PROCEDURA DI GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI ("*DATA BREACH*")

Sommario

I.INTRODUZIONE

A. SCOPO

La presente Procedura ha lo scopo di fornire indicazioni pratiche e adempimenti da eseguire in caso di violazione dei dati personali (di seguito anche "*Data Breach*").
I termini utilizzati si riferiscono alle definizioni riportate nel GDPR (cui si rinvia) e dettagliati nel punto I, lettera d), della presente procedura ("ACRONIMI").

B. CAMPO DI APPLICAZIONE

La presente procedura si applica all'Azienda Sanitaria Locale Torino 4 (di seguito anche "Azienda"), in qualità di Titolare del Trattamento dei dati personali, per tutti i settori che svolgono attività di trattamento dei dati personali nei casi in cui si verifichi una violazione o una sospetta violazione.
SI NOTI BENE. Un *data breach*, così come inteso nell'accezione comune, non è solo un attacco informatico, ma può consistere anche in un accesso abusivo, un incidente (es. un incendio, calamità naturale, ecc.), nella semplice perdita di un dispositivo mobile di archiviazione (es. chiavetta USB, disco esterno, hard disk contente dati personali e/o particolari), nella sottrazione di documenti con dati personali (es. furto di un notebook o tablet di personale dipendente).
SI NOTI BENE. La comunicazione involontaria o errata di informazioni che non impattano sui diritti e le libertà fondamentali dell'interessato, non è da considerare evento di *data breach*. In tal caso si parla di errore di natura procedurale (Ad es. la comunicazione tra Uffici dell'Azienda di un solo documento riferito ad una persona diversa rispetto all'interessato non è classificabile come *data breach*).

C. NORMATIVA DI RIFERIMENTO

La normativa di riferimento comprende oltre al Regolamento europeo in materia di Protezione dei dati personali e al D. Lgs. 196/2003, come emendato dal D. Lgs. 101/2018, anche le altre Leggi e disposizioni normative in materia civile e penale, secondo l'ordinamento nazionale che potrebbero prevedere il ricorso ad altre Autorità competenti. In questa sede, ci si riferisce al *Regolamento Europeo per la Protezione dei Dati Personali* n. 679/2016 (GDPR) e, in particolare ai seguenti articoli.
- Art. 4, par.12, GDPR, dalla cui lettura si distinguono tre tipi di violazione, che possono tuttavia combinarsi tra loro:
1. violazione di riservatezza, quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;
2. violazione di integrità, quando si verifica un'alterazione di dati personali non autorizzata o accidentale;
3. violazione di disponibilità, quando si verifica perdita, inaccessibilità, o distruzione, accidentali o non autorizzate, di dati personali.

- Articolo 33, GDPR, "Notifica di una violazione dei dati personali all'Autorità di controllo"
1. In caso di violazione dei dati personali, il Titolare del Trattamento notifica la violazione all'Autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
2. Il Responsabile del Trattamento informa il Titolare del Trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
3. La notifica di cui al paragrafo 1 deve almeno:
a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di Interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i Dati di contatto del Responsabile della Protezione dei Dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;

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

4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

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

- Articolo 34, GDPR, "Comunicazione di una violazione dei dati personali all'Interessato"

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del Trattamento comunica la violazione all'Interessato senza ingiustificato ritardo.

2. La comunicazione all'Interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).

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

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

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

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

4. Nel caso in cui il Titolare del Trattamento non abbia ancora comunicato all'Interessato la violazione dei dati personali, l'Autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

Ulteriori riferimenti sono rappresentati dalle Linee Guida in materia di notifica delle violazioni dei dati personali (WP250 rev.01, *Guidelines on Personal data breach notification under Regulation 2016/679, aggiornata al 06/02/2018 e al 2022,* e Linee guida dell'EDPB) e dai Provvedimenti, *ratione materiae*, emessi dall'Autorità Garante.

D. ACRONIMI

GDPR	Regolamento UE 2016/679 (General Data Protection Regulation)
Codice Privacy	D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali", come modificato dal D.Lgs. 101/2018
Garante	Autorità Garante per la protezione dei dati personali
WP29	Working Party article 29 – Gruppo di lavoro ex art. 29 (ora Comitato europeo della protezione dei dati) – EDPB (European Data Protection Board)
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»).
Interessato	La persona fisica cui si riferiscono i dati personali
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, punto 7, GDPR)
DPO/ RPD	Data Protection Officer / Responsabile della protezione dei dati ai sensi dell'art. 37, GDPR
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, ai sensi dell'art. 4, punto 8, GDPR. È sempre esterno all'organizzazione del Titolare.
Ufficio Privacy	Area del personale a cui, *ex* art. 2-*quaterdecies* del Codice privacy, l'Azienda può attribuire specifici poteri, oltre che compiti e funzioni, non solo per l'esecuzione di operazioni di trattamento, ma anche per assistere il Titolare nella compliance al GDPR.
Amministratore di Sistema (Interno)	Persona fisica incaricata dal Titolare della gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, così come richiamata dal Provvedimento del Garante per la protezione dei dati personali del 17/11/2008.
Incidente di sicurezza	Evento che comporta la violazione delle policy di sicurezza di un'organizzazione, con il conseguente rischio concreto di minaccia alla sicurezza delle informazioni.
Violazione dei dati (*data breach*)	Una particolare tipologia di incidente di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (art. 4, punto 12, GDPR)
Soggetto autorizzato dal titolare	Soggetto che, in adesione al sistema di gestione della privacy in uso presso l'Azienda, garantisce specifiche funzioni ai fini della compliance al GDPR.

