PROCEDURA DI GESTIONE

DELLE VIOLAZIONI DI DATI PERSONALI

INDICE

1. INTRODUZIONE

1.1 Riferimenti normativi

- Regolamento (UE) 2016/679 del parlamento europeo e del consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/ce (regolamento generale sulla protezione dei dati - GDPR);
- Decreto Legislativo 10 agosto 2018 n, 101 “Disposizioni per l’adeguamento della Normativa Nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)”;
- “Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679” (WP250) del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati Personali del 3 ottobre 2017;
- Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015, come modificata dal Provvedimento del Garante sulla notifica delle violazioni dei dati personali (Data Breach) - 30 luglio 2019 [9126951];
- D.Lgs. 82/2005 Codice dell’Amministrazione Digitale (CAD);
- Artt. 331 e 361 del Codice di Procedura Penale (obbligo di denuncia da parte del pubblico ufficiale);
- Direttiva (UE) 2016/1148 (Direttiva NIS) del Parlamento europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell’Unione Europea;
- Decreto Legislativo 18 maggio 2018 n. 65, Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione;
- Circolare 18 aprile 2017, n. 2/2017, recante “Misure minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del PCM 01.08.2015, pubblicata in G.U. Serie generale n. 103 del 5.5.2017).

1.2 Scopo

Scopo della presente procedura è descrivere le azioni da intraprendere in caso di una violazione o sospetta violazione dei dati personali (ex artt. 33-34 del GDPR) al fine di evitare

o limitare i danni conseguenti alla violazione e consentire che siano rispettati i tempi richiesti per la segnalazione all'Autorità di Controllo, qualora necessaria.

1.3 Area di applicazione

La presente procedura deve essere applicata in tutti i casi in cui si verifichi un potenziale rischio di perdita, distruzione o diffusione indebita di dati personali (ad esempio a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi) che possono determinare pericoli significativi per la protezione dei dati personali degli interessati trattati dall'Istituto Zooprofilattico Sperimentale del Piemonte, Liguria e Valle d'Aosta (di seguito, "**Istituto**" o "**IZSPLV**") in qualità di Titolare del trattamento.

La presente procedura si applica a tutti i soggetti che a qualsiasi titolo trattano in qualsiasi modalità (automatizzata, manuale, digitale, cartacea) dati personali di competenza dell'Istituto quale Titolare del Trattamento, come – a titolo esemplificativo e non esaustivo - : dipendenti, somministrati, tirocinanti, collaboratori, responsabili esterni del trattamento, interessati, etc.

1.4 Acronimi e definizioni

Nella presente procedura sono utilizzati i seguenti acronimi:

- DPO: Data Protection Officer
- GDPR: General Data Protection Regulation
- PEC: Posta Elettronica Certificata

Ai fini della presente procedura per:

- **Incidente di Sicurezza** si intende, secondo la definizione fornita nello standard ISO 27000, "un evento singolo o una serie di eventi non voluti o inaspettati che ha una probabilità significativa di compromettere il funzionamento di processi aziendali e minacciare la sicurezza informativa". Gli Incidenti di Sicurezza possono dare luogo a Data Breach, ma non tutti gli Incidenti di Sicurezza sono Data Breach;

- **Data Breach** si intende una "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, par.1, punto 12 del GDPR). Le violazioni di sicurezza possono manifestarsi in diversi modi ed essere classificate in tre tipologie:

Tipologia di violazione	Evento/Minaccia
Violazione della riservatezza	Accesso o trattamento non autorizzato o illecito
	Divulgazione non autorizzata
Violazione dell'integrità	Modifica non autorizzata o accidentale
Violazione della disponibilità	Perdita o distruzione accidentale o illegale
	Indisponibilità temporanea o prolungata

A seconda dei casi, una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.

Esempi di possibili Data Breach sono elencati nelle Tabelle 1 e 2 allegate alla presente procedura.

2. DESCRIZIONE PROCEDURA

2.1 Fasi del processo di Gestione dei Data Breach

Il processo di gestione di un Data Breach concreto, potenziale o sospetto si articola nelle seguenti fasi:

0	Preparazione
1	Rilevazione evento- acquisizione notizia avvenuto incidente.
2	Analisi preliminare e invio segnalazione.
3	Gestione (contenimento del danno) e valutazione gravità dell'evento.
4	Notifica al Garante Privacy.
5	Altre segnalazioni dovute (es. agli organi di Polizia e, nel caso di incidente informatico, ad ACN, all'autorità NIS competente).
6	Comunicazione agli interessati, ove necessario, e raccolta riscontro dell'avvenuta comunicazione.
7	Inserimento dell'evento nel Registro degli Incidenti di Sicurezza/Registro Data Breach (Comprese le violazioni che non richiedono la notifica).
8	Azioni correttive specifiche e per analogia.

