ALLEGATO A

PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI (DATA BREACH)

ai sensi del Regolamento (UE) 2016/679 (GDPR)

Approvata con Determina del Direttore Generale di ERDIS Marche n. 22 del 27/05/2024

Cronologia delle versioni

Versione n.	Data	Descrizione	Atto/provvedimento di approvazione
1.0	../../….	Prima redazione	Determina del Direttore Generale di ERDIS Marche n. .. del ../../….

Sommario

1. Scopo, ambito d'applicazione e destinatari

Il presente documento disciplina la procedura di gestione delle violazioni di dati personali (c.d. *data breach*) nell'Ente Regionale per il Diritto allo Studio delle Marche (in seguito ERDIS) definendone i principi generali e individuandone i ruoli, le responsabilità e le attività da effettuare qualora si verifichi un incidente di sicurezza che comporti la violazione di dati personali.

Secondo quanto previsto dall'art. 4 («Definizioni») del Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (di seguito GDPR), per violazione dei dati personali si intende «la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati». In tale contesto, il GDPR sancisce l'obbligo per il Titolare del trattamento di notificare tempestivamente l'avvenuta violazione dei dati personali all'autorità di controllo e, in casi determinati e con specifiche modalità, di procedere alla comunicazione direttamente agli interessati.

La procedura ivi descritta si applica a tutte le violazioni di dati personali riscontrate all'interno di ERDIS e si rivolge a tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del Titolare del trattamento, quali:

- il personale dipendente, nonché coloro che, a prescindere dall'inquadramento contrattuale in essere, abbiano accesso ai dati personali per garantire l'esecuzione delle prestazioni richieste;
- qualsiasi soggetto (persona fisica o persona giuridica) che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento abbia accesso ai suddetti dati e agisca in qualità di Responsabile esterno del trattamento, di Titolare autonomo o di Contitolare[1].

Il rispetto della presente procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste dalla stessa potrà comportare provvedimenti disciplinari a carico del personale dipendente inadempiente.

[1] L'accordo di contitolarità può individuare specifiche ed ulteriori procedure e/o modalità di gestione dei data breach, determinando anche la responsabilità per l'adempimento agli obblighi di cui all'art. 33 del GDPR e, in particolare, di notifica delle violazioni emerse.

2. Acronimi e definizioni

Autorità di controllo	Art. 4: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 (in Italia, il Garante per la protezione dei dati personali).
Dato personale	Art. 4 GDPR: qualsiasi informazione riguardante una persona fisica identificata o identificabile («Interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
DPO/RPD	Data Protection Officer/Responsabile della Protezione dei Dati: soggetto designato dal Titolare o dal Responsabile del trattamento per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del GDPR (art. 37).
Garante	Il Garante per la protezione dei dati personali è un'autorità amministrativa indipendente istituita dalla legge sulla privacy (n. 675/1996), poi disciplinata dal Codice in materia di protezione dei dati personali (d. lgs. n. 196/2003), come modificato dal d. lgs. n. 101/2018 che ha confermato che il Garante è l'autorità di controllo designata anche ai fini dell'attuazione del GDPR (art. 51).
GDPR	General Data Protection Regulation - Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.
Interessato	La persona fisica a cui si riferiscono i dati personali.
Responsabile (esterno) del trattamento	Art. 4 GDPR: persona fisica o giuridica, autorità pubblica, servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento.
Autorizzati (designati) al trattamento	Persone fisiche espressamente autorizzate a compiere operazioni di trattamento dall'organizzazione e che agiscono sotto la diretta autorità di questa ultima, che sono state appositamente designate e istruite dal Titolare ai sensi degli artt. 29 del GDPR e 2-quaterdecies del d. lgs. 196/2003, come modificato e adeguato al GDPR dal d. lgs. 101/2018.
Team di Risposta alle Violazioni	Gruppo multidisciplinare composto da soggetti in grado di identificare una violazione di dati personali e gestirla dal punto di vista organizzativo, tecnico e legale
Titolare del trattamento	Art. 4 GDPR: 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.

Trattamento	Art. 4 GDPR: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
Violazione di dati personali o *data breach*	Art. 4 GDPR: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

3. Riferimenti normativi

- GDPR, artt. 33 e 34;
- Gruppo art. 29 (ora Comitato europeo per la Protezione dei Dati – EDPB European Data Protection Board), WP250rev01 (2018), Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679;
- ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches, Working Document, v1.0, December 2013;
- EDPB, Linee guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali;
- EDPB, Guidelines 9/2022 on personal data breach notification under GDPR;
- Provvedimento del Garante 30 luglio 2019, n. 157, sulla notifica delle violazioni dei dati personali (data breach);
- Per approfondire: https://www.garanteprivacy.it/data-breach

4. Team di Risposta alle Violazioni

Il Team di Risposta alle Violazioni (di seguito Team) è un'entità multidisciplinare composta da soggetti che presentano conoscenze e competenze tali da assumersi la responsabilità per identificare una violazione di dati, valutare e porre in essere le misure di contenimento delle conseguenze negative della violazione stessa. Esso gestisce le violazioni dal punto di vista organizzativo, tecnico e legale, e comunica in modo efficace e tempestivo ogni eventuale incidente che possa configurare un data breach.

Il Team deve garantire la prontezza necessaria per una risposta alla violazione dei dati personali, insieme alle risorse e alla preparazione necessarie (come elenchi di persone da chiamare, sostituzione di ruoli chiave, simulazioni, oltre alla revisione richiesta delle politiche, delle procedure e delle pratiche dell'Ente).