E. DESTINATARI DELLA PRESENTE PROCEDURA

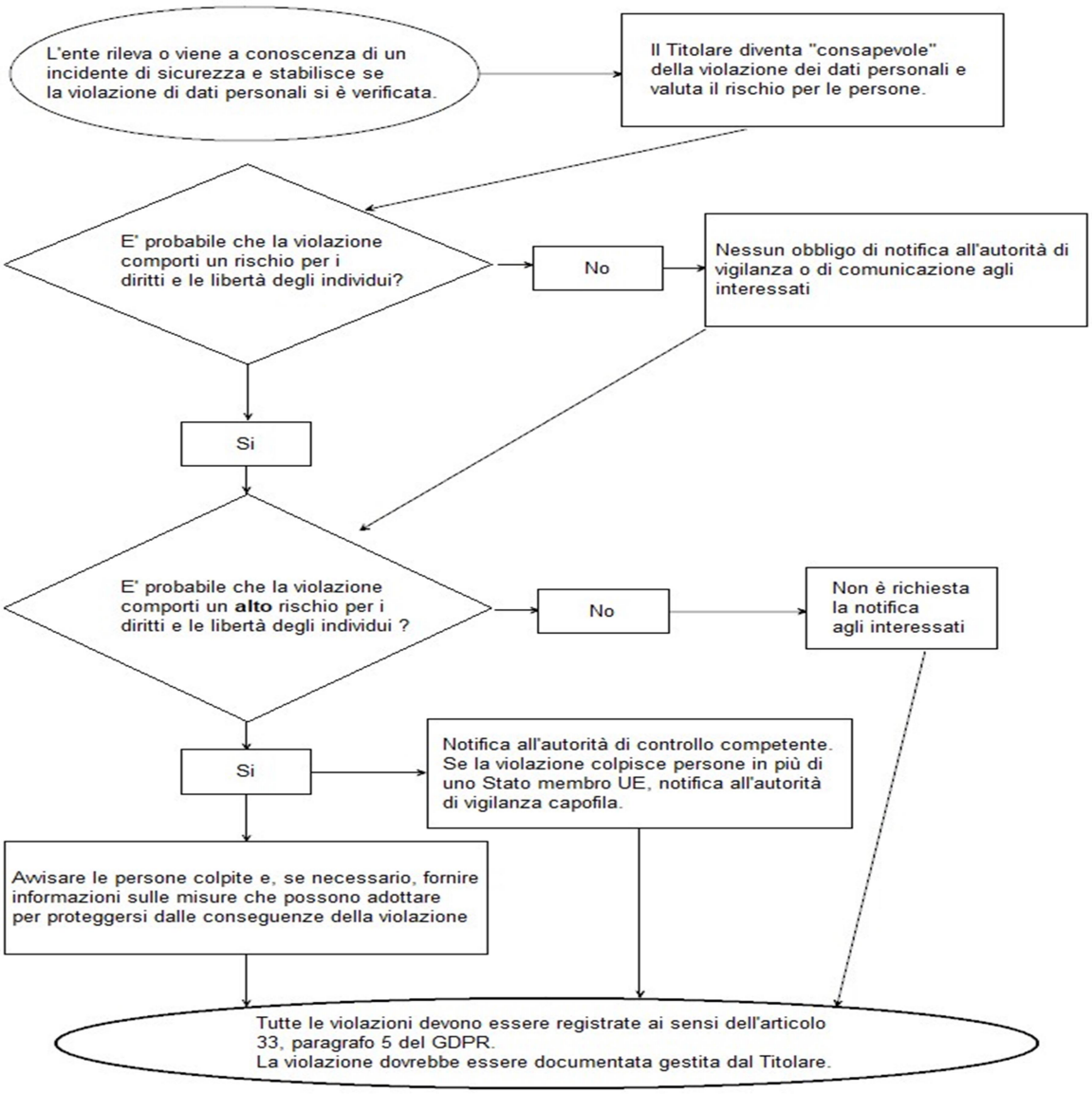
Questo documento è rivolto a tutti i soggetti che, a qualsiasi titolo e livello, trattano dati personali di competenza del Titolare del trattamento.

A titolo esemplificativo e non esaustivo, se ne riportano alcune categorie:

1. i lavoratori dipendenti e collaboratori, nonché coloro che a qualsiasi titolo, e quindi a prescindere dal tipo di rapporto intercorrente, abbiano accesso ai dati personali trattati nel corso del proprio impiego per conto del Titolare del trattamento (di seguito genericamente denominati Delegati e Autorizzati al trattamento);
2. qualsiasi soggetto (persona fisica o persona giuridica) diverso dal Delegato e dall'Autorizzato che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento abbia accesso ai dati personali e agisca in qualità di Responsabile del trattamento ex art. 28 GDPR;
3. contitolari del trattamento.

F. DIAGRAMMA DI FLUSSO DEI REQUISITI DI NOTIFICA

Diagramma di flusso che mostra i requisiti di notifica
tratto dalle linee guida WP29



II. TIPOLOGIE DI SEGNALAZIONE

La rilevazione di un evento di *data breach* può avvenire dalle seguenti fonti:

- **Notizia automatica**: sistemi di segnalazione automatica come, ad esempio, violazioni conseguenti al superamento del firewall dell'Azienda;
- **Notizia interna**:
  - segnalazione ad opera di autorizzati, e/o amministratori di sistema
  - intrusioni fisiche di soggetti non autorizzati nei locali dell'Azienda, furti, smarrimenti di fascicoli cartacei e/o di devices contenenti dati personali;
  - blocco dei sistemi e/o malfunzionamenti degli stessi;
- **Notizia esterna**: segnalazione durante le attività di monitoraggio, manutenzione e assistenza da parte di fornitori esterni.

III. RESPONSABILITÀ/AUTORITÀ E SOGGETTI COINVOLTI

La responsabilità del seguente processo è del Titolare del Trattamento dei dati personali che comunica all'Autorità di controllo e agli Interessati, laddove necessario e possibile, la violazione (*Data breach*) verificatasi.
In particolare, i soggetti che intervengono nel processo, in base ai diversi ruoli ricoperti, sono:

- RAPPRESENTANTE LEGALE E/O SUO DELEGATO (Rappresentanti apicali dell'Azienda);
- UFFICIO PRIVACY;
- DPO/RPD;
- RESPONSABILE DELL'UFFICIO OVE LA VIOLAZIONE SI È VERIFICATA;
- COMPONENTE DEL GRUPPO DI LAVORO PRIVACY DELLA STRUTTURA INTERESSATA;
- ALTRI SOGGETTI INTERNI e/o ESTERNI EVENTUALMENTE COINVOLTI NEL TRATTAMENTO (SOGGETTI DELEGATI; SOGGETTI AUTORIZZATI; RESPONSABILI DEL TRATTAMENTO, loro referenti e loro DPO).

Nelle fasi descritte di seguito sono illustrate le modalità d'intervento operativo di ciascun soggetto coinvolto.

IV. DESCRIZIONE DEL PROCESSO "*DATA BREACH*" PRESSO L'AZIENDA IN QUALITÀ DI TITOLARE

A. FASE 1: RACCOLTA DELLE INFORMAZIONI

1. CANALI INTERNI

Le segnalazioni interne di eventi anomali possono:

- pervenire da tutte le figure coinvolte nel sistema di gestione *privacy*;
- pervenire da tutto il personale dell'Azienda;
- essere inoltrate dal DPO.