2.2 Preparazione

In adempimento all'articolo 32 del GDPR[1], l'Istituto adotta le seguenti misure tecniche ed organizzative per garantire un livello di sicurezza dei dati trattati adeguato al rischio:

[1] L'art. 32 del GDPR dispone che: "1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una

- azioni di sensibilizzazione e formazione del personale;
- strumenti tecnici per individuare intrusioni di rete (es. SIEM e SOC);
- predisposizione della presente procedura;
- predisposizione di procedure sulla continuità operativa;
- corretta allocazione di risorse umane anche in regime di reperibilità;
- audit periodici sui trattamenti e sul sistema informativo;
- interventi di digitalizzazione dei processi previsto dal CAD nel quadro delle misure tecniche previste;
- minimizzazione dei dati mediante:
    - la previsione di un periodo di tempo specifico di conservazione dei dati o del criterio per determinarlo;
    - l'individuazione specifica dei dati gestiti;
    - la previsione di un numero di soggetti autorizzati al trattamento ben individuati;
    - l'esistenza di specifiche autorizzazioni al trattamento dei dati a favore dei singoli autorizzati.

2.3 Rilevazione dell'evento

La segnalazione di un evento che possa compromettere la riservatezza, l'integrità e la disponibilità dei dati (di seguito, l'"**Evento**"), può pervenire da:

a) canali interni, quali

i. chiunque all'interno dell'Istituto rilevi una violazione o sospetti una violazione di dati personali;
ii. il Dirigente S.C. Qualità, Formazione nello svolgimento delle attività di audit;
iii. il Dirigente S.S. Gestione Sistemi informatici e telematici nel caso in cui un incidente di sicurezza informatica comporti una violazione di dati personali;

b) canali esterni, quali

procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. 2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. 3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo. 4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri."

i. l'interessato;
ii. il Responsabile esterno al trattamento *ex* art. 28 GDPR;
iii. le Autorità Pubbliche (AgID, Forze dell'Ordine, ecc.);
iv. il DPO;
v. altri soggetti esterni.

I soggetti interni che vengono a conoscenza di un Evento devono segnalarlo immediatamente di persona o tramite contatto telefonico o via e-mail al Designato Privacy della Struttura in cui si è verificato l'Evento.

Il Designato Privacy deve segnalare immediatamente l'Evento di cui è venuto a conoscenza all'Ufficio Privacy, di persona o tramite contatto telefonico o via e-mail, e al DPO, via e-mail.

I soggetti esterni che vengono a conoscenza di un Evento devono segnalarlo immediatamente via e-mail o via pec all'Ufficio Privacy e al DPO.

I recapiti per la segnalazione di un Evento sono indicati al successivo art. 2.11, comma 1.

2.4 Analisi preliminare e invio segnalazione.

2.4.1. Esecuzione dell'analisi di primo livello

Il segnalante, il Designato Privacy e l'Ufficio Privacy eseguono l'analisi di primo livello nel più breve tempo possibile e, comunque e in ogni caso, entro 48 ore dalla segnalazione.

L'obiettivo dell'analisi di primo livello è quello di verificare che l'evento segnalato: (i) sia effettivamente un Incidente di Sicurezza;

(ii) sia un Incidente di Sicurezza che può anche solo far presumere che si sia verificato un Data Breach.

A tal fine, detta analisi prevede la raccolta delle seguenti informazioni relative all'evento segnalato:

- Data e ora;
- Fonte;
- Tipologia dell'evento e descrizione;
- Stima del numero di interessati coinvolti;
- Stima della numerosità dei dati personali di cui si presume la violazione;
- Luogo in cui è avvenuta la violazione o presunta violazione;

- Descrizione dei sistemi di elaborazione e/o memorizzazione dei dati coinvolti, con indicazione della loro ubicazione;

Nel caso in cui l'analisi di primo livello evidenzi o faccia presumere che si sia verificato un Data Breach, rispettivamente, il Designato Privacy, nel caso di segnalazione proveniente da canali interni, o l'Ufficio Privacy, nel caso di segnalazione proveniente da canali esterni, compilano il modulo "Segnalazione Incidente relativo alla Sicurezza" - allegato *sub* "A" alla presente procedura quale parte integrante e sostanziale.

Il modulo "Segnalazione Incidente relativo alla Sicurezza" dovrà essere inviato, entro il termine di 48 ore di cui all'art. 2.4.1, comma 1, all'Ufficio Privacy all'indirizzo e mail indicato all'art. 2.11, comma 2, che segue.

L'Ufficio Privacy, una volta ricevuto o compilato il modulo "Segnalazione Incidente relativo alla Sicurezza", lo trasmetterà senza indugio ai componenti del Gruppo di Gestione Data Breach convocando contestualmente la riunione del Gruppo.

2.5 Gestione e valutazione gravità dell'Incidente di Sicurezza.

2.5.1 Esecuzione dell'analisi di secondo livello

Il Gruppo di Gestione Data Breach è composto dai seguenti soggetti:

- Ufficio Privacy;
- Dirigente S.S. Gestione Sistemi informatici e telematici o suo delegato;
- DPO. La presenza del DPO può essere garantita anche con contatto telefonico o a distanza;
- Designato Privacy della/e Struttura/e coinvolta/e nell'Incidente di Sicurezza.

Il Gruppo di Gestione Data Breach deve riunirsi ed eseguire l'analisi di secondo livello entro 24 ore dal ricevimento del modulo "Segnalazione Incidente relativo alla Sicurezza".

Eseguita l'analisi di secondo livello, il Gruppo di Gestione Data Breach mette in atto le prime azioni per il contenimento/annullamento del danno.

