PROCEDURA DI NOTIFICA DI VIOLAZIONI DEI DATI PERSONALI (DATA BREACH) AI SENSI DEL REGOLAMENTO UE n. 679/2016

Approvato con Determina A.U. n. 34 del 20/12/2022

INDICE

1.PREMESSA

NAPOLI SERVIZI S.P.A., ai sensi del Regolamento Europeo 2016/679 (di seguito anche "GDPR"), è tenuta a mantenere sicuri i dati personali trattati nell'ambito dello svolgimento delle proprie attività e ad agire senza ingiustificato ritardo in caso di violazione dei dati personali stessi. A tal fine - come previsto dall'art.33 e 34 del GDPR e regolamentato dalle Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679 ("Linee Guida WP250") - è fondamentale definire le azioni da adottare in caso di violazioni concrete, potenziali o sospette di dati personali, volte ad evitare rischi per i diritti e le libertà degli interessati, nonché danni economici all'Azienda e per poter fornire riscontro all'Autorità Garante e, ove previsto e/o necessario, agli Interessati nei tempi e nelle modalità previste dalla normativa vigente.

2. OBIETTIVO DELLA PROCEDURA

Obiettivo di questa procedura è l'individuazione di un flusso di azioni per la gestione delle violazioni dei dati personali trattati da NAPOLI SERVIZI S.P.A. in qualità di Titolare del trattamento. Nel caso in cui l'Azienda sia nominata Responsabile del trattamento, il flusso di azioni è regolamentato nel successivo art. 7.

3. DEFINIZIONE DI DATA BREACH

Per violazione di dati personali si intende ogni infrazione alla sicurezza delle informazioni gestite da NAPOLI SERVIZI S.P.A. che comporti - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o, comunque, trattati dal Titolare.

Le violazioni dei dati personali possono essere classificate in base ai seguenti tre principi di sicurezza delle informazioni:

- violazione della riservatezza, in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali;
- violazione dell'integrità, in caso di alterazione non autorizzata o accidentale dei dati personali;
- violazione della disponibilità, in caso di accidentale o non autorizzata perdita di accesso o distruzione di dati personali.

Le violazioni di dati personali possono verificarsi a seguito di diversi eventi, che possono includere:

- divulgazione di dati confidenziali a persone non autorizzate;
- perdita o furto di dati o di supporti sui quali i dati sono memorizzati;
- perdita o furto di documenti cartacei;

- infedeltà aziendale;
- accesso abusivo ai sistemi informatici con successiva divulgazione delle informazioni acquisite;
- casi di pirateria informatica;
- alterazione o distruzione di banche dati senza autorizzazione del Titolare del trattamento;
- inoculazione di virus o altri attacchi al sistema informatico o alla rete aziendale;
- violazione delle misure di sicurezza fisica (a titolo esemplificativo, effrazione di porte o finestre, serrature, altro);
- smarrimento di dispositivi informatici aziendali (a titolo esemplificativo, laptop, tablet, altro).

4. DESTINATARI DELLA PROCEDURA

La presente procedura è rivolta a tutti i soggetti che a qualsiasi titolo trattano i dati personali di competenza del Titolare del trattamento:

- i lavoratori dipendenti e tutti coloro che a qualsiasi titolo, a prescindere dal tipo di rapporto intercorrente, abbiano accesso ai dati personali trattati nel corso dello svolgimento delle attività per conto dell'Azienda,
- qualsiasi soggetto, persona fisica o persona giuridica, esterno all'organizzazione aziendale che, in ragione del rapporto contrattuale in essere con l'Azienda, abbia accesso ai dati personali e agisca in qualità di Responsabile del trattamento o di autonomo Titolare del Trattamento.

È opportuno, infine, un richiamo, rivolto a tutti i dipendenti, al rispetto delle procedure di gestione password e credenziali, definite agli art. 7.1 e 7.2 del RIA (Regolamento Informatico Aziendale) adottato con Determina AU n. 28 del 27.05.2020.

La mancata conformità alle regole comportamentali previste nella presente procedura potrà comportare l'adozione di provvedimenti disciplinari, a carico del personale inadempiente, ovvero la risoluzione dei contratti in essere con soggetti terzi inadempienti.