Il Team si confronterà per ogni violazione dei dati personali segnalata (anche presunta) e sarà coordinato dal Direttore Generale, delegato pro-tempore dal Titolare del trattamento a compiti e funzioni gestionali, che può scegliere di inserire personale aggiuntivo al gruppo allo scopo di gestire una specifica violazione di dati personali.

È responsabilità del Team stabilire se un incidente di sicurezza debba essere considerato una violazione di dati personali.

Se richiesto, i componenti del gruppo possono anche coinvolgere parti esterne (ad esempio, un fornitore di sicurezza informatica per svolgere attività di informatica forense o un'agenzia di comunicazione esterna per assistere l'Ente in necessità di comunicazione di crisi).
In caso di necessità il Team può avvalersi della collaborazione dei Responsabili EQ dei servizi/uffici coinvolti nell'incidente o il cui coinvolgimento è utile all'analisi, identificazione e gestione dell'incidente stesso. Ove la violazione sia avvenuta su sistemi informatici gestiti da terzi soggetti appositamente nominati ai sensi dell'art. 28 del GDPR, il Team dovrà coinvolgere tali soggetti nella misura prevista dall'atto di nomina a responsabile esterno stipulato con tali fornitori.

Il gruppo esecutivo è composto dai seguenti soggetti o loro delegati:

TEAM DI RISPOSTA ALLE VIOLAZIONI		
Soggetto	***Competenza***	***Ruolo***
Direttore Generale	Delegato pro-tempore dal Titolare del trattamento a compiti e funzioni gestionali	Coordinatore Team
DPO	Funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del GDPR	Componente di base
Responsabile della sicurezza informatica	Conoscenza della gestione tecnico-amministrativa dell'infrastruttura informatica	Componente di base
Referente informatico specialista	Conoscenza dell'infrastruttura di rete, delle misure di sicurezza idonee adottate e delle infrastrutture tecnico-applicative impiegate per il trattamento dei dati	Componente di base
Responsabile EQ Anticorruzione e Trasparenza	Conoscenza della normativa sulla privacy	Componente di base
Responsabile della gestione documentale informatica e Responsabile della conservazione dei documenti informatici	Conoscenze tecnico-archivistiche e conoscenze giuridiche e informatiche in materia di documenti informatici, archivi, conservazione	Componente di base
Responsabile EQ Affari Legali	Conoscenza degli aspetti legali inerenti alla violazione di dati personali	Componente di base
Coordinatore Gruppo di lavoro a supporto del DPO	Ufficio che supporta il DPO nell'adempimento di quanto previsto dall'art. 39 Regolamento UE 2016/679	Componente di base

Una volta che una violazione di dati personali viene portata a conoscenza del Team, questo dovrà:

- Validare/rispondere alla violazione dei dati personali;
- predisporre un'appropriata e imparziale investigazione, documentandola correttamente;
- identificare gli eventuali asset da bonificare e tenere traccia delle misure da porre in essere per risolvere le vulnerabilità;
- coordinarsi con le autorità competenti, se necessario;
- coordinare le comunicazioni interne ed esterne;
- assicurarsi che gli eventuali obblighi di notifica e comunicazione siano rispettati;
- tenere ed aggiornare il Registro delle violazioni.

Il Coordinatore del Team è incaricato della documentazione di tutte le decisioni del gruppo ed è coadiuvato dai componenti del Team nella verbalizzazione degli incontri. Poiché questi documenti potrebbero essere esaminati dalle autorità di controllo, devono essere redatti in modo accurato per garantire la tracciabilità e la responsabilizzazione.

5. Ruoli e responsabilità

Attraverso la seguente matrice delle responsabilità vengono messe in relazione le risorse (i soggetti) con le attività delle quali sono responsabili. La matrice specifica il tipo di relazione fra le risorse e l'attività e permette di individuare "chi fa che cosa" all'interno dell'organizzazione. I tipi di relazione vengono distinti in:

- Responsabile, (Responsible, R): è colui che esegue ed assegna l'attività
- Coinvolto (Consulted, C) è la persona che aiuta e collabora con il Responsabile (R) per l'esecuzione dell'attività
- Informato (Informed, I) è colui che deve essere informato al momento dell'esecuzione dell'attività o al suo completamento

La matrice illustra anche i tempi di esecuzione per ciascuna attività del processo.

MATRICE DELLE RESPONSABILITÀ DEL PROCESSO DI GESTIONE DEI DATA BREACH

Fase	*Attività*	*Soggetto/Struttura*					*Tempo di esecuzione*
		Titolare	**DPO**	**RSI**	**TRV**	**Segnalante**	
RILEVAZIONE	Rilevazione e segnalazione della violazione	**I**				**R**	non appena se ne viene a conoscenza e comunque entro e non oltre le 12 ore
QUALIFICAZIONE	Raccolta informazioni per inquadramento della violazione	**I**	**C**	**C**	**R**		entro 24 ore
	Valutazione dei rischi, identificazione misure tecniche e organizzative adottate e individuazione azioni correttive	**I**	**C**	**C**	**R**		entro 48 ore
	Attivazione delle misure tecniche e organizzative	**R**	**C**	**C**	**C**		ento 48 ore
NOTIFICAZIONE	Notifica della violazione al Garante (se necessaria)	**R**	**I**	**I**	**C**		entro 72 ore
	Comunicazione agli interessati coinvolti (se necessaria)	**R**	**I**	**I**	**C**		nel minor tempo possibile e senza ingiustificato ritardo
GESTIONE POST NOTIFICAZIONE	Analisi post - incidente ed eventuali disposizioni per l'adozione di misure correttive	**R**	**I**	**C**	**C**		al termine delle precedenti attività
REGISTRAZIONE DATA BREACH	Registrazione della violazione/aggiornamenti	**I**	**C**	**I**	**R**		al termine dell'analisi/ogniqualvolta vi sia la necessità

