Allegato 1
Procedura *data breach*

Sommario

1. Fonti normative e regolamentari di riferimento

1. Ai fini del presente Regolamento si applica la seguente normativa:
    a. 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, di seguito anche indicato come “GDPR”; in particolare gli articoli 33 e 34 e i Considerando 85, 87 e 88.
    b. D.lgs. 30 giugno 2003 n. 196 – Codice in materia di protezione dei dati personali – così come modificato dal D.lgs. n. 101/2018, e dal D.L. 8 ottobre 2021, n. 139 convertito dalla L. 3 dicembre 2021, n. 205.
    c. Parere 03/2014 sulla notifica delle violazioni dei dati personali adottato il 25 marzo 2014 dall’EDPB (ex Gruppo di lavoro art. 29 – Working party art. 29).
    d. Linee guida sulla notifica delle violazioni dei dati personali - WP250 (ex Gruppo di lavoro art. 29 – Working party art. 29) adottate il 3 ottobre 2017 e modificate in data 6 febbraio 2018.

2. Scopo del documento e ambito di applicazione

1. Con il presente documento l’ASPAL, in qualità di Titolare del trattamento, stabilisce le corrette modalità di gestione del *data breach* alla luce della normativa vigente in materia di trattamento dei dati personali.

3. Violazione dei dati personali o *data breach*

1. Come disciplinato dall'art. 4 par. 12 del Regolamento (UE) 2016/679, la violazione dei dati personali è "*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*." Si verifica la "distruzione" dei dati quando gli stessi non esistono più o non esistono più in una forma che sia di qualche utilità per il titolare del trattamento; si ha la "perdita" dei dati personali quando i dati potrebbero esistere, ma il titolare del trattamento ne ha perso il controllo o l'accesso, o non ne è più in possesso; il trattamento non autorizzato o illecito può includere la divulgazione di dati personali a (o l'accesso da parte di) destinatari non autorizzati a ricevere (o ad accedere a) i dati.
2. Il considerando 85 precisa che: "*una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata. Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo*."

4. Tipologie di *data breach*

1. Le violazioni possono essere classificate in base ai seguenti tre principi della sicurezza delle informazioni[1]:
    a. "**violazione della riservatezza**", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
    b. "**violazione dell'integrità**", in caso di modifica non autorizzata o accidentale dei dati personali;
    c. "**violazione della disponibilità**", in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.
2. Gli eventi che determinano una violazione dei dati personali possono riguardare il trattamento di dati contenuti su supporti informatici o su supporti cartacei. Di seguito si riportano, a mero titolo esemplificativo e non esaustivo, alcuni esempi.
    a. Eventi relativi ai trattamenti **informatici**: malfunzionamento di un software, rottura di componenti hardware, esecuzione erronea di un comando o di una procedura, erronea pubblicazione di dati sui siti dell'ASPAL o su altri siti facenti capo al Sistema Regione, fornitura e comunicazione dei dati a persona diversa dall'interessato, guasti alla rete, accesso non autorizzato alla rete da soggetti esterni, perdita o furto di un dispositivo mobile o di un supporto di memorizzazione (smartphone, chiavetta USB, tablet, notebook, hard disk, etc.), rivelazione abusiva di credenziali, truffa informatica esterna o esterna (*ransomware*, *malware*, uso illegittimo delle informazioni dal personale interno e

[1] Parere 03/2014 del Gruppo di Lavoro articolo 29.

autorizzato);

b. Eventi relativi ai trattamenti **cartacei**: distruzione accidentale di documenti dovuta a incendio, allagamento o ad altri eventi o calamità naturali, smarrimento di documenti, fornitura involontaria dei dati a persona diversa dall'interessato, distruzione volontaria dei documenti da soggetti interni o esterni (es. incendio doloso o distruzione con altri mezzi), accesso non autorizzato con lettura ed eventuale estrazione di copia dei documenti da parte di personale interno non autorizzato o esterno, furto e divulgazione dei documenti.

5. Segnalazione del *data breach* da parte dei dipendenti e collaboratori

1. La segnalazione di un possibile *data breach* può provenire dall'esterno (cittadini, fornitori, enti istituzionali, etc.) o dall'interno, da parte di dipendenti e collaboratori dell'ASPAL durante lo svolgimento della propria attività lavorativa.
2. Il personale impiegato a vario titolo, i somministrati, i collaboratori e i tirocinanti, qualora rilevino personalmente una violazione di dati personali o ricevano la segnalazione dall'esterno, ossia qualora siano a conoscenza di un evento che possa costituire un potenziale *data breach*, sono tenuti a darne immediata comunicazione al Direttore del proprio Servizio e a inviare la segnalazione via e-mail all'account aspal.databreach@regione.sardegna.it utilizzando l'apposito modulo in allegato al presente documento (All. 2).
3. L'account aspal.databreach@regione.sardegna.it viene monitorato quotidianamente dal Referente data *breach* e dal Referente privacy.
4. Tutti i soggetti menzionati al comma 2 contribuiscono e partecipano, per quanto di loro conoscenza e competenza, alle valutazioni e alle analisi sulle circostanze che hanno causato un fatto o un evento che determini un'acclarata o una potenziale violazione dei dati personali.