5. RACCOLTA DELLE SEGNALAZIONI DI DATA BREACH

A. SEGNALAZIONE PERVENUTA DA CANALI INTERNI

Le segnalazioni interne di eventi anomali possono pervenire dal personale dell'Azienda e vanno inviate, non oltre 12 ore dalla conoscenza della violazione, al Responsabile per la protezione dei dati (Data Protection Officer), in ottemperanza all'art. 37 del Reg. (UE) n. 679/2016 (in prosieguo anche "DPO"), al seguente indirizzo: rpd@napoliservizi.com o al Responsabile del Trattamento Dati (in prosieguo anche "RTD"), al seguente indirizzo: m.baggio@napoliservizi.com entrambi individuati all'interno

dell'organizzazione aziendale di NAPOLI SERVIZI S.P.A.

Per la segnalazione è richiesta la compilazione dell'Allegato A – *Modulo di comunicazione Data Breach.*

B. SEGNALAZIONE PERVENUTA DA CANALI ESTERNI

Le segnalazioni possono pervenire anche da fonti esterne: fornitori, collaboratori, utenti, Responsabili esterni del trattamento. Inoltre, ogni Interessato può segnalare, anche solo in caso di sospetto, che i propri dati personali siano stati utilizzati abusivamente o fraudolentemente da un terzo e richiedere all'Azienda la verifica dell'eventuale violazione.

Le segnalazioni devono essere indirizzate al DPO non oltre 12 ore dalla conoscenza della violazione al seguente indirizzo: rpd@napoliservizi.com. Il DPO informa immediatamente il RTD in merito alla segnalazione ricevuta.

Per la segnalazione da parte di soggetti terzi, essa va fatta scrivendo all'indirizzo del DPO sopra riportato, indicando almeno i seguenti contenuti minimi:

- Dati anagrafici e di contatto del segnalante che ha rilevato la violazione o l'evento con possibile violazione dei dati
- Ruolo del segnalante (fornitori, collaboratori, utenti, Responsabili esterni, ecc.)
- Data in cui è stata scoperta o si è verificata la violazione o l'evento con possibile violazione dei dati
- Luogo in cui si è verificata la violazione o l'evento con possibile violazione dei dati
- Breve descrizione della violazione dei dati personali trattati o dell'evento con possibile violazione dei dati
- Dati anagrafici di eventuali ulteriori soggetti coinvolti nella violazione dei dati personali trattati o nell'evento.

In caso di segnalazioni – interne o esterne - pervenute ad altri soggetti/funzioni interne, i riceventi devono immediatamente inoltrare le segnalazioni al DPO o al RTD agli indirizzi sopra indicati.

6. GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI

La segnalazione di eventi incidentali che comportano e/o possono comportare violazioni di dati personali sono gestite dal DPO - d'intesa con il RTD - che provvede ad informare tempestivamente l'Amministratore Unico, in quanto Titolare del trattamento, e procede mettendo in atto le misure indicate

nel presente documento.

Per la corretta gestione di un *data breach,* il DPO e il RTD procedono secondo le seguenti fasi:

Fase 1. Identificazione e indagine preliminare

Fase 2. Risk assessment: contenimento della violazione e valutazione del rischio

Fase 3. Notifica all'Autorità Garante competente

Fase 4. Comunicazione agli interessati

Fase 5. Documentazione della violazione

Fase 1. Identificazione e indagine preliminare

Il DPO e il RTD avviano un'analisi preliminare finalizzata alla raccolta dei dati concernenti la violazione segnalata, alla disamina delle informazioni raccolte e contenute nel modulo di segnalazione, coinvolgendo le aree interne coinvolte nella segnalazione e, in caso di violazioni riguardanti i sistemi informativi, l'Unità Organizzativa Servizi Informativi. Nel caso di coinvolgimento di soggetti esterni, il DPO attende le risultanze dell'analisi preliminare da questi effettuate, secondo le modalità descritte nel paragrafo 8.

A seguito dell'analisi effettuata, volta ad accertare che nell'evento di sicurezza rilevato siano stati effettivamente violati dati personali la cui titolarità è attribuita a Napoli Servizi, laddove non risulti esservi stata una violazione di dati personali, il DPO registra l'evento nel Registro Data Breach[1] (il cui modello è riportato nell'Allegato D), annotando l'esito dell'istruttoria preliminare effettuata.
Laddove dall'indagine preliminare emerga una violazione di dati personali, si procede con un'indagine più approfondita dell'evento, dando corso alla fase di Risk assessment (Fase 2).

