REGIONE AUTONOMA DELLA SARDEGNA

ISTITUTO SUPERIORE REGIONALE ETNOGRAFICO

Allegato "B" Deliberazione Consiliare n. 39 del 10.12.2018

PROCEDURA DATA BREACH

PREMESSA

L'articolo 4 del Regolamento UE 2016/679 (d'ora in poi GDPR) definisce "data breach" (violazione dei dati personali) 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 presso una Azienda o una Pubblica Amministrazione.
Gli articoli 33 e 34 del GDPR si occupano rispettivamente di disciplinare la notifica di una violazione dei dati personali all'autorità di controllo e la comunicazione di una violazione dei dati personali all'interessato.
Il presente documento espone la procedura per lo svolgimento delle principali attività rivolte all'attuazione delle disposizioni del GDPR in caso di episodi di data breach che riguardino l'ISRE, conformemente a quanto disposto dall'art. 7 dell'Allegato "A" alla Deliberazione Consiliare n. 39 del 10.12.2018 , che ha recepito, adattandolo all'assetto organizzativo dell'Istituto, quanto disposto dall'Amministrazione Regionale con Deliberazioni della Giunta Regionale n. 21/8 del 24 aprile 2018 e successive modificazioni ed integrazioni.

1 - TIPOLOGIE DI VIOLAZIONE DI DATI

L'art. 7, comma 1, dell'Allegato "A" alla Deliberazione Consiliare n. 39 del 10.12.2018 richiama il concetto di violazione di dati personali (data breach) trasmessi, conservati o comunque trattati dall'ISRE.
Di seguito sono elencati possibili eventi che possono determinare violazioni di dati personali (in termini di confidenzialità, integrità, disponibilità). L'elencazione non è esaustiva e il verificarsi di uno degli eventi descritti non costituisce condizione sufficiente per stabilire l'effettiva sussistenza di un data breach. Il verificarsi di un evento (anche non espressamente indicato nel presente documento) che prospetti il rischio di una violazione di dati personali costituisce sempre un fattore di allerta che richiede sempre un'analisi -anche a diversi livelli- per stabilire se si è verificato un data breach. L'elenco è suddiviso in due parti: una riferita ai trattamenti informatici e una ai trattamenti cartacei.

1.1 EVENTI RELATIVI A TRATTAMENTI INFORMATICI

1.1.1 Eventi accidentali

Eventi anomali determinati da fatti fortuiti che causano la perdita delle caratteristiche di sicurezza dei dati personali (confidenzialità, integrità o disponibilità) in caso di trattamenti informatici. Rientrano in tali casistiche eventi generati nella gestione dei sistemi ICT (gestiti internamente oppure in outsourcing) quali:

- **Esecuzione erronea di comandi e/o procedure**, ad esempio: pubblicazione erronea delle informazioni personali (non di dominio pubblico) su siti web dell'ISRE; erroneo invio di informazioni a enti/soggetti esterni all'ISRE, formattazione di dispositivi di memorizzazione, errori nell'implementazione di una policy di controllo e verifica periodica delle abilitazioni degli accessi; divulgazione accidentale di credenziali di accesso a colleghi o personale non autorizzato, ecc.
- **Rottura di componenti hardware**, ad esempio distruzione dei supporti di memorizzazione a causa di sbalzi di temperatura e/o di elettricità, umidità; corto circuito; caduta accidentale; eventi catastrofici; incendi, ecc.
- **Malfunzionamento di software**, ad esempio: esecuzione di uno script automatico non autorizzato; errori di programmazione del software che causano output errati, ecc.
- **Visibilità errata di dati sui siti web dell'ISRE**, ad esempio: visibilità da parte di utenti di dati di altri utenti anche per casi di omonimia, ecc.
- **Fornitura di dati a persona diversa dall'interessato**, ad esempio: comunicazioni di dati di interessati a destinatari errati; gestione di informazioni avanzate da persone diverse dal Titolare o suo delegato, ecc.
- **Guasti alla rete**, ad esempio: caduta delle comunicazioni durante il trasferimento di dati e perdita di dati durante la trasmissione, ecc.

