



PROCEDURA DI GESTIONE DI UN DATA BREACH

DEFINIZIONE DI DATA BEACH

Il Data Breach è una violazione della sicurezza, che comporta accidentalmente o in modo illecito la distruzione, perdita, modifica, divulgazione, accesso, copia o consultazione non autorizzate di dati personali trasmessi, conservati o comunque trattati.

Ciò può avvenire a seguito di un attacco informatico, di un accesso abusivo, di un incidente (es. incendio, allagamento, etc.) o per la perdita di un supporto informatico (smartphone, notebook, chiavetta USB, etc.) o per la sottrazione di documenti con dati personali (furto, etc.).

La violazione dei dati personali può essere suddivisa in tre categorie:

- “**Confidentiality breach**”: divulgazione o accesso non autorizzato o accidentale a dati personali;
- “**Availability breach**”: alterazione non autorizzata o accidentale di dati personali;
- “**Integrity breach**”: modifica non autorizzata o accidentale di dati personali.

PROCEDURA DA SEGUIRE IN CASO DI DATA BREACH ¹

¹

Sanzioni: In caso di mancato rispetto delle procedure di notifica della violazione si applica la [sanzione amministrativa](#) fino ad un importo di 10 milioni di euro oppure il 2% del fatturato dell'intera società. In caso di mancata notifica si configura anche l'assenza di adeguate misure di sicurezza, per cui si cumulano due distinte sanzioni.



Individuazione del tipo di violazione e comunicazione immediata della violazione al Titolare del Trattamento

Chiunque rilevi una qualsiasi violazione o compromissione di dati personali ne dà immediata comunicazione al **Titolare del Trattamento**, specificando i dati coinvolti e descrivendo l'evento secondo la tipologia **(R.I.D.)**:

- R.** Violazione di riservatezza (divulgazione o accesso a dati personali non autorizzato o accidentale);
- I.** Violazione di integrità (alterazione di dati personali non autorizzata o accidentale);
- D.** Violazione di disponibilità (perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali)



Avvio dell'azione correttiva per gestire tecnicamente la violazione e per ripristinare, se necessario, tempestivamente la disponibilità e l'accesso dei dati personali





Analisi dei rischi conseguenti alla violazione. In particolare, si deve valutare se la violazione dei dati personali presenta un rischio per i diritti e le libertà delle persone fisiche



In conseguenza ad una violazione dei dati è necessario, in ogni caso, porre in essere le seguenti attività:

- a. In caso di assenza di rischi per i dati personali:



- procedere alla registrazione della violazione nell'apposito Registro delle violazioni;
- conservare il Registro delle violazioni: pur non essendo obbligatoria la [notifica al Garante della Privacy](#) è comunque necessario comprovare l'assenza dei rischi.

b. In caso di presenza di rischi per i dati personali² :

- raccogliere tutte le informazioni inerenti alla violazione (**data breach**) per la notifica al **Garante della Privacy**;
- entro 72 ore dalla scoperta della violazione, procedere alla notifica al **Garante della Privacy**, tramite apposito modulo scaricabile dal sito <http://www.garanteprivacy.it> (**MODULO NON ANCORA DISPONIBILE**)³;
- registrare la violazione nell'apposito Registro delle violazioni;
- conservare il Registro delle violazioni.

2

Ad esempio: perdita del controllo dei dati personali, limitazione dei diritti, furto di identità, decifrazione non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati sanitari o giudiziari protetti da segreto professionale etc.

3

Contenuto Minimo della notifica al Garante:

- 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;
- comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrizione delle probabili conseguenze della violazione dei dati personali;
- 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.



- c. **In caso di presenza di un ELEVATO RISCHIO**, cioè quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche):
- raccogliere tutte le informazioni inerenti alla violazione (**data breach**) per la notifica al **Garante della Privacy** e ai **diretti interessati del trattamento**;
 - entro 72 ore inviare la notifica al **Garante della Privacy**;
 - senza ingiustificato ritardo inviare la notifica agli **interessati** (per consentire loro l'adozione di ogni precauzione per ridurre al minimo il potenziale danno derivante dalla violazione dei dati);
 - gestire i riscontri da parte degli interessati;
 - registrare la violazione nell'apposito Registro delle violazioni;
 - conservare il Registro delle violazioni.

Non è richiesta la comunicazione all'interessato se:

- a) sono state messe in atto tutte 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**;
- b) sono state successivamente adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- c) la 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.

BARLETTA , il 25 maggio 2018

AZIENDA AGRICOLA F.LLI CARPENTIERE