si sia verificata" e che questa abbia causato una compromissione di dati personali.

Il momento esatto "di presa coscienza" da parte del Titolare è variabile e dipende dalle circostanze; la conoscenza sarà quindi immediata in tutti quei casi in cui il Titolare del trattamento dati sia stato o direttamente informato per la prima volta di una potenziale violazione, in considerazione della segnalazione di un terzo o se abbia rilevato personalmente l'evento. Diversamente, la consapevolezza/conoscenza della violazione potrebbe non essere immediata, richiedendo, al contrario, del tempo per indagare se si sia effettivamente verificata; durante questo periodo, secondo quanto affermato dall'EDPB, il Titolare del trattamento non può dirsi pienamente "consapevole". È, in ogni caso, necessario che l'indagine iniziale venga avviata il prima possibile e sia quanto più dettagliata per permettere di stabilire con un ragionevole grado di certezza la sussistenza e la gravità della violazione. Una volta che il titolare del trattamento sia venuto a conoscenza di una violazione che sia suscettibile di notifica, questa deve intervenire senza giustificato ritardo, in ogni caso, non oltre le 72 ore dal momento di presa conoscenza.

È opportuno evidenziare che, ai sensi della Direttiva NIS2, come recepita dal D.lgs. n.138/2024, è necessario comunicare l'evento all'ACN (Agenzia per la Cybersicurezza nazionale) entro 24 ore dalla conoscenza dell'incidente "significativo" che, ai sensi dell'art.25, è tale soltanto se ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite

finanziarie per il soggetto interessato o che ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

Regolamento	Tempi di Notifica	Soggetto di Notifica
GDPR (Regolamento Generale sulla Protezione dei Dati)	Notifica entro 72 ore dalla presa di conoscenza della violazione dei dati.	Autorità di controllo competente (ad esempio, Garante per la protezione dei dati personali in Italia).
NIS2 (Direttiva sulla Sicurezza delle Reti e dell'Informazione)	Notifica iniziale entro 24 ore, seguita da un rapporto dettagliato entro 72 ore.	Computer Security Incident Response Team (CSIRT) nazionale o l'autorità competente designata.
DORA (Regolamento sulla Resilienza Operativa Digitale)	Notifica immediata (generalmente entro poche ore, anche se il termine specifico non è esplicitamente definito).	Autorità competenti nazionali o europee (come l'Autorità Bancaria Europea o altre autorità di vigilanza finanziaria).

(https://www.edoardolimone.com/2024/08/23/normativa-e-gestione-di-un-data-breach/)

L'art.14, comma 2 lett.b), prevede che, qualora l'ACN venga a conoscenza del fatto che "la violazione degli obblighi di notifica da parte di un soggetto essenziale o importante possa comportare una violazione dei dati personali, che deve essere notificata ai sensi dell'art.33 del GDPR", ne informa senza indebito ritardo il Garante per la protezione dei dati personali".

Si sottolinea il fatto che l'eventuale comunicazione all'ACN deve avvenire nei soli casi in cui si è in presenza di incidenti di cybersicurezza e che ciò non corrisponde a tutte le fattispecie di violazioni di dati personali, che possono avere anche natura analogica. In tal ultimo caso dovranno essere seguite soltanto le procedure previste dall'articolo 33 del Regolamento UE 2016/679.

5.2 CONTENIMENTO DEL DANNO E VALUTAZIONI INIZIALI

Spetta al GP stabilire il momento in cui sia opportuno coinvolgere la Direzione Aziendale, sulla base del grado di certezza della violazione, della gravità del possibile impatto, della necessità di

attivare specifiche misure di contenimento, o di assumere ulteriori provvedimenti ritenuti necessari.

Al ricevimento di una segnalazione di violazione, il GP dovrà innanzitutto valutare, con il supporto delle Unità Operative competenti per la trattazione del caso specifico, se la violazione dei dati è ancora in corso e, in tal caso, dovrà indicare le misure appropriate da prendere immediatamente nel caso si ritenga necessario minimizzare o fermare gli effetti della violazione dei dati (ad es., nella misura ragionevolmente praticabile, richiedendo la modifica, limitazione, o revoca delle autorizzazioni di accesso ai dati informatici, o rendendoli temporaneamente non disponibili).

