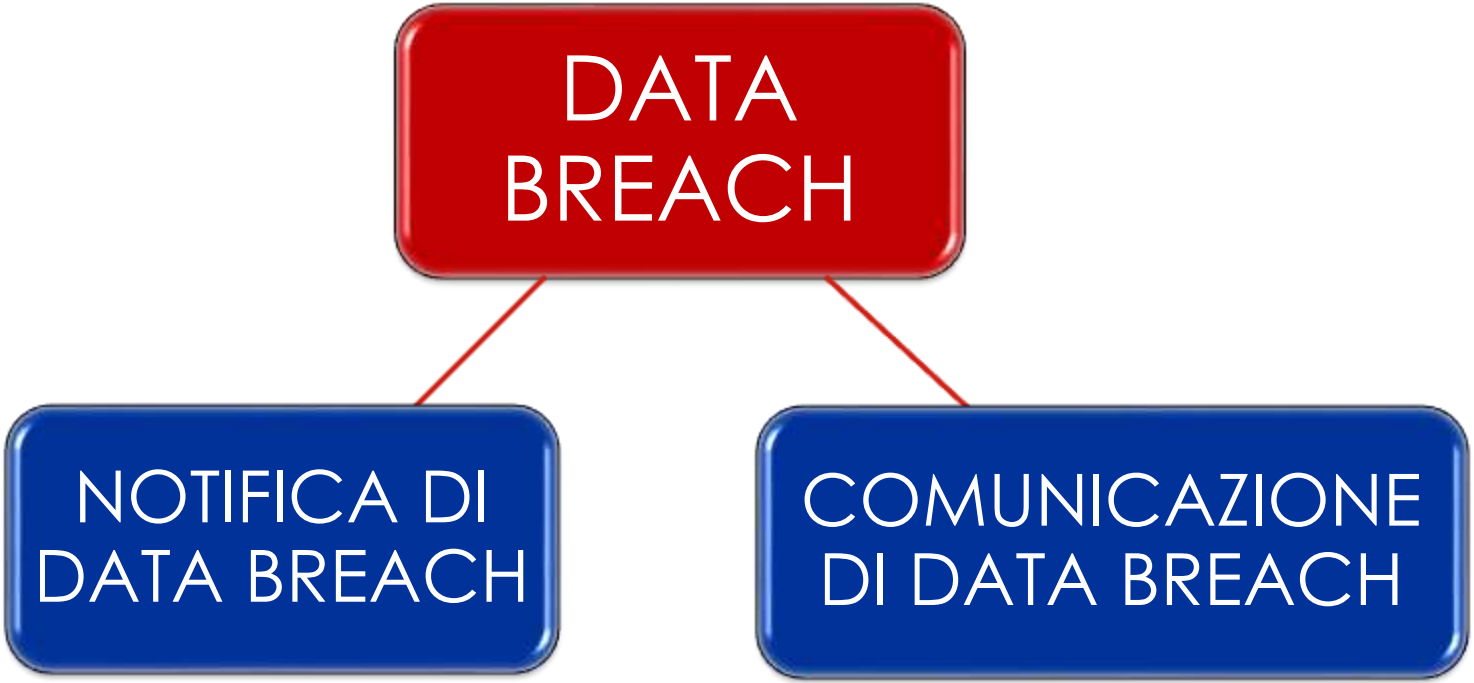
ASSO DPO
Associazione Data Protection Officer

IL RUOLO DEL DPO NELLA CYBERSECURITY

Matteo Colombo
ASSO DPO

DATA BREACH | ART. 33 E SEGG. GDPR



VIOLAZIONE DI DATI PERSONALI

Articolo 33 GDPR | C85, c87, c88 e linee guida WP 29 18/IT 250rev.01

- **Il Titolare del trattamento notifica la violazione dei dati personali** il Data Breach al Garante per la protezione dati personali **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.**

- Il **Responsabile del trattamento** (Art. 33.2 GDPR) **informa il Titolare del trattamento senza ingiustificato ritardo** dopo essere venuto a conoscenza della violazione, nel caso in cui tratti dati personali in nome e per conto suo.

- Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

ALCUNI ESEMPI DI DATA BREACH

Perdita o furto di device mobili non criptati (usb, laptop, smartphone) che contengono dati personali

Invio un file/email contenente dati personali al **destinatario errato**

Invio di una email massiva a una **lista di contatti nel campo "a:" o "cc:"** invece che in "**ccn**:"

Perdita o furto di documenti cartacei contenenti dati personali

Attacchi informatici (malware, virus, criptolocker etc.) a sistemi contenenti dati personali

Dati sanitari | cartelle cliniche **indisponibili** per alcune ore a causa di attacco informatico o distacco elettrico.

REGISTRO DI DATA BREACH

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.

ALLEGATO C: REGISTRO DELLE VIOLAZIONI

Categoria di interessati	Categoria di dati perosnali coinvolti	Numero approssimativo di registrazioni dei dati perso	Conseguenze della violazione	Contromisure adottate	E' stata effettuata notifica all'Autorità Garante privacy?	E' stata fatta comunicazione agli interessati?

IL RUOLO DEL DPO NEL DATA BREACH

Ai sensi dell'articolo 38 del GDPR, il Titolare e il Responsabile assicurano che il DPO sia "**tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali**".

Il DPO deve consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente (linee guida 3.1).

Suggerimento: predisporre linee-guida ovvero programmazioni in materia di protezione dei dati che indichino i casi di consultazione obbligatoria DPO

IL RUOLO DEL DPO NEL DATA BREACH

Assistere, fra l'altro, il titolare del trattamento nel garantire il rispetto degli obblighi:

- Sicurezza del trattamento;
- Notifica di Data Breach;
- Comunicazione di Data Breach.