1.1.2 Eventi dolosi

Eventi dolosi causati da personale interno o soggetti esterni realizzati tramite:

1. accesso non autorizzato ai dati con lo sfruttamento di vulnerabilità dei sistemi interni e delle reti di comunicazione.
2. compromissione o rivelazione abusiva di credenziali di autenticazione;
3. utilizzo di software malevolo;
4. altro.

In tale casistica sono compresi incidenti di sicurezza ICT che comportano la violazione di dati personali:

- **Furto:** furto di supporti di memorizzazione e/o elaborazione contenenti dati personali (es: furto laptop, hard disk, chiavette USB, smartphone, tablet, ecc.).
- **Truffa informatica esterna:** tutti i casi di frodi realizzate da un soggetto esterno all'ISRE rivolto a procurare a sé o ad altri un profitto o, comunque, un vantaggio in termini economici, pubblicitari, ideologici/politici, qualora tali frodi causino perdita delle caratteristiche di sicurezza dei dati personali dei soggetti interessati (confidenzialità, integrità o disponibilità) trattati dall'ente o da suoi fornitori, ad esempio: accesso non autorizzato ed illecito alle basi dati dei sistemi contenenti i dati dei soggetti interessati tramite sfruttamento di vulnerabilità dei sistemi; appropriazione di dati bancari; appropriazione (e diffusione) delle credenziali di autenticazione ai servizi degli utenti.
- **Truffa informatica interna:** tutti i casi di frodi realizzate da personale interno all'ISRE che comportano la violazione dei dati personali. Tali eventi possono derivare dall'utilizzo illecito e/o illegittimo delle informazioni a cui un incaricato del trattamento accede anche se autorizzato.

1.2 EVENTI RELATIVI A TRATTAMENTI CARTACEI

1.2.1 Eventi accidentali

Eventi anomali, determinati da calamità o da fatti fortuiti, nell'ambito dei trattamenti non automatizzati effettuati su archivi cartacei contenenti dati personali in possesso dell'ISRE quali:

- **Distruzione accidentale di documenti,** ad esempio in caso di incendio/allagamento dei locali dove sono presenti gli archivi cartacei presso le sedi dell'ISRE o di propri fornitori; distruzione per errore di documenti originali, senza eventuale copia; ecc.
- **Smarrimento di documenti:** ad esempio perdita di documenti contenenti dati personali; ecc.
- **Fornitura involontaria di dati a persona diversa dall'interessato o a persona non autorizzata al trattamento.**

1.1.2 Eventi dolosi

Comportamenti dolosi da parte di personale interno o soggetti esterni realizzati, attraverso accessi non autorizzati, nell'ambito di trattamenti effettuati su archivi cartacei di dati personali dell'ISRE quali:

- **Distruzione dei documenti:** ad esempio incendio doloso provocato da personale interno o soggetti esterni che rende indisponibile in modo definitivo i documenti contenenti dati personali; accesso non autorizzato da parte di terzi ad archivi interni dell'ISRE e distruzione volontaria di documenti contenenti dati personali.
- **Accesso non autorizzato:** ad esempio accesso non autorizzato da parte di personale interno o soggetti esterni, con lettura e/o copia dei documenti, ad archivi documentali presso le sedi dell'ISRE o propri fornitori. Non si verifica violazione se si ha la ragionevole certezza che non vi è stata lettura o copia dei documenti contenenti dati degli interessati.
- **Furto:** sottrazione da parte di personale interno o soggetti esterni (o non identificati) di documenti cartacei contenenti dati personali.