5.3 VALUTAZIONE DEL DETTAGLIO DI RISCHIO E STIMA SUL RISCHIO PER GLI INTERESSATI

Il GP, avvalendosi delle Strutture competenti e di altre professionalità ritenute necessarie per il caso specifico, effettuerà una valutazione della violazione dei dati.

Non sussiste l'obbligo di notifica della violazione all'Autorità Garante quando è "improbabile" che questa comporti un rischio per i diritti e le libertà delle persone fisiche (art. 33 Reg. UE 2016/679). Occorre quindi effettuare una valutazione dell'evento per decidere se sia necessario notificare il Data Breach.

Per poter valutare l'impatto della violazione sui diritti e le libertà delle persone fisiche, dovranno essere raccolte (o verificate e confermate, se già riportate nella comunicazione della segnalazione) tutte le informazioni volte a valutare il rischio per i soggetti interessati, compilando l'apposito Allegato B. In particolare:

- tipologia del breach (riservatezza, integrità, disponibilità);
- natura, criticità e volume dei dati coinvolti dal Data Breach;
- facilità di identificazione degli interessati;
- criticità delle conseguenze per gli interessati;
- numero degli interessati coinvolti dal Data Breach;
- caratteristiche del Titolare dei dati oggetto del Data Breach.

In tale fase, possono inoltre essere tenuti in considerazione altri elementi rilevanti, ad esempio l'applicazione di misure a protezione dei dati interessati (come la pseudonimizzazione o la crittografia), che rendano quindi i dati inutilizzabili a qualsiasi parte non autorizzata.

La valutazione del dettaglio di rischio viene effettuata utilizzando il tool "Autovalutazione per individuare le azioni da intraprendere a seguito di una violazione dei dati personali", questo strumento, messo a disposizione dall'Autorità Garante, è da considerarsi esclusivamente quale ausilio al processo decisionale del titolare del trattamento e non rappresenta il pronunciamento dell'Autorità sull'applicazione del Regolamento (UE) 2016/679 o del D.lgs. 51/2018.

Nel caso permanga un dubbio considerevole sulla probabilità o meno del rischio, la notifica deve essere effettuata.

La decisione relativa alla notifica spetta al Titolare, il quale si avvale del Gruppo. Nell'ipotesi in cui si decida di non notificare il Data Breach, questo deve comunque essere appuntato nel Registro delle violazioni, secondo quanto indicato nel punto 7.

5.4 NOTIFICA ALL'AUTORITÀ DI CONTROLLO

A meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, il Titolare del trattamento ha l'obbligo di notificare la violazione all'Autorità di controllo competente senza ingiustificato ritardo.

Qualora tale notifica sia effettuata oltre il limite delle 72 ore, deve essere corredata dei motivi del ritardo.

È compito del GP sulla base delle valutazioni di cui ai punti precedenti e con la supervisione del DPO, provvedere alla redazione e invio della notifica seguendo il Modello telematico indicato dall'Autorità Garante.

La notifica deve riportare almeno:

- 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;
- descrizione dei sistemi, software, servizi e infrastrutture IT coinvolti nella violazione, con indicazione della loro ubicazione;
- misure tecniche e organizzative, in essere al momento della violazione, adottate per garantire la sicurezza dei dati personali coinvolti;
- il nome e i dati di contatto del DPO o di altro punto di contatto presso cui ottenere maggiori 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 e, se del caso, per attenuarne i possibili effetti negativi.

All'atto della notifica all'Autorità di controllo, il Titolare del trattamento può ottenere dalla stessa Autorità di controllo consulenza sull'eventuale necessità di informare le persone fisiche interessate. Una volta effettuata la notifica, sarà compito del DPO mantenere i rapporti e i contatti con l'Autorità, supportandola in ogni operazione, attività o indagine, e rispettando tutte le eventuali indicazioni da questa ricevute, fino alla chiusura del procedimento. Dovrà altresì mantenere regolarmente informata e aggiornata la Direzione Aziendale rispetto alla natura di tutte le operazioni e sull'esito del procedimento di notifica (ad es. prescrizioni, sanzioni ecc.).