2. CANALI ESTERNI

Le segnalazioni possono pervenire anche da fonti esterne, o anche dall'analisi di informazioni presenti sul Web, ovvero dai Responsabili esterni.
Inoltre, ogni Interessato può segnalare, anche solo in caso di sospetto, che i propri dati personali siano stati utilizzati abusivamente o fraudolentemente da un terzo; in tal caso, l'Interessato può richiedere all'Azienda la verifica dell'eventuale violazione.

3. MODALITA' DI COMUNICAZIONE

Le segnalazioni in ordine a possibili incidenti di sicurezza, riscontrate dal personale dell'Azienda, devono essere inoltrate immediatamente, via e-mail o PEC ai seguenti soggetti:
- Direttore Generale, il quale provvederà, senza ulteriore ritardo a coinvolgere l'Ufficio Privacy;
- Ufficio Privacy;
- Responsabile dell'Ufficio interessato dall'evento;
- DPO/RPD.

All'inoltro del messaggio deve seguire il contatto telefonico immediato dei predetti soggetti.

B. FASE 2: ANALISI DELLE SEGNALAZIONI

1. ANALISI PRELIMINARE E ELABORAZIONE DELLA SCHEDA EVENTO

Il Responsabile dell'Ufficio interessato dalla potenziale violazione, il componente del Gruppo di lavoro privacy della relativa struttura e l'Ufficio Privacy dell'Azienda, tramite il coinvolgimento e il supporto del DPO/RPD, avvia un'analisi preliminare finalizzata alla raccolta dei Dati concernenti l'anomalia (Allegato 2.1 – RACCOLTA INFORMAZIONI) e alla compilazione della Scheda Evento (Allegato 2.2), contenente tutte le informazioni raccolte (ad esempio, data presunta dell'evento, data e ora in cui si è avuta conoscenza della violazione, fonte della segnalazione, tipologia di violazione e di informazioni coinvolte , descrizione evento, numero di Interessati e di registrazioni di dati coinvolti, luogo della violazione, descrizione dei sistemi di elaborazione o di memorizzazione coinvolti e loro ubicazione).

La Scheda Evento viene, quindi, inviata (insieme ad una convocazione ufficiale della riunione) agli altri soggetti che compongono il **Gruppo di Primo Livello** (anche **GPL**), ossia:

- Amministratore di sistema, ove nominato, o funzioni dei sistemi informativi, nel caso in cui l'evento attenga all'infrastruttura, sistemi informativi e banche dati gestite dall'Azienda;
- Referente individuato del soggetto esterno (Responsabile del trattamento) coinvolto nel richiamato evento, nel caso in cui l'evento attenga ai trattamenti di dati personali svolti dal Responsabile del trattamento;
- DPO/RPD (e, se possibile, referente privacy o Ufficio Privacy) del Responsabile del trattamento.

2. ANALISI DI PRIMO LIVELLO - VERIFICA DELLA SEGNALAZIONE (GPL)

Obiettivo dell'analisi di primo livello è quella di verificare che la segnalazione non sostanzi un cd. "falso positivo".

Il **GPL**, una volta riunito, anche tramite evidenze documentali (ancor meglio mediante stesura di verbale sottoscritto dalle parti interessate) deve ricavare ogni informazione utile a meglio definire la tipologia e le caratteristiche tecniche dell'incidente, così da verificare se l'evento ha compromesso dati personali.

In particolare, all'esito dell'incontro, ove tecnicamente possibile, devono essere fornite le seguenti informazioni:

- il sistema, infrastruttura, applicazione, banca dati oggetto dell'incidente di sicurezza;
- la tipologia dell'evento verificatosi, vale a dire se lo stesso attiene ad una violazione della riservatezza, dell'integrità e/o della disponibilità dei dati;
- il volume dei dati e, ove possibile, il numero degli interessati coinvolti;
- le misure di sicurezza applicate, by design, prima dell'evento;
- le attività correttive appena realizzate per arginare gli effetti dell'evento;
- le attività correttive che si intendono pianificare e adottare nel medio-lungo periodo, allo scopo di minimizzare la possibilità del ripetersi dell'evento.

Il **GPL**, definito il patrimonio informativo appena richiamato, mette in campo tutte le azioni correttive di immediata attuazione.

Di tali azioni, mediante evidenza documentale e comunicazione formale, è informato il Direttore Generale.

Nel caso in cui l'evento segnalato risulti essere un "falso positivo", il **GPL** chiude l'incidente e l'evento viene comunque inserito, a cura dell'Ufficio Privacy dell'Azienda, nel Registro dei "*Data Breach*" (cfr. All. 3) come "falso positivo". Tale azione risulta necessaria per comprovare l'adozione del principio di accountability.

Ove il *data breach* interessi attività svolte dall'Azienda in qualità di Responsabile Esterno del Trattamento, l'Azienda comunica l'evento al Titolare del trattamento, senza ulteriore ritardo.

Redatto apposito verbale, e compilata la Scheda Evento (All. 2.2), la notizia è segnalata dall'Ufficio Privacy al Gruppo di Secondo Livello (di seguito GSL), che viene convocato dallo stesso Ufficio Privacy e messo in contatto tramite i diversi mezzi di comunicazione disponibili (telefono, e-mail, piattaforme digitali, etc.).

3. ANALISI DI SECONDO LIVELLO (GSL) - SCHEDA RISCHIO

Il **GSL** è costituito dalle seguenti professionalità:

- Ufficio Privacy;
- RPD/DPO;
- Funzionario con competenze legali, comunque incardinato nei ruoli dell'Azienda;
- Responsabile dell'Ufficio in cui si è materializzato il *data breach* e altri soggetti interni eventualmente coinvolti;
- Componente del Gruppo di lavoro privacy della relativa struttura;
- Amministratore di sistema, ove nominato, o funzioni dei sistemi informativi, nel caso in cui il *data breach* interessi l'infrastruttura, sistemi informativi e banche dati gestite dall'Azienda;
- Referente individuato del soggetto esterno (Responsabile del trattamento) che, in forza di un contratto, convenzione o altro atto giuridico, ha fornito il bene e/o il servizio da cui è scaturito il *data breach;*
- DPO/RPD del Responsabile del trattamento.

Questa fase è tesa a favorire l'attività investigativa e a individuare i possibili rischi per i diritti e le libertà delle persone fisiche.
Le informazioni di dettaglio sull'evento necessarie alle analisi di secondo livello vengono acquisite dalla Scheda Evento (all. 2.2) ed analizzate al fine di redigere una Scheda Rischio (All. 2.3), per le conseguenti valutazioni.