2.5.2 Valutazione della gravità della violazione

Il Gruppo di Gestione Data Breach esamina il caso e procede alla valutazione del rischio sulla base dei parametri e criteri indicati nella Tabella 3 e nel modulo "Valutazione del Rischio" - allegati, rispettivamente, *sub* 3 e "B" alla presente procedura quale parte integrante e sostanziale -, verificando, il tipo di violazione, la natura e il volume dei dati

personali coinvolti, la facilità di identificazione delle persone fisiche, la gravità delle conseguenze per le persone fisiche, le caratteristiche particolari dell'interessato e il numero delle persone fisiche coinvolte.

Qualora, dopo l'analisi di secondo livello, risulti improbabile che l'Incidente di Sicurezza abbia determinato una violazione dei dati personali o che la violazione dei dati personali verificatasi presenti un rischio per i diritti e le libertà delle persone fisiche non è necessario procedere con la Notifica all'Autorità di Controllo. In questi casi la procedura può terminare dopo aver informato il Direttore Generale e il Direttore Amministrativo e documentato il processo e le scelte operate. La fase di miglioramento può essere innescata per incrementare ulteriormente la protezione del dato, ma non è obbligatoria.

La documentazione prodotta in fase di analisi e corredata dalle relative motivazioni andrà inserita nel Registro degli Incidenti di Sicurezza a cura dell'Ufficio Privacy.

Se, invece, si ritiene che vi sia stata una violazione di dati personali che con ragionevole certezza presenta un rischio per i diritti e le libertà delle persone fisiche[2], il Gruppo Gestione Data Breach informa, entro 24 ore dalla conclusione dell'analisi di secondo livello, il Direttore Generale e il Direttore Amministrativo, fornendo loro tutti i dati raccolti.

2.6 Notifica al Garante Privacy

Il Titolare del trattamento, acquisite le informazioni raccolte, provvede tramite il Dirigente S.S. Gestione Sistemi informatici e telematici o suo delegato a predisporre la notifica al Garante per la protezione dei dati personali, secondo la procedura telematica presente sul sito internet dell'Autorità di Controllo.

La notifica al Garante per la protezione dei dati personali deve descrivere, ove possibile:

- la natura della violazione dei dati personali compresi;
- le categorie e il numero approssimativo di interessati in questione;
- le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

[2]Il criterio dirimente per valutare la necessità di avviare una procedura di notifica all'Autorità di Controllo è la probabilità che l'incidente di sicurezza possa porre a rischio o ad elevato rischio (per la comunicazione agli interessati) le libertà e i diritti degli individui. Di conseguenza, un incidente di sicurezza che determina l'indisponibilità dei dati personali per un certo periodo di tempo costituisce una violazione da notificare al Garante per la protezione dei dati personali e comunicare agli interessati solo qualora la mancanza di accesso alle informazioni/dati possa avere un impatto significativo sui diritti e sulle libertà delle persone fisiche. Non configura invece una "violazione della sicurezza" l'indisponibilità dei dati personali dovuta allo svolgimento di un intervento di manutenzione programmata se accompagnata da opportune misure organizzative tese a salvaguardare i diritti e le libertà fondamentali.

- il nome e i dati di contatto del DPO;
- descrizione delle probabili conseguenze della violazione dei dati personali;
- descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

La notifica deve avvenire senza ingiustificato ritardo ed entro i termini previsti per legge (72 ore), decorrenti dalla conclusione dell'analisi di secondo livello.

Qualora i contorni della compromissione non siano chiari, è opportuno fare una notifica "preliminare", significando che questa è l'inizio di una notifica in più fasi, seguita successivamente da una notifica "integrativa", in cui verranno indicate le informazioni raccolte successivamente.

Se i dati compromessi sono della stessa tipologia e sono stati compromessi con le stesse modalità si potrà effettuare una notifica "cumulativa".

Qualora la notifica al Garante per la protezione dei dati personali non sia effettuata entro i termini di legge deve essere corredata dei motivi del ritardo. A questo proposito, i Garanti europei nelle loro linee guida precisano che la mancata comunicazione può essere sanzionata ma che nessuna sanzione è prevista nel caso di comunicazione incompleta o di comunicazione non necessaria.

Si precisa che la notifica al Garante per la protezione dei dati personali deve essere effettuata nel caso in cui i rischi per le persone fisiche non siano trascurabili e solo nei seguenti casi:

- l'Istituto è Titolare del/i trattamenti dei dati personali coinvolti nella violazione;
- l'Istituto è Responsabile esterno del trattamento dei dati personali coinvolti, con delega alla notifica al Garante per la protezione dei dati personali. In questo caso, l'Istituto deve comunicare la sospetta violazione e/o l'Incidente di Sicurezza riguardante i dati personali al Titolare con le modalità convenute nell'atto di nomina ai sensi dell'art.28 del GDPR e con la massima tempestività, mettendosi a disposizione di quest'ultimo per approfondimenti e contenimento dei danni.

