

Regolamento n. 53

Regolamento per la gestione delle violazioni di dati personali e degli incidenti informatici e per la loro eventuale comunicazione alle Autorità e ai soggetti interessati

Indice

1. Premessa
2. Definizioni
3. Ruoli e responsabilità
4. Riferimenti
5. Procedura di Data Breach
6. Identificazione di un potenziale Data Breach
7. Esecuzione dei riscontri preliminari
8. Valutazione e mitigazione
9. Notifica al Garante
10. Comunicazione agli interessati
11. Aggiornamento del registro delle violazioni
12. Definizione del piano di rimedio
13. Obblighi di comunicazione del ETRA quando opera in qualità di responsabile del trattamento
14. Procedura per l'Ipotesi di Incidente Informatico Significativo
15. Identificazione di un potenziale Incidente Informatico Significativo
16. Notificazioni e Comunicazioni
17. Risposta agli Incidenti Informatici Significativi
18. Varie ed Allegati: Allegato 1 (Format Scheda di Segnalazione); Allegato 2 (Format Scheda Evento); Allegato 3 (Format Registro delle Violazioni)
19. Entrata in vigore ed efficacia

1. Premessa

- 1.1. 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**" o "**Regolamento**"), 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 Regolamento sancisce i) l'obbligo per il titolare del trattamento di notificare tempestivamente l'avvenuta violazione dei dati personali all'autorità di controllo (di seguito, il "**Garante**") e, in casi determinati e con specifiche modalità, di procedere alla comunicazione direttamente agli interessati, e; ii) l'obbligo per il responsabile del trattamento di assistere il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli 33 e 34 del GDPR.
- 1.2. Secondo quanto previsto dall'art. 25, co. 4, del D.Lgs. n. 138/2024 (di recepimento della direttiva (UE) 2022/2555) (di seguito, il "**Decreto NIS2**"), relativo alle misure volte a garantire un livello elevato di sicurezza informatica in ambito nazionale ed a incrementare il livello comune di sicurezza nell'Unione Europea, è considerato significativo un incidente informatico che: "*a) ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato; b) ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli*". In tale contesto, il Decreto NIS2 sancisce l'obbligo per i "*soggetti essenziali e i soggetti importanti*" di notificare, senza ingiustificato ritardo, ogni incidente informatico significativo al Gruppo nazionale di risposta agli incidenti di sicurezza informatica (c.d. **CSIRT Italia**).
- 1.3. Posto che ETRA S.p.A. Società Benefit (di seguito, "**ETRA**" o la "**Società**") è sia soggetta all'applicazione del Regolamento che "*soggetto essenziale*" ai sensi del Decreto NIS2, l'obiettivo del presente documento (di seguito, la "**Regolamento**") è disciplinare il processo di gestione delle violazioni di dati personali e degli incidenti informatici significativi, ossia: definire i principi generali, i ruoli, le responsabilità e le attività da effettuare qualora si verifichi una violazione dei dati personali e/o un incidente informatico significativo. La presente Regolamento si applica a tutte le violazioni di dati personali ed incidenti informatici significativi riscontrati all'interno di ETRA. Le disposizioni del presente documento hanno validità per tutti i soggetti che prestano la propria attività a favore di ETRA.

2. Definizioni

2.1 Con il termine:

- "**Interessato**" si intende la persona fisica identificata o identificabile alla quale si riferiscono i dati personali trattati dal Titolare del trattamento. 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
- "**Violazione**" o "**Data Breach**" si intende una situazione che può comportare, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso a informazioni qualificate dal Regolamento come dati personali trasmessi, memorizzati o elaborati per mezzo di sistemi informatici o di altra natura. Per "*dato personale*" si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile («Interessato»);

2.2 Coerentemente con il Provvedimento n. 157 del Garante del 30 luglio 2019 sulla notifica delle violazioni dei dati personali, la natura della Violazione può essere classificata in base ai seguenti principi di sicurezza delle informazioni:

- "perdita di confidenzialità": diffusione, accesso non autorizzato o accidentale;
- "perdita di integrità": modifica non autorizzata o accidentale;
- "perdita di disponibilità": impossibilità di accesso, perdita, distruzione non autorizzata o accidentale.

2.3 Di seguito si riportano le principali possibili Violazioni di dati personali identificate:

- **furto o smarrimento di beni di ETRA**, ossia di quegli strumenti dati in dotazione e/o utilizzati dai dipendenti e/o collaboratori di ETRA, contenenti e/o utilizzati per gestire/elaborare dati personali, che comporta il venir meno del controllo sui dati medesimi (*i.e. Server, PC/laptop, smartphone, device* per l'archiviazione di dati esterni);
- **accesso illegale da parte di soggetti terzi**, ossia accesso abusivo da parte di terzi, non autorizzati, ai sistemi informatici, ad esempio, mediante:
 - un attacco *ransomware*, mirato al furto di documenti. Tale attacco di solito può essere classificato come violazione della disponibilità dei dati personali, ma spesso potrebbe verificarsi anche una violazione della riservatezza degli stessi;
 - attacchi *injection* (*SQL injection, path traversal*). Tali attacchi mirano a copiare e abusare dei dati personali. Si tratta principalmente di violazioni della riservatezza, ma spesso potrebbe verificarsi anche una violazione dell'integrità degli stessi;
 - attacchi *phishing*, ossia truffe informatiche effettuate inviando un'e-mail con il logo contraffatto di un istituto di credito o di una società di commercio elettronico, in cui si invita il destinatario a fornire dati riservati, motivando tale richiesta con ragioni di ordine tecnico. Tali attacchi sono classificati come violazioni della riservatezza dei dati personali;
- **errore accidentale** da parte di uno dei soggetti che trattano dati personali (*i.e.* invio di una *mail* contenente dati personali ad un destinatario errato);
- **furto di informazioni**, può verificarsi nel caso in cui un dipendente (o ex dipendente) o altro collaboratore (o ex collaboratore) a vario titolo sfrutti la propria conoscenza o le proprie autorizzazioni per sottrarre dolosamente dati/informazioni di carattere personale;
- **inadeguatezza delle misure di sicurezza**, qualora, a causa di un'erronea valutazione sul livello di criticità dei dati e/o informazioni aziendali, non siano state poste in essere le necessarie precauzioni volte alla salvaguardia dei dati medesimi, che sono stati perduti.

2.4 Con il termine:

- "**Incidente Informatico**" si intende un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informativi e di rete o accessibili attraverso di essi;
- "**Incidente Informatico Significativo**" si intende ogni incidente informatico che "*a) ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato; b) ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli*".

2.5 I termini orari indicati nella presente Regolamento sono da intendersi come ore solari e non ore lavorative.

3. Ruoli e responsabilità

3.1 Si riportano i ruoli e le responsabilità di ciascuna figura coinvolta nel processo di gestione e segnalazione dei *Data Breach* e degli Incidenti Informatici Significativi, di cui alla presente Regolamento.

