DETERMINA DIRETTORE GENERALE

N. 03 del 16.01.2024

OGGETTO: Approvazione procedura per la gestione di data breach e istituzione Registro data breach ai sensi del Regolamento (UE) n.679/2016.

PREMESSO CHE ai sensi della L.R. n.69/2011, come modificata in ultimo dalla L.R. n. 10/2018:

- A far data dal 1° gennaio 2012 è stata istituita l'Autorità per il servizio di gestione integrata dei rifiuti urbani Ato Toscana Sud quale ente rappresentativo di tutti i Comuni appartenenti all'ambito territoriale ottimale comprendente i comuni delle province di Arezzo, Siena e Grosseto (art. 30 e 31);
- L'Autorità ha personalità giuridica di diritto pubblico ed è dotata di autonomia organizzativa, amministrativa e contabile (art. 31);
- ai sensi dell'art. 33 della citata L.R. 69/2011 "[…], all'autorità si applicano le disposizioni di cui al titolo IV della parte I e quelle di cui ai titoli I, II, III, IV, V, VI e VII della parte II del decreto legislativo 18 agosto 2000, n.267 (Testo unico delle leggi sull'ordinamento degli enti locali)";
- Gli organi delle autorità servizio rifiuti sono l'assemblea, il direttore generale e il revisore unico dei conti (art. 34);

PRESO ATTO CHE:

- con Deliberazione dell'Assemblea n. 12 del 30.11.2023 è stato approvato il bilancio di previsione 2024-2026 dell'Autorità Ato Toscana Sud;
- con Determinazione del Direttore Generale n. 140 del 27.12.2023 è stato approvato il Piano Esecutivo di Gestione (PEG) 2024-2026;

CONSIDERATO CHE al sottoscritto è stato affidato l'incarico di Direttore Generale dell'Autorità Ato Toscana Sud con delibera di Assemblea n. 24 del 06.07.2022, perfezionato con contratto stipulato con il Presidente dell'Assemblea il 12.09.2022 a valle dell'intesa rilasciata dal Presidente della Regione Toscana;

RISCONTRATA pertanto la propria competenza all'emanazione del presente atto ai sensi dell'art. 107 del D.Lgs. 267/2000, dell'art. 10 dello Statuto dell'Autorità Ato Toscana Sud e dell'art. 18 del vigente regolamento di organizzazione dell'Ente;

RILEVATO che la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale e che l'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano;

VISTO "*Il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché*

alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)" ed in particolare la disposizione dell'art. 33 che introduce l'obbligo di notificare al Garante per la protezione dei dati personali incidenti sulla sicurezza che comportino la violazione dei dati personali (data breach) e di rendere nota la violazione stessa alle persone fisiche interessate;

VISTO il D.Lgs. 196/2023 e ss.mm.ii. «*Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*»;

TENUTO CONTO CHE la violazione dei dati personali è da intendersi come 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 tale da impedire al Titolare del trattamento di garantire l'osservanza dei principi relativi al trattamento dei dati personali di cui all'articolo 5 del Regolamento (UE) 2016/679;

RILEVATO che, per quanto sopra, è necessario istituire:
1. una Procedura data breach;
2. un registro interno data breach, dove vengono annotate sia le violazioni non notificabili che quelle notificabili;

DETERMINA

1. Le premesse formano parte integrante e sostanziale del presente atto.
2. di approvare la *«Procedura di gestione delle violazioni di dati personali (data breach)»* nel testo allegato al presente atto a formarne parte integrante e sostanziale (Allegato n. 1);
3. di stabilire che la suddetta procedura entri in vigore il giorno della sua pubblicazione all'Albo Pretorio on-line dell'Autorità;
4. di trasmettere il presente provvedimento al Responsabile del procedimento di pubblicazione per la pubblicazione all'Albo Pretorio *on-line* dell'Ente e, per le finalità di cui al D.Lgs. 33/2013 e ss.mm.ii., nella sezione "*amministrazione trasparente"* sottosezione "*disposizioni generali*" > "*atti generali*" > "*atti amministrativi generali"* del sito web istituzionale;
5. di comunicare la *«Procedura di gestione delle violazioni di dati personali (data breach)»* approvata con il presente atto ai Responsabili di Area, al personale dipendente e al Data Protection Officer dell'Ente.