Il rischio deldata breach deve essere valutato con riferimento alla gravità (G) delle sue (possibili) conseguenze a danno di persone fisiche, anche diverse dall'interessato a cui si riferiscono i dati, e alla probabilità (P) che esse si verifichino.
Esempi di talune conseguenze dannose sono:

- discriminazioni
- furto o usurpazione d'identità
- perdite finanziarie
- pregiudizio alla 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
- impedito controllo sui dati personali all'interessato
- danni fisici, materiali o immateriali alle persone fisiche.

Il **GSL**, dunque, raccolte le evidenze:
1. definisce le possibili conseguenze ("Impatti") del *data breach* per i diritti e le libertà delle persone fisiche;
2. valuta il livello di rischio del data breach in termini di Gravità e Probabilità dell'evento, analizzata la natura della violazione dei dati personali e, ove possibile, le categorie dei dati e il loro volume, il numero (anche solo approssimativo) e le categorie degli interessati coinvolti (come prescrive il Gruppo di lavoro dei Garanti europei nelle "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679");
3. implementa le misure da adottare nell'immediato in risposta all'emergenza, con il primario scopo di contenere gli effetti negativi.

Per la definizione della **gravità** (G) degli impatti sui diritti e le libertà degli interessati si fa riferimento ai livelli di rischio individuati dal manuale sulla sicurezza nel trattamento dei dati personali (rev. 12/2017) "ENISA" riportati nella seguente tabella:

LIVELLO DI IMPATTO	DESCRIZIONE
Basso	Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).
Medio	Gli individui possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.).
Alto	Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
Molto alto	Gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).

Per la definizione della **probabilità** (P) che si realizzino tali conseguenze dannose sui diritti e le libertà degli interessati si fa riferimento ai livelli di rischio individuati dal manuale sulla sicurezza nel trattamento dei dati personali (rev. 12/2017) "ENISA":

- Basso: l'evento temuto non dovrebbe manifestarsi
- Medio: l'evento temuto potrebbe manifestarsi
- Alto: l'evento temuto si manifesterà quasi certamente o si è già manifestato

In conclusione, il livello di rischio del data breach sarà la risultante dell'incrocio tra il livello della gravità del rischio (G) e il livello della probabilità del rischio (P), da determinarsi mediante la seguente tabella ENISA:

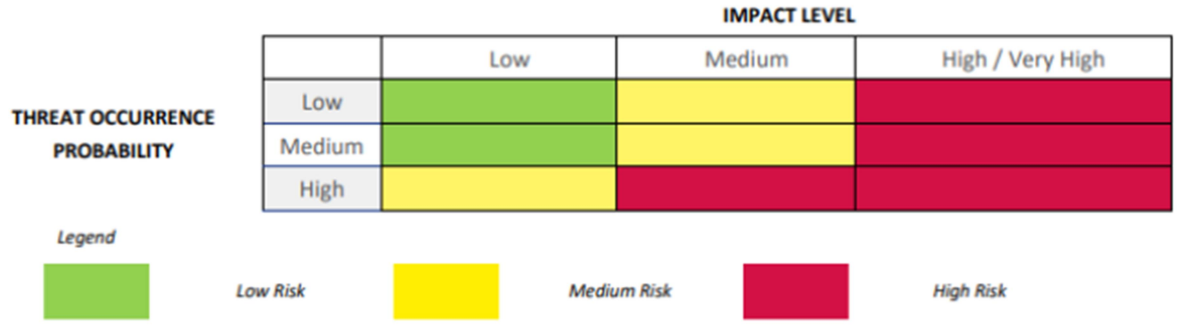


Tabella 6: Valutazione del rischio

Raccolte le evidenze nella Scheda Rischio (All. 2.3), questi i possibili scenari (riportare lo scenario prescelto nella riga "Esito" della Scheda Rischio):

1. Nel caso in cui si ritenga che anche in forza dell'adozione delle misure di sicurezza correttive adottate la probabilità che la violazione conduca ad un rischio per i diritti e le libertà degli Interessati, classificato come Basso, il **GSL** terrà evidenza, mediante stesura della Scheda Rischio (All. 2.3), degli esiti dell'analisi condotta, allegando il parere fornito e formalizzato dal DPO/RPD.
Successivamente, l'Ufficio Privacy cura l'aggiornamento del Registro dei *Data breach (All. 3)*. Copia del verbale deve essere inviata al DPO/RPD.

2. Ove si evidenzi il caso che la violazione possa condurre ad un rischio per i diritti e le libertà degli interessati, l'Ufficio Privacy, senza ulteriore ritardo, si mobilita per:

- circostanziare ed attribuire responsabilità, nonché tempistiche per l'adozione delle misure correttive individuate da **GSL**, altresì nei confronti dei Responsabili, ex art. 28 Reg. UE 2016/679, coinvolti. In tal caso è opportuno recuperare gli estremi della nomina a Responsabile del

trattamento, ex art. 28 Reg. UE 2016/679, utile a comprovare l'adozione di misure tecniche ed organizzative a cura dell'Azienda;

- verbalizzare gli esiti dell'analisi nella Scheda Rischio (All. 2.3), riportando, in essa, il parere fornito e formalizzato dal DPO/RPD;
- compilare il Modello per la notificazione al Garante, indicando esplicitamente se le azioni correttive previste sono già concluse o in corso;
- avvertire il Direttore Generale, che provvede, ove necessario, affinché siano tempestivamente adottate misure che consentano di minimizzare le conseguenze negative della v. A tal proposito si veda il successivo punto C.1.

3. Nel caso si desuma che la violazione possa comportare un rischio elevato per i diritti e le libertà degli interessati, l'Ufficio Privacy, verificato che il verbale del **GSL** evidenzi l'urgenza di comunicare il *data breach* agli interessati, provvede a comporre il modello di comunicazione agli interessati (All. 1), con l'ausilio del DPO/RPD. A tal proposito si veda il successivo punto C.2.

In tutti i casi, il **GSL** deve compilare la Scheda Rischio (All. 2.3).

C. FASE 3: NOTIFICA E COMUNICAZIONE

1. NOTIFICA ALLA AUTORITÀ DI CONTROLLO

Redatta la Scheda Rischio, il **GSL** deve, verificando e validando la documentazione pervenuta dalle precedenti fasi di lavoro, valutare le azioni da intraprendere come, ad esempio, avviare la notificazione verso l'Autorità di Controllo e, ove necessario, la comunicazione agli Interessati (nonché la denuncia alle Autorità competenti quali Polizia Postale e Procura della Repubblica competenti per territorio ai sensi degli articoli 331 e 361 c.p.p.).