Fase 2: Risk assessment: contenimento della violazione e valutazione del rischio

Il DPO e il RTD coinvolgono uno o più referenti individuati all'interno dell'Area interessata dall'evento e, per violazioni che riguardano i sistemi informativi, uno o più referenti individuati all'interno dell'Unità Organizzativa Servizi Informativi ai fini della costituzione di un gruppo di lavoro (di seguito "Gruppo Data Breach") per poter effettuare una valutazione del rischio per i diritti e le libertà delle persone fisiche al fine di stabilire se:

- sia necessario notificare la violazione all'Autorità Garante per la Protezione dei dati personali (ove sia

[1] Il Registro Data Breach (registro interno delle violazioni), è il documento in cui vanno documentate tutte le segnalazioni di violazioni di dati personali, comprese le circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

probabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche[2]).

- sia necessario comunicare la violazione agli interessati (ove la violazione presenti un elevato rischio per i diritti e le libertà delle persone fisiche, a seconda della natura dei dati personali oggetto di violazione e se la gravità delle probabili conseguenze per gli interessati è elevata[3]).

La tabella che segue presenta i principali fattori che devono essere presi in considerazione per la valutazione del Risk assessment, come definiti nelle Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679 ("Linee Guida WP250") -Articolo 29 Working Party.

TABELLA – FATTORI RILEVANTI

Aspetti generali	Valutazione della gravità dell'impatto potenziale sui diritti e sulle libertà delle persone fisiche e della probabilità che tale impatto si verifichi.
Tipo di violazione	Violazione della riservatezza – in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali; Violazione dell'integrità – in caso di alterazione non autorizzata o accidentale dei dati personali; Violazione della disponibilità – in caso di accidentale o non autorizzata perdita di accesso o distruzione di dati personali.
Natura, carattere sensibile e volume dei dati personali	Categorie particolari di dati o combinazione di dati personali, grandi quantità di dati personali relative a molte persone coinvolti nella violazione.
Facilità di identificazione delle persone fisiche	Facilità di identificazione, diretta o indiretta tramite abbinamento con altre informazioni, di specifiche persone fisiche sulla base dei dati personali compromessi dalla violazione
Gravità delle conseguenze per le persone fisiche	Danno potenziale alle persone fisiche che potrebbe derivare dalla violazione comprese le

[2] Gli obblighi di notifica all'Autorità di Controllo scaturiscono dal superamento di una soglia di rischio tale da essere non trascurabile laddove "non sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche" (così l'art. 33 del GDPR).

[3] Potenziali rischi elevati per i diritti e le libertà delle persone fisiche possono essere quelli che determinano un danno fisico, materiale o immateriale ed in particolare:
- possibili discriminazioni, furti o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione;
- qualsiasi altro danno economico o sociale significativo;
- il rischio per gli interessati di essere privati dei loro diritti e delle loro libertà o l'impedimento dell'esercizio del controllo sui dati personali che li riguardano;
- un trattamento di dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;
- una valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;
- un trattamento di dati di persone fisiche vulnerabili, in particolare minori;
- un trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati (così l'art. 34 del GDPR ed il Considerando 75).

	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 del titolare	La natura e il ruolo del Titolare del trattamento e delle sue attività possono influire sul livello di rischio per le persone a seguito di una violazione.
Caratteristiche particolari dell'interessato	La violazione coinvolge in particolare dati personali di minori o altre persone fisiche vulnerabili.
Numero di persone fisiche interessate	Numero di persone fisiche coinvolte nella violazione.

La valutazione può essere agevolata, anche dalla consultazione dell'Allegato B "Esempi di violazioni dei dati personali e dei soggetti a cui notificarle" estratto dalle "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679 – Articolo 29 Working Party" e dalle "Linee guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali" (riportate nell'Allegato C). In entrambi i documenti sono riportati alcuni esempi, sia pure non esaustivi, che possono altresì contribuire a distinguere tra rischio e rischio elevato per i diritti e le libertà delle persone fisiche.