Legenda:

R = Responsabile

C = Coinvolto

I = Informato

Acronimi:

DPO = Data Protection Officer

RSI = Responsabile della sicurezza informatica

TRV = Team di Risposta alle Violazioni

6. Informazioni preliminari per la valutazione delle violazioni

Nell'ambito delle valutazioni relative alla gravità (*severity*) delle violazioni dovranno essere tenuti in considerazione i seguenti fattori di rischio per i diritti e le libertà dei soggetti interessati:

a) natura della violazione e potenziale esposizione degli interessati (c.d. gravità dell'accadimento);
b) priorità, in funzione dell'urgenza (valutata sulla base di quanto velocemente potrebbero verificarsi danni);
c) impatto potenziale dell'esposizione degli interessati (valutazione dell'entità dei danni agli interessati);
d) numero di interessati esposti al rischio;
e) adeguatezza delle misure di sicurezza già implementate rispetto al potenziale danno arrecabile agli interessati;
f) caratteristiche del Titolare del trattamento.

In particolare, e con riguardo alla tipologia delle violazioni, si possono classificare tre macrocategorie di data breach:

1) ***Confidentiality breach*** (violazione della riservatezza), in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
2) ***Integrity breach*** (violazione dell'integrità), in caso di modifica non autorizzata o accidentale dei dati personali;
3) ***Availability breach*** (violazione della disponibilità), in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

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

Per stabilire la gravità di una violazione viene utilizzata la seguente matrice del rischio:

GRADO DI PROBABILITÀ*	RISCHIO	DESCRIZIONE
Improbabile	**Basso**	Gli interessati non incontreranno inconvenienti o potrebbero incontrare alcuni inconvenienti che supereranno senza alcun problema (tempo passato a reinserire informazioni, fastidio, irritazione, ecc.)
Moderatamente probabile	**Medio**	Gli interessati potranno incontrare inconvenienti significativi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici lievi, ecc.)
Probabile	**Alto**	Gli interessati possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, lista nera da parte di banche, danni alla proprietà, perdita di posti di lavoro, citazione, peggioramento della salute, ecc.)
Quasi certo	**Molto alto**	Gli interessati possono incontrare conseguenze significative o addirittura irreversibili che non possono superare (difficoltà finanziarie come debito sostanziale o incapacità al lavoro, disturbi psicologici a lungo termine o disturbi fisici, morte, ecc.)

***** Per **probabilità** si intende la possibilità che, con i dati ottenuti, i terzi possano dar luogo ad attività che generino uno dei rischi elencati.

7. Procedura di gestione delle violazioni di dati personali

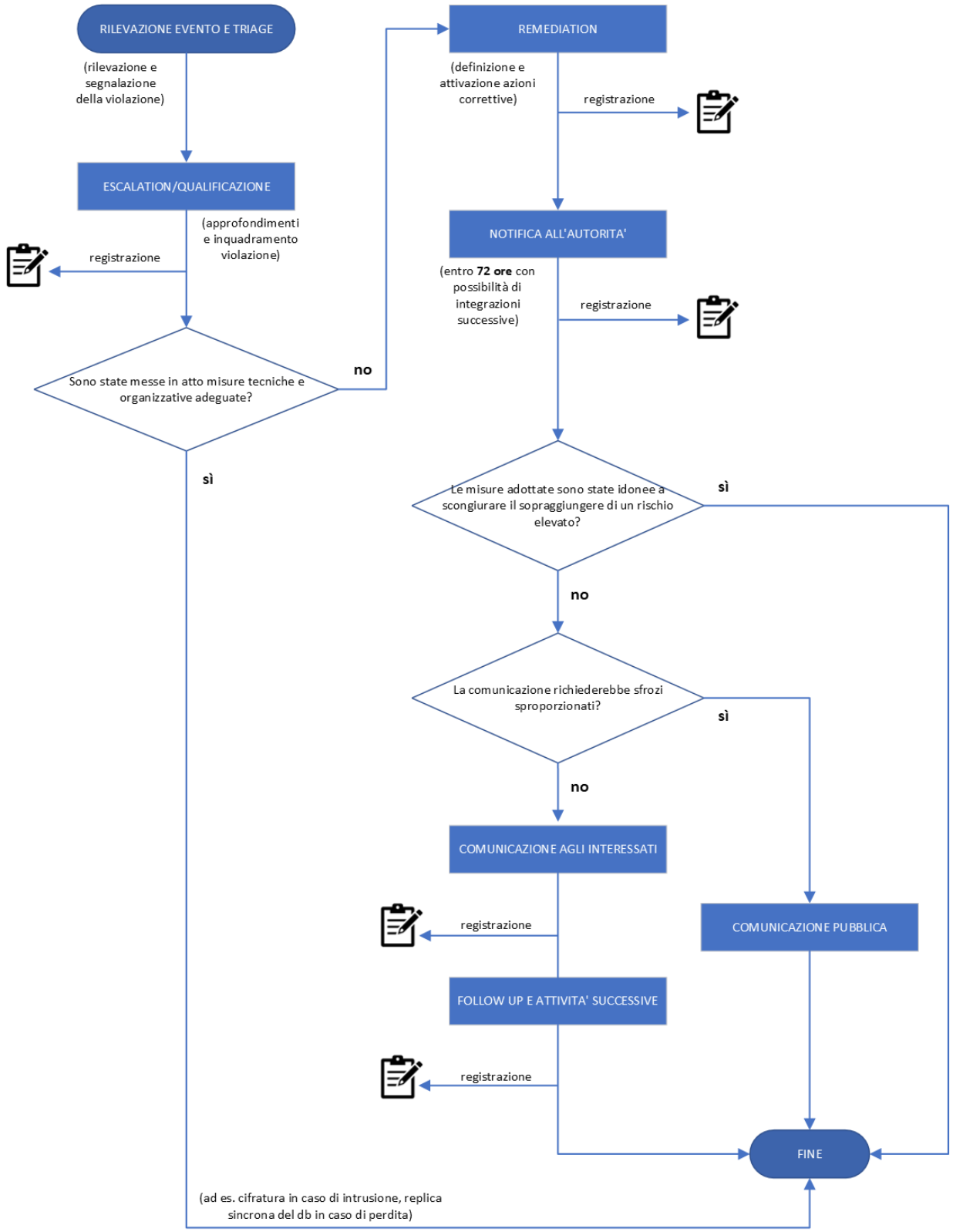
La procedura di gestione delle violazioni di dati personali ivi descritta viene avviata quando uno dei soggetti precedentemente individuati[2] venga a conoscenza di una sospetta, presunta o effettiva violazione dei dati personali e ne dia comunicazione al Titolare del trattamento[3].
Affinché la violazione sia gestita correttamente, è necessario seguire i seguenti step:

1) rilevazione e segnalazione dell'incidente di sicurezza;
2) analisi e classificazione dell'incidente di sicurezza come data breach;
3) eventuale notifica al Garante per la protezione dei dati personali;
4) eventuale comunicazione agli interessati;
5) documentazione della violazione - Registro delle violazioni;
6) attività successive.

Il seguente diagramma di flusso illustra e riassume graficamente le fasi della procedura per la gestione delle violazioni.

[2] Cap. 1 Scopo, ambito di applicazione e destinatari.
[3] Per le modalità di comunicazione si rimanda alla sezione 7.1 Rilevazione e segnalazione dell'incidente di sicurezza.

DIAGRAMMA DI FLUSSO DELLA GESTIONE DI UNA VIOLAZIONE DI DATI PERSONALI



7.1. Rilevazione e segnalazione dell'incidente di sicurezza

Laddove venga rilevato un incidente di sicurezza riguardante dati personali, il soggetto rilevante è tenuto a darne comunicazione (segnalazione) al Titolare del trattamento.
La segnalazione dell'incidente va fatta al Direttore Generale in qualità di delegato pro-tempore del legale rappresentante di ERDIS allo svolgimento di compiti e funzioni gestionali (art. 5 del Regolamento in materia di protezione dati personali di ERDIS).
La segnalazione deve avvenire in maniera tempestiva, entro e non oltre le 12 ore, a mezzo e-mail all'indirizzo direzione@erdis.it o, comunque, laddove non fosse possibile, utilizzando le vie più brevi (telefono, piattaforma di comunicazione, di persona). Il segnalante deve utilizzare l'apposito modulo in calce al presente documento (Modello segnalazione violazione) da compilare ed inviare preferibilmente al momento della segnalazione, oppure in un secondo momento, ma comunque entro e non oltre le 12 ore.
Nel caso in cui la segnalazione dovesse essere fatta ad altro soggetto diverso dal Direttore Generale, sarà cura di tale soggetto comunicargli tempestivamente l'incidente.
In caso di assenza del Direttore Generale, la segnalazione dovrà essere inviata al soggetto che ricopre le funzioni di Vicedirettore.
Il Direttore Generale, ricevuta la segnalazione, allerta il Team di Risposta alle Violazioni per le attività successive.

7.2. Analisi e classificazione dell'incidente di sicurezza come data breach

Il Team di Risposta alle Violazioni avvia la raccolta delle informazioni per stabilire se si sia effettivamente verificata un'ipotesi di data breach e se sia necessaria un'indagine più approfondita.
Il Team ha il compito di verificare, a norma dell'art. 33, par. 1, del GDPR, la probabilità che la violazione dei dati personali presenti un rischio (soprattutto se questo può qualificarsi come "elevato") per i diritti e le libertà delle persone fisiche e, di conseguenza, decidere le misure di risposta all'emergenza. A tal fine, può utilizzare lo strumento di autovalutazione che il Garante mette a disposizione sul proprio portale per individuare le azioni da intraprendere a seguito di una violazione dei dati personali (https://servizi.gpdp.it/databreach/s/self-assessment).
Conclusa la valutazione dei rischi, nel caso in cui sia stato valutato che le misure attivate siano insufficienti alla tutela degli interessati il Team provvede ad identificare le possibili azioni correttive da implementare, selezionandole tra quelle di cui sia valutata la fattibilità immediata ed il miglior esito ai fini della minimizzazione del possibile danno agli interessati. Entro 48 ore, il Titolare del trattamento provvede ad attivare le misure tecniche e organizzative per porre rimedio o contenere la violazione, coinvolgendo il Team ed eventuali altri soggetti il cui apporto sia ritenuto fondamentale in questa fase.
Nel caso in cui la violazione – in funzione dell'adeguatezza delle misure implementate – non costituisca un rischio per gli interessati, il Team procederà ad archiviare la documentazione e ad aggiornare il Registro delle violazioni.