IL DIRETTORE GENERALE
Ing. Enzo Tacconi (*)
(*) *Documento amministrativo informatico sottoscritto con firma digitale ai sensi dell'art.24 del D.Lgs. 82/2005*

Visto di regolarità contabile attestante la copertura finanziaria
(D.lgs. 18.08.2000, n.267 art. 153)

Si attesta la copertura finanziaria della spesa prevista dalla presente determinazione ai sensi dell'art. 153 e la compatibilità del programma dei conseguenti pagamenti con i relativi stanziamenti di cassa.

Data _____

IL DIRIGENTE DELL'AREA
AMMINISTRATIVA E CONTABILE
Marco Morgione (*)
(*) *Documento amministrativo informatico sottoscritto con firma digitale ai sensi dell'art.24 del D.Lgs. 82/2005*

ORIGINALE IN FORMATO ELETTRONICO CON FIRME DIGITALI Le firme, in formato digitale, sono state apposte sull'originale elettronico del presente atto ai sensi dell'art. 24 del D.Lgs. 7/3/2005 n. 82 e s.m.i. L'originale elettronico del presente atto è conservato negli archivi informatici dell'ATO Toscana Sud ai sensi dell'art. 22 del D.Lgs. 7/3/2005 n. 82.

PROCEDURA DI GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI

Approvato con Determina del Direttore Generale n. 03 del 16.01.2024

PREMESSA

La normativa vigente in termini di Protezione dei Dati Personali, di cui al Regolamento (UE) 679/2016 – Regolamento sulla Protezione dei Dati (di seguito anche il "Regolamento") e dal D.Lgs. 196/2003 – Codice in materia di Protezione dei Dati Personali (di seguito anche il "Codice"), come modificato dal D.Lgs. 101/2018, ha l'obiettivo di proteggere i dati personali degli interessati garantendo che un uso non corretto delle informazioni possa danneggiare o ledere le libertà fondamentali e la dignità degli interessati.

Le tipologie di dati personali trattati dall'Autorità sono costituite principalmente sia da dati personali c.d. comuni, che da "*particolari categorie di dati personali*" quali dati di salute e dati giudiziari.

L'Autorità predispone il presente documento nell'ambito del proprio sistema organizzativo a tutela dei dati personali degli interessati. È di fondamentale importanza predisporre azioni da attuare nell'eventualità in cui si presentino violazioni concrete, potenziali o sospette di dati personali, ciò al fine di evitare rischi per i diritti e le libertà degli interessati, nonché danni economici all'Autorità e per poter riscontrare nei tempi e nei modi previsti dalla normativa europea l'Autorità Garante e/o gli interessati.

Le sanzioni previste dal GDPR per omessa notifica di Data Breach all'Autorità di Controllo o omessa comunicazione agli interessati o entrambi gli adempimenti, nei casi in cui siano soddisfatti i requisiti di cui agli artt. 33 e 34 GDPR, può comportare l'applicazione in capo all'Autorità di una sanzione amministrativa pecuniaria fino a 10 milioni di euro o fino al 2% del "fatturato" annuo totale dell'esercizio precedente, anche accompagnata da una misura correttiva ai sensi dell'art. 58 c. 2.

SCOPO

Lo scopo del presente documento è di individuare un flusso per la gestione delle violazioni dei dati personali trattati dall'Autorità in qualità di Titolare del trattamento (di seguito "Titolare del trattamento"). Il presente documento descrive le modalità operative adottate dall'Autorità per poter rispettare quanto previsto dagli artt. 33 e 34 del Regolamento (UE) 679/2016: in particolare viene definito un flusso di attività da attivarsi nel caso in cui dovesse manifestarsi un evento di violazione dei dati personali rispetto a quanto definito esplicitamente dalla normativa vigente.