La valutazione viene effettuata sulla base dei criteri definiti nelle citate Linee guida che prendono in considerazione i due (2) parametri della:

- gravità: intesa come rilevanza degli effetti pregiudizievoli che la violazione è in grado di produrre sui diritti e le libertà delle persone coinvolte (a titolo esemplificativo, se la violazione impedisca il controllo da parte dell'interessato sulla diffusione dei propri dati);
- probabilità: intesa come grado di possibilità che si verifichino uno o più eventi temuti (a titolo esemplificativo, la perdita di ogni traccia dei dati).

Sulla base degli elementi sopra indicati:

i. il Gruppo Data Breach stima la gravità e la probabilità della violazione e classifica il rischio, esprimendosi, con apposita relazione finale, in merito al data breach rilevato ed ai rischi per i diritti e le libertà delle persone fisiche evidenziati, circa l'esigenza di notifica all'Autorità di Controllo/comunicazione agli interessati:
   - nel caso in cui il rischio sia considerato non rilevante e sia improbabile che il data breach presenti rischi per i diritti e le libertà degli interessati, ed il Gruppo Data Breach non ritenga necessario procedere con la notifica della violazione, la relazione specifica le motivazioni di tale scelta;
   - nel caso in cui sia accertato un rischio rilevante, il Gruppo Data Breach evidenzia nella relazione

l'esigenza di notifica all'Autorità di Controllo secondo le modalità indicate nella Fase 3, specificando la motivazione di tale scelta;

- nel caso in cui sia accertato un rischio elevato, il Gruppo Data Breach evidenzia nella relazione se occorre o meno procedere anche alla comunicazione agli Interessati, secondo le modalità indicate nella Fase 4, specificando la motivazione di tale scelta.

ii. Nel caso in cui sia accertata la violazione, il Gruppo Data Breach - al fine di contenerne le conseguenze - con sollecitudine:

- valuta l'adozione di azioni idonee al contenimento della violazione (a titolo esemplificativo, utilizzo dei file di backup per recuperare dati persi o danneggiati, cambio dei codici di accesso, altro);
- identifica i soggetti deputati all'attuazione delle azioni individuate;

iii. il DPO - con il supporto del RTD - documenta le risultanze della valutazione del rischio nel *Registro Data Breach*;

iv. il DPO – con il supporto del RTD - comunica all'Amministratore Unico, in quanto Titolare del trattamento, adeguate informazioni sulla violazione riscontrata e gli esiti della valutazione del rischio, anticipando la misura che si intende attuare.

Fase 3: Notifica all'Autorità Garante competente

Laddove, a seguito della valutazione sulla violazione effettuata nei termini di cui alla Fase 2 che precede, risulti un rischio tale da rendere necessaria la notifica della violazione dei dati personali all'Autorità di controllo, l'Azienda - secondo quanto prescritto dal Regolamento (UE) 2016/679 - deve provvedervi senza ingiustificato ritardo e, ove possibile entro 72 ore dal momento in cui ne è venuta a conoscenza.

Il DPO – con il supporto del RTD - provvede a redigere il documento di notifica della violazione, utilizzando idonea modulistica (in particolare, quella messa a disposizione dall'Autorità Garante in allegato al Provvedimento del 30 luglio 2019 sulla notifica delle violazioni dei dati personali). Il documento compilato viene sottoposto dal DPO a preventiva firma dell'Amministratore Unico ed inviato dal DPO - senza ingiustificato ritardo e, ove possibile entro 72 ore dal momento in cui si è venuti a conoscenza della violazione - all'Autorità di controllo tramite posta certificata (PEC), all'indirizzo PEC dell'Autorità: dcrt@pec.gpdp.it.

La notifica per essere considerata valida ed efficace deve comprendere:

a. la descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati coinvolti nonché le categorie e il numero approssimativo di

dati personali implicati;

b. il nome e i dati di contatto del Responsabile della protezione dei dati e, se necessario, di altro contatto utile cui rivolgersi per eventuali informazioni;
c. le probabili conseguenze della violazione dei dati personali;
d. le misure adottate e/o da adottarsi da parte del Titolare del trattamento per rimediare e/o contenere le conseguenze della violazione dei dati personali.

