

ALLEGATO 7

VIOLAZIONE DI DATI PERSONALI MODELLO DI COMUNICAZIONE AL GARANTE

Secondo quanto prescritto dal **Provvedimento del 2 luglio 2015**, le amministrazioni pubbliche sono tenute a comunicare al Garante all'indirizzo: databreach.pa@pec.gpdp.it le violazioni dei dati personali (*data breach*) che si verificano nell'ambito delle banche dati (qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti, art. 4, comma 1, lett. *p* del Codice) di cui sono titolari.

La comunicazione deve essere effettuata entro 48 ore dalla conoscenza del fatto, compilando il modulo che segue.

Amministrazione titolare del trattamento

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

Denominazione della/e banca/banche dati oggetto di data breach e breve descrizione della violazione dei dati personali ivi trattati

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/codice fiscale
- ☐ Dati di accesso e di identificazione (user name, password, customer ID, altro)
- ☐ Dati relativi a minori
- ☐ Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
- ☐ Dati personali idonei a rivelare lo stato di salute e la vita sessuale
- ☐ Dati giudiziari
- ☐ Copia per immagine su supporto informatico di documenti analogici
- ☐ 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)?

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