

**VIOLAZIONE DI DATI PERSONALI**  
**MODELLO DI COMUNICAZIONE AL GARANTE**

A seguito del recepimento della direttiva 2009/136/Ce ad opera del decreto legislativo 28 maggio 2012, n. 69, i fornitori di servizi di comunicazione elettronica sono oggi tenuti a comunicare al Garante e, in alcuni casi, al contraente o ad altre persone interessate, le violazioni dei dati personali (Data breach) che detengono nell'ambito delle proprie strutture.

**Titolare che effettua la comunicazione**

Denominazione o ragione sociale: .....

Provincia.....Comune.....

Cap. .... Indirizzo .....

Nome                      persona                      fisica                      addetta                      alla  
comunicazione.....

Cognome                      persona                      fisica                      addetta                      alla  
comunicazione.....

Funzione rivestita.....

Indirizzo Email/PEC per eventuali comunicazioni.....

Recapito telefonico per eventuali comunicazioni.....

Eventuali Contatti (altre informazioni) .....

**Natura della comunicazione**

- Nuova comunicazione
- Inserimento ulteriori informazioni sulla precedente comunicazione (Numero di riferimento)
- Ritiro precedente comunicazione

**Breve descrizione del trattamento di dati personali**

**Quando si è verificata la violazione di dati personali?**

- Il.....
- Tra il..... e il .....
- In un tempo non ancora determinato
- È possibile che sia ancora in corso

**Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)**

**Modalità di esposizione al rischio?**

**Tipo di violazione**

- Lettura (presumibilmente i dati non sono stati copiati)
- Copia (i dati sono ancora presenti sui sistemi del titolare)
- Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
- Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
- Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
- Altro: .....

**Dispositivo oggetto della violazione**

- Postazione di lavoro
- Dispositivo di acquisizione o dispositivo-lettore
- Smart card o analogo supporto portatile
- Dispositivo mobile
- File o parte di un file
- Strumento di *backup*
- Rete
- Altro: .....

**Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:**

**Quante persone sono state colpite dalla violazione di dati personali?**

- N. .... di persone
- Circa ..... persone
- Un numero (ancora) sconosciuto di persone

**Che tipo di dati sono coinvolti nella violazione ?**

- Dati anagrafici
- Numero di telefono (fisso o mobile)
- Indirizzo di posta elettronica
- Dati di accesso e di identificazione (*user name, password, customer ID*, altro)
- Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro)
- Altri dati di personali (sesso, data di nascita, età, ...), dati sensibili e giudiziari Ancora sconosciuto
- Altro: .....

**Livello di gravità della violazione dei dati biometrici (secondo le valutazioni del titolare)?**

- Basso/trascurabile
- Medio
- Alto
- Molto alto

**Misure tecniche e organizzative applicate ai dati colpiti dalla violazione**

**La violazione è stata comunicata anche agli interessati?**

- Sì, è stata comunicata il .....
- No, perché .....

**Qual è il contenuto della comunicazione ai contraenti (o alle persone interessate)?**

**Quale canale è utilizzato per la comunicazione ai contraenti (o alle persone interessate)?**

**Quali misure tecnologiche ed organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?**

**La violazione coinvolge contraenti (o altre figure interessate) che si trovano in altri Paesi UE?**

- Sì
- No

**La comunicazione è stata effettuata alle competenti autorità di altri Paesi UE?**

- No
- Sì