3.2 Data Breach:

- **Titolare del trattamento**: ETRA S.p.A. Società *Benefit*, che con il supporto del DPO: (*i*) dopo aver valutato la portata e il livello di rischio dell'avvenuta violazione di dati personali, si occupa di individuare e adottare possibili misure di rimedio e di notificare la Violazione al Garante senza ingiustificato ritardo e, ove possibile entro 72 ore dal momento in cui ne è venuto a conoscenza, vale a dire dal momento in cui è ragionevolmente certo che si è verificato un incidente di sicurezza che ha portato

alla compromissione dei dati personali, salvo che si riveli improbabile che la Violazione medesima possa presentare un rischio per i diritti e le libertà delle persone fisiche; (ii) comunica la Violazione agli Interessati, qualora la stessa sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche; (iii) prevede attività di verifica periodica volte a garantire l'efficacia delle procedure e degli strumenti di risposta agli incidenti relativi alle violazioni di dati personali;

- **Responsabile della Protezione dei Dati (o DPO):** soggetto esterno alla Società, da essa selezionato ed incaricato, che funge da punto di contatto tra il Titolare, il Garante e gli Interessati. Nell'ambito della gestione degli incidenti, può raccogliere segnalazioni, interne e/o esterne, di possibili violazioni di dati personali e supporta il Titolare del trattamento nell'attività di valutazione della avvenuta violazione di dati e nella gestione dei rapporti con il Garante. Il DPO ha una funzione di sorveglianza, consulenza e supporto, non potendosi in alcun caso sostituire al Titolare del trattamento nell'assolvimento dei compiti e nelle decisioni che spettano a quest'ultimo, salva diversa disposizione di legge;
- **Referente Privacy:** il responsabile dell'Ufficio Privacy o, in sua assenza, altro funzionario dell'ufficio a tanto delegato, che svolge attività di supporto alla Società per le questioni relative alla tutela dei dati personali trattati e rappresenta il punto di contatto tra il DPO e il Consiglio di Amministrazione di ETRA (di seguito, il **CDA**), nonché tra il DPO e le altre figure/soggetti indicati nel presente comma 2. In tale veste, il Referente Privacy si occupa di: (i) trasmettere tutte le segnalazioni di potenziali *Data Breach*, ricevute o altrimenti rilevate, al Soggetto Designato la cui area aziendale è stata coinvolta, affinché quest'ultimo possa istruire la Violazione, con il Team; (ii) informare e collaborare con il DPO affinché quest'ultimo possa supportare il CDA nella valutazione, notifica, comunicazione e gestione del *Data Breach*, attraverso la messa a disposizione in favore del DPO di tutti gli elementi necessari all'espletamento dei suoi compiti, per come raccolti/ricevuti/istruiti dai Soggetti Designati, dagli Amministratori di Sistema e dalle altre figure/soggetti di cui al presente comma;
- **Soggetto Designato:** soggetto che, in qualità di dirigente a capo dell'area organizzativa aziendale dove si è verificata la potenziale *Violazione*, collabora con il Referente Privacy ed il DPO, al fine di valutare se si è verificato un *Data Breach* ed affinché il Referente Privacy ed il DPO possano supportare il Presidente del Consiglio di Amministrazione e legale rappresentante di ETRA o soggetto dallo stesso delegato nella valutazione, notifica, comunicazione e gestione della violazione dei dati;
- **Autorizzati:** soggetti preposti materialmente ad una o più attività di trattamento che coadiuvano il Soggetto Designato e il Referente Privacy, svolgendo le seguenti attività: (i) comunicano immediatamente e senza ingiustificato ritardo eventuali violazioni di dati personali di cui sono a conoscenza mediante l'invio al DPO di una comunicazione da indirizzare agli appositi strumenti e canali messi a disposizione da ETRA; (ii) forniscono supporto in fase di identificazione dell'incidente, comunicando al Soggetto Designato ed al Referente Privacy, informazioni utili per la classificazione delle violazioni verificatesi;
- **Amministratori di Sistema** (di seguito anche "**AdS**"): soggetti che, in qualità di preposti alle attività di gestione e manutenzione dei sistemi informatici aziendali, coadiuvano il Soggetto Designato, il Referente Privacy e il DPO, coerentemente con le responsabilità attribuitegli, svolgendo le seguenti attività: (i) monitorano i sistemi di sicurezza; (ii) comunicano immediatamente e senza ingiustificato ritardo, in caso di Violazione, tutte le informazioni necessarie alla sua comprensione e le trasmettono ai Soggetti Designati e al Referente Privacy; (iii) comunicano immediatamente e senza ingiustificato ritardo le eventuali azioni poste in essere per la gestione della Violazione ai Soggetti Designati e al Referente Privacy; (iv) monitorano di continuo le attività necessarie a prevenire eventuali Violazioni e le attività che rilevino le eventuali non conformità delle misure di sicurezza; (v) comunicano immediatamente e senza ingiustificato ritardo ai Soggetti Designati e al Referente Privacy eventuali situazioni che potrebbero comportare violazioni di dati personali; (vi) raccolgono immediatamente e senza ingiustificato ritardo le

informazioni per quanto di competenza, necessarie a formulare compiutamente le comunicazioni verso il Garante e l'interessato.

- **Team:** composto dal Referente Privacy, dal DPO, dal Soggetto Designato e, per quanto coinvolti, dagli Autorizzati e dagli AdS ovvero da qualsiasi soggetto, anche esterno, ritenuto necessario alla corretta e completa gestione del potenziale o accertato Data Breach;
- **Responsabile del Trattamento:** persona fisica o giuridica, autorità pubblica, servizio o altro organismo che tratta i dati personali per conto del Titolare del trattamento. Ai sensi e fini di cui alla presente Regolamento, il Responsabile del Trattamento deve: (i) tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento dei dati di ETRA, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, mettere in atto misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio, che comprendono quelle di cui all'art. 32 del Regolamento; (ii) notificare, tempestivamente e senza ingiustificato ritardo, comunque non oltre le 24 h da quando ne ha avuto conoscenza, o nel diverso termine previsto nei contratti di nomina di cui all'art. 28 del GDPR, al Titolare del Trattamento e al DPO la violazione dei dati personali di cui sia venuto a conoscenza, fornendo tutte le informazioni di cui all'art. 32, co. 3, del Regolamento e collaborando con il Titolare del trattamento e il DPO per la valutazione e successiva notificazione, entro il termine di cui al Regolamento, della violazione al Garante e, in eventualità, agli interessati.

3.3 Incidente Informatico Significativo:

- **Soggetto essenziale:** ETRA S.p.A. Società *Benefit* che, con il supporto del Referente aziendale per la Cybersicurezza o, in mancanza, del Responsabile della U.O. ICT, adotta misure tecniche, operative e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete utilizzati nella propria attività o nella fornitura dei servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi. Con particolare riguardo alla presente Regolamento, il Soggetto essenziale individua il Punto di Contatto con l'Agenzia per la *cybersicurezza* nazionale (di seguito, l'"**ACN**"), anche al fine di eventualmente notificare al CSIRT Italia – per il tramite di quest'ultimo - senza ingiustificato ritardo, ogni Incidente Informatico Significativo che, ai sensi del comma 4 dell'art. 25 del Decreto NIS2, ha un impatto significativo sulla fornitura dei propri servizi.
- **Referente per la Cybersicurezza:** è il soggetto che, ex. art. 8, co. 2, della Legge n. 90 del 28.06.2024, provvede a: (a) lo sviluppo delle politiche e delle procedure di sicurezza delle informazioni; b) la produzione e l'aggiornamento di sistemi di analisi preventiva di rilevamento e di un piano per la gestione del rischio informatico; c) la produzione e l'aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'amministrazione; d) la produzione e l'aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture dell'amministrazione; e) la pianificazione e l'attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici, in coerenza con i piani di cui alle lettere b) e d); f) la pianificazione e l'attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la cybersicurezza nazionale; g) il monitoraggio e la valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza;
- **Punto di Contatto:** soggetto interno alla Società dotato di adeguate competenze gestionali, legali e tecniche, individuato e delegato dal Soggetto essenziale, che ha il compito di curare l'attuazione delle disposizioni del Decreto NIS2, tra cui la registrazione sulla piattaforma e, ai fini della presente Regolamento, la eventuale notifica degli Incidenti Informatici Significativi al CSIRT Italia, nei modi e termini di cui agli artt. 25 e 26 del Decreto Nis2 medesimo.