Finalità della presente procedura è di fornire una descrizione generale del processo di gestione delle violazioni di Dati Personali e le relative indicazioni operative immediate per poter procedere con la rilevazione, la valutazione ed il contenimento della violazione; vengono inoltre, date indicazioni per la comunicazione all'Autorità Garante per la Protezione dei Dati Personali ed eventualmente all'interessato.

La presente procedura è soggetta ad integrazioni e modifiche alla luce dell'evoluzione normativa italiana ed europea, nonché delle prassi che saranno, di volta in volta, riscontrate all'interno dell'Ente.

AMBITO DI APPLICAZIONE OGGETTIVO

L'art. 4, punto 12, del Regolamento definisce la "*violazione dei dati personali*" come "*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 tal caso si può verificare:

- la "*distruzione*" dei dati: si verifica ogni qual volta gli stessi non esistono più o non esistono più in una forma che sia di qualche utilità per il titolare del trattamento;
- il "*danno*": quando i dati personali sono stati modificati, corrotti o non sono più completi;
- la "*perdita*" dei dati personali: è il caso in cui i dati risultano comunque esistere, ma il titolare del trattamento potrebbe averne perso il controllo o l'accesso, oppure non averli più in possesso.

Esempio: perdita di dati personali può essere la perdita o il furto di un dispositivo contenente una copia della banca dati dei clienti del titolare del trattamento; oppure il caso in cui l'unica copia di un insieme di dati personali sia stata crittografata da un ransomware (malware del riscatto) oppure dal titolare del trattamento mediante una chiave non più in suo possesso;

- il "*trattamento non autorizzato o illecito*": si verifica quando viene effettuata una divulgazione di dati personali (o l'accesso da parte di) a destinatari non autorizzati a ricevere (o ad accedere) ai dati oppure quando viene svolta qualsiasi altra forma di trattamento in violazione del Regolamento.

La presente procedura si applica, pertanto, nel caso in cui si registrino incidenti che possono minacciare la sicurezza dei dati personali trattati dall'Ente, la cui immediata conseguenza consiste nel fatto che il titolare del trattamento non è più in grado di garantire l'osservanza dei principi relativi al trattamento come stabiliti dall'art. 5 del Regolamento.
Come evidenziato dal Gruppo di Lavoro ex art. 29 nelle linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento "*mentre tutte le violazioni di dati personali sono incidenti di sicurezza non tutti gli incidenti di sicurezza sono necessariamente violazioni di dati personali*".

AMBITO SOGGETTIVO DI APPLICAZIONE

La presente procedura è rivolta a tutti i soggetti che a qualsiasi titolo trattano dati personali di

competenza del Titolare del trattamento (ATS):

a) i lavoratori dipendenti, nonché coloro che a qualsiasi titolo, e quindi a prescindere dal tipo di rapporto contrattuale intercorrente, abbiano accesso ai dati personali trattati nel corso delle prestazioni richieste per conto del Titolare del trattamento;

b) qualsiasi soggetto (persona fisica o persona giuridica) diverso dal destinatario interno che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento, abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento (art. 28 Regolamento) o di autonomo Titolare;

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 dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia.

TIPOLOGIA DI VIOLAZIONI DI DATI PERSONALI

Si possono distinguere tre categorie di violazioni di dati:

a) violazione della riservatezza: quando si ha una divulgazione di dati o un accesso agli stessi non autorizzato o accidentale;

b) violazione dell'integrità: quando il dato è alterato in modo accidentale o non autorizzato;

c) violazione della disponibilità: quando in modo accidentale o per dolo il Titolare non accede ai dati o i dati sono stati distrutti.

Una violazione di dati personali può comprendere una o tutte e tre le categorie o anche loro combinazioni.