5.5 COMUNICAZIONE ALL'INTERESSATO

Il Titolare sentito il Gruppo Privacy, deve informare gli interessati dell'evento anomalo in tutti i casi in cui, a norma degli artt. 33-34 GDPR, il Gruppo Privacy valuti che la violazione risulti presentare rischi elevati per i diritti e le libertà delle persone fisiche.

Possono risultare un utile riferimento le "Linee Guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali "adottate il 14/12/2021, in cui si riporta una lista di esempi in cui si può considerare che la violazione comporti un alto rischio per l'interessato.

Il Titolare del trattamento, ove possibile, dovrebbe contattare tutti gli interessati a cui si riferiscono i dati personali e particolari oggetto di trattamento ("Interessati") senza ingiustificato ritardo dall'avvenuta conoscenza e valutazione della violazione, attraverso il canale di comunicazione ritenuto più idoneo, se tale operazione implica uno sforzo sproporzionato, è invece possibile procedere con una comunicazione pubblica. Il GP predispone la comunicazione, a firma del Titolare da inviare nei tempi e nei modi che lo stesso, anche attraverso la funzione consulenziale del DPO, individuerà come più opportuna tenendo anche conto di eventuali indicazioni fornite dall'Autorità Garante. Tale comunicazione deve essere intellegibile, concisa, trasparente e facilmente accessibile; deve utilizzare un linguaggio semplice e chiaro adottando, se possibile, la stessa lingua parlata dall'Interessato; dovrà descrivere la natura della violazione dei dati personali, le probabili conseguenze della stessa, nonché le misure individuate per il rimedio.

I contenuti della comunicazione sono definiti dall'Articolo 34 del Reg. (UE) 2016/679, secondo cui devono essere riportati almeno:

- una descrizione della natura della violazione;
- il nome e le coordinate di contatto del DPO o di un altro punto di contatto;

- una descrizione delle probabili conseguenze della violazione
- una descrizione delle misure prese o proposte per gestire la violazione e, ove possibile, le misure appropriate per mitigare le possibili conseguenze negative.
- Ulteriori e opportuni elementi da valutare nello svolgimento della comunicazione sono:
- eventuali considerazioni particolari applicabili a determinate categorie di soggetti interessati (come minori o persone vulnerabili);
- i modi per agevolare le persone coinvolte nella violazione di dati nel contattare il Titolare per ottenere maggiori informazioni sulla violazione dei dati;
- l'ulteriore assistenza che l'Azienda dovrebbe fornire agli interessati, ove opportuno.

Tutte le operazioni e attività realizzate per la comunicazione agli interessati (ad es. contratti con società terze sull'invio di sms/e-mail, copia dell'articolo di giornale, report, ecc.), compresa la comunicazione agli interessati, saranno conservate e archiviate presso la SS.S Generali e Legali.

Non è prevista la comunicazione all'Interessato se è soddisfatta una delle seguenti condizioni:

- Sono state messe in atto le misure di protezione tecniche e organizzative adeguate e tali misure sono 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; salvo i casi in cui la violazione della sicurezza ha comportato la distruzione o la perdita dei Dati Personali degli Interessati;
- 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 (Allegato B);
- 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.

6. GESTIONE DEL PROCESSO DEL DATA BREACH DA PARTE DEL RESPONSABILE DEL TRATTAMENTO

Ogni qualvolta l'Azienda si trovi ad affidare il trattamento di dati a 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. A tal fine è necessario che la presente procedura di segnalazione di Data Breach sia resa nota a tutti i Responsabili del

trattamento con l'obiettivo di fornire le istruzioni per informare il Titolare del trattamento, senza ingiustificato ritardo, di ogni potenziale evento di Data Breach.