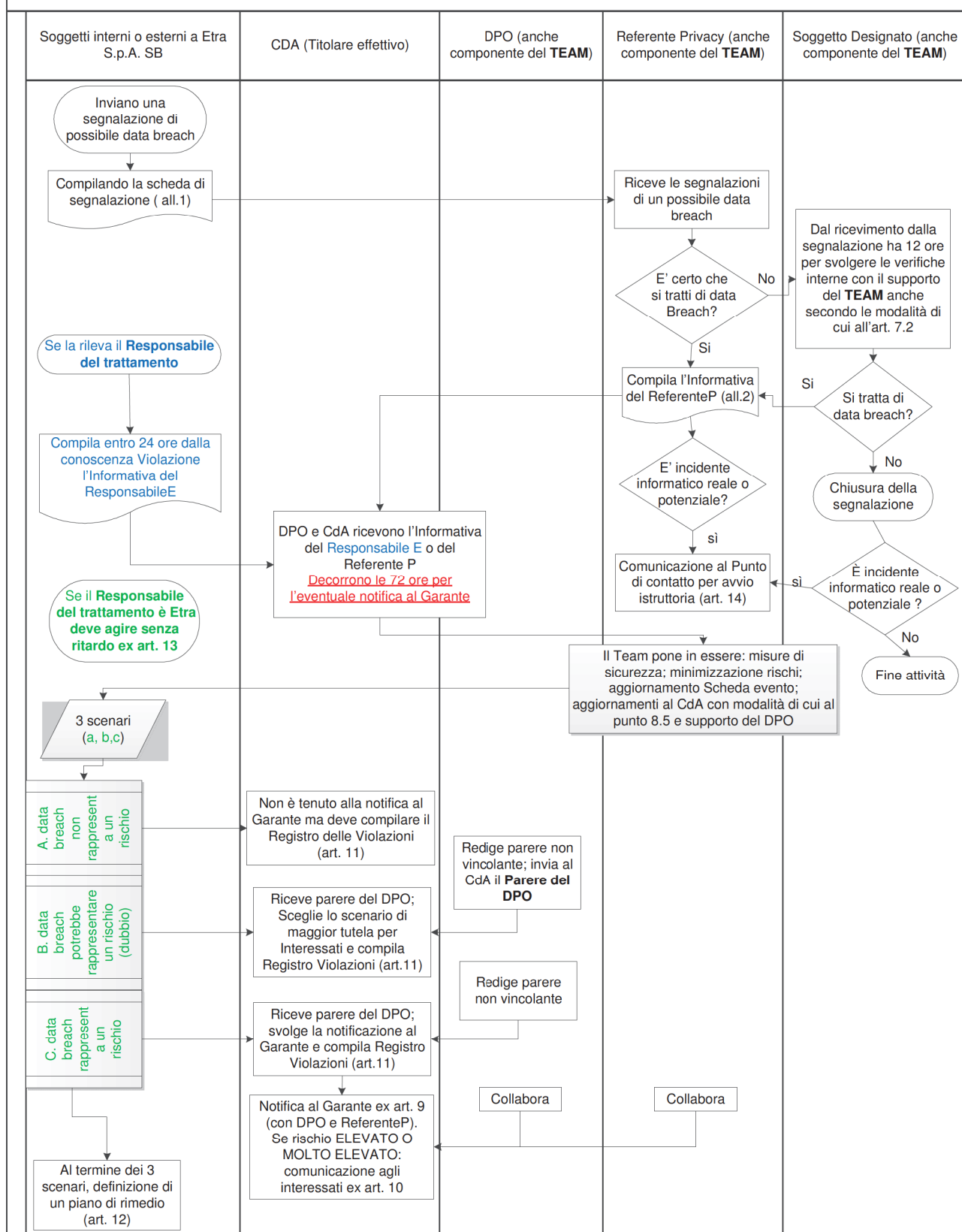
4. Riferimenti

4.1 Di seguito si riporta l'elenco dei documenti che costituiscono il riferimento per la presente Regolamento:

- Regolamento UE n. 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla protezione dei dati);
- D.Lgs. n. 196/03 Codice in materia di protezione dei dati personali e successive modifiche e integrazioni;
- Linee guida in materia di notifica delle violazioni di dati personali (*Data Breach Notification*) – WP 250, adottate dal Gruppo di lavoro Art. 29 il 06 febbraio 2018;
- Provvedimento n. 157 del Garante del 30 luglio 2019 sulla notifica delle violazioni dei dati personali;
- Linee guida in materia di notifica delle violazioni di dati personali (*Examples regarding Data Breach Notification*), adottate dall'*European Data Protection Board* il 14 gennaio 2021;
- Provvedimento n. 209 del Garante del 27 maggio 2021 sulla Procedura telematica per la notifica di violazioni di dati personali (Data Breach).
- D.Lgs. n. 138/2024, di recepimento della direttiva (UE) 2022/2555, relativo alle misure volte a garantire un livello elevato di sicurezza informatica in ambito nazionale ed a incrementare il livello comune di sicurezza nell'Unione Europea;
- Determinazione dell'Agenzia per la Cybersicurezza Nazionale (**ACN**) del 26.11.2024 “*recante termini, modalità e procedimenti di utilizzo e accesso alla piattaforma digitale nonché ulteriori informazioni che i soggetti devono fornire all'Autorità nazionale competente NIS e termini, modalità e procedimenti di designazione dei rappresentanti NIS nell'Unione*”; nonché Determinazione dell'ACN n. 164179 del 14.04.2025.

5. Procedura per l'ipotesi di Data Breach

5.1 La procedura di Data Breach adottata da ETRA è articolata nelle fasi riportate all'interno dei seguenti diagrammi di flusso:



5.2 Di seguito si riporta la descrizione delle attività previste per ciascuna fase del processo di Data Breach di cui ai diagrammi di flusso sub art. 5.1, evidenziando che – a determinate condizioni – una ipotesi di Data Breach può dar luogo anche ad un Incidente Informatico o a un Incidente Informatico Significativo e che dunque il processo di Data Breach tiene conto anche di tale ipotesi aggiuntiva.