Una violazione della riservatezza o dell'integrità del dato è facilmente individuabile. Meno chiara è l'individuazione di una violazione della disponibilità[1] del dato. Ci sarà sempre una violazione della disponibilità del dato nel caso di perdita o distruzione permanente dei dati. L'indisponibilità dei dati è quindi da considerare una violazione quando potrebbe avere un impatto significativo sui diritti e le libertà delle persone fisiche.

Non si tratta invece di una violazione quando l'indisponibilità è dovuta a interruzioni programmate per la manutenzione.

Esempio:

le violazioni di dati personali possono includere:

1. divulgazione di dati personali a soggetti non autorizzati;
2. perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
3. perdita o furto di documenti cartacei;
4. infedeltà aziendale (ad esempio: Data Breach causato da una persona interna che, avendo autorizzazione ad accedere ai dati, ne produce una copia che viene distribuita in ambiente

[1] L'"*accesso*" è una componente fondamentale della "disponibilità". In tal senso, si veda il documento NIST SP800-53rev4, che definisce la "disponibilità" come la "garanzia di un accesso e un uso tempestivi e affidabili delle informazioni", nonché la norma ISO/IEC 27000:2016, che definisce la "disponibilità" come la "proprietà di essere accessibile e utilizzabile su richiesta da un soggetto autorizzato.

pubblico);
5. accesso abusivo (ad esempio: Data Breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
6. casi di pirateria informatica (usurpazione delle credenziali di accesso – fishing);
7. banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo "owner";
8. virus o altri attacchi al sistema informatico o alla rete aziendale;
9. violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o armadi contenenti archivi con informazioni riservate);
10. smarrimento di pc portatili, devices o attrezzature informatiche aziendali;
11. invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario;
12. pubblicazioni errate non rispettose dei principi in materia di protezione dei dati personali;

GESTIONE DELLA VIOLAZIONE DI DATI PERSONALI

In caso di concreta, sospetta e/o avvenuta violazione dei dati personali, è indispensabile assicurare che la stessa sia affrontata immediatamente e correttamente al fine di minimizzare l'impatto della violazione e prevenire che si ripeta.
Il coordinamento delle attività di gestione di una violazione di dati personali, con particolare riferimento agli obblighi di comunicazione e notifica imposti dal Regolamento, è assicurato dal DPO, dall'Amministratore di Sistema e dal Responsabile per la transizione al digitale. Di seguito le fasi di gestione di una violazione di dati personali:

A) <u>RILEVAZIONE E SEGNALAZIONE</u> di una potenziale violazione:

CHI	Chiunque ne venga a conoscenza (personale, collaboratori, fornitori, responsabili del trattamento, Titolare, utenti esterni, DPO, etc.)
A CHI	Al Dirigente/Responsabile dell'Area/Servizio interessato dall'incidente di sicurezza, informando anche l'Amministratore di Sistema ed il Dirigente per la transizione al digitale;
QUANDO	Non appena se ne viene a conoscenza
COME	Utilizzando le vie più brevi (e-mail, telefonicamente, di persona)

Se al momento della rilevazione dell'incidente di sicurezza non è disponibile una descrizione particolareggiata dell'evento, è comunque essenziale procedere immediatamente alla comunicazione anche con informazioni incomplete.

B) <u>RACCOLTA DELLE INFORMAZIONI</u> sulla potenziale violazione:

CHI	Il Dirigente/Responsabile dell'Area/Servizio interessato dall'incidente di sicurezza deve coordinare la raccolta delle informazioni nel più breve tempo possibile, anche con il supporto del DPO, dell'Amministratore di Sistema e del Dirigente per la

	transizione al digitale.
QUANDO	Appena ricevuta la segnalazione
COME	Utilizzando il modulo di cui all'Allegato A - Modulo di comunicazione Data Breach e raccogliendo tutte le informazioni dai soggetti coinvolti nella segnalazione

L'Allegato A, debitamente compilato, permette di condurre una valutazione iniziale al fine di stabilire se si sia effettivamente verificata un'ipotesi di Data Breach (violazione) e se sia necessaria un'indagine più approfondita dell'accaduto.