E', altresì, consigliabile riportare:

e. la data anche presunta della violazione e del momento della sua scoperta;
f. l'indicazione del luogo in cui è avvenuta la violazione dei dati, specificando altresì se essa sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili.

Laddove non sia possibile fornire immediatamente una o più informazioni tra quelle sopra elencate, sono inviate le informazioni in quel momento a disposizione del Titolare del trattamento, con riserva di successivi approfondimenti.

Qualora la notifica all'Autorità di controllo non sia effettuata entro il termine di 72 ore dalla conoscenza dell'evento, il DPO deve dare evidenza dei motivi del ritardo nella comunicazione all'Autorità di controllo.

Fase 4: Comunicazione agli interessati

Laddove, a seguito della valutazione sulla violazione effettuata nei termini di cui alla Fase 2 che precede, risulti un rischio elevato per i diritti e le libertà delle persone fisiche, secondo quanto prescritto dal Regolamento (UE) 2016/679, per individuare se procedere o meno alla comunicazione agli interessati, il Gruppo Data Breach valuta se sia soddisfatta una delle seguenti condizioni:

- sono state adottate le misure tecniche e organizzative adeguate di protezione e tali misure sono 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;
- sono state successivamente adottate misure atte a evitare il sopraggiungere di un rischio elevato per i diritti e le libertà delle persone fisiche.

In assenza di almeno una delle presenti condizioni, la violazione dei dati personali deve essere comunicata agli Interessati, senza ingiustificato ritardo.

La comunicazione agli Interessati è predisposta dal DPO – con il supporto del RTD - e sottoscritta a firma dell'Amministratore Unico; essa deve contenere almeno:

a. la natura della violazione dei dati personali;
b. il nome e i dati di contatto del Responsabile della protezione dei dati personale e, se necessario, di altro contatto utile cui rivolgersi per eventuali informazioni;

c. le probabili conseguenze della violazione dei dati personali;
d. la descrizione delle misure adottate e/o da parte del Titolare del trattamento per rimediare e/o contenere le conseguenze della violazione dei dati personali.

Quanto alle modalità di comunicazione, si devono sempre privilegiare la modalità di comunicazione diretta con i soggetti interessati (quali, lettera o e-mail). Il messaggio deve essere comunicato in maniera evidente e trasparente. Nel caso in cui la segnalazione diretta richieda uno sforzo ritenuto sproporzionato, si può utilizzare una comunicazione pubblica purché idonea a raggiungere l'interessato.

La necessità di effettuare la comunicazione agli Interessati può derivare anche da una richiesta dell'Autorità di controllo a cui sia stata effettuata la notifica della violazione: l'Autorità, infatti, nel caso in cui, dalla disamina della notifica, valuti la probabilità che la violazione dei dati personali presenti un rischio elevato anche se non rilevato dal Titolare del trattamento, può chiedere al Titolare stesso di darne comunicazione agli Interessati.

Fase 5: Documentazione della violazione

Indipendentemente dalle risultanze della valutazione della violazione, ogni qualvolta perviene la segnalazione di un evento di violazione di dati personali, il DPO – con il supporto del RTD - è obbligato a documentarlo.

In caso di accertato rischio derivante dalla violazione, a seconda della gravità rilevata, devono essere indicate nel *Registro Data Breach*:

- le conseguenze della violazione
- i provvedimenti adottati per porvi rimedio o attenuarne le conseguenze
- l'eventuale notificazione all'Autorità di Controllo
- l'eventuale comunicazione all'Interessato.

La corretta tenuta del *Registro Data Breach* ed il suo costante aggiornamento sono di competenza del DPO, con il supporto del RTD. Il DPO raccoglie e conserva tutti i documenti relativi a ciascuna violazione, compresi i provvedimenti adottati per porvi rimedio.

Tale documentazione è resa disponibile all'Autorità di controllo per le verifiche di competenza.