2.7 Altre segnalazioni dovute

Il Titolare, per il tramite il Gruppo Gestione Data Breach, provvede ad informare, ricorrendone i presupposti, altri organi quali:

- ACN – Agenzia Nazionale per la cybersicurezza (in caso di incidenti informatici);
- Organi di Polizia (in caso di violazioni di dati conseguenza di comportamenti illeciti o fraudolenti), tra cui la Polizia Postale e delle comunicazioni;
- CNAIPC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche).
- Gestore di Identità Digitale e Agid nel caso in cui si individui un uso anomalo di un'identità SPID (Sistema Pubblico di Identità Digitale).
- Autorità Competente NIS

2.8 Comunicazione della violazione all'Interessato

Il Titolare, tramite l'Ufficio Privacy, deve informare gli interessati dell'Incidente di Sicurezza, in tutti i casi in cui, a norma degli artt. 33 e 34 GDPR, la violazione presenta gravi rischi per i diritti e le libertà delle persone fisiche.

La comunicazione deve essere rivolta all'interessato senza ingiustificato ritardo dall'avvenuta conoscenza e valutazione della violazione, attraverso il canale di comunicazione ritenuto più idoneo.

La comunicazione deve essere intellegibile, coincisa, trasparente e facilmente accessibile. Deve essere utilizzato un linguaggio semplice e chiaro adottando, se possibile, la stessa lingua parlata dall'interessato.

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

- data e ora della violazione, anche solo presunta, e data e ora in cui si è avuto conoscenza della stessa;
- la natura della violazione dei dati personali;
- il nome e i dati di contatto del DPO;
- le probabili conseguenze della violazione dei dati personali;
- la descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi;

- le eventuali misure che l'Istituto suggerisce agli interessati di adottare per limitare i danni[3].

Per la comunicazione può essere utilizzato il modulo "Comunicazione del Data Breach all'interessato", allegato *sub* "C" alla presente procedura di cui costituisce parte integrante e sostanziale.

Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

- sono state messe in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati 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 nel Registro dei Data Breach e nella notifica al Garante per la protezione dei dati personali;
- 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.

2.9 Inserimento nel registro dei Data Breach

L'Art. 33 del GDPR prescrive al Titolare e al Responsabile del Trattamento di documentare qualsiasi violazione dei dati personali, al fine di consentire all'Autorità di controllo di verificare il rispetto della norma.

Nel registro dei Data Breach, il Gruppo Gestione Data Breach documenta ogni singolo Data Breach precisando:

- il tipo, la data e l'ora (ove possibile) del Data Breach;
- le conseguenze del Data Breach;
- i provvedimenti adottati per porvi rimedio o attenuarne le conseguenze;
- l'eventuale notificazione al Garante per la protezione dei dati personali;

[3] Si ricorda che in base all'art. 82 del GDPR Titolari e Responsabili rispondono in solido dei danni arrecati ed è, quindi, interesse dell'Ente prendere tutte le iniziative possibili per limitare i danni per gli interessati.

- l’eventuale comunicazione all’interessato.

Per quanto riguarda la documentazione delle violazioni, Il Titolare del trattamento tiene conto del parere del DPO in merito alla struttura, all’impostazione e all’amministrazione della documentazione stessa.

Gli Incidenti di Sicurezza occorsi, anche se non notificati al Garante e non comunicati agli interessati, nonché l’indicazione delle circostanze e conseguenze in cui la violazione si è verificata ed i provvedimenti adottati in merito, dovranno essere comunque sempre annotati e documentati sul Registro degli Incidenti di Sicurezza.

La conservazione del Registro dei Data Breach e del Registro degli Incidenti di Sicurezza è a cura dell’Ufficio Privacy.

2.10 Azioni correttive specifiche e per analogia

Il Titolare, sentito il Gruppo di Gestione Data Breach, nonché figure tecniche-professionali competenti, al termine dell’analisi dell’incidente individua le aree vulnerabili, promuovendo l’adozione delle seguenti azioni di miglioramento:

- Audit specifico e tempestivo sui trattamenti coinvolti da parte dell’Ufficio Privacy e del DPO;
- adozione di nuovi sistemi tecnici di prevenzione/protezione e/o di sistemi di controllo/monitoraggio/allarme;
- individuazione di controlli e misure di sicurezza che diminuiscano la probabilità dell’incidente o i relativi impatti sul sistema colpito e su sistemi analoghi;
- valutazione su possibilità di copertura assicurativa;
- azioni informative rivolte ai dipendenti;
- revisione delle relazioni con Clienti e Fornitori;
- pianificazione di test periodici per verificare la validità della presente procedura;
- revisione della presente procedura, se necessario, e di eventuali altri documenti collegati.

2.11 Contatti

I contatti per la segnalazione di un incidente di sicurezza, ai sensi dell'art. 2.3, commi 3 e 4, che precede, sono i seguenti:

- PEC IZSPLV: izsto@legalmail.it;
- PEO Ufficio Privacy: ufficioprivacy@izsto.it;
- Telefono Ufficio Privacy: 011 2686 306 – 459 - 312
- Ubicazione Ufficio Privacy: Via Bologna 148 – Torino, Palazzina A;
- PEO DPO: dpo@izsto.it

Il modulo "Segnalazione Incidente relativo alla Sicurezza" – allegato *sub* "A" alla presente procedura di cui costituisce parte integrante e sostanziale – di cui all'art. 2.4.1, comma 4, che precede, deve essere inviato al seguente indirizzo di posta elettronica ordinaria: ufficioprivacy@izsto.it.

Le comunicazioni ai Direttori Generale e Amministrativo devono essere effettuate al seguente indirizzo di posta elettronica: direzione.segreteria@izsto.it.