Pertanto il Responsabile del trattamento, qualora venga a conoscenza di un potenziale caso di Data Breach, deve avvisare, senza ingiustificato ritardo e nel rispetto dei tempi previsti nell'atto di nomina, l'Azienda all'indirizzo PEC aziendale protocollo@pec.aziendazero.piemonte.it o alla maill databreach@aziendazero.piemonte.it, utilizzando il report per la segnalazione di un sospetto caso di Data Breach (Allegato A).

Da questo momento vengono eseguiti i medesimi step della procedura illustrata al paragrafo 5.

7. REGISTRO DELLE VIOLAZIONI

Il Regolamento UE n. 679/2016 prescrive al Titolare del trattamento dei dati di documentare qualsiasi violazione di dati personali, al fine di consentire all'Autorità di Controllo di verificare il rispetto delle norme in materia di notificazione delle Violazioni di Dati Personali. Pertanto, la SS.S Affari Generali e Legali aggiorna e conserva il Registro delle violazioni dei dati personali secondo le indicazioni fornite dal DPO, attraverso l'utilizzo del tool aziendale.

L'annotazione deve essere effettuata anche nell'eventualità in cui sia stato deciso di omettere la notifica all'Autorità Garante. In questo caso, deve essere annotata la motivazione per la quale la notifica è stata ritenuta non necessaria. Allo stesso modo, deve essere annotata nel registro la motivazione per la quale non si è ritenuta necessaria la comunicazione agli interessati.

8. MODALITA' DI VERIFICA E CONTROLLO

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. Tale valutazione deve esser fatta in collaborazione con il DPO che coinvolgerà la struttura coinvolta, con eventuale supporto da parte di altre aree funzionali e tecniche.

Tale analisi potrebbe portare a identificare possibili aree di miglioramento del processo suggerendo una serie di azioni quali:

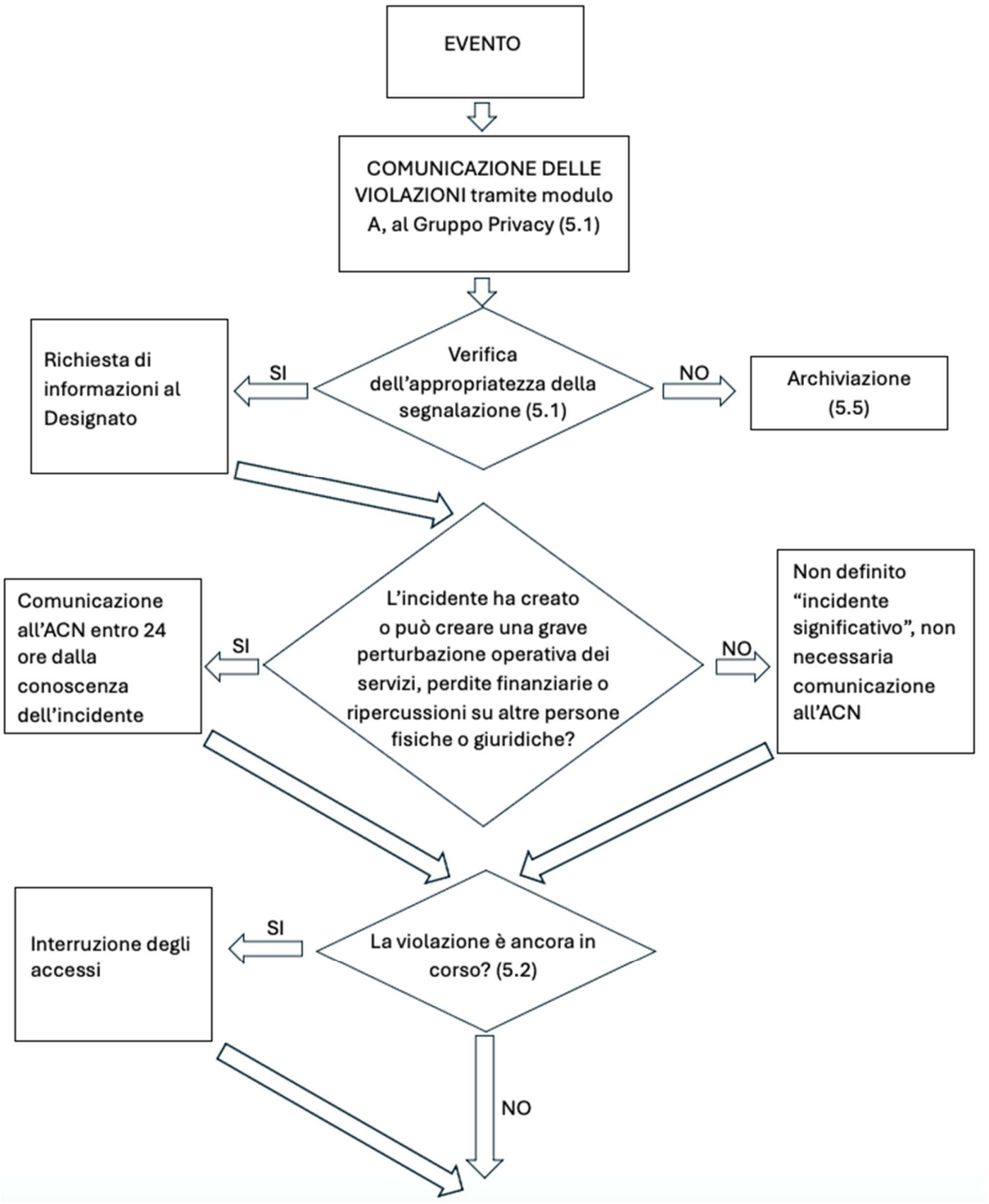
- Eventuale revisione della presente procedura e di eventuali altri documenti collegati (es. Analisi del rischio, Misure di sicurezza);