C) COMUNICAZIONE DELLA VIOLAZIONE

CHI	Il Dirigente/Responsabile dell'Area/Servizio interessato dall'incidente di sicurezza
QUANDO	Non appena raccolte le informazioni di base sulla violazione e comunque nel più breve tempo possibile da quando riceve la notizia
A CHI	Al Titolare del trattamento, al DPO, all'Amministratore di Sistema ed al Responsabile per la transizione al digitale
COME	A mezzo protocollo

D) VALUTAZIONE DELLA VIOLAZIONE

Una volta stabilito che un Data Breach è avvenuto, il Titolare del trattamento con il supporto del DPO, dell'Amministratore di Sistema e del Responsabile per la transizione al digitale, deve stabilire:

- la gravità della violazione;
- se esistono azioni che possano limitare i danni che la violazione potrebbe causare;
- se sia necessario notificare la violazione all'Autorità Garante per la Protezione dei Dati Personali (ove sia probabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche);
- se sia necessario comunicare la violazione agli interessati (ove la violazione presenti un elevato rischio per i diritti e le libertà delle persone fisiche).

Al fine di individuare la necessità di notificazione all'Autorità Garante e di comunicazione agli interessati, il Titolare del trattamento, con il supporto del DPO, dell'Amministratore di Sistema e del Responsabile per la transizione al digitale, valuterà la gravità della violazione tenendo in debita considerazione i principi e le indicazioni di cui agli artt. 33 e 34 del Regolamento.
La gravità di una violazione di dati personali è definita come la stima dell'entità del potenziale impatto sulle persone fisiche derivante dalla violazione medesima. Di seguito si riportano i principali elementi definiti nelle linee guida WP250 del Gruppo di Lavoro Art. 29 che devono essere considerati nella valutazione di impatto della gravità di una violazione sulla base delle informazioni raccolte:

- Tipo di violazione (distruzione, modifica, perdita, divulgazione);

- Natura, carattere sensibile e volume di dati personali;
- Facilità di identificazione delle persone fisiche;
- Gravità delle conseguenze per le persone fisiche;
- Danno potenziale alle persone fisiche che potrebbe derivare dalla violazione comprese le categorie degli interessati e dei dati personali coinvolti e la permanenza a lungo termine delle conseguenze del danno (furto di identità, danni fisici, disagio psicologico, danni reputazionali);
- Caratteristiche particolari dell'interessato;
- Caratteristiche particolari del titolare;
- Numero di persone fisiche interessate;
- Aspetti generali (il titolare del trattamento deve considerare tanto la gravità dell'impatto potenziale sui diritti e sulle libertà delle persone fisiche e quanto la probabilità che tale impatto si verifichi.

Le valutazioni degli elementi sopra elencati servono per stabilire la necessità di notifica al Garante (se è probabile un rischio per la libertà e diritti delle persone fisiche) e di comunicazione anche agli interessati (nel caso in cui tale rischio sia elevato).

E) NOTIFICA AL GARANTE (se necessaria)

Ai sensi dell'art. 33 del Regolamento "*In caso di violazione di dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'art. 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo*".

CHI	Il titolare del trattamento
A CHI	Autorità Garante per la protezione dei dati personali
QUANDO	Senza ingiustificato ritardo e, ove possibile entro 72 ore dal momento in cui ne è venuto a conoscenza[2]
COME	Accedendo al servizio telematico, messo a disposizione del Garante sul proprio sito web, dedicato al data breach

F) COMUNICAZIONE AI SOGGETTI INTERESSATI (se necessaria)

CHI	Il titolare del trattamento

[2] Il Gruppo di lavoro articolo 29 nelle Linee Guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679, ritiene che il titolare del trattamento debba considerarsi a "conoscenza" della violazione, nel momento in cui è ragionevolmente certo che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali.

