DISCIPLINARE IN CASO DI VIOLAZIONE DEI DATI PERSONALI (DATA-BREACH)

1.0 SCOPO

In risposta agli artt. 33 e 34 del regolamento generale sulla protezione dei dati dell'Unione europea, l'istituto ha adottato questo disciplinare in caso di violazione dei dati personali. Il disciplinare informa il personale dei propri doveri e definisce le procedure che aiutano ad adempiere agli obblighi previsti dalle leggi applicabili in caso di data-breach che coinvolga dati personali per i quali l'istituto è titolare del trattamento.

2.0 AMBITO DI APPLICAZIONE

Il presente disciplinare si applica a tutti i dipendenti, collaboratori e funzioni dell'istituto.

3.0 DEFINIZIONI

3.1 "dati personali" significa qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

3.2 "Sistemi informatici" significa hardware e software del computer, elementi di rete, database, dispositivi di comunicazione e altri dispositivi, apparecchiature o software utilizzati per elaborare, trasmettere o archiviare i dati. Ciò si estende a reti, laptop, assistenti digitali e altri dispositivi elettronici utilizzati per memorizzare i dati.

3.3 "data-breach" significa qualsiasi incidente che comporti o potenzialmente possa comportare (i) l'accesso non autorizzato, tentato o riuscito, a sistemi informatici dell'istituto o comunque a dati riservati o personali; (ii) tentativo o successo di utilizzo non autorizzato, divulgazione, modifica, archiviazione, distruzione o perdita di dati personali; (iii) violazioni o interferenze con il sistema informatico dell'istituto; (iv) eventi relativi a perdita di dati dai sistemi informatici dell'istituto.

4.0 DISCLIPLINARE

4.1 Responsabilità generali

Il personale deve proteggere la sicurezza dei dati personali, inclusi quelli che risiedono nei sistemi informatici. Se il personale sospetta qualsiasi violazione della sicurezza, deve prontamente avvisare i vertici a cui fa riferimento.

4.1.1 I data-breach riguardanti risorse informatiche devono essere segnalati in conformità con le policy IT pertinenti, compresi i disciplinari di conformità di utilizzo.

4.1.2 Gli incidenti che comportano perdita di dati personali o potenziali rischi di perdita di dati devono essere segnalati immediatamente da tutti i dipendenti o dai responsabili esterni

nominati. Le segnalazioni saranno sempre dirette verso il titolare del trattamento o un suo rappresentante.

4.1.3 I fornitori che trattano dati personali per i quali l'istituto è il titolare del trattamento, si sono impegnati contrattualmente a segnalare incidenti o violazioni della sicurezza. tali segnalazioni avverranno entro un periodo di tempo definito a decorrere dal momento della scoperta. Questo processo è coordinato dai soggetti di contatto tra le parti.

4.2 Team di intervento data-breach

4.2.1 All'interno dell'istituto sarà presente un team di intervento incaricato di esaminare, indagare e gestire la risposta ai data-breach e di segnalare, se necessario, tali violazioni della sicurezza ai vertici dirigenziali. A seconda della natura dei dati coinvolti e del tipo di violazione, il team sarà composto da:

- Responsabile area coinvolta;
- Responsabile IT (amministratore di sistema);
- DPO.

4.2.2 Il team verrà immediatamente attivato alla ricezione di segnalazioni su data-breach interni o relativi a fornitori responsabili del trattamento.

4.3 Risposta ai data-breach

4.3.1 Una volta appreso che si è verificato un data-breach, il team di intervento, o un delegato di questo, adotterà immediatamente le misure appropriate per indagare sull'incidente determinando:

- la natura e la portata dell'incidente;
- se l'incidente è il risultato di una qualsiasi vulnerabilità nei sistemi informatici;
- il tipo di dati coinvolti e se sono a rischio dati personali;
- se sono state adottate misure tecniche per la protezione dei dati coinvolti;
- le possibili conseguenze per la privacy degli interessati coinvolti.

4.3.2 Il delegato segnala tempestivamente le sue conclusioni al team di intervento.

4.3.3 Nel condurre le sue ulteriori indagini, il team di intervento valuterà se sono necessarie risorse esterne per l'assistenza, tra cui, a titolo esemplificativo, il coinvolgimento delle forze dell'ordine nelle indagini, la consultazione di un legale esterno o l'avvalersi di altra assistenza di terze parti. Se necessario, Il team di intervento deve assistere e guidare il personale nel condurre le indagini e / o nell' adottare gli accorgimenti necessari per preservare le prove relative all'incidente.