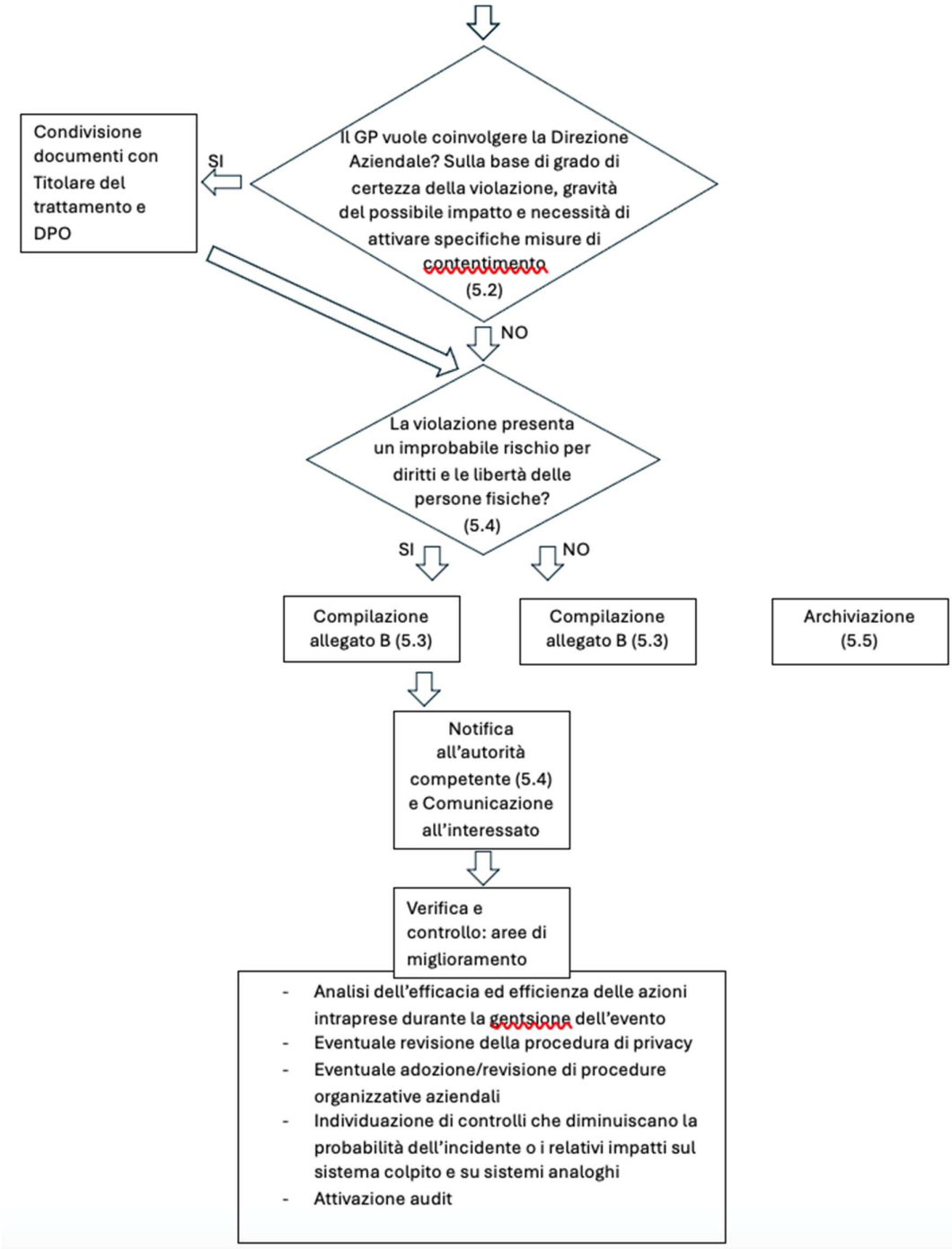
- Eventuale adozione/revisione di procedure organizzative aziendali;
- Individuazione di controlli che diminuiscano la probabilità dell'incidente o i relativi impatti sul sistema colpito e su sistemi analoghi;
- Attivazione di audit.