7.3. Eventuale notifica al Garante per la protezione dei dati personali

Qualora dall'analisi dell'incidente emerga la sussistenza di un grave rischio per i diritti e le libertà degli interessati, è necessario effettuare la notifica all'Autorità: il Titolare, in qualità di delegato pro-tempore del legale rappresentante di ERDIS allo svolgimento di compiti e funzioni gestionali, coadiuvato dal Team, predispone la segnalazione e la invia al Garante per la protezione dei dati personali, senza ingiustificato ritardo e, comunque, entro 72 ore dal momento in cui si è venuti a conoscenza della

violazione, cioè da quando si abbia un ragionevole grado di certezza di un avvenuto incidente di sicurezza che riguardi dati personali.
Per l'invio della notifica verrà utilizzata l'apposita procedura telematica resa disponibile dal Garante nel portale dei servizi online https://servizi.gpdp.it/databreach/s/scelta-auth
Il Titolare è tenuto a valutare le circostanze specifiche di ogni effettiva violazione avvenuta. Pertanto, qualora non disponga di tutti gli elementi di dettaglio dell'incidente, è tenuto comunque ad effettuare la notifica della violazione al Garante entro 72 ore, con le informazioni in suo possesso, classificando come preliminare la notifica effettuata. Una volta ricostruito il quadro completo della violazione, provvederà alla compilazione del medesimo modulo, individuando come integrativa la notifica in essere. Nell'ipotesi in cui la segnalazione sia effettuata oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo.
Il Team di Risposta alle Violazioni curerà l'archiviazione della documentazione riguardante la violazione in modo regolare e puntuale, anche durante il suo sviluppo, così da raccogliere le informazioni necessarie e tutti i dettagli rilevanti, tenute a disposizione dell'Autorità Garante.
Ai sensi dell'art. 33, par. 3, del GDPR, la notifica dovrà contenere le seguenti informazioni:

- tipo di notifica: se è preliminare (il Titolare avvia il processo di notifica pur in assenza di un quadro completo della violazione con riserva di effettuare notifica integrativa), completa o integrativa;
- generalità del soggetto che effettua la notifica e dati dell'Ente;
- riferimenti del soggetto da contattare per ottenere informazioni aggiuntive inerenti alla violazione (DPO, Responsabile del trattamento, altri soggetti coinvolti);
- informazioni di sintesi sulla violazione: indicazioni temporali della violazione, modalità in cui il Titolare è venuto a conoscenza dell'incidente, motivi del ritardo della segnalazione;
- descrizione della violazione: natura della violazione (perdita di confidenzialità, perdita di integrità, perdita di disponibilità), cause della violazione (azione intenzionale interna, azione accidentale interna, azione intenzionale esterna, azione accidentale esterna o causa sconosciuta), categorie di dati personali oggetto di violazione (dati anagrafici, dati di contatto, dati di accesso e di identificazione, dati di pagamento, dati relativi alla fornitura di un servizio di comunicazione elettronica, dati di profilazione, dati giudiziari, dati di localizzazione, dati relativi a documenti di identificazione/riconoscimento, dati particolari), volume dei dati raccolti, categorie di interessati coinvolti (dipendenti/consulenti, utenti, contraenti/abbonati, clienti attuali o potenziali, associati/soci/aderenti, soggetti che ricoprono cariche sociali, beneficiari o assistiti, pazienti, minori, persone vulnerabili, etc.);
- informazioni di dettaglio sulla violazione: indicazione delle infrastrutture IT coinvolte e loro ubicazione, misure di sicurezza tecniche e organizzative adottate per garantire la sicurezza dei sistemi e delle infrastrutture IT coinvolte;
- probabili conseguenze della violazione dei dati (i dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento, i dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito, i dati sono stati modificati e resi inconsistenti, malfunzionamento e difficoltà nell'utilizzo di servizi, etc.);
- potenziali effetti negativi per gli interessati (perdita del controllo dei dati, limitazione dei diritti, discriminazione, furto o usurpazione d'identità, frodi, perdite finanziarie, decifratura non

autorizzata delle pseudonimizzazione, pregiudizio alla reputazione, danno economico o sociale significativo, etc.);

- eventuali misure adottate dal Titolare per porre rimedio o attenuare l'infrazione e per prevenire simili violazioni future;
- comunicazione agli interessati (ragioni dell'avvenuta/mancata comunicazione, numero degli interessati a cui è stata trasmessa, contenuto della comunicazione, canale utilizzato);
- altre informazioni (comunicazioni ad altre autorità di controllo, ad organismi di vigilanza o di controllo, all'autorità giudiziaria o di polizia, indicazione dell'appartenenza dei paesi coinvolti allo Spazio Economico Europeo).

7.4. Eventuale comunicazione agli interessati

Laddove una violazione dei dati personali comporti un rischio elevato per i diritti e le libertà delle persone fisiche, l'art. 34 del GDPR obbliga il Titolare a darne comunicazione agli interessati, senza ingiustificato ritardo, per consentire loro di attivarsi a tutela dei propri interessi.
La comunicazione agli interessati descrive, con un linguaggio semplice e chiaro, la natura della violazione e deve contenere almeno i seguenti elementi:

- una descrizione della natura della violazione;
- il nome e dati di contatto del Responsabile della protezione dei dati (RPD/DPO) o di altro punto di contatto presso cui ottenere più informazioni;
- una descrizione delle probabili conseguenze della violazione dei dati personali;
- una descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e anche, se del caso, per attenuare i possibili effetti negativi per gli interessati.

