BOZZA COMUNICAZIONE EMAIL DA INVIARE AGLI UTENTI E AGLI INCARICATI DEL TRATTAMENTO SULLE POSSIBILI VIOLAZIONI (DATA BREACH) DEI DATI PERSONALI E SUL PIANO DI EMERGENZA AZIENDALE

VIOLAZIONE DEI DATI PERSONALI (*DATA BREACH*)

Premessa

Il regolamento europeo per la protezione dei dati personali UE 2016/679 (GDPR) ha introdotto l'obbligo, per tutte le organizzazioni, di comunicare all'Autorità di Controllo (il Garante per la Privacy) alcuni tipi di violazioni dei dati personali.

Quando prevista, la segnalazione deve avvenire entro 72 ore dalla scoperta della violazione, laddove possibile. Qualora la violazione subita possa comportare un rischio elevato di pregiudicare i diritti e le libertà delle persone è necessario, senza ingiustificato ritardo, informare anche i diretti interessati.

Per poter rispettare questa prescrizione, ed evitare possibili sanzioni, è stato predisposto e condiviso con tutti i responsabili dell'Amministrazione un "**Piano di Emergenza per violazioni dei dati personali (*data breach*)**", cioè una procedura che permetta di rilevare e segnalare le potenziali violazioni, di effettuare le necessarie verifiche interne e di acquisire tutte le informazioni utili a valutare la gravità della situazione e la necessità o meno di notificare la violazione all'Autorità di Controllo pertinente e alle persone interessate.

È stato inoltre approntato un "**Registro delle violazioni dei dati personali**", in cui sarà riportato ogni evento (*data breach*) rilevato, indipendentemente dal fatto che sia poi necessario notificarlo formalmente.

Per poter rendere efficace questa procedura è necessaria la collaborazione di tutti gli utenti dei sistemi informativi e di coloro che trattano i dati anche su supporto cartaceo, ed in particolare degli incaricati al trattamento dei dati personali, nella segnalazione delle possibili violazioni.

Cos'è una Violazione dei Dati Personali (*Data Breach*)?

Una violazione della sicurezza dei dati personali trattati dall'Amministrazione è **un'azione che comporti, 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.

Una violazione è più che una semplice perdita di dati personali e può essere causata, ad esempio da:

- attacco informatico o accesso ai sistemi, o ai locali di archivio, da parte di terzi non autorizzati;
- azione, deliberata o accidentale (o anche derivante da inazione), da parte di un operatore o di un responsabile (personale interno);
- invio di dati personali ad un errato destinatario;
- perdita o furto di server, computer, altri dispositivi informatici (notebook, smartphone, chiavette USB, hard disk esterni, ecc.) e fascicoli cartacei contenenti dati personali;
- alterazione dei dati personali avvenuta senza la debita autorizzazione;
- perdita della disponibilità dei dati personali (inaccessibilità da parte degli interessati).

Una violazione dei dati personali può essere quindi definita come un problema/violazione di sicurezza che ha influito sulla riservatezza, l'integrità o la disponibilità dei dati personali. Ci potrà essere una violazione dei dati personali ogni qualvolta i dati personali vengano persi, distrutti, corrotti o divulgati, in caso qualcuno acceda ai dati o li diffonda senza esserne stato autorizzato, o se i dati siano resi non più disponibili, ad esempio, quando fossero crittografati da azioni di ransomware (blocco dei dati con richiesta di riscatto) o fossero andati persi o distrutti accidentalmente.

Tutti gli utenti dei sistemi informativi aziendali ed gli addetti alla gestione dei fascicoli cartacei, ed in particolare gli incaricati al trattamento dei dati personali e i loro responsabili di area/funzione, dovranno

informare tempestivamente il proprio superiore diretto, i responsabili dei Sistemi Informativi, il Titolare del trattamento o suo delegato e/o il DPO **di qualsiasi violazione certa o presunta** di cui fossero venuti a conoscenza e fornire il maggior numero di dettagli possibile utilizzando i seguenti canali:

e-mail rpd@crabruzzo.it

PEC avvocatobonaldi@pec.it

Alla scoperta di una possibile violazione dei dati personali l'Amministrazione potrà intraprendere le seguenti **azioni**:

- **Contenimento e recupero**: contenere la violazione e limitarne la portata e l'impatto,
- **Valutazione del rischio**: indagine sulla violazione e valutazione dei rischi per gli interessati e per l'Amministrazione
- **Notifica** formale della violazione **all'Autorità di Controllo,**
- Valutazione delle cause della violazione e **azioni correttive.**

In particolare, **la collaborazione di tutti è importante nell'attività di contenimento e recupero**.

Chi è responsabile di questa attività?

L'individuo che ha causato la violazione o che ha rilevato una possibile violazione, il suo responsabile e il Responsabile di area/funzione.

Quali sono le attività da svolgere?

La priorità immediata è quella di contenere la violazione e limitarne la portata e l'impatto.

In caso i dati personali siano stati inviati a qualcuno non autorizzato a trattarli il personale dovrebbe:

- dire al destinatario di non trasmetterli o discuterli con nessun altro,
- comunicare al destinatario di distruggere o cancellare i dati personali ricevuti e farsi confermare per iscritto che sia stato fatto,
- avvisare il destinatario di eventuali implicazioni se divulgasse ulteriormente i dati,
- informare gli interessati dei quali sono stati trasmessi dati personali di cosa è successo in modo che possano intraprendere le azioni necessarie per proteggersi.

Il Responsabile dell'area/funzione in cui si è verificata la violazione deve essere informato e deve immediatamente segnalarlo ai Responsabili dei Sistemi Informatici, al Responsabile del trattamento, al DPO ed al Titolare del trattamento o suo delegato, fornendo le seguenti informazioni:

- data e ora della violazione o della rilevazione della violazione,
- chi ha commesso la violazione,
- dettagli della violazione,
- numero di soggetti interessati,
- dettagli delle azioni già intraprese in relazione al contenimento e al recupero.

Con il contributo di tutti l'Amministrazione potrà individuare e gestire efficacemente ogni problema e garantire una corretta protezione dei dati personali.

Per qualsiasi informazione e/o chiarimento potete contattare Il Responsabile della protezione dei dati Avv. WALTER BONALDI, E-MAIL: rpd@crabruzzo.it - PEC: avvocatobonaldi@pec.it

La Direzione