2 – GLI ATTORI DEL DATA BREACH

2.1 Soggetti attivi

I soggetti attivi (o attori) sono tutti coloro che si occuperanno dell'episodio di data data breach dalla fase di rilevazione dell'incidente alla fase di notifica di cui agli artt. 33 e 34 del GDPR, tenendo presente le direttive approvate con Deliberazione Consiliare n. 39 del 10.12.2018, di recepimento della DGR n. 21/8 del 24/04/2018 e ss.mm.ii.; i ruoli coinvolti sono:

- **Titolare, nella persona del suo delegato**: è la persona, fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; l'ISRE con la citata Deliberazione Consiliare n. 39 del 10.12.2018 all'art.3 ha disposto la delega di funzioni in capo al Direttore generale. Il Titolare, pertanto, in caso di data breach, è il Direttore generale dell'ISRE.
- **RPD**: Responsabile Protezione Dati o Data Protection Officer (DPO): il soggetto nominato dall'ISRE con riferimento agli articoli 37, 38, 39 del GDPR..
- **Referente data breach:** è il soggetto che svolge funzioni di referente per il supporto giuridico/procedurale per il data breach per il cui tramite il delegato del titolare trasmette le notifiche in esito alla procedura di data breach.
- **Responsabile IT (Security Manager)**: è la figura preposta alla gestione e supervisione del processo di Security Incident Management in ambito informatico che controlla gli assetti generali di rete, i sistemi di base dell'ISRE e gli accessi al dominio.
- **Responsabile IT di dominio (Security Manager di dominio dedicato – Amministratore di dominio):** è la figura preposta alla gestione e supervisione del processo di Security Incident Management in ambito informatico con riferimento al dominio dedicato, in quanto controlla gli accessi al dominio.
- **Responsabile della conservazione**: si tratta della figura preposta alla gestione e supervisione del processo di conservazione dei documenti (digitali o cartacei).

- **Referente interno**: è il dipendente/collaboratore che ha rilevato o a cui è stato segnalato un evento anomalo di potenziale violazione di dati personali ed è tenuto alla comunicazione dell'incidente.

3 – PROCESSO DI GESTIONE DEL DATA BREACH

Qualsiasi dipendente o collaboratore dell'ISRE, a prescindere dal ruolo rivestito, nel momento in cui è a conoscenza di un episodio di potenziale data breach deve dare immediata comunicazione dello stesso al Delegato del titolare e al dirigente responsabile della struttura presso la quale presta servizio secondo la procedura definita al paragrafo successivo.
Se dalla prima analisi da parte del Delegato del Titolare emergono elementi tali da escludere la possibile violazione dei dati personali, l'anomalia viene gestita all'interno della struttura interessata. Se, invece, dalla prima analisi emergono gli estremi per una probabile violazione, si procede ai necessari approfondimenti. La seconda parte del processo è, pertanto, soltanto eventuale e si verifica quando il Delegato del Titolare ravvisa un data breach o ritiene che un evento possa configurarsi come data breach: in questo caso procede senza indugio (entro 24 ore dalla conoscenza della violazione da parte del dipendente o collaboratore), a segnalare l'episodio ad un gruppo di intervento costituito dallo stesso e dai seguenti soggetti:

- il referente data breach per il supporto giuridico/procedurale;
- il/i Responsabile IT;
- il RPD;
- il Responsabile della conservazione;

al fine di compiere le azioni necessarie per ridurre i rischi e comunque procedere alla raccolta delle informazioni necessarie per coadiuvare il Delegato del Titolare nell'effettuare le valutazioni in ordine alla sussistenza, dimensione e impatto della violazione e supportare lo stesso nella redazione della notifica all'autorità di controllo (Garante per la protezione dei dati personali), se dovuta.
Il gruppo degli attori sopra indicati si riunisce in tempi brevissimi e coinvolge all'occorrenza altri soggetti (anche fornitori esterni) che possano dare un contributo alle azioni di cui sopra.
In caso di constatazione di violazione dei dati personali, il Delegato del Titolare, per il tramite del Referente data breach, notifica, ai sensi dell'art. 33 c. 1 del GDPR, la violazione 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 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.
Il Delegato del Titolare, nel caso in cui ricorrano le condizioni previste dall'art. 34 del GDPR procede altresì alla comunicazione agli interessati valutando la modalità idonea a garantire le finalità della disposizione normativa.
Qualora l'episodio riveli una matrice criminale o dolosa il Delegato del Titolare procede al coinvolgimento dell'Autorità di Pubblica Sicurezza (con ogni probabilità la Polizia Postale) mettendola a conoscenza di tutti gli elementi in proprio possesso ed evidenziando l'obbligo di notifica entro 72 ore dalla conoscenza della violazione all'autorità Garante Nazionale e se sussistano i presupposti per la notifica anche agli interessati.
Le azioni poste in essere devono risultare da atti formali. Pertanto, anche se per velocizzare gli interventi ci si avvarrà delle modalità più immediate si dovranno formalizzare i passaggi salienti anche con la redazione di verbali.