Il testo del presente documento è messo a disposizione di tutto il personale dell'Azienda mediante inserimento nell'apposita sezione della Rete Intranet Aziendale inoltre è pubblicata nel sito internet, alla sezione "Amministrazione trasparente".

I responsabili del trattamento dei dati saranno informati mediante inserimento di clausola apposita nel contratto di nomina a responsabile del trattamento, con indicazione del link di collegamento alla presente procedura.

9. FLOW CHART


EVENTO
COMUNICAZIONE DELLE VIOLAZIONI tramite modulo A, al Gruppo Privacy (5.1)
Verifica dell'appropriatezza della segnalazione (5.1)
SI
Richiesta di informazioni al Designato
NO
Archiviazione (5.5)
L'incidente ha creato o può creare una grave perturbazione operativa dei servizi, perdite finanziarie o ripercussioni su altre persone fisiche o giuridiche?
SI
Comunicazione all'ACN entro 24 ore dalla conoscenza dell'incidente
NO
Non definito "incidente significativo", non necessaria comunicazione all'ACN
La violazione è ancora in corso? (5.2)
SI
Interruzione degli accessi
NO


Il GP vuole coinvolgere la Direzione Aziendale? Sulla base di grado di certezza della violazione, gravità del possibile impatto e necessità di attivare specifiche misure di contenimento (5.2)
SI
Condivisione documenti con Titolare del trattamento e DPO
NO
La violazione presenta un improbabile rischio per diritti e le libertà delle persone fisiche? (5.4)
SI
NO
Compilazione allegato B (5.3)
Compilazione allegato B (5.3)
Archiviazione (5.5)
Notifica all'autorità competente (5.4) e Comunicazione all'interessato
Verifica e controllo: aree di miglioramento
- Analisi dell'efficacia ed efficienza delle azioni intraprese durante la gestione dell'evento
- Eventuale revisione della procedura di privacy
- Eventuale adozione/revisione di procedure organizzative aziendali
- Individuazione di controlli che diminuiscano la probabilità dell'incidente o i relativi impatti sul sistema colpito e su sistemi analoghi
- Attivazione audit

ALLEGATO A – MODULO DI COMUNICAZIONE DEL DATA BREACH

SERVIZIO SANITARIO NAZIONALE
REGIONE PIEMONTE
Azienda Sanitaria ZERO
Costituita con D.P.G.R. 18/02/2022 n. 9
Codice Fiscale / P.I. 12685160017
Sede legale: Via San Secondo, 29 bis – 10128 Torino

Data e ora in cui si è verificata la violazione:

- o Il_____
- o dal_____ (la violazione è ancora in corso)
- o dal_____al_____
- o In un tempo non ancora determinato

Soggetto segnalante (nome, cognome, qualifica):

_____

Struttura di appartenenza:

_____

Recapiti (mail, numero di cellulare):

_____

Natura della violazione:

- o Perdita della riservatezza (ad es. diffusione dati su intenet)
- o Perdita di integrità (ad es. i dati vengono modificati)
- o Perdita di disponibilità (ad es. furto chiavetta contenente unica copia dati)

Causa della violazione:

- o Azione intenzionale interna
- o Azione accidentale interna
- o Azione intenzionale esterna
- o Azione accidentale esterna
- o Sconosciuta:

  _____
- o Non ancora determinata

Descrizione della violazione:

_____
_____
_____

Descrizione dei sistemi, software, servizi e infrastrutture IT coinvolti nella violazione, con indicazione della loro ubicazione:

_____
_____
_____

Categorie di interessati coinvolti nella violazione:

- o Dipendenti/consulenti
- o Utenti/contraenti/abbonati/clienti (attuali o potenziali)
- o Associati, soci, aderenti, simpatizzanti, sostenitori
- o Soggetti che ricoprono cariche sociali
- o Beneficiari o assistiti
- o Pazienti
- o Minori
- o Persone vulnerabili (es. vittime di violenza o abusi, rifugiati, richiedenti asilo)
- o Altro: _____

Numero di interessati coinvolti nella violazione

- o N. ___ interessati
- o Circa n. ___ interessati
- o Non determinabile
- o Non ancora determinato

Categorie di dati personali oggetto di violazione

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

- Altro
  _____

Numero (anche approssimativo di registrazioni dei dati personali oggetto di violazione
- N. ___
- Circa n. ___
- Non determinabile
- Non ancora determinato

L'incidente è occorso presso un Responsabile di trattamento dei dati personali?
- SI
- NO

Se Responsabile specificare i trattamenti oggetto di nomina:
_____
_____
_____

Eventuali azioni già intraprese per porre rimedio alla violazione:
_____
_____
_____

Data _____

Firma del segnalante_____

ALLEGATO B – SCHEDA DI VALUTAZIONE DELLA VIOLAZIONE

SERVIZIO SANITARIO NAZIONALE
REGIONE PIEMONTE
Azienda Sanitaria ZERO
Costituita con D.P.G.R. 18/02/2022 n. 9
Codice Fiscale / P.I. 12685160017
Sede legale: Via San Secondo, 29 bis – 10128 Torino

Data e ora dell'evento:
Data e ora della rilevazione:
Data e ora della segnalazione:
Segnalante:
Struttura di appartenenza: _____ Designato:_____
Eventuale Responsabile del trattamento dati:
Altro: _____
Scheda comunicazione data breach (numero protocollo):
Livello di rischio:

- o Falso positivo
- o Positivo
- o Nullo
- o Basso
- o Medio
- o Alto

Natura della violazione:

- o Perdita della riservatezza (ad es. diffusione dati su intenet)
- o Perdita di integrità (ad es. i dati vengono modificati)
- o Perdita di disponibilità (ad es. furto chiavetta contenente unica copia dati)

Causa della violazione:

- o Azione intenzionale interna
- o Azione accidentale interna
- o Azione intenzionale esterna
- o Azione accidentale esterna
- o Sconosciuta:

  _____

- o Non ancora determinata

Descrizione della violazione:

_____
_____
_____

Descrizione dei sistemi, software, servizi e infrastrutture IT coinvolti nella violazione, con indicazione della loro ubicazione:

_____
_____
_____

Misure tecniche e organizzative, in essere al momento della violazione, adottate per garantire la sicurezza dei dati personali coinvolti:

_____
_____

Categorie di interessati coinvolti nella violazione:

- o Dipendenti/consulenti
- o Utenti/contraenti/abbonati/clienti (attuali o potenziali)
- o Associati, soci, aderenti, simpatizzanti, sostenitori
- o Soggetti che ricoprono cariche sociali
- o Beneficiari o assistiti
- o Pazienti
- o Minori
- o Persone vulnerabili (es. vittime di violenza o abusi, rifugiati, richiedenti asilo)
- o Altro: _____

