TEATRONAZIONALE
TEATRO STABILE TORINO

DATA BREACH POLICY

1. Finalità e scopo della procedura.
Scopo della presente procedura è di definire le attività e le modalità operative da attuare nei casi in cui si verifichi una violazione dei dati (cd "data breach") nel trattamento di dati personali effettuato, in qualità di Titolare, dalla Fondazione Teatro Stabile di Torino ai sensi degli artt. 33 e 34 GDPR.

2. Destinatari.
La procedura in questione si rivolge a tutti coloro i quali, a qualsiasi titolo, trattano dati personali di competenza del Titolare del trattamento. I destinatari comprendono, a titolo esemplificativo ma non esaustivo: dipendenti (in qualità di autorizzati al trattamento), collaboratori, fornitori (previamente nominati responsabili esterni del trattamento), eventuali destinatari cui dovessero essere comunicati i dati personali degli interessati.

3. Definizioni ed esempi.
Ai sensi dell'art. 4, par. 1, n. 12 GDPR, una "violazione dei dati personali" (cd "data breach") 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".
Un data breach, pertanto, può compromettere la riservatezza, l'integrità o la disponibilità dei dati trattati dal Titolare.
In via esemplificativa, secondo il Garante per la Privacy, costituiscono violazione dei dati personali:
- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;

- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

4. Notifica al Garante.
Il Titolare del trattamento con l'ausilio del DPO senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, deve notificare la violazione al Garante per la protezione dei dati personali a meno che sia improbabile che la violazione dei dati comporti un rischio per i diritti e le libertà delle persone fisiche.
Le notifiche effettuate al Garante oltre le 72 ore devono essere accompagnate dai motivi di ritardo.
Nel caso in cui il Titolare, all'esito della valutazione, abbia rilevato la sussistenza di rischi per gli interessati, questi procede alla notifica al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/

5. Comunicazione agli interessati.
Nel caso in cui, all'esito della valutazione, il Titolare abbia rilevato che la violazione di dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, questi comunica il data breach all'interessato senza ingiustificato ritardo (art. 34, par. 1, GDPR).
La comunicazione, ai sensi dell'art. 34, par. 2 GDPR, deve contenere, con un linguaggio semplice e chiaro, le seguenti informazioni:
- la natura della violazione dei dati personali;
- i dati di contatto del Responsabile della Protezione dei Dati (DPO/RPD) o di altro punto di contatto;
- le probabili conseguenze della violazione dei dati;
- le misure adottate o di cui si propone l'adozione da parte del Titolare per porre rimedio alla violazione dei dati personali e, se del caso, per attenuarne i possibili effetti negativi.

6. Eccezione alla comunicazione agli interessati.
Ai sensi dell'art. 34, par. 3, GDPR, non è richiesta la comunicazione del data breach all'interessato se è soddisfatta una delle seguenti condizioni:
- il Titolare ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- il Titolare ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- tale comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
In base all'art. 34, par. 4, GDPR, nel caso in cui il Titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'Autorità di controllo (il Garante Privacy) può richiedere, dopo aver valutato la probabilità che la violazione dei dati presenti un rischio elevato, che vi si provveda o che sia soddisfatta una delle condizioni precedenti.

7. Gestione del data breach.
Le violazioni di dati personali sono gestite dal Titolare ovvero da un suo delegato, sotto la supervisione del Data Protection Officer o del consulente privacy esterno.
In caso di sospetta, concreta e/o avvenuta violazione dei dati personali è fondamentale assicurare che la stessa sia affrontata tempestivamente e correttamente al fine di minimizzare l'impatto del data breach.

Tutti i soggetti, a vario titolo coinvolti, devono attivarsi, nell'ottica di prevenzione e di mitigazione degli effetti di una violazione di dati personali, nelle seguenti fasi come in seguito meglio descritte:
- rilevazione della violazione dei dati;
- raccolta delle informazioni sulla violazione dei dati;
- comunicazione della violazione dei dati.

8. Rilevazione della violazione.
- Soggetti coinvolti: tutto il personale dipendente/autorizzati al trattamento, fornitori/responsabili esterni, referenti interni, ecc…
- Destinatari: Titolare del Trattamento, responsabile dell'ufficio/di funzione.
- Tempistiche: prima possibile, non appena se ne ha conoscenza.
- Modalità: utilizzando le vie più brevi (telefonicamente, di persona, tramite e-mail).

9. Raccolta delle informazioni sulla violazione dei dati.
- Soggetti coinvolti: Responsabile dell'ufficio/di funzione, suo Delegato (eventuale), persona che ha rilevato il data breach.
- Tempistiche: non appena è ricevuta la segnalazione di data breach.
- Modalità: raccogliendo e documentando le informazioni di cui all'art. 33, par. 3, GDPR.

