PROCEDURA DI NOTIFICA DELLE VIOLAZIONI

Procedura operativa da applicare qualora un incaricato del trattamento verifichi o abbia sospetto di una violazione dei dati personali.

La presente procedura potrà essere soggetta ad eventuali aggiornamenti. La versione aggiornata è sempre disponibile all'indirizzo: http://www.uniroma3.it/privacy/.

Sommario

1. NOTIFICA AL RESPONSABILE DELLA PROTEZIONE DEI DATI

2. Qualora si verifichi una violazione dei dati personali, l'incaricato del trattamento coinvolto informa tempestivamente e con qualsivoglia mezzo il proprio responsabile interno del trattamento e/o il responsabile della protezione dei dati subito dopo essere venuto a conoscenza della violazione. Inoltre, l'incaricato del trattamento è contestualmente tenuto ad inviare al responsabile della protezione dei dati una e-mail, contrassegnata come urgente, avente il seguente oggetto: "URGENTE – VIOLAZIONE DATI PERSONALI [NOME UFFICIO]". Tale comunicazione è dovuta in ogni caso, a prescindere che il responsabile della protezione dei dati sia già stato informato o meno.
3. L'email deve contenere una descrizione quanto più possibile dettagliata di:
    a. natura della violazione
    b. tipologie di dati e interessati coinvolti
    c. indicazione della portata della violazione (in termini numerici)
    d. misure eventualmente adottate
4. Il responsabile della protezione dei dati provvede a convocare, se necessario, una riunione con gli interlocutori interessati al fine di acquisire maggiori informazioni ed eventualmente decidere le azioni successive.

2. NOTIFICA AL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

1. L'Università notifica la violazione all'Autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuta a conoscenza, salvo che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà degli interessati. Il titolare del trattamento adotta i provvedimenti del caso sentito il parere del Direttore Generale, del Dirigente competente a seconda degli uffici coinvolti dalla violazione e del responsabile della protezione dei dati.
2. I soggetti sopra elencati valutano le azioni da intraprendere tenuto conto delle indicazioni fornite dalle competenti strutture informatiche (se del caso) e dai risultati dell'indagine interna condotta dal responsabile della protezione dei dati ai sensi del Regolamento di Ateneo.
3. Qualora la notifica al Garante non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
4. La notifica all'Autorità di Controllo deve contenere almeno i seguenti elementi:
    a. descrivere la natura della violazione compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
    b. comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
    c. descrivere le probabili conseguenze della violazione;
    d. descrivere le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.
5. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni devono essere fornite in fasi successive senza ritardo.

3. NOTIFICA AGLI INTERESSATI

1. Quando la violazione presenta potenzialmente un rischio elevato per i diritti e le libertà degli Interessati, l'Università comunica la violazione all'interessato, anche in questo caso senza ingiustificato ritardo.
2. La comunicazione all'interessato descrive con un linguaggio semplice e chiaro la natura della violazione e contiene almeno le seguenti informazioni e misure:
    a. l'indicazione del nome e i dati di contatto del soggetto interno all'Università presso cui è possibile ottenere più informazioni sull'incidente;
    b. una descrizione delle probabili conseguenze della violazione;
    c. la descrizione delle misure adottate, o di cui si propone l'adozione da parte del titolare del trattamento, per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.
3. Non è richiesta la comunicazione all'interessato in questione se è soddisfatta una delle seguenti condizioni:
    a. siano state attuate le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
    b. siano state successivamente adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli Interessati;
    c. detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, l'Università deve procedere a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
4. I soggetti di cui al paragrafo 2.1 valutano la sussistenza delle circostanze per le quali non è necessario notificare agli interessati l'avvenuta Violazione.

4. MODELLO DI COMUNICAZIONE AL RESPONSABILE DELLA PROTEZIONE DATI

La persona che ha rilevato la violazione, al fine di consentirne la prevista comunicazione all'Autorità di controllo, entro e non oltre 48 ore dall'acquisizione della conoscenza dell'accadimento, deve informare, con urgenza immediata, il Responsabile della protezione dei dati, utilizzando il presente Allegato, da trasmettere esclusivamente al seguente indirizzo e-mail: rpd@uniroma3.it e PEC rpd@ateneo.uniroma3.it.

I Responsabili esterni del trattamento, nominati dal Titolare del trattamento dei dati personali, devono, allo stesso modo informare, con urgenza immediata, il Responsabile della protezione dei dati, utilizzando il presente Allegato, da trasmettere esclusivamente al seguente indirizzo e- mail: rpd@uniroma3.it. e PEC rpd@ateneo.uniroma3.it.

Direzione/Area/Dipartimento

Denominazione

_____

Sede

_____

Nome e cognome della persona che ha rilevato la violazione

_____

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 _____
   - In un tempo non ancora determinato
   - È 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 viola- zione)
   - 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, lì

_____

[Nome e Cognome]

_____

Firma

_____