In caso di violazione dati il responsabile del trattamento deve notificarla al Titolare del trattamento «**senza ingiustificato ritardo**».

La valutazione del rischio spetta al Titolare.

Attenzione: Il responsabile può effettuare la notifica per conto del titolare qualora quest'ultimo gli abbia concesso l'opportuna autorizzazione e ciò faccia parte degli accordi contrattuali.

DATA BREACH: CASO 1

Perdita dati da parte del responsabile esterno

Facendo seguito alla comunicazione di violazione dei dati personali in data xxx lo scrivente Dipartimento chiede di fornire con ogni consentita urgenza e comunque non oltre il xxx **ogni elemento e informazione utile alla valutazione dei profili di protezione dei dati personali** di competenza di questa Autorità, con particolare riferimento:

1. **Agli ulteriori soggetti eventualmente coinvolti** nel trattamento dei dati personali oggetto di valutazione, con l'indicazione del loro ruolo (titolare autonomo, contitolare o responsabile);
2. **Alla designazione a responsabile del trattamento** della società xxx (art. 29 del Codice) e alle attività di vigilanza poste in essere dal titolare in merito ai trattamenti effettuati dal responsabile:
3. **Ad una breve descrizione del data flow**, con particolare riguardo alle modalità di trasmissione dei dati fra il sistema locale e centrale, all'architettura IT, alle banche dati coinvolte e all'ubicazione dei data center;
4. **Ai soggetti che possono avere accesso al sistema centrale** di archiviazione e al presupposto di liceità in base ai quali avvengono i suddetti accessi;
5. **Alle circostanze in cui l'azienda xxx ha scoperto la mancata archiviazione delle immagini** degli studi radiologici oggetto di violazione fornendo copia della comunicazione che la Società ha effettuato a codesta Azienda in merito;
6. **Alla console di monitoraggio e agli accorgimenti tecnici** di cui sono dotati i sistemi di gestione delle copie dai PACS;
7. **Ai controlli a campione sulla copia dei file** nel sistema di archiviazione centrale;
8. **Alla possibilità di recuperare le immagini degli studi radiologici** oggetto della segnalazione.

FACSIMILE

DATA BREACH: CASO 2

Accesso non autorizzato e diffusione di dati particolari relativi alla salute

All. 1 | Prospetto degli elementi da fornire all'Autorità per le valutazioni di cui all'art. 83, par. 2 del Regolamento.

Al fine di consentire al Garante di effettuare tutte le valutazioni del caso, **con riferimento ai provvedimenti anche di carattere sanzionatorio da adottare**, si invita a fornire tutti gli elementi di cui all'art. 83, par. 2 e, in particolare:

ARTICOLO	SPECIFICHE	ELEMENTI RICHIESTI
Art. 83, par. 2 lett. A)	Elementi in ordine a natura, gravità e durata della violazione tenendo in considerazione la natura, l'oggetto o la finalità del trattamento in questione nonché il numero di interessati coinvolti nella violazione.	È richiesto di fornire elementi di valutazione specifici e obiettivi in rapporto alle violazioni contestate. 
Art. 83, par. 2 lett. B)	Carattere doloso o colposo della violazione.	Elementi di fatto che consentano di valutare l'elemento soggettivo che ha determinato la condotta.
Art. 83, par. 2 lett. C)	Misure adottate per attenuare gli effetti della violazione per gli interessati.	Descrizione delle misure adottate, nel caso specifico, per attenuare le conseguenze della violazione. […]

DATA BREACH: CASO 2

ARTICOLO	SPECIFICHE	ELEMENTI RICHIESTI
Art. 83, par. 2 lett. D)	Le misure tecniche e organizzative messe in atto ai sensi degli articoli 25 e 32.	Elementi che consentano di rilevare, in generale, l'adozione di un livello di sicurezza adeguato al rischio, per i diritti e le libertà delle persone fisiche, nonché l'attuazione della protezione dei dati fin dalla progettazione e per impostazione predefinita (procedure interne, istruzioni operative al personale sul trattamento dei dati personali, corsi di formazione e ogni altra iniziativa assunta o che si intenda assumere in conformità delle disposizioni vigenti.
Art. 83, par. 2 lett. F)	Il grado di cooperazione con l'Autorità per porre rimedio alla violazione e attenuarne i possibili effetti negatici	
Art. 83, par. 2 lett. G)	Le categorie di dati personali interessate dalla violazione	Se la violazione ricada sul trattamento di dati «particolari» (di cui all'art. 9 del Regolamento) ovvero «relativi a condanne penali e reati» (di cui all'art. 10 del Regolamento)
Art. 83, par. 2 lett. H)	La maniera in cui l'Autorità ha preso conoscenza della violazione	In particolare se l'Autorità sia venuta a conoscenza della violazione per effetto della notifica effettuata dal titolare ai sensi dell'art. 33 del Regolamento
Art. 83, par. 2 lett. I)	Elementi in ordine al rispetto degli specifici provvedimenti correttivi già adottati dal Garante con riferimento alla specifica violazione contestata	Documentazione dalla quale si possa rilevare l'attuazione delle prescrizioni, limitazioni o divieti eventualmente già disposti dal Garante
Art. 83, par. 2 lett. J)	L'adesione a codici di condotta, approvati ai sensi dell'art. 40 del Regolamento, o ai meccanismi di certificazione di cui all'art. 42 del Regolamento	Documenti dai quali si possa rilevare tale adesione
Art. 83, par. 2 lett. K)	Eventuali altri fattori attenuanti applicabili alle circostanze del caso	

GRAZIE PER L'ATTENZIONE

Dott. Matteo Colombo

www.assodpo.it