



**VIOLAZIONE DI DATI PERSONALI  
MODELLO DI COMUNICAZIONE AL RESPONSABILE PROTEZIONE  
DATI**

Secondo quanto prescritto dall'art. 33 del **Regolamento Europeo 2016/679 GDPR**, in caso di violazione dei dati personali, avvenuta accidentalmente o in modo illecito, che si concretizzi con la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, i Dirigenti/Rappresentanti di struttura, al fine di consentirne la prevista comunicazione all'Autorità di controllo, entro e non oltre 48 ore dall'acquisizione della conoscenza dell'accadimento, devono informare, con urgenza immediata, il Responsabile della protezione dei dati, utilizzando il presente modello Allegato 1), da trasmettere esclusivamente al seguente indirizzo e-mail [responsabileprotezionedati@uniroma1.it](mailto:responsabileprotezionedati@uniroma1.it).

I Responsabili esterni del trattamento, eventualmente nominati e delegati dai Dirigenti/Rappresentanti di struttura, devono, allo stesso modo informare, con urgenza immediata, il Responsabile della protezione dei dati, utilizzando il presente modello Allegato 1), da trasmettere esclusivamente al seguente indirizzo e-mail [rpd@cert.uniroma1.it](mailto:rpd@cert.uniroma1.it);

**Area/Struttura**

Denominazione o ragione sociale

---

Sede

---

Nome e cognome della persona fisica addetta alla comunicazione

---

Funzione rivestita

---

Indirizzo PEC e/o EMAIL per eventuali comunicazioni

---

Recapito telefonico per eventuali comunicazioni

---



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

---

---

---

---

---

**2. 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 \_\_\_\_\_

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

---

---

---

---

---

**4. Modalità di esposizione al rischio**

---

---

---

---

---

**5. 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 \_\_\_\_\_

---



**6. Dispositivo oggetto della violazione**

- Computer
- Rete
- Dispositivo mobile
- File o parte di un file
- Strumento di *backup*
- Documento cartaceo
- Altro \_\_\_\_\_

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

---

---

---

---

---

**8. 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

**9. 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 \_\_\_\_\_

**10. Livello di gravità della violazione dei dati personali trattati nell'ambito della banca dati (secondo le valutazioni del Dirigente/Rappresentante di struttura)?**

- Basso/trascurabile
- Medio
- Alto



- Molto alto

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

---

---

---

---

---

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

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

---

---

---

---

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

---

---

---

---

---

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

---

---

---

---

---

---

Roma \_\_\_\_\_

**Il Dirigente/Rappresentante di struttura**

---