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

Nei casi in cui NAPOLI SERVIZI S.P.A. agisce in qualità di Responsabile del trattamento per conto di un Titolare del trattamento terzo, laddove il DPO ed il RTD segnalino notizie di eventi anomali, che possono aver determinato una violazione potenziale o concreta di dati personali, l'Azienda, nella persona

dell'Amministratore Unico, deve informare il Titolare del trattamento per conto del quale svolge operazioni di trattamento su dati personali, senza ingiustificato ritardo e non al più tardi di 12 ore dal momento in cui ha conoscenza della violazione o, comunque, secondo i tempi e i modi concordati con il Titolare stesso.

Il DPO ed il RTD devono inoltre avviare tempestivamente un'analisi preliminare finalizzata alla verifica della violazione e, se del caso, il *risk assessment*, seguendo le modalità di cui alle fasi I e II o seguendo le specifiche modalità messe in atto dal Titolare e con esso concordate - da concludersi, in considerazione della complessità della verifica, entro 24 o 36 ore dalla conoscenza della violazione, o, comunque, secondo i tempi e i modi concordati con il Titolare stesso; l'esito delle attività svolte nelle suddette fasi viene trasmesso dall'Amministratore Unico - dopo aver ricevuto adeguate informazioni dal DPO e dal RTD - al Titolare del trattamento.

L'evento accaduto e le risultanze delle analisi condotte (analisi preliminare ed, eventualmente, *risk assessment*) vengono registrate dal DPO, con il supporto del RTD, all'interno del *Registro Data Breach*, avendo cura di segnalare che l'attività è stata svolta in relazione al ruolo di NAPOLI SERVIZI S.P.A. quale Responsabile esterno del trattamento.

8. OBBLIGHI DI COMUNICAZIONE DI UN RESPONSABILE NEI CONFRONTI DELL'AZIENDA

Quando un terzo agisce in qualità di Responsabile del trattamento dei dati personali di cui NAPOLI SERVIZI S.P.A. è Titolare del trattamento, in caso di violazione dei dati personali, il Responsabile del trattamento deve:

- informare tempestivamente NAPOLI SERVIZI S.P.A. (in quanto Titolare del trattamento) e comunque non oltre 12 ore dalla conoscenza della violazione, inviando una segnalazione al DPO al seguente indirizzo: rpd@napoliservizi.com come descritto al par. 5 lett. B;
- avviare tempestivamente un'analisi preliminare finalizzata alla verifica della violazione da concludersi, in considerazione della complessità della verifica, entro 24 o 36 ore dalla conoscenza della violazione;
- collaborare con NAPOLI SERVIZI S.P.A. per consentire di adempiere agli obblighi previsti dalla normativa di cui agli artt. 33 e 34 del GDPR.

Nel caso in cui l'evento segnalato non risulti essere una violazione di dati personali, il Responsabile comunica l'esito dell'istruttoria a NAPOLI SERVIZI S.P.A. Il DPO – avvalendosi del supporto del RTD - procede con la registrazione dell'evento e delle risultanze dell'indagine preliminare svolta dal Responsabile nel *Registro Data Breach*.

Laddove dall'indagine preliminare emerga una violazione di dati personali, il Responsabile del trattamento raccoglie tutte le informazioni di dettaglio necessarie per effettuare la valutazione del rischio e le trasmette al DPO per dar corso ad un'indagine più approfondita dell'evento.

NAPOLI SERVIZI S.P.A., in qualità di Titolare del trattamento, ricevute le informazioni, procede secondo le prescrizioni di cui alle Fasi 2, 3, 4 e 5 del paragrafo 6 del presente documento, richiedendo, se necessario, il coinvolgimento del Responsabile del trattamento.

Presa Visione:

Resp. Trattamento Dati
Rag. Mario Baggio

Resp. Protezione Dati
Dott.ssa Angela Longobardi

L'Amministratore Unico

Procedura di notifica di violazioni dei dati personali (Data Breach) ai sensi del Regolamento UE 679/2016

Allegato A - Modulo di comunicazione Data Breach

Comunicazione di Data Breach	**Note**
Data e ora in cui è stata scoperta la violazione	
Data e ora in cui si è verosimilmente verificata la violazione	
Luogo in cui si è verificata la violazione (specificando se è avvenuta a seguito di smarrimento di dispositivo o supporti informatici)	
Estremi del soggetto che ha riferito della violazione	
Dati di contatto del soggetto che ha riferito della violazione	
Ruolo aziendale / professionale ricoperto dal segnalante	
Denominazione della/e banca/che dati oggetto di Data Breach e breve descrizione della violazione dei dati personali ivi trattati:	
Categorie e numero approssimativo di interessati coinvolti nella violazione:	
Breve descrizione di eventuali azioni poste in essere al momento della scoperta della violazione	
Eventuali note	
Data e ora di redazione modulo	
Firma del segnalante	

Allegato B - Esempi di violazioni dei dati personali e dei soggetti a cui notificarle, secondo quanto riportato dalle "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679 – Articolo 29 Working Party".