6. Identificazione di un potenziale Data Breach

- 6.1 La fase di identificazione di una violazione di dati personali ha l'obiettivo di rilevare un potenziale Data Breach derivante dalla perdita, divulgazione non autorizzata, trattamento illecito e/o perdita di disponibilità di dati personali di cui ETRA è titolare.
- 6.2 Tutte le possibili violazioni dei dati personali devono essere identificate e indirizzate immediatamente e senza ingiustificato ritardo al Referente Privacy, mediante la compilazione della scheda segnalazioni (All. 1) (di seguito, le **Segnalazioni**).
- 6.3 Le Segnalazioni possono provenire da fonti interne e fonti esterne ad ETRA, quali (a titolo esemplificativo e non esaustivo):
- Strumenti informatici di monitoraggio di eventi di sicurezza o attraverso misure tecniche di sicurezza finalizzate alla protezione dei sistemi informativi;
 - Dipendenti/autorizzati al trattamento;
 - Punto di Contatto;
 - Cittadini;
 - Utenti e/o Soci di ETRA;
 - Fornitori e terze parti;
 - Autorità di vigilanza;
 - DPO;
 - Media (es. stampa, telegiornali, agenzie di informazione multimediale, ecc.).
- 6.4 Ogni soggetto che presta la propria attività a favore di ETRA, che venga a conoscenza o sospetti che sia avvenuta una Violazione, deve inviare immediatamente e senza ingiustificato ritardo la Segnalazione al Referente Privacy. La Segnalazione deve contenere un'indicazione chiara dell'evento verificatosi, delle caratteristiche dei dati personali coinvolti e, ove possibile, dell'unità organizzativa aziendale interessata dalla Violazione.
- 6.5 Il Referente Privacy, una volta ricevuta la Segnalazione, trasmette immediatamente e senza ingiustificato ritardo la Segnalazione medesima a:
- (i) **ove vi sia** la ragionevole certezza del fatto che si sia effettivamente verificato un Data Breach, al DPO e al CDA, affinché si proceda alle valutazioni di cui sub art. 8 ed alla eventuale Notificazione al Garante, di cui sub art. 9 che segue. Il ricevimento di questa comunicazione da parte del CDA determinerà il decorrere dei termini per la Notificazione al Garante;
 - (ii) **ove non vi sia** la ragionevole certezza del fatto che si sia effettivamente verificato un Data Breach, al DPO e al/ai Soggetto/i Designato/i la cui Area aziendale è stata coinvolta, affinché si proceda come indicato nei commi che seguono.
- 6.6 Nell'ipotesi di cui sub art. 6.5(ii), il Referente Privacy collabora, avvalendosi della consulenza del DPO, con il/i Soggetto/i Designato/i la cui Area aziendale è stata coinvolta nell'attività di istruttoria e valutazione preliminare del livello e delle potenzialità di rischio per gli interessati dell'evento descritto nella Segnalazione.
- 6.7 Qualora la presunta Violazione abbia riguardato dati conservati/trasmessi/elaborati o servizi offerti dai sistemi informativi e di rete di ETRA o accessibili attraverso di essi, e dunque qualora la presunta Violazione possa aver dato luogo o dar luogo ad un Incidente Informatico, il Referente Privacy dovrà trasmettere, immediatamente, la Segnalazione anche al Punto di Contatto, al fine di dare parallelamente avvio all'istruttoria, valutazione ed eventuale notificazione di cui al successivo art. 14.
- 6.8 Qualora la presunta Violazione inerisca a dati personali trattati da un Responsabile del Trattamento, sarà dovere dello stesso rilevarla tempestivamente e darne, immediatamente e senza ingiustificato ritardo, comunque non oltre 24h dalla conoscenza della Violazione, o nel diverso termine indicato nei contratti di nomina di cui all'art. 28 del GDPR, comunicazione ad ETRA, con cui ha contrattualizzato il rapporto professionale, nei modi di cui al successivo art. 7.5.

7. Esecuzione dei riscontri preliminari interni

- 7.1 Il Soggetto Designato la cui Area è stata interessata dal potenziale Data Breach, ricevuta la Segnalazione dal Referente Privacy, effettua senza ingiustificato ritardo, e comunque in un tempo massimo di 12h dalla Segnalazione, le verifiche preliminari interne volte a vagliarne l'attendibilità e dunque ad accertare se trattasi, con ragionevole certezza, di un Data Breach, con il supporto del Team.
- 7.2 Al fine di condurre una valutazione sulla presunta violazione, il Team si potrà avvalere dell'ausilio del *tool* di autovalutazione messo a disposizione dei titolari del trattamento dal Garante e reperibile al seguente link <https://servizi.gpdp.it/databreach/s/self-assessment>. Il *tool* supporterà il Team nel valutare se dall'incidente di sicurezza occorso si sia effettivamente verificato un Data Breach.
- 7.3 Al termine delle verifiche sub 7.2, ove le stesse – ai sensi del Regolamento e del Codice Privacy:
- (i) **diano esito negativo**: si procederà alla chiusura della Segnalazione;
 - (ii) **diano esito positivo**:
 - a. il Referente Privacy ne darà immediatamente informativa al CDA e al DPO in copia, comunicando il Data Breach, con la specifica indicazione delle seguenti informazioni, ove disponibili (di seguito, l'**Informativa del ReferenteP**):
 - l'Area e l'Unità Organizzativa aziendale coinvolta;
 - la data e l'ora del Data Breach, anche solo presunta (specificando se è presunta);
 - la data e ora in cui si è avuta conoscenza della Violazione;
 - la fonte della Segnalazione;
 - la natura della Violazione;
 - una sintetica descrizione della Violazione;
 - il numero e la categoria di interessati coinvolti;
 - la categoria e il volume di dati personali di cui si presume la violazione;
 - la descrizione dei sistemi di elaborazione e/o memorizzazione dei dati coinvolti, con indicazione della loro ubicazione;
 - l'indicazione dell'eventuale Responsabile del Trattamento coinvolto con indicazione delle attività svolte;
 - le misure di sicurezza adottate al set di dati oggetto di violazione;
 - le misure proposte per la mitigazione della Violazione;
 - l'esito della autovalutazione condotta mediante il *tool* messo a disposizione dal Garante;
 - se la Violazione ha dato luogo anche ad un Incidente.
 - b. Il Team individua e pone in essere tempestivamente le misure di sicurezza necessarie a interrompere la Violazione e minimizzare i rischi per i diritti e le libertà degli interessati (di seguito "**Rischi**" o "**Rischio**") avendo cura di conservare ogni informazione utile alle indagini.
- 7.4 L'Informativa del ReferenteP è effettuata utilizzando l'apposita scheda dell'evento (All. 2 - di seguito, la **Scheda Evento**), che sarà firmata dal Referente Privacy medesimo e dal Soggetto Designato coinvolto e comunicata al CDA e al DPO in copia.
- 7.5 Qualora la Violazione sia stata riscontrata dal Responsabile del Trattamento, le verifiche del caso saranno poste in essere dal responsabile medesimo, che provvederà a darne tempestiva comunicazione al CDA e al DPO, sempre mediante la compilazione ed invio della Scheda Evento (di seguito, l'**Informativa del ResponsabileE**. L'informativa del ReferenteP e/o l'Informativa del ResponsabileE, di seguito indistintamente, l'**Informativa**).
- 7.6 Dal momento della ricezione da parte del CDA dell'Informativa del ReferenteP e/o dell'Informativa del ResponsabileE, ovvero dalla comunicazione del Referente Privacy sub art. 6.5, decorrono le tempistiche previste dal Regolamento per la gestione degli adempimenti connessi alle violazioni accertate (in seguito "**Tempo zero – T0**").

8. Valutazione e mitigazione

- 8.1 Il Team prosegue nelle attività di valutazione e mitigazione, e, ove del caso, provvede ad aggiornare la Scheda Evento, inviando gli aggiornamenti al CDA.

- 8.2 Il Team valuta la probabilità che la Violazione comporti un Rischio, basandosi sulle informazioni ricevute e/o raccolte, tenendo in particolare considerazione i seguenti elementi:
- i dati personali sono di carattere particolare e/o di natura finanziaria;
 - i sistemi informatici oggetto di violazione sono complessi per qualità/quantità di informazioni elaborate;
 - la Violazione comprende le chiavi di accesso/cifratura in possesso degli interessati (i.e. password).
- 8.3 Per ciascuna Violazione dei dati personali, il Team deve identificare opportune misure correttive tecniche e organizzative da adottare, al fine di mitigare i relativi effetti e ridurre la probabilità di impatto e ricorrenza della Violazione.
- 8.4 Nell'ipotesi in cui risulti improbabile che il Data Breach presenti un rischio per i diritti e le libertà delle persone fisiche interessate, il Titolare del trattamento non è tenuto a notificare la violazione al Garante, pur restando fermo il dovere di censire il Data Breach medesimo all'interno del registro delle violazioni.
- 8.5 Per tutte le attività valutative di cui al presente art. 8, e dunque: (i) la valutazione sulla probabilità che il Data Breach presenti o meno un rischio per i diritti e le libertà delle persone fisiche, nonché; (ii) la valutazione sul tipo di misure correttive tecniche e/o organizzative da adottare, al fine di mitigare i relativi effetti e ridurre la probabilità di impatto e ricorrenza della violazione, il Team si avvarrà del tool messo a disposizione dal Garante e reperibile al seguente link <https://servizi.gpdp.it/databreach/s/self-assessment>, della consulenza e del supporto tecnico del DPO.
- 8.6 In casi dubbi circa la valutazione di probabilità o meno di Rischi della Violazione, il Titolare del trattamento sceglierà lo scenario di maggior tutela per gli Interessati.
- 8.7 Per le finalità sub 8.6, in particolare, il DPO: (i) potrà, con l'ausilio del Referente Privacy, svolgere ulteriori riscontri, al fine di reperire le evidenze mancanti rispetto alle prime analisi condotte; (ii) all'esito dell'approfondimento sub (i), dovrà aggiornare l'apposita Scheda Evento messa a disposizione dal Referente Privacy, e; (iii) dovrà redigere/inviare al CDA, un proprio parere scritto in merito alla probabilità di Rischi della Violazione (di seguito, il **Parere del DPO**). Tale attività dovrà essere compiuta tempestivamente e senza indugio, onde consentire al CDA di rispettare il termine di 72 ore per la notifica al Garante della violazione.
- 8.8 Il Parere del DPO non ha carattere vincolante, sicché il Titolare del trattamento potrà, in ogni caso, notificare la violazione al Garante ogni qual volta lo ritenga opportuno, motivando le sue valutazioni all'interno dell'apposita Scheda Evento.