La notifica al Garante per la protezione dei dati personali va effettuata tramite la procedura presente sul sito internet dell'Autorità di controllo al seguente link https://servizi.gpdp.it/databreach/s/.

3. RUOLI E RESPONSABILITÀ: GRUPPO GESTIONE DATA BREACH

Ruoli	Referenti	Sostituti
Ufficio Privacy	Dott.ssa Cristina Cerutti, Dott.ssa Alice Ferrario, Dott. Luca Di Pellegrini	
Dirigente S.S. Sistemi Informatici e telematici	Dott. Enrico Aliberti	Sig. Carlo Palazzo, Sig.ra Elena Desantis, Sig. Giuseppe Terribilio
DPO	Liguria Digitale S.p.A. - Dott. Nicola Faravelli	
Designato Privacy della/e Struttura/e coinvolta/e	Responsabili di S.C. e di S.S. in staff alla Direzione Generale e Amministrativa, nonchè i soggetti individuati come Designati Privacy dal Titolare del Trattamento	

ALLEGATI

TABELLA 1. ESEMPI VIOLAZIONI TRATTI DALLE LINEE GUIDA ADOTTATE DAL GRUPPO DI LAVORO ART. 29.

Vengono riportati da *"WP 250 Guidellines on personal data breach notification under Regulation 2016/679 del 03.10.2017"* diversi scenari di violazione dei dati personali che si possono verificare da valutare come probabili data breach e che possono essere di aiuto nella gestione dell'evento:

Esempio	Notifica al Garante?	Comunicazione all'interessato?	Note/raccomandazioni
Il Titolare del trattamento ha effettuato un backup di un archivio di dati personali crittografati su una chiave USB. La chiave viene rubata durante un'effrazione.	No.	No.	Fintantoché i dati sono crittografati con un algoritmo all'avanguardia, esistono backup dei dati, la chiave univoca non viene compromessa e i dati possono essere ripristinati in tempo utile, potrebbe non trattarsi di una violazione da segnalare. Tuttavia, se la chiave viene successivamente compromessa, è necessaria la notifica.
Una breve interruzione di corrente di alcuni minuti presso il call center di un titolare del trattamento impedisce agli utenti di accedere al servizio.	No.	No.	Questa non è una violazione soggetta a notifica, ma costituisce comunque un incidente registrabile ai sensi dell'articolo 33, paragrafo 5 del GDPR
Il Titolare del trattamento subisce un attacco tramite *ransomware* che provoca la cifratura di tutti i dati. Non sono disponibili backup e i dati non possono essere ripristinati. Durante le indagini, diventa evidente che l'unica funzionalità dal *ransomware* era la cifratura dei dati e che non vi erano altri *malware* presenti nel sistema.	Sì, effettuare la segnalazione all'autorità di controllo, se vi sono probabili conseguenze per le persone fisiche in quanto si tratta di una perdita di disponibilità.	Sì, effettuare la segnalazione alle persone fisiche, a seconda della natura dei dati personali interessati e del possibile effetto della mancanza di disponibilità dei dati, nonché di altre possibili conseguenze.	Se fosse stato disponibile un backup e i dati avessero potuto essere ripristinati in tempo utile non sarebbe stato necessario segnalare la violazione all'autorità di controllo o alle persone fisiche, in quanto non si sarebbe verificata nessuna perdita permanente di disponibilità o di riservatezza. Tuttavia, qualora l'autorità di controllo fosse venuta a conoscenza dell'incidente con altri mezzi, avrebbe potuto prendere in considerazione lo svolgimento di un'indagine al fine di valutare il rispetto dei requisiti di sicurezza più ampi di cui all'articolo 32.
I dati sanitari di un ospedale non sono disponibili per un periodo di trenta ore a causa di un attacco informatico.	Sì, l'ospedale è tenuto a effettuare la notifica in quanto può verificarsi un rischio elevato per la salute e la tutela della vita privata	Si, informare le persone fisiche coinvolte.	
I dati personali di un grande numero di studenti vengono inviati per errore ad una mailing list sbagliata, con più di mille destinatari	Sì	Si, segnalare l'evento alle persone fisiche coinvolte in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze	

TABELLA 2. ESEMPI POSSIBILI SCENARI DI VIOLAZIONE

Sia per quanto riguarda i trattamenti cartacei che quelli elettronici, gli eventi che possono dare origine a potenziali situazioni di *data breach* possono essere di natura dolosa o accidentale.

Tipologie di violazione	Definizione	Quando segnalare	Esempi	Controesempi
Distruzione	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non più nella disponibilità del Titolare e/o di altri. Non è possibile produrre il dato all'interessato nel caso di sua richiesta.	Dati non recuperabili o provenienti da procedure non ripetibili. I soli dati appartenenti a **documenti definitivi e validati**	Guasto non riparabile dell'hard disk contenenti dati particolari salvati localmente. Incendio di archivio cartaceo .	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). Non è possibile produrre il dato all'interessato nel caso di sua richiesta.. E' possibile che terzi possano avere impropriamente accesso al dato.	Dati non sono recuperabili o provengono da procedure non più ripetibili. 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 con dati originali; smarrimento di un telefonino aziendale nel caso in cui contenga dati personali e non sia stato opportunamente cifrato. Smarrimento di fascicolo personale cartaceo dei dipendenti.	Smarrimento di un documento, ad esempio a causa di un guasto di sistema, appena avvenuta la stampa.
Accesso non autorizzato	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	I dati appartenenti a documenti definitivi e validati	Accesso alla rete aziendale da parte di persone esterne tramite vulnerabilità insite ne Accesso da parte di un utente a dati non di sua pertinenza l sistema Accesso ed uso improprio dei dati di pertinenza	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.	I dati non sono disponibili per un periodo di tempo che lede i diritti dell'interessato	Infezione del sistema che comporta temporanea perdita e impossibilità di recupero Cancellazione accidentale di dati da parte di personale non autorizzato. Perdita di chiave di decrittografia di dati crittografati	Indisponibilità dei dati personali a causa della manutenzione programmata del sistema in corso