10. Comunicazione della violazione dei dati.
- Soggetti coinvolti: titolare del trattamento, DPO, consulente informatico esterno e responsabile ICT
- Tempistiche: non appena vengono raccolte le informazioni relative al data breach. In ogni caso, nel più breve tempo possibile dalla rilevazione della violazione.
- Destinatari: Figura apicale/Vertice gerarchico del Titolare, DPO.
- Modalità: via e-mail.

11. Contenuto della notifica al Garante.
La notifica di cui all'art. 33, par. 3, GDPR contiene almeno:
- la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione. Occorre pertanto dettagliare la violazione rilevata (ad esempio indicando data e ora in cui la stessa è avvenuta, se sia ancora in corso di svolgimento o meno, dove si è verificata nel caso di smarrimento o furto di dispositivi contenenti dati personali);
- i dati di contatto del Responsabile della Protezione dei Dati (DPO/RPD) o di altro punto di contatto (specificando, ad esempio, recapito telefonico o indirizzo mail);
- le probabili conseguenze della violazione dei dati (in termini di danni da stimare secondo una valutazione di probabilità);
- le misure adottate o di cui si propone l'adozione da parte del Titolare per porre rimedio alla violazione dei dati personali e, se del caso, per attenuarne i possibili effetti negativi.

12. Violazione di dati personali trattati in qualità di responsabile del trattamento.
Nel caso in cui l'Azienda/l'Ente effettui un trattamento di dati personali per conto di altro Titolare e, in virtù del rapporto contrattuale sottoscritto, sia stato nominato responsabile del trattamento, questi si attiva tempestivamente per analizzare l'evento e verificare se possa trattarsi di una violazione di dati personali. In caso affermativo, viene attivato un processo di gestione della violazione allo scopo di fornire al Titolare ogni informazione e/o documentazione utile alla trasmissione della notifica del data breach secondo le tempistiche e le modalità sottoscritte tra le Parti nel Contratto e/o nell'atto di nomina.

13. Violazione di dati personali trattati dal responsabile del trattamento.
Qualora un data breach si verifichi nell'ambito di un trattamento di dati personali effettuato per conto del Titolare da un soggetto esterno all'organizzazione in qualità di responsabile del trattamento, la procedura sarà quelle contenuta nelle clausole contrattuali previste nell'atto di nomina.
In particolare, il Responsabile informa tempestivamente il Titolare di ogni violazione dei dati, nonché di ogni situazione anomala che possa compromettere la sicurezza o il corretto trattamento dei dati a norma del GDPR.
Il Responsabile è tenuto a collaborare diligentemente con il Titolare effettuando un'analisi puntuale e documentata del tipo di violazione e indicando al Titolare ogni informazione e/o documentazione utile alla predisposizione e alla segnalazione della notifica di data breach al Garante.
In ogni caso il Responsabile si adopera per ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico.

14. Data Breach e sub-responsabile.
Quando un responsabile del trattamento si avvale di un altro responsabile (cd "sub-responsabile") per l'esecuzione di specifiche attività di trattamento per conto del Titolare, su tale sub-responsabile gravano gli stessi obblighi contenuti nell'Accordo sottoscritto tra il Titolare e il responsabile principale, che conserva nei confronti della Fondazione TST l'intera responsabilità.

15. Registro Data Breach.
Il Titolare del trattamento, a prescindere dall'obbligo di notifica al Garante, documenta tutte le violazioni dei dati personali, comprese le circostanze ad esse relative, le possibili conseguenze e i provvedimenti adottati per porvi rimedio, predisponendo un apposito registro.
Tale documentazione, richiesta ai sensi dell'art. 33, par. 5, GDPR, potrà essere messa a disposizione dell'Autorità al fine di effettuare verifiche e controlli sul rispetto della normativa nonché, in particolare, delle procedure di cui agli artt. 33 e 34 GDPR.

16. Formazione del personale e diffusione della Data Breach Policy.
Il Titolare, in ossequio al principio di responsabilizzazione (cd *"accountability"*), organizza e pianifica specifici momenti di formazione finalizzati a illustrare al proprio personale i ruoli, i compiti, le responsabilità e le sanzioni contenuti nella presente Data Breach Policy.
Il rispetto della procedura è obbligatorio per tutti i soggetti individuati nel precedente art. 2.
La presente procedura verrà diffusa mediante apposite circolari o comunicazioni ai dipendenti nonché presentata in occasione delle attività formative.

17. Responsabilità.
Il mancato rispetto della presente procedura può comportare, nei confronti dei soggetti coinvolti, l'applicazione di sanzioni disciplinari nonché, nei casi più gravi, l'attribuzione di responsabilità civili e penali.

18. Aggiornamento.
La Data Breach Policy sarà costantemente aggiornata alla luce delle modifiche che interverranno in materia: tutti i soggetti coinvolti verranno opportunamente informati, mediante circolari e istruzioni, di qualsiasi cambiamento relativo alla stessa.

Torino, 28 ottobre 2022