L'Azienda, quale Titolare del trattamento, **deve notificare l'accaduto all'Autorità Garante a mezzo di compilazione on line al link** https://servizi.gpdp.it/databreach/s/ (**o altre modalità intervenute, successivamente, in base agli indirizzi, *ratione materiae*, diramati dall'EDPB e dall'Autorità di controllo, per le quali, sin d'ora, si rimanda**) **entro 72 ore** dall'avvenuta conoscenza, **a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche**.

Ove la notifica avvenga oltre il limite delle 72 ore, in caso di *data breach* particolarmente articolato o in presenza di molteplici attacchi, è necessario dare conto delle motivazioni che hanno comportato il ritardo.

La notifica all'Autorità di Controllo, curata dall'Ufficio Privacy, deve:

a) descrivere, ove possibile:

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

b) comunicare il nome e i Dati di contatto del DPO/RPD o di altro punto di contatto presso cui ottenere più informazioni;

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

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

Tali informazioni sono desumibili dagli allegati 2.1 e 2.2 e sopratutto dalla Scheda Rischio elaborata dal **GSL** (All. 2.3).

È bene precisare che qualora non si disponga di tutte le informazioni, è possibile inviare una prima notifica parziale (c.d. notifica per fasi), da completare non appena disponibili le ulteriori informazioni.

Se dopo la notifica iniziale, una successiva indagine dimostra che l'incidente di sicurezza è stato contenuto e che non si è verificata alcuna violazione dei dati personali, l'Azienda può chiedere all'Autorità Garante la rettifica e la cancellazione della notifica eseguita e l'incidente sarà registrato, dal DPO/RPD, come un evento rubricato come "falso positivo" nel Registro dei *Data breach* (All. 3).

2. COMUNICAZIONE DELLA VIOLAZIONE ALL'INTERESSATO

Nei casi in cui l'Ufficio Privacy, verificato che il verbale ricevuto del **GSL**, in presenza di un rischio elevato (ALTO o MOLTO ALTO) per i diritti e le libertà delle persone fisiche, evidenzi l'urgenza di comunicare il *data breach* agli interessati "senza ingiustificato ritardo, a norma dell'art. 34, GDPR:

1. provvede a comporre il modello di comunicazione agli interessati (All. 1), secondo un linguaggio chiaro e semplice, con le seguenti caratteristiche:
   a) data e ora della violazione, anche solo presunta, e data e ora in cui si è avuto conoscenza della stessa;
   b) natura della violazione dei dati personali;
   c) probabili conseguenze della violazione dei dati personali;
   d) misure adottate o di cui si propone l'adozione per limitare la violazione e anche, se del caso, per attenuarne i possibili effetti negativi;
   e) nome e dati di contatto del DPO/RPD.
2. in accordo con il DPO/RPD, definisce le modalità di comunicazione agli interessati:
   - trasmissione della comunicazione a ciascun interessato, nel caso in cui l'Azienda disponga dei dati di contatto e tale azione possa essere compiuta senza sforzi sproporzionati (indirizzo di posta elettronica ordinaria o certificata);
   - comunicazione pubblica (pubblicazione della notizia relativa all'evento sul sito istituzionale, comunicati stampa, ecc.), nel caso in cui non sia possibile identificare con precisione i singoli interessati coinvolti.
3. Sottopone al Direttore Generale, per l'approvazione, il testo relativo alla comunicazione e, individua, in accordo con DPO/RPD, le idonee modalità di trasmissione del testo.

N.B.: Deve essere valutata l'opportunità o meno di comunicazione all'Interessato se è soddisfatta una delle seguenti condizioni:

a. sono state messe in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare, quelle destinate a rendere i dati 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;

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

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

D. FASE 4: REGISTRAZIONE SEGNALAZIONE NEL REGISTRO DEI "*DATA BREACH*"

Nel Registro dei *Data Breach* (cfr. Allegato 3 alla presente procedura), l'Ufficio Privacy documenta ogni singolo evento, compresi i falsi positivi, compilandone tutti i campi, con il coinvolgimento e il supporto del DPO/RPD.

Tale documentazione consente all'Autorità di Controllo di verificare il rispetto delle norme in materia di notificazione delle Violazioni di dati personali.

Il Registro dei *Data Breach,* così come tutta la documentazione relativa alla violazione verificatasi (Schede Evento e Scheda Rischio) sono tenuti a cura dell'Ufficio Privacy, o da un soggetto da lui autorizzato, sotto il controllo del DPO/RPD.

E. FASE 5: ANALISI POST VIOLAZIONE

L'ultima fase del processo di gestione delle Violazioni di dati personali prevede la raccolta finale delle evidenze, l'analisi delle informazioni giunte sul contesto di violazione osservato, e la valutazione delle stesse al fine di effettuare un'analisi post-incidente, per verificare l'efficacia e l'efficienza delle azioni intraprese durante la gestione dell'evento ed identificare possibili aree di miglioramento.

Tale attività prevede il coinvolgimento, laddove necessario, dell'Amministratore di Sistema, ove nominato, e funzioni dei Sistemi informativi dell'Azienda, con eventuale supporto da parte di altre aree funzionali.

V. DESCRIZIONE PROCESSO: "*DATA BREACH*" PRESSO L'AZIENDA O PRESSO UN TERZO IN QUALITÀ DI RESPONSABILE ESTERNO

A. OBBLIGHI DI COMUNICAZIONE DELL'AZIENDA QUANDO OPERA IN QUALITÀ DI RESPONSABILE ESTERNO

Quando l'Azienda agisce in qualità Responsabile esterno, in caso di violazione dei dati personali, essa è tenuta a informare il Titolare (solitamente il soggetto per il quale tratta i dati e/o è tenuto a trattarli), senza ingiustificato ritardo secondo i tempi e i modi concordati nel contratto per il Trattamento dei dati personali trasmesso da quest'ultimo.