9. Notifica al Garante.

- 9.1 Qualora, all'esito delle verifiche/valutazioni di cui sub art. 8 e di quanto espresso nel Parere del DPO, risulti probabile che il Data Breach possa rappresentare un rischio per i diritti e le libertà degli interessati, il Titolare del trattamento è tenuto a notificare l'avvenuta violazione di dati personali al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal T0 di cui all'art. 7.6 (di seguito, la **Notificazione al Garante**). La Notificazione al Garante dovrà essere operata dal legale rappresentante di ETRA o soggetto dallo stesso delegato, con il supporto del DPO e del Referente Privacy, tramite l'apposita procedura telematica, resa disponibile nel portale dei servizi online del Garante, e raggiungibile all'indirizzo <https://servizi.gpdp.it/databreach/s/> e dovrà contenere almeno: a) la descrizione della 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) l'indicazione del nome e dei dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni; c) la descrizione delle probabili conseguenze della violazione dei dati personali; d) la descrizione delle 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.
- 9.2 I tempi di notifica, nonché l'oggetto delle Notificazioni al Garante devono essere formalizzati all'interno del registro delle violazioni.
- 9.3 Nelle ipotesi in cui, malgrado le valutazioni sub art. 8, il Titolare ritenga necessari ulteriori riscontri, oltre il termine di 72 ore dal T0, è tenuto comunque a comunicare entro il predetto

termine gli estremi della Violazione al Garante, indicando nella Notificazione stessa le informazioni confermate e il termine entro il quale si ritiene termineranno le ulteriori attività istruttorie (di seguito, il **Supplemento di Istruttoria**).

- 9.4 Al termine del Supplemento di Istruttoria, il legale rappresentante di ETRA o soggetto dallo stesso delegato – con il supporto del DPO e del Referente Privacy – dovrà inviare una (o più) ulteriore Notificazione al Garante, in cui dovranno essere illustrati gli esiti dei successivi riscontri effettuati e le valutazioni compiute in ordine alle conseguenze e ai potenziali Rischi dell'avvenuta Violazione.

10. Comunicazione agli Interessati

- 10.1 Al fine di valutare se la Violazione occorsa possa presentare un rischio elevato o molto elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento si avvarrà del supporto del DPO e del *tool* messo a disposizione dal Garante e reperibile al seguente link <https://servizi.gpdp.it/databreach/s/self-assessment>.
- 10.2 Qualora l'esito della valutazione sub art. 10.1 rappresenti che la Violazione dei dati personali è suscettibile di comportare un rischio elevato o molto elevato per i diritti e le libertà degli Interessati, il legale rappresentante di ETRA o soggetto dallo stesso delegato, con il supporto del DPO, predispone ed invia la comunicazione agli Interessati, senza ingiustificato ritardo, utilizzando i canali ufficiali di comunicazione a disposizione di ETRA.
- 10.3 Segnatamente, qualora la comunicazione risulti necessaria, il legale rappresentante o soggetto dallo stesso delegato, con il supporto del DPO e del Referente Privacy:
- comunica la Violazione agli Interessati, senza ingiustificato ritardo;
 - la comunicazione avviene preferibilmente su base individuale per e-mail, salvo che sia impossibile procedere in tal modo, nel qual caso la comunicazione viene effettuata tramite il sito *internet* di ETRA e/o tramite pubbliche affissioni presso gli sportelli aperti al pubblico di ETRA e/o tramite messaggi *push* inviati da *app* ad uso interno od esterno, ove disponibili;
 - la comunicazione all'Interessato deve descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contenere almeno le seguenti informazioni:
 - una descrizione della natura della Violazione;
 - il nome e i dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni;
 - una descrizione delle probabili conseguenze della violazione;
 - una descrizione delle misure adottate o di cui si propone l'adozione da parte della Società per porre rimedio alla Violazione e anche, se del caso, per attenuarne i possibili effetti negativi.
- 10.4 Ai sensi dell'art. 34, par. 3 del Regolamento, non è richiesta la comunicazione all'Interessato se è soddisfatta una delle seguenti condizioni: 1) 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; 2) 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; 3) detta comunicazione richiederebbe sforzi sproporzionati. In tale ultimo caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
- 10.5 Nel caso in cui il Titolare del trattamento abbia deciso di non comunicare la violazione di dati personali agli Interessati, deve far menzione all'interno del registro delle violazioni delle ragioni a fondamento della propria decisione. In tal caso, resta comunque salvo il potere del Garante, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato per i diritti e le libertà degli Interessati, di chiedere che il Titolare del Trattamento provveda alla comunicazione.

11. Aggiornamento del registro delle violazioni.

- 11.1 Ricevuta l'Informativa, ed anche qualora – al termine delle verifiche di cui sub art. 8 – si decida di non procedere alla Notificazione al Garante e/o alla comunicazione agli

Interessati, il Titolare del trattamento dovrà provvedere all'annotazione del Data Breach nel citato registro delle violazioni, anche tenuto digitalmente tramite software e strutturato come da schema di registro delle violazioni, allegato sub 3).

- 11.2 Segnatamente, il registro dovrà contenere le seguenti informazioni: a) Codice Identificativo Data Breach; b) Data in cui è avvenuta la violazione; c) Data, orario e modalità in cui si è avuta conoscenza della violazione; d) Natura e causa della violazione; e) Descrizione del Data Breach; f) Categoria di interessati coinvolti; g) Numero di interessati coinvolti (anche approssimativo); h) Categoria di dati personali coinvolti; i) Numero di dati personali coinvolti (anche approssimativo); j) Descrizione dei sistemi e delle infrastrutture IT coinvolti nell'incidente, con indicazione della loro ubicazione; k) Misure di sicurezza tecniche e organizzative adottate al momento della violazione; l) Responsabili del Trattamento coinvolti, ove applicabile; m) Possibili conseguenze della violazione sugli interessati; n) Potenziali effetti negativi per gli interessati; o) Azioni intraprese in risposta all'incidente per mitigare il danno e ridurre la probabilità di una recidiva simile; p) Stima della gravità della violazione; q) Indicazione dell'avvenuta Notificazione al Garante (nei casi in cui non si sia proceduto con tale notifica, è necessario specificarne le ragioni); r) Comunicazione della violazione agli interessati (nei casi in cui non si sia proceduto con tale comunicazione, è necessario specificarne le ragioni); s) (eventuale) Numero di interessati a cui è stata comunicata la violazione; t) (eventuale) Canale utilizzato per la comunicazione agli interessati; u) Eventuale notifica ad altre autorità di controllo, organismi di vigilanza o di controllo o all'autorità giudiziaria o di polizia; v) Allegati prodotti tra cui Informativa e aggiornamenti Scheda Evento.