A CHI	alle persone fisiche i cui dati sono stati violati
QUANDO	Senza ingiustificato ritardo
COME	contattando direttamente gli interessati oppure rendendo nota la violazione e le possibili conseguenze mediante pubblicazione accessibile alle categorie di interessati

Una volta valutata la necessità di effettuare la comunicazione della violazione dei dati agli interessati, l'Autorità provvede senza ingiustificato ritardo.
La comunicazione deve contenere:

- il nome e i dati di contatto del Responsabile della protezione dei dati (DPO);
- la descrizione delle probabili conseguenze della violazione dei dati personali;
- 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, se del caso, per attenuarne i possibili effetti negativi. Nel caso in cui la segnalazione diretta richieda uno sforzo ritenuto sproporzionato, è possibile utilizzare una comunicazione pubblica.

REGISTRO DEI DATA BREACH

Indipendentemente dalla valutazione circa la necessità di procedere alla notificazione all'Autorità Garante e/o alla comunicazione della violazione dei dati personali ai soggetti interessati, ogni qualvolta si verifichi un incidente di sicurezza comunicato attraverso l'Allegato A, l'Ente è tenuto a documentarlo attraverso la compilazione dell'apposito Registro (Allegato B).
Il Registro dei Data Breach contiene almeno le seguenti informazioni:

- data e ora della violazione;
- luogo violazione;
- tipo violazione;
- Dispositivo oggetto della violazione;
- numero persone coinvolte dalla violazione;
- categorie di interessati coinvolte;
- categorie di dati personali coinvolte;
- effetti della violazione;
- contromisure adottate;
- data consultazione DPO;
- se sia stata effettuata notifica all'Autorità Garante;
- se sia stata effettuata comunicazione agli interessati;
- esito procedura.

Il Registro dei Data Breach deve essere continuamente aggiornato e messo a disposizione del Garante, qualora l'Autorità chieda di accedervi.
Tutta la documentazione relativa ai processi di gestione dei dati breach deve essere conservata nel sistema documentale dell'Ente in apposito fascicolo appositamente costituito.

Il Direttore Generale

Ing. Enzo Tacconi (*)

(*) Documento informatico sottoscritto con firma digitale
ai sensi del D.Lgs. 82/2005

Allegato A – Modulo di comunicazione Data Breach

In caso di incidente di sicurezza che possa comportare una violazione di dati personali il

Dirigente/Responsabile dell'Area/Servizio interessato, ai fini di una valutazione e gestione dell'incidente stesso e, in caso di violazione accertata, ai fini della notifica al Garante nonché alla comunicazione agli interessati, deve compilare il presente modulo,

Le informazioni relative all'incidente devono essere raccolte tempestivamente ed inviate al Titolare, al DPO, all'Amministratore di Sistema ed al Dirigente per la transizione al digitale.

Se al momento della rilevazione dell'incidente di sicurezza non è disponibile una descrizione dettagliata dell'evento, è comunque essenziale procedere immediatamente alla comunicazione dell'incidente per una prima valutazione d'impatto, anche con informazioni incomplete.

Laddove necessario, alla prima valutazione possono seguirne altre, in base alle informazioni che vengono acquisite nella prosecuzione dell'indagine.