6. Segnalazione del *data breach* da parte dei fornitori

1. I fornitori dell'ASPAL, nominati Responsabili del trattamento, qualora vengano a conoscenza di una presunta violazione di dati personali ne informano immediatamente per le vie brevi il referente (Direttore del servizio, responsabile del procedimento o comunque il dipendente ASPAL indicato nella nomina e/o nel contratto) e successivamente inviano una Pec all'indirizzo agenzialavoro@pec.regione.sardegna.it, come previsto nel documento di nomina a Responsabile del trattamento, e una mail all'indirizzo aspal.databreach@regione.sardegna.it, utilizzando il modulo allegato alla nomina a responsabile del trattamento.
2. Il fornitore garantisce assistenza, fornisce tutte le informazioni utili e svolge le dovute attività al fine di consentire che il Gruppo di gestione del *data breach* possa effettuare una corretta valutazione dell'evento e procedere con i dovuti adempimenti, quali le segnalazioni all'Autorità Garante per la protezione dei dati personali e, se del caso, all'Autorità di Pubblica Sicurezza.

7. Gruppo di gestione del *data breach*

1. È costituito il "*Gruppo di gestione del data breach"* con la funzione di valutare e gestire le segnalazioni di *data breach.*
2. Il Gruppo di gestione del *data breach* è composto da:

   a) Il **Responsabile del *data breach***, nominato con determinazione del Direttore

Generale, che assume la funzione di coordinatore del Gruppo. Il Responsabile del data breach individua un sostituto con propria determinazione;

b) Il **Titolare del trattamento**, nella persona del Direttore Generale;

c) **Il Dirigente del Servizio** delegato al trattamento oggetto della violazione;

d) **Il Dirigente del Servizio Sistemi Informativi**, se la violazione concerne i sistemi informativi;

e) Il **Referente privacy,** con funzioni di supporto al Responsabile del data *breach* per tutte le attività legate all'analisi e alla gestione dell'evento;

f) Il **DPO/RPD**;

3. Possono essere coinvolti tutti i soggetti (fornitori e personale di cui all'art. 5 comma 2) che possano apportare un contributo utile alle valutazioni e alle attività.
4. Le riunioni tra i componenti del gruppo possono avvenire anche con strumenti telematici e in modalità asincrona.
5. Sono componenti necessari: il Responsabile del data *breach* o il suo delegato, il DPO o il suo delegato e il Titolare del trattamento o un suo delegato. L'individuazione dei delegati avviene con atto formale.

8. Processo di gestione del *data breach*

1. Il Gruppo è deputato allo svolgimento delle seguenti attività:
    a. analisi tecnica dell'evento;
    b. valutazione della gravità dell'evento;
    c. analisi del rischio (in caso di violazione accertata);
    d. raccomanda le misure dirette a mitigare e a contenere il danno;
    e. individuazione delle misure da adottare per porre rimedio alla violazione e per attenuarne gli effetti;
    f. altre segnalazioni dovute.
2. Il Responsabile del data breach o il Referente privacy, ricevuta la segnalazione, provvedono a darne immediata comunicazione ai componenti del gruppo (inclusi i sostituti formalmente individuati) al loro account istituzionale. La comunicazione, avente ad oggetto "Data Breach: convocazione del gruppo di gestione" deve essere inviata entro 24 ore dal momento in cui ne sono venuti a conoscenza[2]. Fin dalla prima comunicazione il Responsabile del data *breach* e il Referente privacy possono proporre l'archiviazione per le segnalazioni manifestamente infondate. Se i componenti del gruppo non si oppongono, si procede all'archiviazione con la conclusione del procedimento senza l'iscrizione dell'evento nel registro del data *breach*.
3. Salvo quanto indicato al comma 2, il Gruppo di gestione del data *breach* svolge un'analisi preliminare (comma 1 lettere a e b) al fine di verificare se i fatti per cui si procede costituiscono un mero incidente di sicurezza o se vi sia la violazione di dati personali e se questa presenti un rischio per i diritti e le libertà delle persone fisiche.
4. Qualora, a seguito della prima analisi, il Gruppo di gestione del data breach verifichi

[2] Il Gruppo si riunisce nel minor tempo possibile e comunque entro 24 ore tenendo conto che l'eventuale comunicazione al Garante Privacy deve essere effettuata entro 72 ore dal momento in cui il Titolare o il suo Delegato ne sono venuti a conoscenza, ossia quando si è ragionevolmente certi che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali (Gruppo di lavoro Articolo 29 per la protezione dei dati - Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679 https://ec.europa.eu/newsroom/article29/items/612052)

l'esistenza di elementi tali da escludere la possibile violazione dei dati personali, provvede all'archiviazione. L'archiviazione determina la conclusione del procedimento, senza iscrizione dell'evento nel Registro del data *breach*.