In calce al presente documento è l'apposito modello da utilizzare all'occorrenza (Modello comunicazione interessati).
La comunicazione agli interessati non è richiesta 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;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede a una comunicazione pubblica o a una misura simile che permetta di informare gli interessati con analoga efficacia.

Nell'eventualità in cui il Titolare si trovi nell'impossibilità di contattare i soggetti interessati dalla violazione, in quanto non dispone delle informazioni necessarie per riuscire a mettersi in contatto con questi, effettuerà la comunicazione non appena sia ragionevolmente possibile farlo.
Dell'avvenuta comunicazione è data informazione al DPO.

7.5. Documentazione della violazione - Registro delle violazioni

In virtù di quanto disposto dall'art. 33, par. 5, del GDPR, nel rispetto del principio di responsabilizzazione, il Titolare del trattamento è tenuto a documentare tutte le violazioni dei dati personali che si verificano, indipendentemente dal fatto che una violazione debba o meno essere notificata al Garante. Per tale motivo, il Titolare ha predisposto il Registro delle violazioni che viene

compilato ed aggiornato dal Team di Risposta alle Violazioni ogniqualvolta ve ne sia la necessità. Il Registro delle violazioni è messo a disposizione del Garante per effettuare eventuali verifiche sul rispetto della normativa.
Il GDPR non specifica un periodo di conservazione per tale tipologia di documentazione; laddove tali registrazioni contengano dati personali, spetta al Titolare determinare il periodo adeguato di conservazione, in conformità ai principi applicabili al trattamento dei dati personali, e individuare la corretta base legale per svolgere tale trattamento; tale documentazione potrebbe peraltro risultare idonea prova di conformità alla normativa vigente.
Qualora i "data breach record" non contengano dati personali, il principio di limitazione della conservazione del GDPR non si applica.

7.6. Attività successive

Al termine delle attività di notificazione al Garante ed agli interessati o, laddove tali attività non si fossero rese necessarie, dopo aver posto in essere le misure tecniche e organizzative per porre rimedio o contenere la violazione, il Titolare supportato dal Team di Risposta alle Violazioni procede ad effettuare un'analisi post-incidente per verificare l'efficacia e l'efficienza delle azioni intraprese durante la gestione dell'evento e identificare possibili aree di miglioramento.
Laddove si fosse proceduto a notificare la violazione al Garante, il Titolare provvede a dare disposizioni al Team per l'adozione di misure correttive comunicate dal Garante stesso.

8. Scheda di sintesi della procedura

Chi deve segnalare?	I soggetti che a qualsiasi titolo trattano dati personali di competenza del Titolare del trattamento e che ne vengano a conoscenza
A chi deve segnalare?	Al Direttore Generale in qualità di delegato pro-tempore del Legale rappresentante di ERDIS allo svolgimento di compiti e funzioni gestionali
Come segnalare?	Preferibilmente mediante apposito modulo (Modello segnalazione violazione) trasmesso via e-mail o, comunque, laddove non è possibile, procedere immediatamente anche telefonicamente o di persona. Il modulo può essere inviato anche in un secondo momento. La segnalazione può essere trasmessa al seguente indirizzo mail: direzione@erdis.it
Quando segnalare?	Tempestivamente, e comunque non oltre le 12 ore dalla presa di conoscenza dell'evento che potrebbe aver dato luogo ad una possibile violazione di dati personali.
Quando effettuare la notifica al Garante?	Qualora il Titolare ritenga probabile la sussistenza di un grave rischio per i diritti e le libertà degli interessati. La notifica, almeno preliminare, deve essere effettuata entro 72 ore dalla conoscenza della violazione.

Quando effettuare la comunicazione agli interessati?	In caso di violazione suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
Quando va registrata la violazione?	Sempre, a prescindere dalla notifica e/o dalla comunicazione.
Cosa succede se violo la procedura?	La presente procedura ha valore di regolamento interno e, pertanto, la sua violazione può comportare un provvedimento disciplinare.

9. Esempi di violazioni

Per meglio contestualizzare il riconoscimento di una violazione di dati personali nell'Ente, di seguito vengono proposti alcuni casi a titolo esemplificativo ma non esaustivo basati su quelli proposti dall'European Data Protection Board in appendice alle linee guida per la gestione dei data breach.

Tipologia data breach	Esempio	Notifica al Garante?	Notifica agli interessati?	Note
Confidentiality Breach	Furto o smarrimento di chiavetta USB o notebook o tablet o smartphone o hard disk su cui sono memorizzati dati non cifrati o cifrati con algoritmi non allo stato dell'arte	SI	SI se la natura dei dati e la gravità del furto può avere importanti conseguenze per gli interessati	
Confidentiality Breach	Furto o smarrimento di chiavetta USB o notebook o tablet o smartphone o hard disk su cui sono memorizzati dati cifrati con algoritmi allo stato dell'arte	NO	NO	Non deve essere notificato, ma va inserito nel registro delle violazioni
Confidentiality Breach	Un'applicazione informatica subisce un attacco informatico a fronte del quale gli attaccanti hanno avuto accesso a dati personali e c'è il ragionevole sospetto che li abbiano consultati e/o sottratti (esempi di applicativi: Gestione Documentale, Gestione carriera studenti, Gestione Risorse Umane, Gestione Diritto allo studio, Gestione prestito bibliotecario, Servizio di Posta Elettronica Office 365, etc.)	SI	SI se la natura dei dati e la gravità del furto può avere importanti conseguenze per gli interessati	
Availability Breach	Temporanea non disponibilità di un server, un applicativo o della connettività di rete (ad esempio per mancanza energia elettrica, guasto degli apparati)	NO	NO	Non deve essere notificato, ma va inserito nel registro delle violazioni

