



**Allegato B al Provvedimento n.513 del Garante del 12 novembre 2014**

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

A seguito del Provvedimento del 12 novembre 2014, i titolari di trattamento di dati biometrici sono tenuti a comunicare al Garante le violazioni di tali dati (*data breach*) che si verificano nell'ambito dei propri sistemi.

La comunicazione deve essere effettuata in base al presente modello, allegando eventualmente ulteriore documentazione ritenuta utile.

**Titolare del trattamento di dati biometrici**

**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)

**Breve descrizione del trattamento di dati biometrici (finalità, caratteristiche biometriche utilizzate..)**

**Breve descrizione della violazione di dati biometrici**

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

- Il \_\_\_\_\_
- Tra il \_\_\_\_\_ e il \_\_\_\_\_
- 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 biometrici?**

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

**Altri dati 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**

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

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

- Sì, è stata comunicata il
- No, perché

**La violazione coinvolge interessati che si trovano in altri Paesi UE?**

- Sì
- No

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

- No
- Sì