TABELLA 3. ESEMPI PER LA VALUTAZIONE DEL RISCHIO

Cosa verificare		Esempi
Natura e volume dei dati personali coinvolti	La natura dei dati personali compromessi dalla violazione: maggiore è il rischio di danni per gli interessati ove questi rientrino nelle categorie particolari di dati.. Fermo quanto precede, ai fini di una puntuale valutazione occorre prendere in considerazione anche altri elementi, posto che anche la semplice violazione di dati comuni potrebbe comportare un rischio rilevante ai fini della notifica e della comunicazione. Di norma una combinazione di dati personali ha un carattere più sensibile rispetto a un singolo dato personale. Analogamente, una piccola quantità di dati personali altamente sensibili può avere un impatto notevole su una persona fisica, mentre una vasta gamma di dettagli può rivelare molte più informazioni in merito alla stessa persona. Inoltre, una violazione che interessa grandi quantità di dati personali relative a molte persone può avere ripercussioni su un numero corrispondentemente elevato di persone.	Ad esempio, violazioni relative a dati sulla salute, documenti di identità o dati finanziari come i dettagli di carte di credito, possono tutte causare danni di per sé, ma se tali dati fossero usati congiuntamente si potrebbe avere un'usurpazione d'identità.
Facilità di identificazione delle persone fisiche	Un fattore importante da considerare è la facilità con cui un soggetto che può accedere a dati personali compromessi riesce a identificare persone specifiche o ad abbinare i dati con altre informazioni per identificare persone fisiche. A seconda delle circostanze, l'identificazione potrebbe essere possibile direttamente dai dati personali oggetto di violazione senza che sia necessaria alcuna ricerca speciale per scoprire l'identità dell'interessato, oppure potrebbe essere estremamente difficile abbinare i dati personali a una particolare persona fisica, ma sarebbe comunque possibile a determinate condizioni. L'identificazione può essere direttamente o indirettamente possibile a partire dai dati oggetto di violazione, tuttavia può dipendere anche dal contesto specifico della violazione e dalla disponibilità pubblica dei corrispondenti dettagli personali. Quest'ultima eventualità potrebbe essere più rilevante per le violazioni della riservatezza e della disponibilità.	Ad esempio, i dati personali protetti da un livello appropriato di cifratura saranno incomprensibili a persone non autorizzate che non dispongono della chiave di decifratura. Inoltre, anche una pseudonimizzazione opportunamente attuata (definita all'articolo 4, punto 5 del GDPR come "*il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato 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*") può ridurre la probabilità che le persone fisiche vengano identificate in caso di violazione. Tuttavia, le tecniche di pseudonimizzazione da sole non possono essere considerate sufficienti a rendere i dati incomprensibili.
Gravità delle conseguenze per le persone fisiche	A seconda della natura dei dati personali coinvolti in una violazione, ad esempio categorie particolari di dati, il danno potenziale alle persone che potrebbe derivarne può essere particolarmente grave soprattutto nei casi di furto o usurpazione di identità, danni fisici, disagio psicologico, umiliazione o danni alla reputazione. Parimenti, se la violazione riguarda dati personali relativi a persone fisiche vulnerabili, queste ultime potrebbero essere esposte a un rischio maggiore di Il fatto che il titolare del trattamento sappia o meno che i dati personali sono nelle mani di persone le cui intenzioni sono sconosciute o potenzialmente dannose può incidere sul livello di rischio potenziale. Prendiamo una violazione della riservatezza nel cui ambito i dati personali vengono comunicati a un	Il fatto che il destinatario sia affidabile può neutralizzare la gravità delle conseguenze della violazione. Si dovrebbe altresì tener conto della permanenza delle conseguenze per le persone fisiche laddove l'impatto possa essere considerato maggiore qualora gli effetti siano a lungo termine