Confidentiality Breach/ Availability Breach	Una postazione di lavoro, o un server vengono compromessi da un ransomware e conseguentemente i dati vengono cifrati, non esiste un backup dei dati e/o c'è una ragionevole evidenza che i dati personali possono essere stati esfiltrati dal dispositivo	SI	SI se la natura dei dati e la gravità del furto può avere importanti conseguenze per gli interessati	
Confidentiality Breach/ Availability Breach	Una postazione di lavoro, o un server vengono compromessi da un ransomware e conseguentemente i dati vengono cifrati, esiste un backup dei dati per cui possono essere ripristinati in tempi ragionevoli e c'è una ragionevole evidenza che i dati personali non sono stati sottratti dal dispositivo	NO	NO	Non deve essere notificato, ma va inserito nel registro delle violazioni
Confidentiality Breach	Un titolare di credenziali di accesso a sistemi informatici che trattano dati personali segnala una perdita di confidenzialità delle proprie credenziali (ad esempio per aver dato seguito ad un messaggio di Phishing), da una veloce investigazione risulta che le credenziali siano state usate per accedere a dati personali con attività non riconducibili all'utente autorizzato	SI	SI se la natura dei dati e la gravità del furto può avere importanti conseguenze per gli interessati	
Confidentiality Breach	A seguito di un attacco informatico sono state trafugate le credenziali di utenze con privilegi di accesso a dati personali, tali credenziali erano memorizzati sul server in modalità non cifrata o cifrate con algoritmi non allo stato dell'arte o con meccanismi di cifratura non reversibile (hash) non allo stato dell'arte.	SI	SI	

Confidentiality Breach	A seguito di un errore di programmazione e configurazione di un sistema informatico o di una applicazione informatica, sono stati resi accessibili dati personali a soggetti non autorizzati al trattamento o diversi dagli interessati, inoltre da una rapida investigazione risulta che sono stati fatti accessi in violazione di quanto sopra	SI	SI se la natura dei dati e la gravità del furto può avere importanti conseguenze per gli interessati	
Confidentiality Breach	Comunicazione di dati personali ad errato destinatario (ad esempio per invio ad indirizzo e-mail errato)	SI	SI se la natura dei dati e la gravità del furto può avere importanti conseguenze per gli interessati	
Confidentiality Breach	Invio a mailing list di uno o più messaggi con gli indirizzi e-mail dei destinatari in chiaro nel campo 'A' o nel campo 'CC'	SI se l'evento coinvolge un largo numero di individui	Dipende dallo scopo e dalla finalità della mailing list	

10.Modulistica

10.1. Modello segnalazione violazione

MODULO PER LA SEGNAZIONE DI UN POTENZIALE DATA BREACH

AI SENSI DEL REGOLAMENTO (UE) 2016/679

Il presente modulo deve essere utilizzato per segnalare un potenziale data breach relativo a dati personali afferenti a banche dati di cui è titolare ERDIS Marche. Per data breach si intende «la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati» (art. 4 del Regolamento UE 2016/679).

Il modulo compilato in tutte le sue parti va inviato tramite e-mail all'indirizzo: direzione@erdis.it

ATTENZIONE: le informazioni fornite attraverso il presente modulo potrebbero essere inviate all'Autorità Garante al momento della notifica del data breach; per tale motivo, si ricorda l'importanza di rendere dichiarazioni veritiere, onde evitare di incorrere nella sanzione penale prevista dall'art. 168 del D.lgs. 196/03 in caso di false dichiarazioni al Garante.

DATI DI CONTATTO DI CHI EFFETTUA LA SEGNALAZIONE (*campi obbligatori)

Nome e cognome*: _____

Recapiti per comunicazioni dal DPO e/o dal Team di risposta alle violazioni:

Indirizzo e-mail* _____ Telefono*: _____

AFFERENZA ORGANIZZATIVA

Servizio/Ufficio di appartenenza*: _____

Ruolo/Funzione ricoperta*: _____

Nominativo del Responsabile della Struttura*: _____

MACROCLASSIFICAZIONE DELL'INCIDENTE (può essere selezionata anche più di una voce):

☐ Furto/Smarrimento di device o supporto di memorizzazione (ad esempio: computer, smartphone, tablet, chiavetta USB, documenti cartacei, etc.), indicare:

- quale device: _____

- si conosce il luogo in cui è avvenuto?

  ☐ NO

  ☐ SI, indicare il luogo: _____

☐ Accesso abusivo a sistema informatico (ad esempio: Server, Data Base, Applicazione), specificare:

- denominazione del sistema: _____
- struttura che si occupa della gestione del sistema: _____
- collocazione fisica del sistema:

  ☐ se interno all'Ateneo (locale, edificio, indirizzo): _____

  ☐ se esterno all'Ateneo (nome del fornitore ed indirizzo): _____

- referente di un tecnico che si occupa della gestione del sistema:

  nome e cognome: _____

  recapito e-mail: _____

  recapito telefonico: _____

☐ Perdita/smarrimento/furto di credenziali di accesso a device (ad esempio: computer, smartphone, tablet, etc.) contenenti dati personali, indicare:

- nome account: _____
- consente accesso a: _____

☐ Perdita/smarrimento/furto di credenziali di accesso ad applicazioni centrali (ad esempio: sistema gestione Diritto allo Studio, sistema di rilevazione presenze, posta elettronica istituzionale, etc.) contenenti dati personali, indicare:

- nome account: _____
- consente accesso a: _____

☐ Perdita/smarrimento/furto di credenziali di accesso ad applicazioni dipartimentali contenenti dati personali indicare:

- nome account: _____
- consente accesso a: _____
- struttura che si occupa della gestione del sistema: _____
- referente di un tecnico che si occupa della gestione del sistema:
  - nome e cognome: _____
  - recapito e-mail: _____
  - recapito telefonico: _____

Tipologia dei dati coinvolti (può essere selezionata più di una voce):

☐ Dati personali di dipendenti o collaboratori

☐ Dati personali degli studenti

☐ Dati personali di fornitori

☐ Altri dati personali, specificare quali: _____

Dispositivo oggetto della violazione:

☐ Computer

☐ Rete

☐ Dispositivo mobile

☐ File o parte di un file

☐ Strumento di backup

☐ Documento cartaceo

☐ Altro

Finalità per cui sono usati i dati coinvolti (compilare se sono note, può essere selezionata più di una voce):

☐ Processi amministrativi e gestionali dell'Ente

☐ Borse di studio e altri benefici a studenti

☐ Servizio ristorativo

☐ Servizio abitativo

☐ Appalti e contratti

☐ Concorsi e selezioni

☐ Altro, specificare: _____

Categorie dei dati coinvolti (può essere selezionata più di una voce):

☐ dati anagrafici/codice fiscale/numero di matricola

☐ dati di accesso e di identificazione (user name, password)

☐ dati personali idonei a rivelare l'origine razziale ed etnica, 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 personali idonei a rivelare lo stato di salute, la vita sessuale e le preferenze sessuali

☐ dati relativi a minori

☐ dati giudiziari

☐ dati biometrici

☐ dati genetici

☐ ancora sconosciuto

☐ altro, specificare: _____

Tipo di violazione sui dati (può essere selezionata più di una voce):

☐ lettura (presumibilmente i dati sono stati consultati ma non sono stati copiati)

☐ copia (i dati sono ancora presenti sul sistema/device ma sono anche stati copiati altrove)

☐ alterazione (i dati sono presenti sul sistema/device ma sono stati alterati

☐ cancellazione (i dati non sono più presenti sul sistema/device e non li ha neppure l'autore della violazione

☐ furto (i dati non sono più sul sistema/device e li ha l'autore della violazione)

☐ ancora sconosciuto

☐ altro, specificare: _____

Natura della violazione dei dati (può essere selezionata più di una voce):

☐ distruzione o cancellazione non voluta di dati personali

☐ perdita di dati personali

☐ modifica non voluta di dati personali

☐ divulgazione non autorizzata o non voluta di dati personali

☐ accesso da parte di terzi ai dati personali trasmessi, conservati o comunque trattati

Numero di dati personali coinvolti (selezionare solo una voce):

☐ è noto il numero preciso di dati personali, indicare il numero:

☐ è nota una stima del numero di dati personali, indicare un valore stimato:

☐ non è noto il numero di dati personali

Numero di interessati coinvolti (selezionare solo una voce):

☐ è noto il numero preciso di interessati, indicare il numero:

☐ è nota una stima del numero di interessati, indicare il numero:

☐ non è noto il numero di interessati

Quando si è verificata la violazione dei dati personali? (selezionare solo una voce):

☐ È possibile identificare la data precisa della violazione ed è ancora in corso, il: _____

☐ È possibile identificare la data precisa di inizio della violazione ed è ancora in corso, il: _____

☐ È possibile identificare il seguente intervallo temporale nel quale è avvenuta la violazione, dal _____al _____

Eventuali ulteriori informazioni utili relative all'incidente:

_____

_____

_____

Eventuali ulteriori informazioni utili relative ai sistemi su cui si è verificato l'incidente:

_____

_____

_____

Luogo e data

Firma del segnalante

10.2. Modello comunicazione interessati

COMUNICAZIONE DI UNA VIOLAZIONE DI DATI PERSONALI AGLI INTERESSATI

(art. 34 del Regolamento (UE) 2016/679)

Gentile [Nome e Cognome dell'interessato]

Secondo quanto prescritto dall'art. 34 del Regolamento europeo in materia di protezione dei dati personali (Regolamento UE 2016/679), l'ERDIS Marche, Titolare del trattamento dei dati, con la presente è a comunicarLe l'intervenuta violazione dei Suoi dati personali (*data breach*) che si è verificata in data _____/_____/_____, alle ore_____:_____, di cui si è avuto conoscenza in _____ _____.

A) Descrizione della natura della violazione:

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

_____
_____
_____
_____

b) Tipo di violazione:

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

c) Dispositivo oggetto di violazione:

☐ Computer,
☐ Rete,
☐ Dispositivo mobile
☐ Strumento di backup
☐ Documento cartaceo

d) Che tipo di dati sono oggetto di violazione:

☐ Dati anagrafici (nome, cognome, numero di telefono, e-mail, CF, indirizzo)
☐ Dati di accesso e di identificazione (user name, 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

Tale violazione è suscettibile di presentare un rischio elevato per Suoi diritti e le libertà

B) Descrizione delle probabili conseguenze della violazione dei dati personali:

_____
_____
_____
_____

C) Descrizione delle misure tecnologiche e 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 il Titolare del trattamento nella figura del delegato del Legale rappresentante, il Direttore Generale, i cui contatti sono: e-mail direzione@erdis.it pec erdis@emarche.it, nonché il Responsabile della Protezione dei Dati/Data Protection Officer (RPD/DPO) alla e-mail dpo@erdis.it

Distinti saluti.

Luogo e data

Firmato
Il Titolare del trattamento/
Delegato del Legale rappresentante