3.1 FASI DEL PROCESSO

3.1.1. Rilevazione dell'incidente e segnalazione

In questa fase si acquisisce la notizia di una possibile violazione di dati personali.
La segnalazione di un possibile data breach può provenire dall'esterno (cittadini, fornitori esterni, enti istituzionali ecc.) o dall'interno, da parte di qualsiasi dipendente o collaboratore dell'ISRE durante il normale svolgimento dell'attività lavorativa.
Il dipendente/collaboratore che riceve la segnalazione dall'esterno o che rileva dall'interno l'evento anomalo di potenziale violazione di dati personali deve segnalarlo immediatamente, anche per le vie brevi, al Delegato del Titolare e al Dirigente della struttura organizzativa presso la quale presta servizio che potranno avvalersi del supporto del Responsabile IT di dominio della stessa struttura organizzativa e/o di altri soggetti responsabili di attività da cui possono derivare ulteriori elementi conoscitivi, al fine di effettuare insieme una prima valutazione (rapida e di massima) ed assicurarsi con certezza che l'evento segnalato non costituisca un data breach.
Qualora venga ravvisato un pericolo di violazione di dati personali (data breach) e, comunque, nei casi dubbi, al fine di porre in essere le eventuali successive azioni da attivare tempestivamente per mitigare o eliminare i rischi, il Delegato del Titolare dovrà avvisare gli altri soggetti attivi, ossia:

- il Referente data breach
- il RPD
- il Responsabile della Conservazione
- il/i Responsabile/i IT

La fase di rilevazione dell'incidente e segnalazione deve concludersi entro 24 ore dalla conoscenza della violazione da parte del dipendente o collaboratore.

3.1.2 Raccolta delle informazioni inerenti l'evento

Qualora sia stato ravvisato un potenziale data breach e il Delegato del Titolare abbia proceduto a coinvolgere gli altri soggetti attivi, dovranno essere acquisiti gli elementi necessari per condurre la fase successiva di ulteriore valutazione al fine di escludere o confermare la sussistenza del data breach.

A tal fine è attivata senza indugio da parte del Referente data breach la riunione con i restanti soggetti attivi (Delegato del Titolare, Responsabile/i IT, Responsabile della Conservazione, RPD e, se necessario, Referente interno). Gli stessi procedono alla raccolta delle informazioni necessarie per la successiva fase di valutazione e a una prima analisi di identificazione della tipologia di violazione.

Il Referente data breach, anche su richiesta degli altri soggetti attivi, al fine di integrare l'analisi, coinvolge altri soggetti responsabili di attività da cui possono derivare ulteriori elementi conoscitivi, i quali devono garantire tempestivamente il supporto richiesto.

Se dalla prima analisi del gruppo di intervento emergono elementi tali da escludere la possibile violazione dei dati personali, la gestione dell'anomalia viene rimandata all'interno della struttura interessata.

Se, invece, emergono gli estremi per una probabile violazione, si procede ai necessari approfondimenti.

Nella pratica, rilevazione e valutazione dell'evento sono spesso interconnesse e già nell'immediato può essere riscontrato un rischio ragionevole di violazione e, anche se non sono disponibili subito maggiori informazioni di dettaglio, si rende necessaria una preventiva comunicazione al Garante da parte del Delegato del Titolare, per il tramite del Referente data breach.