4.3.4 Sulla base della sua indagine, il team intervento svilupperà raccomandazioni per porre rimedio alle vulnerabilità e / o per contribuire a prevenire incidenti simili in futuro. Ciò può includere il fornire adeguate istruzioni ai dipendenti o intraprendere azioni disciplinari appropriate contro i dipendenti che si siano resi responsabili nell'incidente.

4.3.5 Se dati personali vengono messi a rischio dal data-breach, il team di intervento deve fare il possibile per determinare:

- il tipo e la quantità di dati personali a rischio;
- la disponibilità di registri d'accesso per aiutare a determinare se i dati personali sono stati scaricati o copiati;
- se i dati personali sono stati effettivamente trattati da una persona non autorizzata;
- se i dati personali sono in possesso di una persona non autorizzata;
- se l'incidente è stato parte di un vasto attacco alla rete;
- se le autorità competenti debbano essere informate della violazione e le tempistiche per provvedere a tale notifica;
- se gli interessati coinvolti o che si ritiene siano stati coinvolti nell'incidente debbano essere informati e le tempistiche per provvedere a tali notifiche;
- qualsiasi altro accorgimento richiesto da qualsiasi legge applicabile o idoneo a mitigare il rischio per le persone interessate.

4.3.6 Se la notifica alle autorità di controllo competenti, come l'autorità di vigilanza sulla protezione dei dati, è richiesta dalla legge o è altrimenti ritenuta appropriata, un soggetto designato all'interno del team di intervento, a seguito di consultazione del DPO, assume la responsabilità di provvedere a tale notifica, ove possibile, entro 72 ore dalla scoperta del data-breach. La notifica contiene:

- una descrizione della 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;
- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- una descrizione delle probabili conseguenze della violazione dei dati personali;
- una 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 anche, se del caso, per attenuarne i possibili effetti negativi;
- eventualmente, il motivo per cui la notifica non si è potuta effettuare entro 72 ore.

4.3.7 Se la notifica agli interessati coinvolti è richiesta dalla legge o è altrimenti ritenuta appropriata, questi devono essere informati nel più breve tempo possibile, compatibilmente con i termini di legge e la necessità di condurre e / o completare eventuali investigazioni. Un soggetto designato all'interno del Team d'intervento, in consultazione con il DPO, si assume la responsabilità di effettuare la notifica. La notifica agli interessati dovrebbe includere, come minimo:

- una descrizione generale della violazione, nonché il tipo di dati personali coinvolti;
- una descrizione delle probabili conseguenze della violazione;
- una descrizione degli accorgimenti che l'istituto ha adottato o intende adottare per proteggere i dati personali da ulteriori pregiudizi;
- un contatto al quale l'interessato potrà rivolgere eventuali domande e richiedere chiarimenti;
- qualsiasi altra informazione richiesta dalla legge applicabile, tra cui quelle di cui al paragrafo 4.3.6.

4.3.8 Se la notifica agli interessati in merito a un potenziale data-breach non è richiesta dalla legge, il team di intervento dovrà esaminare i risultati di ogni indagine per determinare se la notifica debba comunque essere fatta. Qualora effettuata, tale notifica dovrà seguire la procedura descritta nel precedente paragrafo 4.3.7. Se la notifica non viene effettuata, il soggetto designato responsabile all'interno del team d'intervento conserverà una relazione che spiega i motivi di tale decisione.

4.3.9 Lo stesso responsabile tiene un registro di tutti i data-breach, contenente una descrizione delle conseguenze e delle misure correttive adottate. Il registro sarà messo a disposizione delle autorità di vigilanza competenti su richiesta.

5.0 ANALISI ASSICURATIVA

In caso di possibile applicabilità di un rimborso assicurativo, un soggetto all'uopo designato, con l'ausilio di eventuali consulenti, provvede a valutare i potenziali diritti e obblighi dell'istituto all'interno di polizze assicurative e accordi di indennizzo relativi al data-breach.

Tale soggetto deve, se è il caso, fornire tempestivamente le comunicazioni richieste da accordi assicurativi o altri accordi potenzialmente coinvolti e deve adottare qualsiasi altra misura necessaria per tutelare gli interessi dell'istituto.

6.0 REVISIONE

Le procedure vengono riesaminate annualmente.

7.0 DOMANDE

Eventuali domande relative al presente disciplinare dovranno essere rivolte al responsabile designato del proprio dipartimento.

La Direzione

_____