Numero di interessati coinvolti nella violazione

- o N. ___ interessati
- o Circa n. ___ interessati
- o Non determinabile
- o Non ancora determinato

Categorie di dati personali oggetto di violazione

- o Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale)
- o Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
- o Dati di accesso e di identificazione (username, password, customer ID, altro)
- o Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro)
- o Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro)
- o Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza
- o Dati di profilazione
- o Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro)
- o Dati relativi all'ubicazione
- o Dati che rivelano l'origine razziale o etnica
- o Dati che rivelano le opinioni politiche
- o Dati che rivelano le convinzioni religiose o filosofiche

- o Dati che rilevano l'appartenenza sindacale
- o Dati relativi alla vita sessuale o all'orientamento sessuale
- o Dati relativi alla salute
- o Dati genetici
- o Dati biometrici
- o Altro

  _____

Numero (anche approssimativo di registrazioni dei dati personali oggetto di violazione

- o N. ___
- o Circa n. ___
- o Non determinabile
- o Non ancora determinato

In caso di perdita di riservatezza:

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

  _____

- o In corso di valutazione

In caso di perdita di integrità:

- o I dati sono stati modificati e resi inconsistenti
- o I dati sono stati modificati mantenendo la consistenza
- o Altro _____
- o In corso di valutazione

In caso di perdita di disponibilità:

- o Mancato accesso a servizi
- o Malfunzionamento e difficoltà nell'utilizzo di servizi
- o Altro_____
- o In corso di valutazione

Ulteriori considerazioni sulle probabili conseguenze:

_____

_____

Potenziale impatto per gli interessati:

- o Perdita del controllo dei dati personali
- o Limitazione dei diritti
- o Discriminazione
- o Furto o usurpazione di identità frodi
- o Perdite finanziarie
- o Decifratura non autorizzata della pseudonimizzazione
- o Pregiudizio alla reputazione
- o Perdita di riservatezza dei dati personali protetti da segreto professionale

- Conoscenza da parte di terzi non autorizzati
- Qualsiasi altro danno economico o sociale significativo

  _____
  _____
- Non ancora definito

Gravità del potenziale impatto per gli interessati
- Trascurabile
- Bassa
- Media
- Alta
- Non ancora definita

Motivazioni

_____
_____

Misure tecniche e organizzative adottate (o di cui si propone l'adozione) per porre rimedio alla violazione e attenuarne i possibili effetti negativi per gli interessati:

_____
_____

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

_____
_____

Comunicazione agli interessati:
- Si
- No

Valutazioni:

_____
_____

Valutazione del Gruppo Privacy:

_____
_____

Parere DPO:

_____
_____
_____

Data _____

Firma dei componenti del Gruppo Privacy_____ _____

Allegato C: 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.

Tipo di Breach	Definizione	Estensione minima /Soglia di segnalazione	Esempi	Controesempi
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	• Guasto non riparabile dell'hard disk contenente dati del personale di Azienda Zero che, in violazione al regolamento, erano salvati localmente • Incendio di archivio cartaceo delle schede 118	• 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 personali 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.	• Consegna di un CD con dati dei pazienti ad altra struttura senza autorizzazione	• Il personale del NOCC seleziona il paziente Mario Rossi invece del paziente Luca Bianchi. Inserisce diagnosi e dati del ricovero ed invia a Garsia. • Trasmissione non autorizzata di un documento non ancora validato dal proprio autore.
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.	• 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 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 i diritti 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	• Indisponibilità dei dati personali a causa della manutenzione programmata del sistema in corso

			• cancellazione accidentale dei dati da parte di una persona non autorizzata • perdita della chiave di decrittografia di dati crittografati in modo sicuro • irraggiungibilità di un sito di stoccaggio delle cartelle 118 per evento atmosferico	

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 notebook 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 persona fisica è riferito il testo;

• L'interessato non è danneggiato poiché nessun riferimento alla sua persona è stato diffuso.