Vi sono casi in cui è possibile definire se l'evento costituisca una violazione ai sensi del GDPR solo al termine della fase di valutazione a cui partecipano tutti i soggetti attivi. In quest'ultimo caso la decorrenza delle tempistiche per la comunicazione al Garante (72 ore) è dal momento della constatazione. La notifica deve essere redatta dal Delegato del Titolare ai sensi dell'art. 33 del GDPR e inviata all'Autorità di controllo a cura del Referente data breach.

Il WP29 ha chiarito che, nell'ipotesi in cui il titolare del trattamento (o suo delegato) non sia in possesso di tutte le informazioni relative alla violazione nelle 72 ore successive al suo verificarsi, con *Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) – WP250, versione emendata e adottata il 6 febbraio 2018 (https://www.garanteprivacy.it/regolamentoue/databreach)*, esso ha la possibilità di comunicare entro il termine di legge all'Autorità di controllo la sola violazione subita, per poi fornire in un successivo momento tutte le informazioni richieste dal suddetto art. 33, corredandole con i motivi del ritardo.

3.1.3 Valutazione dell'evento

Scopo di questa fase è quello di confermare o meno l'avvenuta violazione, di circostanziare in modo completo l'evento e fornire una valutazione del possibile pregiudizio per gli interessati.

I soggetti attivi effettuano un'analisi di dettaglio, esaminano le informazioni aggiuntive e valutano il livello di rischio dell'evento e il livello di pregiudizio per gli eventuali interessati impattati dalla violazione.

Nel caso in cui, dall'analisi, si constati che l'evento costituisce una violazione dei dati personali, da questo momento decorrono le tempistiche (dal momento della conoscenza 72 ore) previste dalla normativa in tema di comunicazioni al Garante.

La notifica all'Autorità di controllo deve essere redatta dal Delegato del Titolare ai sensi dell'art. 33 del GDPR e trasmessa a cura del Referente data breach.

Il gruppo di intervento accerta anche se la violazione di dati comporti un elevato pregiudizio per i diritti e le libertà degli interessati (cittadini, dipendenti, soggetti terzi, ecc.) a fini della comunicazione agli stessi. Nel caso in cui ricorrano le condizioni previste dall'art. 34 del GDPR, il Delegato del Titolare procede alla comunicazione agli interessati valutando la modalità idonea a garantire le finalità della disposizione normativa.

Qualora l'episodio riveli una matrice criminale o dolosa il Delegato del Titolare procede al coinvolgimento dell'Autorità di Pubblica Sicurezza (con ogni probabilità la Polizia Postale) mettendola a conoscenza di tutti gli elementi in proprio possesso. Nella comunicazione dovranno essere evidenziati l'obbligo di notifica entro 72 ore dalla conoscenza della violazione all'autorità Garante Nazionale e l'eventuale sussistenza dei presupposti per la notifica anche agli interessati.

3.1.4 Comunicazione

In caso di violazione dei dati che comporti un elevato pregiudizio per i diritti e le libertà degli interessati (cittadini, dipendenti, soggetti terzi, ecc.), ai sensi dell'art. 34 del GDPR, il Delegato del Titolare comunica la violazione agli stessi senza ingiustificato ritardo.

Il gruppo di intervento supporta il Delegato del Titolare nel verificare che siano o meno soddisfatte le condizioni di cui al c. 3 dell'art. 34 del GDPR per le quali non è previsto l'obbligo di comunicazione agli interessati.

Qualora non ricorra nessuna tali condizioni, il gruppo di intervento supporta il Delegato del Titolare nella predisposizione del testo della comunicazione e nella individuazione della modalità di diffusione.

La comunicazione agli interessati dovrà descrivere con un linguaggio semplice e chiaro la natura della violazione e contenere almeno le informazioni e le misure di cui all'art. 33 par. 3, lett. b), c) e d) del GDPR.
Nel caso in cui l'Autorità di Pubblica Sicurezza, interessata all'evento data breach, dovesse richiedere di ritardare la comunicazione agli interessati per non pregiudicare lo svolgimento delle indagini, il Referente data breach - su disposizione della Autorità di P.S. - può chiedere al Garante l'autorizzazione a ritardare la citata comunicazione per il tempo necessario all'espletamento delle stesse.