Esempio	Notifica all'autorità di controllo?	Comunicazione all'interessato?	Note/raccomandazioni
i. Un titolare del trattamento ha effettuato un backup di un archivio di dati personali crittografati su una chiave USB. La chiave viene rubata durante un'effrazione.	No.	No.	Fintantoché i dati sono crittografati con un algoritmo all'avanguardia, esistono backup dei dati, la chiave univoca non viene compromessa e i dati possono essere ripristinati in tempo utile, potrebbe non trattarsi di una violazione da segnalare. Tuttavia, se la chiave viene successivamente compromessa, è necessaria la notifica.
ii. Un titolare del trattamento gestisce un servizio online. A seguito di un attacco informatico ai danni di tale servizio, i dati personali di persone fisiche vengono prelevati. Il titolare del trattamento ha clienti in un solo Stato membro.	Sì, segnalare l'evento all'autorità di controllo se vi sono probabili conseguenze per le persone fisiche.	Sì, segnalare l'evento alle persone fisiche a seconda della natura dei dati personali interessati e se la gravità delle probabili conseguenze per tali persone è elevata.	
iii. Una breve interruzione di corrente di alcuni minuti presso il call center di un titolare del trattamento impedisce ai clienti di chiamare il titolare del trattamento e accedere alle proprie registrazioni.	No.	No.	Questa non è una violazione soggetta a notifica, ma costituisce comunque un incidente registrabile ai sensi dell'articolo 33, paragrafo 5. Il titolare del trattamento deve conservare adeguate registrazioni in merito.
iv. Un titolare del trattamento subisce un attacco tramite *ransomware* che provoca la	Sì, effettuare la segnalazione all'autorità di controllo, se vi sono probabili conseguenze per le	Sì, effettuare la segnalazione alle persone fisiche, a seconda della natura dei dati personali	Se fosse stato disponibile un backup e i dati avessero potuto essere ripristinati in tempo utile non sarebbe stato necessario segnalare la violazione all'autorità di

cifratura di tutti i dati. Non sono disponibili backup e i dati non possono essere ripristinati. Durante le indagini, diventa evidente che l'unica funzionalità dal *ransomware* era la cifratura dei dati e che non vi erano altri *malware* presenti nel sistema.	persone fisiche in quanto si tratta di una perdita di disponibilità.	interessati e del possibile effetto della mancanza di disponibilità dei dati, nonché di altre possibili conseguenze.	controllo o alle persone fisiche, in quanto non si sarebbe verificata nessuna perdita permanente di disponibilità o di riservatezza. Tuttavia, qualora l'autorità di controllo fosse venuta a conoscenza dell'incidente con altri mezzi, avrebbe potuto prendere in considerazione lo svolgimento di un'indagine al fine di valutare il rispetto dei requisiti di sicurezza più ampi di cui all'articolo 32.
v. Una persona telefona al call center di una banca per segnalare una violazione dei dati. La persona ha ricevuto l'estratto conto mensile da un soggetto diverso. Il titolare del trattamento intraprende una breve indagine (ossia la conclude entro 24 ore) e stabilisce con ragionevole certezza che si è verificata una violazione dei dati personali e che vi è una potenziale carenza sistemica che potrebbe comportare il coinvolgimento già occorso o potenziale di altre persone fisiche.	Sì.	La comunicazione va effettuata soltanto alle persone fisiche coinvolte in caso di rischio elevato e se è evidente che altre persone fisiche non sono state interessate dall'evento.	Se dopo ulteriori indagini si stabilisce che l'evento ha interessato un numero maggiore di persone fisiche è necessario comunicare questo sviluppo all'autorità di controllo, e il titolare del trattamento deve informarne le altre persone fisiche interessate se sussiste un rischio elevato per loro.
vi. Un titolare del trattamento gestisce un mercato online e ha clienti in più Stati membri. Tale mercato subisce un attacco informatico a	Sì, segnalare l'evento all'autorità di controllo capofila se la violazione riguarda un trattamento transfrontaliero.	Sì, dato che la violazione potrebbe comportare un rischio elevato.	Il titolare del trattamento dovrebbe prendere delle misure, ad esempio forzare il ripristino delle password degli account interessati, e altri provvedimenti per attenuare il rischio. Il titolare del trattamento dovrebbe altresì

