Procedura 10 – Data breach

Qualora all'interno dell'ente si verifichi una violazione di sicurezza che comporta - accidentalmente o in modo illecito – il trattamento illecito o non consentito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, si dovrà agire come di seguito indicato.

Descrizione dettagliata delle fasi:

FASE 1 - SEGNALAZIONE

La procedura Data breach viene avviata quando si viene a conoscenza "effettiva" del fatto che una sospetta, presunta o effettiva violazione dei dati personali si sia verificata. Di detto evento bisogna darne immediata comunicazione al proprio Responsabile (Posizione Organizzativa o Dirigente), il quale provvederà nel più breve tempo possibile a darne comunicazione a:

1. DPO
2. Responsabile IT (Amministratore di sistema);
3. Segretario Comunale (che avviserà Sindaco e/o Assessore competente
4. e - se coinvolta - alla Società esterna che gestisce gli aspetti IT della risorsa violata, anche quale responsabile del trattamento ex art. 28 GDPR.

I soggetti da 1 a 3 sono definiti: "Gruppo Data Breach" e agiscono per conto del Titolare del Trattamento.

La comunicazione al Gruppo Data Breach deve comprendere quanto segue:

a. Denominazione della/e banca/banche dati oggetto di data breach;
b. Breve descrizione dei dati personali ivi trattati;
c. Quando si è verificata la violazione dei dati personali;
d. Dove e come è avvenuta la violazione dei dati (ad esempio a seguito di virus informatico, attacco informatico, sottrazione o smarrimento di dispositivi o di supporti portatili ecc.).

FASE 2 - ISTRUTTORIA

Il "Gruppo Data Breach" assume nel più breve tempo possibile eventuali ulteriori informazioni sull'evento, qualora ritenute necessarie. Tale attività istruttoria può avvenire con

a. Richieste di informazioni a dipendenti e referenti del Servizio oggetto di potenziale Data Breach
b. Richieste di relazioni tecnico informatiche al Responsabile IT, al Responsabile esterno del trattamento art. 28, ad un tecnico informatico esterno
c. Acquisizioni di informazioni ed approfondimenti

FASE 3 - RELAZIONE PRELIMINARE SU POTENZIALE DATA BREACH

Entro 36 ore dalla FASE 1 (termine indicativo, perché può dipendere dalla durata dell'istruttoria), il Gruppo Data Breach procede tempestivamente alla valutazione degli elementi acquisiti nella fase istruttoria, redigendo una relazione (anche sottoforma di verbale di incontro) che contenga elementi essenziali quali:

i. Tipo di violazione (ad es. lettura, copia, alterazione, diffusione dei dati);
ii. Dispositivo oggetto della violazione (PC, dispositivi portativi, ecc);
iii. Soggetti interessati dall'evento;
iv. Gravità della violazione anche in relazione ai diritti e alle libertà eventualmente compromesse dell'interessato;
v. Misure di sicurezza tecniche ed organizzative applicate ai dati oggetto di violazione.

A tale fine, potrà essere utilizzato altresì il tool di valutazione messo a disposizione dal Garante o comunque in ossequio al provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach) di data 30 luglio 2019.

In tale documento il Gruppo Data Breach dichiara motivatamente se l'evento segnalato costituisce un'effettiva violazione di dati personali, tale da integrare gli estremi dell'art. 33 e ss. GDPR. Nello specifico verrà deciso motivatamente:

a. Se necessario notificare o meno al Garante privacy l'evento di data breach (art. 33 par. 1 gdpr) in caso positivo, dare mandato di eseguire la notificazione nelle forme previste dall'Autorità Garante per la Protezione dei dati personali
b. Se necessario comunicare o meno agli interessati l'evento di data breach (art. 34 par 1) in caso positivo, dare mandato di eseguire la comunicazione nelle forme ritenute più opportune
c. Le misure tecnologiche e organizzative assunte o da assumere per contenere la violazione dei dati e prevenire simili violazioni in futuro.

FASE 4 CONCLUSIONE

Verranno protocollate e, al termine delle operazioni, archiviate:

- la RELAZIONE PRELIMINARE SU POTENZIALE DATA BREACH
- l'eventuale NOTIFICA DI DATA BREACH ai sensi dell'art. 33 par 1 GDPR
- l'eventuale comunicazione agli interessati ai sensi dell'art. 34 par. 1 GDPR

Verrà infine compilato e sottoscritto un "REGISTRO DATA BREACH" su cui viene annotata ogni attività svolta nel contesto di questa procedura