B. OBBLIGHI DI COMUNICAZIONE DI UN RESPONSABILE ESTERNO NEI CONFRONTI DELL'AZIENDA

Nel caso in cui vi sia la presenza di un soggetto che agisca in qualità di Responsabile esterno del Trattamento, al verificarsi di una violazione dei dati personali, questi deve informare l'Azienda, senza ingiustificato ritardo e non oltre le 24 ore (o altro termine indicato nella nomina a Responsabile del trattamento ex art. 28, GDPR, comunque non superiore alle 48 ore) dal momento in cui ha conoscenza della violazione, inviando una comunicazione agli indirizzi PEC dell'Ufficio Protocollo e del DPO/RPD dell'Azienda, nonché contattando telefonicamente l'Ufficio medesimo e, successivamente, collaborare con l'Azienda per consentire allo stesso di adempiere agli obblighi previsti dalla normativa agli artt. 33 e 34 del GDPR.

Il Responsabile deve assistere l'Azienda avviando un'analisi preliminare finalizzata alla raccolta dei Dati concernenti l'anomalia e compilando tutti i campi della Scheda Raccolta Informazioni (All. 2.1) allegata alla presente procedura.

Una volta condotta l'analisi preliminare, il Responsabile deve condurre una prima analisi per verificare che la segnalazione non rappresenti un "falso positivo".

All'esito dell'accertamento, qualora si tratti di un "falso positivo", il Responsabile deve comunicarlo immediatamente all'Azienda allo stesso indirizzo di cui sopra, al fine di consentire l'inserimento dell'evento nel Registro dei *Data Breach* dell'Azienda.

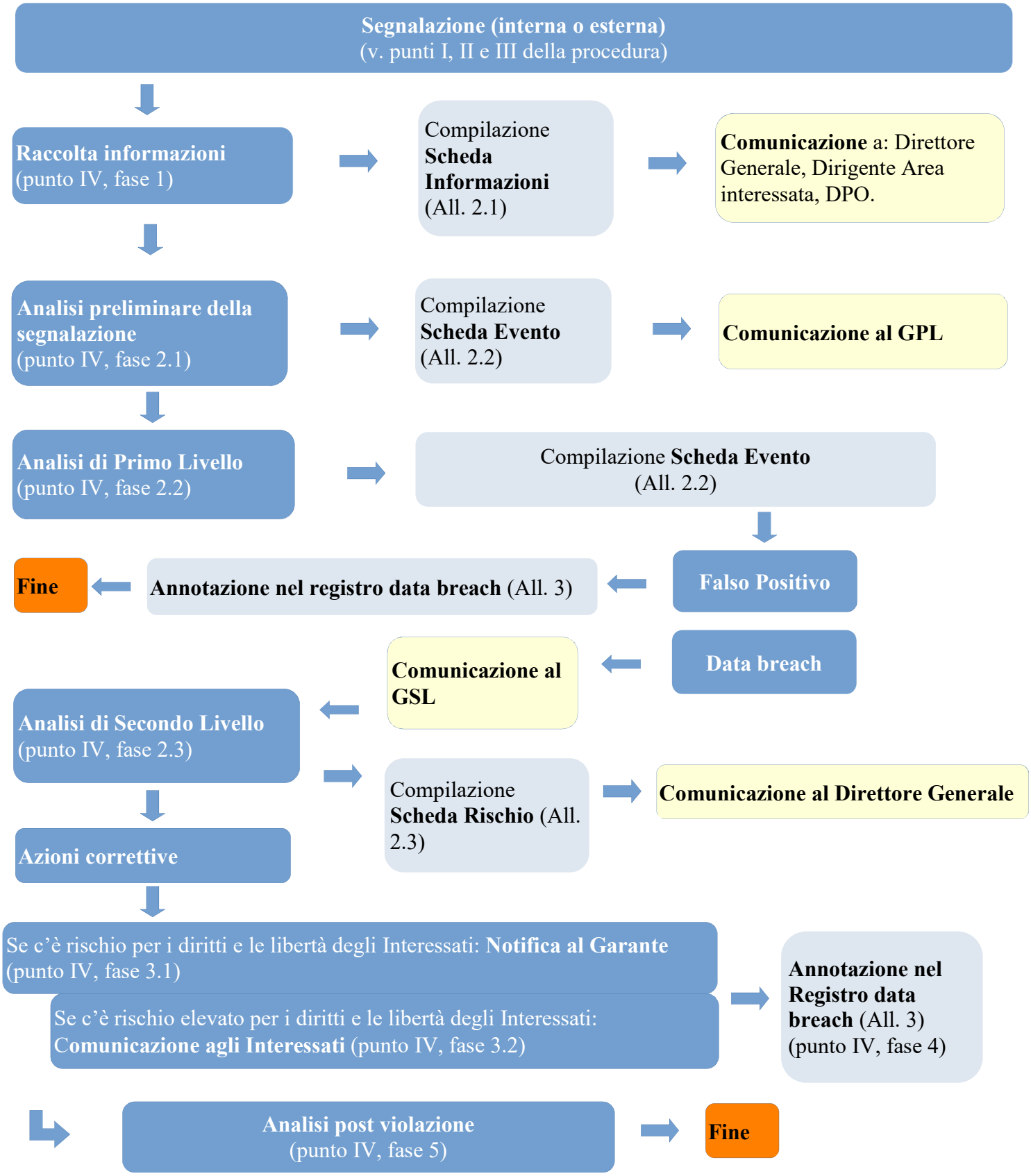
In caso contrario, e dunque se l'evento non è un "falso positivo", il Responsabile recupera le informazioni di dettaglio sull'evento, necessarie alle successive analisi, e le comunica, mediante la Scheda "Raccolta di informazioni" (All. 2.1), non oltre 24 ore (o altro termine indicato nella nomina a Responsabile del trattamento ex art. 28, GDPR, comunque non superiore alle 48 ore) dal momento in cui ha conoscenza della violazione, agli indirizzi PEC dell'Ufficio Protocollo e del DPO/RPD dell'Azienda, che devono essere costantemente tenuti aggiornati.

L'Azienda, una volta ricevuta la documentazione, procede secondo le prescrizioni di cui al paragrafo IV della presente procedura.

VI. ALLEGATI

- Allegato 1: MODELLO DI "COMUNICAZIONE ALL'INTERESSATO DELLA VIOLAZIONE DEI DATI PERSONALI";
- Allegato 2.1: MODELLO DI "SCHEDA RACCOLTA INFORMAZIONI" UTILE PER LA SUCCESSIVA COMPILAZIONE DELLA NOTIFICA AL GARANTE PROTEZIONE DATI PERSONALI, MEDIANTE LA PROCEDURA ON LINE. IL MODELLO PUÒ ESSERE ANCHE INVIATO, COME ALLEGATO, ALL'ATTO DI NOMINA AL RESPONSABILE DEL TRATTAMENTO;
  Allegato 2.2: MODELLO DI "SCHEDA EVENTO";
  Allegato 2.3: MODELLO DI "SCHEDA RISCHIO";
- Allegato 3: immagine del MODELLO DI "REGISTRO DEI *DATA BREACH*".