12. Definizione del piano di rimedio.

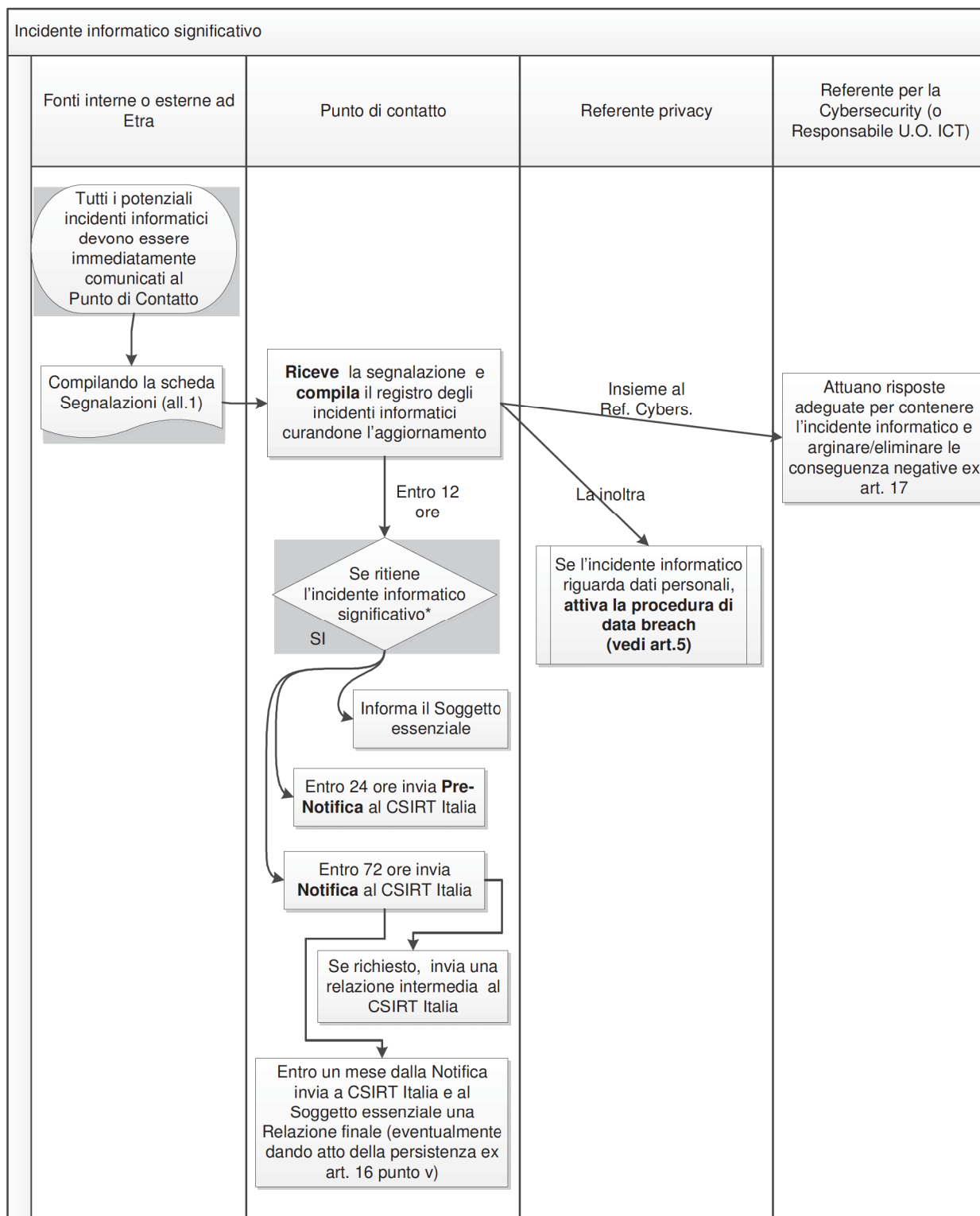
- 12.1. Una volta concluso il processo di registrazione e, ove necessario, di Notificazione al Garante e comunicazione della violazione di dati personali agli Interessati, il Titolare del trattamento, supportato dal DPO, svolge le seguenti attività:
- Analizza le cause che hanno determinato la violazione di dati personali;
 - Valuta le opportunità di miglioramento dei presidi e dei processi di monitoraggio delle violazioni dei dati personali, al fine di mettere in atto misure tecniche e organizzative adeguate a garantire il rispetto del Regolamento;
 - Definisce un piano di rimedio al fine di garantire un livello di sicurezza adeguato ai rischi in ordine alla protezione dei dati personali trattati.
- 12.2. Per ciascuna violazione di dati personali, il Titolare del trattamento è tenuto a verificare se l'incidente è il risultato di un errore umano o di un problema di natura tecnica e/o organizzativa e valutare misure correttive volte a prevenire il ripetersi dell'evento, coinvolgendo – laddove la causa sia di natura tecnica – il Punto di Contatto e il Referente della Cybersecurity o, ove non nominato, il Responsabile della U.O. ICT.
- 12.3. È, altresì, necessario che il Titolare del trattamento preveda attività di verifica periodiche volte a garantire l'efficacia delle procedure e degli strumenti di risposta agli incidenti relativi alle violazioni di dati personali.
- 12.4. Il CDA, insieme ai Soggetti Designati e il Referente Privacy, nonché con il supporto del DPO, deve periodicamente monitorare quelle Violazioni che hanno maggiore probabilità di verificarsi, in modo da applicare azioni correttive specifiche a fronte delle situazioni rilevate (di seguito, i **Test di Monitoraggio**).

13. Obblighi di comunicazione di ETRA quando opera in qualità di responsabile del trattamento

- 13.1. Quando ETRA agisce in qualità di Responsabile del Trattamento, in caso di Violazione dei dati personali, deve informare il proprio committente e/o il titolare del trattamento competente, senza ingiustificato ritardo secondo i tempi e i modi concordati negli accordi per il trattamento dei dati personali, fornendo la necessaria assistenza per garantire il rispetto degli obblighi di cui agli artt. 33 e 34 GDPR.

14. Procedura per l'ipotesi di Incidente Informatico Significativo

14.1. La procedura per l'ipotesi di Incidente Informatico Significativo adottata da ETRA è articolata nelle fasi riportate all'interno dei seguenti diagrammi di flusso:



14.2. Di seguito si riporta la descrizione delle attività previste per ciascuna fase del processo di Incidente Informatico Significativo di cui ai diagrammi di flusso sub art. 14.1, evidenziando che – a determinate condizioni – una ipotesi di Incidente Informatico Significativo può dar luogo anche ad un Data Breach e che dunque il processo afferente agli Incidenti Informatici Significativi tiene conto anche di tale ipotesi aggiuntiva.