	terzo o ad altri destinatari per errore. Una tale situazione può verificarsi, ad esempio, nel caso in cui i dati personali vengano inviati accidentalmente all'ufficio sbagliato di un'organizzazione o a un'organizzazione fornitrice utilizzata frequentemente. Il titolare del trattamento può chiedere al destinatario di restituire o distruggere in maniera sicura i dati ricevuti. In entrambi i casi, dato che il titolare del trattamento ha una relazione continuativa con tali soggetti e potrebbe essere a conoscenza delle loro procedure, della loro storia e di altri dettagli pertinenti, il destinatario può essere considerato "affidabile". In altre parole, il titolare del trattamento può ritenere che il destinatario goda di una certa affidabilità e può ragionevolmente aspettarsi che non leggerà o accederà ai dati inviati per errore e che rispetterà le istruzioni di restituirli. In caso di violazione di riservatezza occorre verificare che le misure di sicurezza (es.: cifratura dei dati) in vigore rendano improbabile l'identificazione degli interessati (non compromissione della chiave, algoritmo di cifratura o impronta senza vulnerabilità note). In caso di perdita di integrità o disponibilità di dati occorre valutare se è possibile il recupero degli stessi in tempi compatibili con i diritti degli interessati danni.	
Caratteristiche particolari dell'interessato	Una violazione può riguardare dati personali relativi a minori o ad altre persone fisiche vulnerabili, che possono di conseguenza essere soggette a un rischio più elevato di danno. Altri fattori concernenti la persona fisica potrebbero influire sul livello di impatto della violazione sulla stessa.	Violazioni relative a dati sulla salute relative a determinate patologie (es. paziente affetto da sclerosi multipla, HIV, etc.) possono causare rischi di discriminazione per l'interessato.
Numero di persone fisiche interessate	Una violazione può riguardare solo una o poche persone fisiche oppure diverse migliaia di persone fisiche, se non molte di più. Di norma, maggiore è il numero di persone fisiche interessate, maggiore è l'impatto che una violazione può avere. Tuttavia, una violazione può avere ripercussioni gravi anche su una sola persona fisica, a seconda della natura dei dati personali e del contesto nel quale i dati sono stati compromessi.	Un'interruzione di rete per più di una giornata può riguardare dati di molte persone, determinando un maggior impatto della violazione.

ALLEGATO A

SEGNALAZIONE INCIDENTE RELATIVO ALLA SICUREZZA

DATI DEL SEGNALANTE	
Nome, cognome, qualifica	
Recapito telefonico, mail	
Struttura di appartenenza	
DATA DELL'INCIDENTE	
Quando si è verificata la violazione dei dati personali?	[] Il ___/___/_____ [] Tra il ___/___/____e il [] In un tempo non ancora determinato [] E' possibile che sia ancora in corso
LUOGO DELL'INCIDENTE	
Dove si è verificata la violazione dei dati personali?	
DESCRIZIONE DELL'INCIDENTE	
Classificazione dell'incidente	[ ] Violazione della riservatezza [ ] Violazione dell'integrità [ ] Violazione della disponibilità

Tipo di violazione	[ ] **Lettura** (presumibilmente i dati sono stati consultati, ma non sono stati copiati) [ ] **Copia** (I dati sono ancora presenti sul sistema/device, ma sono stati anche copiati altrove) [ ] **Alterazione** (I dati sono presenti sul sistema/device, ma sono stati alterati) [ ] **Cancellazione** (I dati non sono più sul sistema/device e non li ha più l'autore della violazione) [ ] **Furto di dati** (I dati non sono più sul sistema/device e li ha l'autore della violazione) [ ] **Furto di device o supporto di memorizzazione o materiale cartaceo** (es. computer, chiavetta USB, documenti cartacei contenenti particolari categorie di dati) - Specificare quale device, supporto di memorizzazione _____ [ ] **Furto di materiale cartaceo contenente categorie particolari di dati.** - Specificare la tipologia di documentazione_____ [[ ] **Furto di credenziali di accesso a** (es. account personale, password, applicazioni:, etc.) [ ] **Accesso abusivo al sistema informatico:** - Denominazione del sistema _____ - Collocazione fisica del sistema (se interno o esterno all'Azienda) [ ] **Divulgazione non autorizzata o non voluta di dati personali** [ ] Altro _____
Oggetto della violazione	[ ] PC [ ] Rete [ ] Dispositivo mobile [ ] File o parte di un file [ ] Strumento di Backup [ ] Materiale cartaceo [ ] Altro
Quali categorie di soggetti interessati sono coinvolti dalla violazione?	[ ] Dipendenti [ ] Utenti [ ] Altro

Tipo di dato oggetto della violazione	[ ] Dati personali (es. dati anagrafici/codice fiscale/indirizzo di posta elettronica) [ ] Dati di accesso e di identificazione (username, password) [ ] Dati relativi a minori [ ] Dati personali idonei a rivelare l'origine razziale ed etnica [ ] Dati personali idonei a rivelare le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale [ ] Dati genetici [ ] Dati biometrici [ ] Dati relativi alla salute [ ] Dati relativi alla vita sessuale o all'orientamento sessuale [ ] Dati giudiziari [ ] Altro :
Numero approssimativo degli interessati coinvolti nella violazione	[ ] numero certo di persone ____ [ ] numero presunto di persone____ [ ] numero sconosciuto di persone _____
Livello di gravità della violazione dei dati	[ ] Basso/trascurabile [ ] Medio [ ] Alto [ ] Molto alto
Effetti e conseguenze della violazione:	
Quali misure tecniche ed organizzative sono state adottate per contenere la violazione dei dati e prevenire violazioni future	
L'incidente è occorso presso un Responsabile del trattamento dei dati personali?	[ ] Si, specificare i trattamenti oggetto di nomina _____ [ ] No