Grafica della procedura step by step



Allegato 1

MODELLO DI COMUNICAZIONE ALL'INTERESSATO DELLA VIOLAZIONE DEI DATI PERSONALI

Nota: Il seguente modello illustra le modalità di comunicazione di una violazione*. Rispetto ai diversi campi indicati dovrà essere scelta l'opzione che si può riferire allo specifico caso, in base agli esempi riportati.*

Secondo quanto prescritto dall'art. 34 del Regolamento Generale in materia di protezione dei dati personali RE (UE) n. 679/2016, l'Azienda Sanitaria Locale ASL TO 4, Titolare del Trattamento, con la presente è a comunicarLe, l'intervenuta violazione *dei Suoi* dati personali *(Data breach)*

- *che si è verificata:*

A. in data _____, alle ore_____;
B. tra il _____e il_____;
C. in un tempo non ancora determinato;
D. è possibile che sia ancora in corso.

- *di cui si è avuto conoscenza in data _____alle ore_____.*

A) Descrizione della natura della violazione:

_____
_____
_____
_____
_____
_____

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

_____
_____
_____
_____
_____
_____

b) Tipo di violazione, per esempio:
   - ☐ lettura (presumibilmente i Dati non sono stati copiati)
   - ☐ copia (i Dati sono ancora presenti sui sistemi del Titolare)
   - ☐ alterazione (i Dati sono presenti sui sistemi ma sono stati alterati)
   - ☐ cancellazione (i Dati non sono più sui sistemi del Titolare e non li ha neppure l'autore della violazione)
   - ☐ furto (i Dati non sono più sui sistemi del Titolare e li ha l'autore della violazione)
   - ☐ altro _____

c) Dispositivo oggetto di violazione, per esempio:
   - ☐ computer
   - ☐ rete
   - ☐ dispositivo mobile
   - ☐ strumento di backup
   - ☐ documento cartaceo
   - ☐ altro _____

d) Descrizione dei sistemi di elaborazione o di memorizzazione dei Dati coinvolti, con indicazione della loro ubicazione:

_____
_____
_____
_____
_____
_____

e) Che tipo di Dati sono oggetto di violazione, per esempio:

- ☐ Dati anagrafici (nome, cognome, numero di telefono, e mail, CF, indirizzo ecc..)
- ☐ Dati di accesso e di identificazione (username, password, customer ID, altro)
- ☐ Dati personali idonei a rivelare l'origine razziale ed etnica
- ☐ Dati personali idonei a rivelare le convinzioni religiose
- ☐ Dati personali idonei a rivelare filosofiche o di altro genere
- ☐ Dati personali idonei a rivelare le opinioni politiche
- ☐ Dati personali idonei a rivelare l'adesione a partiti
- ☐ Dati personali idonei a rivelare sindacati,
- ☐ Dati personali idonei a rivelare associazioni od organizzazioni a carattere religioso
- ☐ Dati personali idonei a rivelare associazioni od organizzazioni a carattere filosofico
- ☐ Dati personali idonei a rivelare associazioni od organizzazioni a carattere politico
- ☐ Dati personali idonei a rivelare associazioni od organizzazioni a carattere sindacale
- ☐ Dati personali idonei a rivelare lo stato di salute
- ☐ Dati personali idonei a rivelare la vita sessuale
- ☐ Dati giudiziari
- ☐ Dati genetici
- ☐ Dati biometrici
- ☐ Copia per immagine su supporto informatico di documenti analogici
- ☐ Ancora sconosciuto
- ☐ Altro _____

B) Descrivere le probabili conseguenze della violazione dei dati personali;

_____
_____
_____
_____
_____
_____

C) Descrivere quali sono le misure tecnologiche ed organizzative assunte per porre rimedio alla violazione e, se del caso, per contenere la violazione dei dati o per attenuarne i possibili effetti negativi;

_____
_____
_____
_____
_____
_____

Per poter ottenere maggiori informazioni relativamente alla violazione in oggetto, può contattare l'Ufficio Privacy dell'Azienda e/o il DPO/RPD *ai seguenti indirizzi*:

Dati di contatto Azienda:
indirizzo di posta elettronica: _____
indirizzo di posta PEC: _____
indirizzo posta cartacea: _____
numero telefonico dedicato: _____
numero di fax dedicato: _____
Dati di contatto DPO:
indirizzo di posta elettronica: _____
indirizzo di posta PEC: _____
indirizzo posta cartacea: _____
numero telefonico dedicato: _____
numero di fax dedicato: _____

Data, Luogo _____

Il Titolare del Trattamento

_____

[*Ufficio Privacy****]***

_____

Distinti saluti

Allegato 2.1

MODELLO DI "SCHEDA RACCOLTA INFORMAZIONI"

Data	
Nome e cognome del segnalante	
Struttura di afferenza, funzione e dati di contatto del segnalante (tel., e-mail ecc.)	
Ulteriori soggetti coinvolti nel trattamento	
Informazioni sulla violazione	
1. Momento in cui è avvenuta la violazione	☐ Il _____ ☐ Dal _____ (la violazione è ancora in corso) ☐ Dal _____ al _____ ☐ In un tempo non ancora determinato
2. Modalità con la quale il Titolare del trattamento è venuto a conoscenza della violazione	
3. Momento nel quale il Titolare del trattamento è venuto a conoscenza della violazione (e motivi del ritardo, se la segnalazione è inviata dopo il termine previsto nella "Nomina a Responsabile del trattamento")	
4. Tipo di violazione	☐ Ransomware
	☐ Lettura (presumibilmente i dati non sono stati copiati)
	☐ Copia (i dati sono ancora presenti sui sistemi del titolare)
	☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
	☐ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
	☐ Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)