15. Identificazione di un potenziale Incidente Informatico Significativo

- 15.1 La fase di rilevazione degli Incidenti Informatici ha l'obiettivo di individuare un potenziale Incidente Informatico Significativo, derivante dalla compromissione della disponibilità, dell'autenticità, dell'integrità o della riservatezza di dati conservati/trasmessi/elaborati o dei servizi offerti dai sistemi informativi e di rete di ETRA o accessibili attraverso di essi.
- 15.2 Tutti i potenziali Incidenti Informatici devono essere identificati e indirizzati immediatamente e senza ingiustificato ritardo al Punto di Contatto, mediante la compilazione della scheda Segnalazioni (All. 1).
- 15.3 Le Segnalazioni possono provenire da fonti interne e fonti esterne ad ETRA, quali (a titolo esemplificativo e non esaustivo):
- Strumenti informatici di monitoraggio di eventi di sicurezza o attraverso misure tecniche di sicurezza finalizzate alla protezione dei sistemi informativi;
 - Dipendenti/autorizzati al trattamento;
 - DPO;
 - Cittadini;
 - Utenti e/o Soci di ETRA;
 - Fornitori e terze parti;
 - Autorità di vigilanza;
 - Media (es. stampa, telegiornali, agenzie di informazione multimediale, ecc.).
- 15.4 Ogni soggetto che presta la propria attività a favore ETRA, che venga a conoscenza o sospetti che sia avvenuto un Incidente Informatico, deve inviare la Segnalazione al Punto di Contatto. La Segnalazione deve contenere un'indicazione chiara dell'evento sospetto verificatosi, delle caratteristiche dei dati coinvolti e, ove possibile, dell'unità organizzativa aziendale interessata dall'Incidente Informatico.
- 15.5 Il Punto di Contatto, una volta ricevuta la Segnalazione, deve:
- (i) trasmettere, immediatamente, la Segnalazione al Referente Privacy, affinché quest'ultimo – ove rilevi che i dati coinvolti dall'Incidente Informatico siano dati personali ai sensi del Regolamento, e non abbia già attivato la procedura di Data Breach a seguito di una Segnalazione avente il medesimo oggetto – attivi tale procedura, ai sensi e secondo quanto previsto negli articoli da 5 a 13 che precedono;
 - (ii) valutare, senza ingiustificato ritardo e comunque entro 12 ore dalla Segnalazione, se l'Incidente Informatico occorso sia qualificabile come Incidente Informatico Significativo o meno, al fine di dare attuazione a quanto prescritto al successivo art. 16.

16. Notificazioni e comunicazioni

16.1 Qualora, a seguito della valutazione sub 15.5(ii), sia appurato che l'Incidente Informatico si sostanzia in un Incidente Informatico Significativo, il Punto di Contatto deve:

- (i) informare, senza ritardo, il Soggetto essenziale dell'Incidente Informatico Significativo occorso;
- (ii) inviare al CSIRT Italia:
 - a) senza ingiustificato ritardo, e comunque entro 24 ore dalla ricezione della Segnalazione, una pre-notifica che, ove possibile, indichi/contenga: data e ora dell'Incidente Informatico Significativo; la descrizione dell'Incidente Informatico Significativo; se tale incidente possa ritenersi il risultato di atti illegittimi o malevoli o possa avere un impatto transfrontaliero; eventuali *screenshot*, *log* o altre prove rilevanti e le informazioni di contatto per eventuali *follow-up* (di seguito, la "**Pre-Notifica**");
 - b) senza ingiustificato ritardo, e comunque entro 72 ore dalla ricezione della Segnalazione, una notifica dell'Incidente Informatico Significativo che, ove possibile, aggiorni le informazioni di cui alla Pre-Notifica e indichi una valutazione iniziale dell'Incidente Informatico Significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione (di seguito, la "**Notifica**");

- (iii) inviare al CSIRT Italia, dopo la Notifica e solo qualora tale organismo ne faccia richiesta, una relazione intermedia sui pertinenti aggiornamenti della situazione;
 - (iv) inviare al CSIRT Italia ed al Soggetto essenziale, entro un mese dalla trasmissione della Notifica, una relazione finale dell'Incidente Informatico Significativo, che comprenda (di seguito, la **Relazione Finale**):
 - a. una descrizione dettagliata dell'Incidente Informatico Significativo, ivi inclusi la sua gravità e il suo impatto;
 - b. il tipo di minaccia o la causa originale (root cause) che ha probabilmente innescato tale incidente;
 - c. le misure di attenuazione adottate e in corso;
 - d. ove noto, l'impatto transfrontaliero dell'Incidente Informatico Significativo.
 - (v) ove l'Incidente Informatico Significativo sia ancora in corso al momento della trasmissione della Relazione Finale, dare atto di tale persistenza nella Relazione Finale medesima e, successivamente all'invio della stessa, trasmettere al CSIRT Italia ed al Soggetto essenziale una relazione mensile sui progressi e una nuova Relazione Finale entro un mese dalla conclusione della gestione dell'Incidente Informatico Significativo.
 - (vi) In ogni caso, sia che trattasi di Incidenti Informatici Significativi che di Incidenti Informatici, il Punto di Contatto dovrà riportare gli stessi nell'apposito registro degli incidenti informatici, che dovrà essere aggiornato qualora e man man si acquisiscano ulteriori dettagli ed informazioni in merito allo stesso.
 - (vii) qualora si sospetti che l'Incidente Informatico Significativo abbia carattere criminale, chiedere al CSIRT Italia di fornire i propri orientamenti sulla necessità o opportunità di segnalare l'incidente medesimo anche all'organo centrale del Ministero dell'Interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155 (c.d. Autorità di contrasto);
 - (viii) se ritenuto opportuno e qualora possibile, previa interlocuzione con il CSIRT Italia, comunicare, senza ingiustificato ritardo, ai destinatari dei servizi erogati da ETRA l'Incidente Informatico Significativo occorso che possa ripercuotersi negativamente sulla fornitura di tali servizi.
- 16.2 Il Punto di Contatto, se ritenuto opportuno e qualora possibile, sentito il CSIRT Italia, comunica, senza ingiustificato ritardo, ai destinatari dei servizi erogati da ETRA che sono potenzialmente interessati da una minaccia informatica significativa, misure o azioni correttive o di mitigazione che tali destinatari possono adottare in risposta a tale minaccia. Inoltre, sentito il CSIRT Italia, se ritenuto opportuno, il Punto di Contatto comunica ai medesimi destinatari anche la natura di tale minaccia informatica significativa.
- 16.3 In aggiunta all'obbligo di notifica di un Incidente Informatico Significativo di cui al comma 1 che precede, ove ritenuto opportuno, il Punto di Contatto può trasmettere, su base volontaria e previa condivisione con il Soggetto essenziale, a notificare al CSIRT Italia Incidenti Informatici, e/o minacce informatiche e/o i quasi-incidenti.

17. Risposta agli Incidenti Informatici Significativi

- 17.1 Dopo aver intercettato, classificato e, qualora significativi, segnalato gli Incidenti Informatici, il Punto di Contatto, in collaborazione con il Referente per la Cybersecurity o, ove non nominato, con il Responsabile della U.O. ICT, attuerà risposte adeguate e tempestive per contenere e/o rimuovere l'Incidente Informatico, nonché laddove possibile per arginare/eliminare le conseguenze negativa da esso prodotte, in conformità con le procedure tecniche aziendali sulla cybersicurezza.
- 17.2 Le procedure di risposta agli incidenti, di cui sub 17.1 che precede, devono comprendere le seguenti fasi:
- contenimento, per impedire che le conseguenze dell'Incidente Informatico si diffondano;
 - eradicazione, per impedire che l'Incidente Informatico continui o si ripeta;
 - recupero dall'Incidente Informatico, ove necessario.

- 17.3 Anche per le finalità di cui sub art. 17.1, all'atto della Pre-Notifica, il Punto di Contatto potrà richiedere al CSIRT orientamenti o consulenza sull'attuazione di possibili misure tecniche di mitigazione dell'Incidente Informatico Significativo, nonché di ricevere un'ulteriore supporto tecnico.