3.1.5 Processo di gestione del data breach in caso di segnalazione da parte di fornitori

Nel caso in cui un fornitore dell'ISRE, in qualità di responsabile del trattamento, venga a conoscenza di una violazione (o presunta tale) di dati personali trattati nell'ambito dell'erogazione di un servizio, effettua una prima analisi dell'accaduto e, ove accerti che si tratti di un data breach, invia la segnalazione al Delegato del Titolare, al RPD, al/ai Responsabile/i IT, al Referente data breach e al Responsabile della conservazione senza ingiustificato ritardo.
La segnalazione deve contenere tutti gli elementi utili alla comprensione/identificazione dell'evento.
Il fornitore garantisce, inoltre, assistenza al Delegato del Titolare fornendo eventuali informazioni aggiuntive per la corretta valutazione e gestione dell'evento.
Il Delegato del Titolare che riceve la segnalazione procede secondo quanto previsto ai paragrafi 3.1.2, 3.1.3, 3.1.4.

3.2 ASPETTI SANZIONATORI

Secondo quanto disposto dall'art. 83 c. 4 del GDPR, la violazione degli obblighi del titolare del trattamento e del responsabile del trattamento previsti dagli artt. 8, 11, da 25 a 39, 42 e 43 è soggetta a sanzioni amministrative pecuniarie fino a 10.000.000 euro; rientrano, pertanto, anche le violazioni alla procedure in materia di data breach, previste dagli artt. 33-34 del GDPR. Inoltre, l'art. 82 prevede che chiunque subisca un danno materiale o immateriale causato da una violazione del GDPR ha il diritto di ottenere il risarcimento del danno dal soggetto al quale l'obbligo (violato) era imposto (salvo che quest'ultimo dimostri che l'evento dannoso non gli è imputabile).
Lo stesso GDPR, all'art. 83 c. 2, indica dei fattori che possono mitigare o aggravare la violazione; un elemento che può sicuramente mitigare il livello sanzionatorio, a fronte di una violazione, è legato al comportamento del titolare che può dimostrare come, intervenendo con tempismo, abbia fatto il possibile per ridurre la gravità, la natura e la durata della violazione. L'atteggiamento reattivo e cooperativo comporta sicuramente un'attenuazione delle sanzioni applicabili. Una corretta gestione della procedura è importante per limitare, in caso di violazione di una disposizione, l'applicazione delle sanzioni connesse.
In tal senso, fermo restando la necessità di una continua formazione del personale, si raccomanda di scoraggiare atteggiamenti reticenti o non pienamente collaborativi in quanto la segnalazione del possibile data breach e un pronto intervento di gestione rappresentano sicuramente comportamenti valutabili in senso positivo secondo quanto detto sopra.

3.3 REGISTRO VIOLAZIONI

L'art. 33 c. 5 del GDPR dispone: "*Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.*"
L'ISRE si è dotata di un apposito registro dei trattamenti in cui è presente una sezione per la registrazione delle violazioni dei dati personali.
In detta sezione sono annotate a cura del RPD tutte le informazioni richieste dalla normativa vigente, quali, ad es.: (a) le circostanze relative alla violazione; (b) le conseguenze; (c) i provvedimenti adottati per contrastarla e limitarne gli effetti; (d) i dati personali coinvolti, ecc.
A tal fine al RPD è trasmessa, a cura del Referente data breach, tutta la documentazione necessaria allo stesso per procedere alle registrazioni compresi i verbali delle riunioni dei soggetti attivi.
Le comunicazioni inviate al CERT-PA ai sensi dell'art. 4 della Circolare 18 aprile 2017, n. 2/2017 dell'Agenzia per l'Italia digitale devono essere altresì trasmesse al RPD anche ai fini delle eventuali segnalazioni nel registro.
I dati presenti nel registro sono trattati nel rispetto del principio di minimizzazione e secondo le misure per mitigare i rischi di violazione dei dati personali.