	☐ Altro:_____ (*DESCRIVERE*)
5. Natura della violazione dal punto di vista del RID	☐ Perdita di riservatezza del dato personale (R) ☐ Perdita di integrità del dato personale (I) ☐ Perdita di disponibilità del dato personale (D)
6. Causa della violazione	☐ Azione intenzionale interna ☐ Azione accidentale interna ☐ Azione intenzionale esterna ☐ Azione accidentale esterna ☐ Sconosciuta
7. Descrizione dei sistemi, software, servizi e delle infrastrutture IT coinvolti nella violazione, con indicazione della loro ubicazione	
8. Misure tecniche e organizzative, in essere al momento della violazione, adottate per garantire la sicurezza dei dati personali coinvolti	
9. Categorie di interessati coinvolti nella violazione	☐ Dipendenti/Consulenti ☐ Utenti/Contraenti/Abbonati/Clienti (attuali o potenziali) ☐ Associati, soci, aderenti, simpatizzanti, sostenitori ☐ Soggetti che ricoprono cariche sociali ☐ Beneficiari o assistiti ☐ Pazienti ☐ Minori ☐ Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo) ☐Altro _____
10. Numero (anche approssimativo) di interessati coinvolti nella violazione.	☐ N. ___ interessati ☐ Circa n. ____ interessati ☐ Non determinabile ☐ Non ancora determinato
11. Categorie di dati personali oggetto di violazione	☐ Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale) ☐Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile) ☐ Dati di accesso e di identificazione (username, password, customer ID, altro…) ☐Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…) ☐Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro…)

	☐Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza ☐ Dati di profilazione ☐Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…) ☐ Dati di localizzazione ☐ Dati che rivelino l'origine razziale o etnici ☐ Dati relativi a opinioni politiche ☐ Dati relativi a convinzioni religiose o filosofiche ☐ Dati che rivelino l'appartenenza sindacale ☐ Dati relativi alla vita sessuale o all'orientamento sessuale ☐ Dati relativi alla salute ☐ Dati genetici ☐ Dati biometrici ☐ Altro _____ ☐ Categorie ancora non determinate
12. Numero (anche approssimativo) di registrazioni dei dati personali oggetto di violazione	☐ N.0 ☐ Circa N. ☐ Non determinabile ☐ Non ancora determinato
13. Descrizione di dettaglio delle categorie di dati personali oggetto della violazione per ciascuna categoria di interessati	
Probabili conseguenze della violazione	
1. Probabili conseguenze della violazione per gli interessati	**In caso di perdita di riservatezza:** ☐ I dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento ☐ I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati ☐ I dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito ☐ Altro _____ ☐ In corso di valutazione **In caso di perdita di integrità:** ☐ I dati sono stati modificati e resi inconsistenti ☐ I dati sono stati modificati mantenendo la consistenza ☐ Altro _____ ☐ In corso di valutazione **In caso di perdita di disponibilità:** ☐ Mancato accesso a servizi ☐ Malfunzionamento e difficoltà nell'utilizzo di servizi ☐ Altro _____ ☐ In corso di valutazione

	Eventuali ulteriori considerazioni sulle conseguenze della violazione: _____
2. Potenziale impatto per gli interessati	☐ Perdita del controllo dei dati personali ☐ Limitazione dei diritti ☐ Discriminazione ☐ Furto o usurpazione d'identità ☐ Frodi ☐ Perdite finanziarie ☐ Decifratura non autorizzata della pseudonimizzazione ☐ Pregiudizio alla reputazione ☐Perdita di riservatezza dei dati personali protetti da segreto professionale ☐ Conoscenza da parte di terzi non autorizzati ☐ Qualsiasi altro danno economico o sociale significativo _____ ☐ Non ancora definito
3. Gravità del potenziale impatto per gli interessati	☐ Trascurabile ☐ Bassa ☐ Media ☐ Alta ☐ Non ancora definita _____
Misure adottate a seguito della violazione	
1. Misure tecniche e organizzative adottate (o di cui si propone l'adozione) per porre rimedio alla violazione e ridurne gli effetti negativi per gli interessati	
2. Misure tecniche e organizzative adottate (o di cui si propone l'adozione) per prevenire simili violazioni future	

Allegato 2.2

MODELLO DI "SCHEDA EVENTO"

SCHEDA EVENTO					
EVENTO				**PROVVEDIMENTI**	
DATA EVENTO		**DATA E ORA DI CONOSCENZA**		**NOTIFICA AL GARANTE (X)**	
ORA EVENTO		**SEGNALANTE**		SI	NO
LUOGO DELLA VIOLAZIONE		**NATURA EVENTO**		(inserire data di notifica)	(motivare mancata notifica)
ENTE/SOCIETA' COINVOLTO/A		**N. INTERESSATI COINVOLTI**			
CATEGORIE DI DATI INTERESSATI		**CATEGORIE DI INTERESSATI COINVOLTI**		**(eventuale) COMUNICAZIONE ALL'INTERESSATO**	
				SI	NO
				(inserire data di comunicazione	(motivare mancata comunicazione)
				INTERVENTI DI RIPRISTINO (RECOVERY)	
CONSEGUENZE VIOLAZIONE		**SISTEMI E DISPOSITIVI COINVOLTI**			
				TEMPO DI RIPRISTINO (RECOVERY)	
DESCRIZIONE ANALITICA DELL'EVENTO				**ULTERIORI AZIONI DA INTRAPRENDERE**	
CODICE EVENTO					
DATA DI COMPILAZIONE		FIRMA			
LUOGO DI COMPILAZIONE					
DATA ULTIMA MODIFICA					

Allegato 2.3

MODELLO DI "SCHEDA RISCHIO"

SCHEDA RISCHIO	
Data Segnalazione	
Soggetto segnalante	
Evento rilevato dal GPL	
Data convocazione del GSL	
Categorie di interessati	
Possibili conseguenze per i diritti e le libertà delle persone fisiche (Impatto)	
Valutazione del livello di rischio ENISA (Gravità * Probabilità)	
Valutazione dell'adeguatezza delle misure di sicurezza già implementate dal Titolare per far fronte alla violazione ed evitare impatti sugli interessati	
Azioni correttive da adottare per contenere gli effetti negativi	
Parere del RPD/DPO	
Esito della valutazione (indicare uno degli scenari previsti nel punto 3 della procedura)	
Data	

Allegato 3

MODELLO DI REGISTRO *DATA BREACH*

Si veda il file di calcolo annesso alla presente procedura (qui riprodotto soltanto come immagine)

N. EVENTO	DETTAGLI DELLA VIOLAZIONE					CONSEGUENZE DELLA VIOLAZIONE		AZIONI CORRETTIVE		NOTIFICHE / COMUNICAZIONI		
	Data evento e data conoscenza	Ufficio coinvolto	Natura dell'evento e breve descrizione della violazione	Tipologie di dati interessati	Categorie interessati coinvolti	Effetti accertati	Effetti ipotizzabili / possibili	Azioni correttive implementate	Azioni correttive da intraprendere	Notifica Garante	Comunicazione interessati	Doc. / allegati e/o email