Informazioni di contatto:

Dati identificativi del segnalante (nome e cognome):

Area/Servizio di riferimento:

Telefono: E-mail:

Informazioni sull'incidente di sicurezza

Data scoperta violazione	
Luogo incidente	
Data e ora dell'incidente	
Descrizione sintetica dell'incidente	
Tipo di violazione	□ Lettura (presumibilmente è stato effettuato un accesso ai dati ma i dati non sono stati copiati) □ Copia (i dati sono ancora presenti sui sistemi del Titolare ma copiati dall'autore della violazione) □ Alterazione (i dati sono presenti sui sistemi del Titolare ma sono stati alterati) □ Cancellazione (i dati non sono più sui sistemi del Titolare e non sono neppure in possesso dell'autore della violazione)

	□ Furto (i dati non sono più sui sistemi del Titolare ma sono presumibilmente in possesso dell'autore della violazione) □ Indisponibilità (i dati sono presenti sui sistemi del Titolare ma non sono disponibili per un certo periodo di tempo) □ Altro:_____ _____
Dispositivo oggetto della violazione	□ Personal computer fisso □ Computer portatile □ Server □ Storage □ Dispositivo di rete □ Dispositivo mobile □ Sistema di backup □ Documento cartaceo □ Altro: _____
Denominazione della/e banca/che dati oggetto di Data Breach e breve descrizione della violazione dei dati personali ivi trattati	
Categorie di soggetti coinvolti	□ Personale dipendente □ Soggetti vulnerabili □ Collaboratori e consulenti □ Operatori economici □ Utenti del SII □ Altri soggetti_____
Categorie di dati personali oggetto della violazione	□ Dati anagrafici/codice fiscale □ Dati di contatto □ Dati di accesso e di identificazione (es. username, password, altro) □ Dati relativi a soggetti vulnerabili □ 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 □ Dati economico finanziari (es. numero carta di credito, IBAN, etc.) □ Dati genetici □ Dati relativi alla salute

	□ Dati relativi all'orientamento sessuale □ Dati giudiziari □ Dati biometrici
Breve descrizione di eventuali azioni poste in essere al momento della scoperta della violazione	Descrizione
Numero di persone colpite dalla violazione dei dati personali trattati	Descrizione
Natura dei dati coinvolti (compilare le sezioni sottostanti)	Descrizione
a) Dati personali generici	Descrizione
b) Dati particolari: □ origine razziale ed etnica □ convinzioni religiose, filosofiche o di altro genere, opinioni politiche; □ **adesione a partiti, sindacati** □ **Dati genetici** □ **Dati relativi alla salute** □ **Dati relativi all'orientamento sessuale** □ **Dati giudiziari** □ Dati biometrici	Descrizione
c) informazioni che possono essere utilizzate per commettere furti d'identità (es. dati di accesso e di identificazione, codice fiscale e copie di carta d'identità, passaporto o carte di credito)	Descrizione
d) informazioni personali relative a soggetti fragili (es. anziani, disabili)	Descrizione
e) informazioni relative a performance lavorative, salario o stato di famiglia, sanzioni disciplinari, che potrebbero causare danni significativi alle persone	Descrizione
Altro:	Descrizione
La violazione può comportare pregiudizio alla reputazione, perdita di riservatezza di dati protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale	SI/NO Descrizione

significativo	
Gli interessati rischiano di essere privati dell'esercizio del controllo sui dati personali che li riguardano	SI/NO Descrizione
Misure tecniche e organizzative adottate precedentemente alla violazione (es. pseudonimizzazione, cifratura dei dati personali, etc.)	Descrizione
Misure adottate per scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati successivamente alla violazione	Descrizione
Notificazione del Data Breach all'Autorità Garante	SI/NO Se sì, notificato in data: Dettagli:
Comunicazione del Data Breach agli interessati	SI/NO Se sì, notificato in data: Dettagli:

Allegato B – Registro dei Data Breach

n. violaz.	**Data e ora violazione**	**Luogo violazione**	**Tipo violazione**	**Dispositivo oggetto della violazione**	**Nr. persone colpite dalla violaz**	**Categorie interessati coinvolti**	**Categorie dati oggetto della violazione**	**Effetti della violazione**	**Misure applicate ai dati oggetto della violazione**	**Misure assunte per contenere la violazione dei dati**	**Date di consultaz. DPO/PDO**	**Data comunicaz. violazione agli interessati**	**Data notifica al garante**	**Esito procedura**