

Allegato B alla determinazione 24 maggio 2018, n. 349

**REGISTRO DELLE VIOLAZIONI DEI DATI PERSONALI (C.D. REGISTRO DEI  
DATABREACH)**  
(articolo 33, paragrafo 5. del Regolamento (UE) 2016/679)

**TITOLARE DEL TRATTAMENTO:** CONSIGLIO REGIONALE DEL LAZIO

**DATI DI CONTATTO:** Via della Pisana 1301, 00163 ROMA - PEC: [segreteria generale@cert.consreglazio.it](mailto:segreteria generale@cert.consreglazio.it).

**RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD):** MARIA GRAZIA TOSIANI

**DATI DI CONTATTO:** PEC: [rpdcrl@cert.consreglazio.it](mailto:rpdcrl@cert.consreglazio.it); email istituzionale: [rpdcrl@regione.lazio.it](mailto:rpdcrl@regione.lazio.it); recapito telefonico: 06.65937140;  
recapito postale: Via della Pisana 1301, 00163 ROMA.

N.	Soggetto competente e relativa struttura	Attività di trattamento	Descrizione natura violazione e circostanze della stessa (art. 33, par. 3., lett. a) e par. 5. del Regolamento (UE) 2016/679)	Analisi conseguenze della violazione (art. 33, par. 3., lett. c) e par. 5. del Regolamento (UE) 2016/679)	Descrizione misure adottate o proposte (art. 33, par. 3., lett. d) del Regolamento (UE) 2016/679)	Livello gravità violazione	Date violazioni e notifica della stessa	Comunicazione e della violazione all'interessato (art. 34 del Regolamento (UE) 2016/679)
1	Indicare il soggetto competente al trattamento dei dati personali e la relativa struttura	Descrivere l'attività di trattamento dei dati personali, indicando anche la finalità e la relativa base giuridica	Descrivere la natura della violazione dei dati personali, compresi, ove possibile, le categorie e il numero approssimativo di interessati nonché le categorie e il numero approssimativo di registrazioni dei dati personali	Descrivere le probabili conseguenze della violazione dei dati personali	Descrivere le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.	Qualificare la gravità della violazione in ragione, in particolare, della misura del rischio per i diritti e le libertà delle persone fisiche:  <u>Basso</u>  <u>Medio</u>  <u>Elevato</u>  <u>Molto Elevato</u>	<u>Data violazione</u>  --/--/---  <u>Data notifica violazione</u>  --/--/--	<u>Si (indicazione data)/No</u>



**GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI**

**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.gdpd.it](mailto:databreach.pa@pec.gdpd.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 PEC e/o EMAIL per eventuali comunicazioni \_\_\_\_\_

Recapito telefonico per eventuali comunicazioni \_\_\_\_\_

Eventuali Contatti (altre informazioni) \_\_\_\_\_

**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 dei dati personali trattati nell'ambito della banca dati?**

- Il \_\_\_\_\_
- Tra il \_\_\_\_\_ e il \_\_\_\_\_
- In un tempo non ancora determinato
- E' 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**

- Computer
- Rete
- Dispositivo mobile
- File o parte di un file
- Strumento di *backup*
- Documento cartaceo
- 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 dei dati personali trattati nell'ambito della banca dati?**

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

**Che tipo di dati sono oggetto di 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 personali trattati nell'ambito della banca dati (secondo le valutazioni del titolare)?**

- Basso/trascurabile
- Medio
- Alto
- Molto alto

**Misure tecniche e organizzative applicate ai dati oggetto di violazione**

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

- Sì, è stata comunicata il
- No, perché \_\_\_\_\_

**Qual è il contenuto della comunicazione resa agli interessati?**

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