seguito del quale i nomi utente, le password e la cronologia degli acquisti vengono pubblicati online dall'autore dell'attacco.			considerare qualsiasi altro obbligo di notifica, ad esempio ai sensi della direttiva NIS, trattandosi di un fornitore di servizi digitali.
vii. Una società di *hosting* di siti web che funge da responsabile del trattamento individua un errore nel codice che controlla l'autorizzazione dell'utente. A causa di tale vizio, qualsiasi utente può accedere ai dettagli dell'account di qualsiasi altro utente.	In veste di responsabile del trattamento, la società di *hosting* di siti web deve effettuare la notifica ai clienti interessati (i titolari del trattamento) senza ingiustificato ritardo. Supponendo che la società di *hosting* di siti web abbia condotto le proprie indagini, i titolari del trattamento interessati dovrebbero essere ragionevolmente certi di aver subito una violazione e pertanto è probabile che vengano considerati "a conoscenza" della violazione nel momento in cui hanno ricevuto la notifica da parte della società di *hosting* (il responsabile del trattamento). Il titolare del trattamento deve quindi effettuare la notifica all'autorità di controllo.	Qualora non vi siano probabili rischi elevati per le persone fisiche non è necessario effettuare una comunicazione a tali persone.	La società di *hosting* di siti web (responsabile del trattamento) deve prendere in considerazione qualsiasi altro obbligo di notifica (ad esempio ai sensi della direttiva NIS, trattandosi di un fornitore di servizi digitali). Qualora non vi sia alcuna prova che tale vulnerabilità sia sfruttata presso uno dei suoi titolari del trattamento, la violazione potrebbe non essere soggetta all'obbligo di notifica, tuttavia potrebbe essere una violazione da registrare o essere il segno di un mancato rispetto dell'articolo 32.
viii. Le cartelle cliniche di un ospedale sono indisponibili per un periodo di 30 ore a causa di un attacco informatico.	Sì, l'ospedale è tenuto a effettuare la notifica in quanto può verificarsi un rischio elevato per la salute e la tutela della vita privata dei pazienti.	Sì, informare le persone fisiche coinvolte.	
ix. I dati personali di un gran numero	Sì, segnalare l'evento all'autorità	Sì, segnalare l'evento alle	

di studenti vengono inviati per errore a una mailing list sbagliata con più di 1000 destinatari.	di controllo.	persone fisiche coinvolte in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze.	
x. Una e-mail di marketing diretto viene inviata ai destinatari nei campi "a:" o "cc:", consentendo così a ciascun destinatario di vedere l'indirizzo e-mail di altri destinatari.	Sì, la notifica all'autorità di controllo può essere obbligatoria se è interessato un numero elevato di persone, se vengono rivelati dati sensibili (ad esempio una mailing list di uno psicoterapeuta) o se altri fattori presentano rischi elevati (ad esempio, il messaggio di posta elettronica contiene le password iniziali).	Sì, segnalare l'evento alle persone fisiche coinvolte in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze.	La notifica potrebbe non essere necessaria se non vengono rivelati dati sensibili e se viene rivelato soltanto un numero limitato di indirizzi di posta elettronica.

Allegato C - Registro Data Breach

N. segnalazione	Data segnalazione	Natura segnalazione/ violazione (tipo di incidente)	Ruolo NAPOLI SERVIZI (Titolare / Responsabile)	Titolare terzo /Responsabile esterno eventualmente coinvolto	Categoria Interessati coinvolti	Categoria dati coinvolti	Entità di dati personali violati	Conseguenze segnalazione /violazione	Contromisure adottate	Notifica Garante Si/No	Comunicazione Interessati Si/No