ALLEGATO B

VALUTAZIONE DEL RISCHIO	
Classificazione dell'incidente	[ ] Violazione della riservatezza [ ] Violazione dell'integrità [ ] Violazione della disponibilità
Tipo di dato oggetto della violazione	[ ] Dati personali (es. dati anagrafici/codice fiscale/indirizzo di posta elettronica) [ ] Dati di accesso e di identificazione (username, password) [ ] Dati relativi a minori [ ] Dati personali idonei a rivelare l'origine razziale ed etnica [ ] Dati personali idonei a rivelare le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale [ ] Dati genetici [ ] Dati biometrici [ ] Dati relativi alla salute [ ] Dati relativi alla vita sessuale o all'orientamento sessuale [ ] Dati giudiziari [ ] Altro
Tipo di violazione	[ ] **Lettura** (presumibilmente i dati sono stati consultati, ma non sono stati copiati) [ ] **Copia** (I dati sono ancora presenti sul sistema/device, ma sono stati anche copiati altrove) [ ] **Alterazione** (I dati sono presenti sul sistema/device, ma sono stati alterati) [ ] **Cancellazione** (I dati non sono più sul sistema/device e non li ha più l'autore della violazione) [ ] **Furto di dati** (I dati non sono più sul sistema/device e li ha l'autore della violazione) [ ] **Furto di device o supporto di memorizzazione o materiale cartaceo** (es. computer, chiavetta USB, documenti cartacei contenenti particolari categorie di dati) - Specificare quale device, supporto di memorizzazione _____ - Consente l'accesso a _____ [ ] **Furto di materiale cartaceo contenente categorie particolari di dati.** Specificare la tipologia di documentazione_____ [ ] [ ] **Furto di credenziali di accesso a** (es. account personale, password, applicazioni.) - nome account_____ - consente l'accesso a _____ [ ] [ ] **Accesso abusivo al sistema informatico:** - Denominazione del sistema _____ - Collocazione fisica del sistema (se interno o esterno all'Azienda) [ ] **Divulgazione non autorizzata o non voluta di dati personali** [ ] Violazione che riguarda una notevole quantità di dati personali [ ] Violazione che riguarda un vasto numero di interessati [ ] Violazione [ ] Altro_____

Effetti sui dati personali	[ ] Distruzione illecita [ ] Distruzione accidentale [ ] Perdita illecita [ ] Perdita accidentale [ ] Divulgazione non autorizzata [ ] Accesso illecito [ ] Altro
Eventi dannosi che potrebbero verificarsi nei confronti dell'interessato	[ ] Discriminazione [ ] Furto o usurpazione di identità [ ] Perdite finanziarie [ ] Pregiudizio per la reputazione [ ] Perdita di riservatezza dei dati personali protetti da segreto professionale [ ] Decifratura non autorizzata della pseudonimizzazione [ ] danno economico o sociale significativo [ ] Privazione o limitazione di diritti o libertà [ ] Perdita di controllo sui dati personali dell'interessato [ ] Danni fisici, materiali o immateriali alle persone fisiche [ ] Altro :
Quali misure tecniche e organizzative sono state adottate preventivamente? (es. Pseudonimizzazione e cifratura dei dati personali, conservazione documentazione in locali accessibili solo da personale autorizzato; etc.)	
Successivamente alla violazione sono state adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti le libertà degli interessati?	
Livello di gravità della violazione dei dati personali	[ ] **Basso/trascurabile**: le persone fisiche possono incontrare alcuni piccoli inconvenienti, superabili senza alcun problema (es. reinserendo le informazioni) [ ] **Medio:** le persone fisiche possono incontrare notevoli disagi, che saranno in grado di superare nonostante alcune difficoltà (es. costi aggiuntivi, rifiuto di accesso ai servizi aziendali, stress) [ ] **Alto**: le persone fisiche possono incontrare conseguenze significative che dovrebbero essere in grado di superare anche se con gravi difficoltà [ ] **Molto alto**: le persone fisiche possono avere conseguenze significative o addirittura irreversibili, che non possono superare Altro: _____
Notificazione del data Breach all'Autorità Garante	[ ] Si [ ] No Note _____
Comunicazione del data Breach agli interessati	[ ] Si [ ] No Note _____

ALLEGATO C

COMUNICAZIONE DEL DATA BREACH ALL'INTERESSATO

Gentile (*nome e cognome dell'interessato*),

Con la presente si comunica che l'Ente XXX, Titolare del trattamento, in data_____ è venuta a conoscenza di un evento che potrebbe aver coinvolto i Suoi dati personali.

In particolare, è accaduto quanto di seguito descritto.

Inserire breve descrizione dell'incidente in relazione al quale si ritiene necessaria la comunicazione all'interessato ed indicazione dei dati personali violate.

Dall'analisi dei fatti sopra riportati, in considerazione della natura della violazione e della tipologia di dati personali coinvolti, si comunicano le possibili conseguenze dell'evento:

Inserire descrizione delle probabili conseguenze del data breach

L'Ente, venuta a conoscenza dell'incidente, ha tempestivamente posto in essere le seguenti misure tecniche ed organizzative:

Descrizione delle azioni già poste in essere o di cui si propone l'adozione per porre rimedio o attenuare gli effetti del data breach

Come previsto dall'art. 33 del Regolamento UE 2016/679 l'Ente ha provveduto a notificare questa violazione al garante Privacy.

Per ricevere ulteriori conformazioni, può contattare:

XXXXXXXX

Distinti saluti

Il Titolare del Trattamento

_____