18. Varie ed Allegati

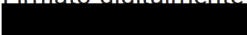
- 18.1. Per tutto quanto non previsto nella presente Regolamento troveranno applicazione le disposizioni normative e regolamentari, nazionali ed internazionali, di cui all'art. 4, e tutte le altre disposizioni afferenti alle ipotesi di Data Breach e di Incidenti Informatici.
- 18.2. Stante il possibile intreccio tra una ipotesi di Data Breach e una ipotesi di Incidente Informatico, qualora sia appurato che un Incidente Informatico determini anche una Violazione, le figure del DPO, del Referente Privacy e del Punto di Contatto dovranno confrontarsi e collaborare costantemente al fine di armonizzare l'agire aziendale e, dunque, di garantire l'ottimale rispetto di quanto previsto nella presente Regolamento e dalla normativa e regolamentazione vigente.
- 18.3. Sono allegati alla presente Regolamento a formarne parte integrante e sostanziale, i seguenti documenti:
- All. 1: Format Segnalazione;
 - All. 2: Format Scheda dell'evento.
 - All. 3: Format Registro delle Violazioni

19. Comunicazioni e recapiti

- 19.1. Ai fini della presente Regolamento, tutte le comunicazioni da indirizzare:
- **Al Titolare del trattamento**, dovranno essere operate mezzo mail al seguente indirizzo: privacy@etraspa.it;
 - **Al Referente Privacy**, dovranno essere operate mezzo mail al seguente indirizzo: privacy@etraspa.it;
 - **Al DPO**, dovranno essere operate mezzo mail al seguente indirizzo: dpo@etraspa.it;
 - **Al Punto di Contatto**, dovranno essere operate mezzo mail al seguente indirizzo: puntocontattoNIS2@etraspa.it;
 - **Al CDA**, dovranno essere operate mezzo mail al seguente indirizzo: segreteria generale@etraspa.it.

20. Entrata in Vigore ed Efficacia

20.1 La presente Regolamento entrerà in vigore e diverrà efficace dal giorno successivo alla sua pubblicazione sul sito internet istituzionale di ETRA S.p.A. Società Benefit.

1	16/09//2025	Aggiornamento indirizzo mail del punto di contatto	LEG 	PRE 
Rev.	Data	Descrizione modifiche	Redazione Firmato digitalmente da:  Data: 17/09/2025 09:01:49	Approvazione Firmato digitalmente da:  Data: 18/09/2025 11:13:58

Allegato 1

Scheda Segnalazione

C.A.

Referente privacy di ETRA S.p.A. Società Benefit

Pec/Mail: _____

E / Oppure

C.A.

Punto di Contatto di ETRA S.p.A. Società Benefit

Pec/Mail: _____

- **Segnalante (Nome/Cognome/C.F. o Ragione Sociale/P.Iva):**

_____;

- **Recapiti Segnalante (recapito telefonico; indirizzo pec e/o indirizzo e-mail):**

_____;

- **Ruolo Segnalante (ad es., dipendente con indicazione U.O., fornitore, socio, utente, cittadino):**

_____;

- **Descrizione Evento:**

_____;

Nel caso in cui l'Evento consista nello smarrimento/furto di dispositivi personali rispondere alle seguenti domande

Il dispositivo era protetto da un codice di accesso/password? _____

In caso di risposta positiva alla domanda precedente, era presente unitamente al dispositivo anche documentazione cartacea contenente l'indicazione della password di accesso al dispositivo personale?

I dati personali conservati all'interno del dispositivo sono protetti da un sistema di cifratura? _____

Sono stati oggetto di furto/smarrimento anche documenti cartacei contenenti dati personali conservanti unitamente al dispositivo personale? In caso positivo, che tipo di documenti? _____

Con che frequenza sono stati eseguiti i backup del dispositivo personale e a quando risale l'ultimo backup?

Dove sono stati salvati i backup effettuati sul dispositivo personale? _____

- **Data in cui è accaduto Evento:**

_____;

- **Data e modalità con cui si è venuti a conoscenza dell'Evento:**

_____;

- **Caratteristiche dei dati coinvolti, con specifica del se trattasi di dati personali:**

- **(ove possibile la specificazione) Unità Organizzativa aziendale interessata dalla violazione:**

- **La Violazione ha coinvolto sistemi informativi e/o di rete dove sono conservati, trasmessi, elaborati i dati e/o i servizi offerti da ETRA?**

☐ SI ☐ NO

- **(in caso di risposta affermativa alla domanda che precede) Indicazione dei sistemi informativi e/o di rete dove sono conservati, trasmessi, elaborati i dati e/o i servizi offerti da ETRA.**

(Luogo/Data):

Firma

Allegato 2

Scheda Evento

C.A.

CDA

DPO

Pec/Mail: _____

- **Referente Privacy (nome e cognome; e-mail):**

_____;

- **Soggetto Designato (nome e cognome; Area aziendale; e-mail):**

_____;

(oppure)

- **Responsabile del Trattamento (nome/cognome/C.F. oppure ragione sociale/P.iva):**

_____;

- **Recapiti Segnalante recapito telefonico; indirizzo pec e/o indirizzo e-mail):**

_____;

- **Titolare del Trattamento (nome/cognome/C.F. oppure ragione sociale/P.iva; e-mail/pec):**

_____;

- **DPO (nome/cognome/C.F. oppure ragione sociale/P.iva; e-mail/pec):**

_____;

- **Area e l'Unità Organizzativa aziendale coinvolta:**

_____;

- **Data e ora del Data Breach, anche solo presunta (specificando se è presunta):**

_____;

- **Data e ora in cui si è avuta conoscenza della Violazione:**

_____;

- **Fonte della Segnalazione (la Segnalazione dovrà essere allegata alla Scheda Evento):**

_____;

- **Natura della Violazione:**

_____;

- **Sintetica descrizione della Violazione:**

_____;

- **Numero e categoria di interessati coinvolti:**

_____;

- **Categoria e volume di dati personali di cui si presume la violazione:**

_____;

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

_____;

- **Indicazione dell'eventuale Responsabile del Trattamento coinvolto nella gestione del sistema informatico:**

_____;

- **Misure di sicurezza adottate al set di dati oggetto di violazione:**

_____;

- **Misure proposte per la mitigazione della Violazione:**

_____;

- **Esito della autovalutazione condotta mediante il *tool* messo a disposizione dal Garante:**

_____;

- **Altro:**

_____;

(Luogo/Data): _____

Firmato

(Il Referente Privacy): _____

(Il Soggetto Designato): _____

(oppure)

(Il Responsabile del Trattamento): _____

SEGUE

- **Esito Parere del DPO (in merito al livello di rischio del Data Breach e all'opportunità di notificarlo al Garante/ comunicarlo agli interessati (il Parere dovrà essere allegato alla Scheda Evento):**

_____;

- **Valutazione del Titolare del trattamento in merito al livello di rischio del Data Breach e all'esigenza della Notificazione al Garante/comunicazione agli interessati:**

_____;

(Luogo/Data): _____

Firmato

(Il Titolare del Trattamento): _____

(Luogo/Data): _____

(Il DPO): _____

Allegato 3

Format Registro delle Violazioni

All'interno del Registro delle violazioni sono contenute le seguenti informazioni:

- Codice data breach;
- Data in cui è avvenuta la violazione;
- Data, orario e modalità in cui si è venuti a conoscenza della violazione;
- Natura della violazione;
- Causa della violazione;
- Descrizione data breach;
- Categoria di interessati coinvolti;
- Numero di interessati coinvolti (anche approssimativo);
- Categoria di dati personali coinvolti;
- Numero di dati personali coinvolti (anche approssimativo);
- Descrizione dei sistemi e delle infrastrutture IT coinvolti nell'incidente;
- Misure di sicurezza tecniche e organizzative adottate al momento della violazione;
- Responsabili Esterni del Trattamento Coinvolti (Se Applicabile);
- Possibili conseguenze della violazione sugli interessati, in caso di:
 - perdita di confidenzialità;
 - perdita di integrità;
 - perdita di disponibilità;
- Potenziali effetti negativi per gli interessati;
- Stima della gravità della violazione;
- Azioni intraprese in risposta all'incidente;
- Notifica al Garante (Se NO, specificare le ragioni);
- Data della notifica al Garante;
- Comunicazione all'interessato (Se NO, specificare le ragioni);
- Numero di interessati a cui è stata comunicata la violazione;
- Canale utilizzato per la comunicazione agli interessati;
- Data della comunicazione all'interessato;
- Altre autorità di controllo, organismi di vigilanza o di controllo o all'autorità giudiziaria o di polizia a cui pure è stata, eventualmente, notificata la violazione;
- Eventuali note.