5. Una volta effettuate le analisi congiunte (comma 1 lettere c, d, e, f) e constatata la violazione dei dati personali, il Gruppo di gestione del data *breach* redige una sintetica relazione contenente le risultanze e le valutazioni svolte in merito alla necessità di procedere con la notifica della violazione al Garante e agli interessati. La relazione viene inviata al Titolare per le dovute considerazioni.
6. Il Titolare, valutata la relazione, approva le risultanze o assume differenti determinazioni, con particolare riferimento alla necessità di procedere con la notifica del *data breach* al Garante e agli interessati.
7. Il Responsabile del data breach, sulla base di quanto determinato dal Titolare, provvede a:
    a. inserire l'evento nel Registro delle violazioni (o Registro *data breach*), dando atto dell'eventuale notifica al Garante Privacy e agli interessati;
    b. notificare l'evento al Garante Privacy entro 72 ore dalla conoscenza della violazione, tenendo conto che le informazioni possono essere fornite in fasi successive, specie nei casi in cui si rendano necessari ulteriori approfondimenti e analisi di natura tecnica, anche al fine di determinare l'entità dell'evento, le sue conseguenze e il numero degli interessati. Qualora la notifica all'Autorità Garante per la protezione dei dati personali non possa essere effettuata entro le 72 ore, è corredata dei motivi del ritardo;
    c. inviare la comunicazione agli interessati, come previsto dall'art. 34 GDPR, qualora la violazione dei dati personali presenti un rischio elevato per i diritti e le libertà delle persone.
8. Qualora, all'esito delle analisi svolte dal Gruppo, emergano degli elementi tali per cui l'incidente di sicurezza appaia collegato, connesso o dipendente a un reato, il Titolare (o un suo delegato) provvede a segnalare il fatto all'Autorità di Pubblica Sicurezza.

9. Stima della gravità del *data breach*

1. La gravità di una violazione dei dati personali è definita come la "stima dell'entità del potenziale impatto sugli individui derivante dalla violazione dei dati".
2. Al fine di valutare la gravità del data *breach* dovrà essere utilizzata la metodologia Enisa allegata al presente documento (All. 3) che fornisce al Gruppo di gestione del data *breach* una guida per una valutazione complessiva.
3. Il punteggio finale della valutazione della gravità della violazione di dati personali è dato dalla seguente formula: **Gravità = (Contesto di trattamento dati * Facilità identificazione) + Circostanze violazione.**
4. Dell'esito della decisione si informa il Titolare del trattamento che ha la facoltà, comunque, di valutare diversamente la gravità del danno.
5. Sulla base della casistica in cui si ricade, debbono essere svolte le seguenti azioni, tenendo conto del significato associato a:
    A. RISCHIO BASSO: non è necessario notificare il data breach all'Autorità Garante per la protezione dei dati personali, ma l'incidente deve essere annotato all'interno del registro delle violazioni;
    B. RISCHIO MEDIO: non è necessario notificare il data breach all'Autorità Garante per la protezione dei dati personali, ma devono essere adottate ulteriori misure

organizzative e tecniche al fine di migliorare la sicurezza dei dati personali e deve essere annotato l'incidente all'interno del registro delle violazioni;

C. **RISCHIO ALTO**: è necessario notificare il data breach all'Autorità Garante per la protezione dei dati personali e deve essere annotato l'incidente all'interno del registro delle violazioni

D. **RISCHIO MOLTO ALTO**: è necessario notificare il data breach all'Autorità Garante per la protezione dei dati personali, annotare l'incidente all'interno del registro delle violazioni e darne comunicazione ai soggetti interessati secondo quanto disposto dal successivo articolo 10.

10. Comunicazione agli interessati

1. Come previsto dall'art. 34 del GDPR, se la violazione presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
2. La comunicazione viene effettuata, non appena ragionevolmente possibile e in collaborazione con l'Autorità Garante per la protezione dei dati personali, a cura del Referente del *data breach* con la collaborazione del Referente privacy. Qualora la portata dell'evento o il numero dei destinatari richieda una comunicazione pubblica è possibile coinvolgere il Team Comunicazione.
3. La comunicazione contiene almeno le seguenti informazioni:
    a. la descrizione della natura della violazione;
    b. i dati di contatto del RPD/DPO o di altro punto di contatto (es. Referente privacy);
    c. la descrizione delle probabili conseguenze della violazione;
    d. la descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione ed eventualmente per attenuarne i possibili effetti negativi.

11. Attività successive alla segnalazione del *data breach*

1. Il Titolare del trattamento e i Delegati del Titolare si adoperano affinché qualsiasi avvertimento, ammonimento, ingiunzione o richiesta proveniente dal Garante per la protezione dei dati personali, incluse quelle volte a soddisfare le richieste degli interessati e l'esercizio dei loro diritti, vengano eseguite tempestivamente o secondo i termini da essa indicati.
2. Il Gruppo di gestione del *data breach* dà atto, tramite verbale, di aver dato seguito alle disposizioni impartite dal Garante e lo trasmette al Titolare del trattamento.