UNIVERSITÀ EUROPEA DI ROMA

REGOLAMENTO SUL TRATTAMENTO DEI DATI PERSONALI SVOLTO DALLA UNIVERSITÀ DEGLI STUDI EUROPEA DI ROMA

ALLEGATO A
PROCEDURA DATA BREACH

SOMMARIO

1. Premessa 2

2. Destinatari della Procedura 2

3. Ambito di applicazione della Procedura 3

4. Definizione di violazione di dati personali (*data breach*) 4

5. Gestione e comunicazione dei *data breaches* 4

5.a Verifica della segnalazione 5

5.b Contenimento della violazione e procedura di recupero 5

5.c Eventuale notifica all'Autorità Garante 5

5.d Eventuale comunicazione agli interessati 5

6. Documentazione della procedura 6

Allegato A – Modulo per la segnalazione di sospetta Violazione dei dati personali 7

Allegato B - Modulo di valutazione del Rischio connesso al Data Breach 8

1. PREMESSA

Lo scopo della presente procedura predisposta, nel rispetto del Regolamento (UE) n. 2016/679 recante il Regolamento Generale sulla Protezione dei Dati personali (RGPD), ai sensi dell'art. 25 del "Regolamento sul trattamento dei dati personali svolto dalla Università degli Studi Europea di Roma" (di seguito anche "Regolamento"), per la gestione delle violazioni dei dati personali (di seguito anche "Procedura") trattati dall'Università Europea di Roma in qualità di Titolare del trattamento (di seguito anche "Università" o "Titolare"), è quello di definire le attività che tutti i soggetti coinvolti nei trattamenti di dati personali operati dall'Università devono seguire qualora scoprano o vengano a conoscenza di una violazione di dati, c.d. *data breach*, anche solo potenziale o non definita in tutti i suoi elementi.

Per *data breach* si intende la violazione di sicurezza che comporti, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati dall'Università.

Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare notevoli danni, materiali o immateriali, alle persone fisiche i cui dati personali oggetto della violazione sono riferibili, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata. Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento deve notificare la violazione dei dati personali all'Autorità Garante per la protezione dei dati personali (di seguito anche "Garante"), senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che non sia in grado di dimostrare che è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche interessate. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo.

2. DESTINATARI DELLA PROCEDURA

La Procedura è rivolta a tutti gli Autorizzati ai sensi dell'art. 4 del Regolamento, i Designati ai sensi dell'art. 6 del Regolamento, gli AdS ai sensi dell'art. 7 del Regolamento, nonché ai contitolari ai sensi dell'art. 26 RGPD e ai responsabili ai sensi dell'art. 28 RGPD (di seguito indicati come "Destinatari") che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto intercorrente - abbiano accesso ai dati personali trattati dall'Università.

La conoscibilità è assicurata mediante invio ai Destinatari (via PEC ai contitolari e ai responsabili, con mail per le altre categorie), nonché mediante pubblicazione sul sito internet dell'Università. In modo da garantire la capillare conoscibilità della procedura, la stessa sarà anche pubblicata nello spazio cloud condiviso tra i dipendenti.

In caso di dubbi sulle indicazioni contenute nella Procedura i Destinatari possono rivolgersi al Responsabile della Protezione dei Dati personali (di seguito anche "DPO") dell'Università,

contattabile in qualsiasi momento via mail dpo.emaggio@unier.it o chiamando al numero 333.2160001.

Il mancato rispetto della Procedura comporta per gli autorizzati e i designati al trattamento la responsabilità disciplinare e per i contitolari e i responsabili costituisce una giusta causa per la revoca dei rispettivi accordi e la risoluzione dei contratti che ne hanno giustificato la sottoscrizione anche qualora da ciò non consegua un danno diretto per l'Università o gli interessati o un provvedimento sanzionatorio da parte del Garante.

3. AMBITO DI APPLICAZIONE DELLA PROCEDURA

La Procedura si riferisce ai trattamenti di dati personali svolti in qualsiasi formato e con qualsiasi mezzo.

Le principali categorie di dati personali sono:

- **Dati Biometrici**: i dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.
- **Dati Comuni**: sono tutti i dati personali che non appartengono alle categorie dei dati particolari e dei dati giudiziari.
- **Dati Genetici**: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.
- **Dati Giudiziari**: dati personali relativi a condanne penali o a reati commessi o a connesse misure di sicurezza.
- **Dati Particolari**: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, ovvero i trattamenti di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
- **Dato Personale**: qualsiasi informazione riguardante una persona fisica identificata o identificabile (c.d. "Interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
- **Dati relativi alla Salute**: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

Università Europea di Roma
Via degli Aldobrandeschi, 190 - 00163 Roma (Italia) - Tel. (+39) 06-665431 - Fax (+39) 06-66543840
E-mail: rettorato@unier.it - Website: http://www.universitaeuropeadiroma.it

4. DEFINIZIONE DI VIOLAZIONE DI DATI PERSONALI (*DATA BREACH*)

Ai sensi dell'art. 4, n. 12, del RGPD per "violazione di dati personali" si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
A mero titolo esemplificativo e non esaustivo, costituiscono violazioni di dati personali:

- la divulgazione di dati confidenziali a persone non autorizzate;
- la perdita o il furto di dati, pc, supporti per la memorizzazione (cd, dvd, pen drive) contenenti dati personali;
- la perdita o il furto di documenti cartacei;
- la realizzazione di copie degli archivi non autorizzate, c.d. infedeltà aziendale;
- l'accesso non autorizzato a sistemi informativi, con o senza diffusione dei dati;
- i casi di pirateria informatica;
- le banche dati alterate o distrutte senza autorizzazioni;
- i virus o altri attacchi al sistema informatico o alla rete;
- l'accesso fisico non autorizzato ad archivi cartacei;
- lo smarrimento di pc portatili, devices o attrezzature informatiche aziendali;
- l'invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

5. GESTIONE E COMUNICAZIONE DEI *DATA BREACHES*

Le violazioni di dati personali sono gestite dal DPO supportato dal Designato dell'unità organizzativa oggetto di violazione e dall'AdS. Qualora la violazione interessi una unità organizzativa di secondo livello è chiamato a fornire supporto al DPO anche il Designato dell'unità organizzativa di primo livello.
In caso di concreta, sospetta e/o avvenuta violazione dei dati personali, è di estrema importanza assicurare che la stessa sia affrontata immediatamente e correttamente al fine di minimizzare l'impatto della violazione e prevenire che si ripeta.
Nel caso in cui uno dei Destinatari si accorga di una concreta, potenziale o sospetta violazione dei dati personali, è tenuto ad informare immediatamente dell'incidente il DPO e il Designato, mediante il modulo di cui all'Allegato A che deve essere inviato a databreach@unier.it, entro e non oltre 24 ore dalla conoscenza, anche generica, della violazione.
La gestione della segnalazione può essere scadenzata nelle seguenti fasi:

a. Verifica della segnalazione;
b. Contenimento della violazione e procedura di recupero;
c. Eventuale notifica al Garante;
d. Eventuale comunicazione agli interessati.

Università Europea di Roma
Via degli Aldobrandeschi, 190 - 00163 Roma (Italia) - Tel. (+39) 06-665431 - Fax (+39) 06-66543840
E-mail: rettorato@unier.it - Website: http://www.universitaeuropeadiroma.it

5.a Verifica della segnalazione

Le informazioni da inserire nel modulo, allegato A, sono atte a permettere al DPO, al Designato e all'AdS di svolgere una valutazione iniziale sull'effettiva natura dell'incidente segnalato, al fine di stabilire se si sia effettivamente verificata un'ipotesi di Data Breach.
In particolare, saranno prese in esame le seguenti informazioni:

- la data di scoperta della violazione;
- il ruolo del soggetto che è venuto a conoscenza della violazione;
- la descrizione dell'incidente;
- la natura della violazione;
- la natura dei dati coinvolti;
- le categorie e il numero approssimativo degli interessati coinvolti nella violazione;
- la descrizione di eventuali azioni già poste in essere.

5.b Contenimento della violazione e procedura di recupero

Verificato l'effettivo accadimento di una violazione e circoscritto il perimetro della stessa, il DPO, con il supporto del Designato e dell'AdS definiscono le azioni che possano limitare i danni che la violazione potrebbe causare (ad esempio: riparazione fisica di strumentazione; utilizzo dei file di *back up* per recuperare dati persi o danneggiati; isolamento/chiusura di un settore compromesso della rete; cambio dei codici di accesso) e i soggetti che devono porre in essere le azioni individuate.

5.c Eventuale notifica all'Autorità Garante competente

Il DPO, con il supporto del Designato e dell'AdS, valutano la sussistenza dell'obbligo di notifica della violazione al Garante, ove sia probabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche.
Per la valutazione di cui sopra viene impiegato l'Allegato B "*Modulo di valutazione del Rischio connesso al Data Breach*" che deve essere esaminato unitamente all'Allegato A, tenendo, altresì, in debita considerazione i principi e le indicazioni di cui all'art. 33 RGPD.
La notifica deve essere effettuata dal DPO senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ha ricevuto la segnalazione.

5.d Eventuale comunicazione agli interessati

Il DPO, con il supporto del Designato e dell'AdS valutano la sussistenza dell'obbligo, o anche solo dell'opportunità, di notifica della violazione agli interessati, ove la violazione presenti un elevato rischio per i diritti e le libertà delle persone fisiche.
Per la valutazione di cui sopra viene impiegato l'Allegato B "*Modulo di valutazione del Rischio connesso al Data Breach*" che deve essere esaminato unitamente all'Allegato A, tenendo, altresì, in debita considerazione i principi e le indicazioni di cui all'art. 34 RGPD.
Il DPO senza ingiustificato ritardo effettua la comunicazione agli interessati che contiene:

- il nome e i dati di contatto del DPO;
- descrizione delle probabili conseguenze della violazione dei dati personali;

Università Europea di Roma
Via degli Aldobrandeschi, 190 - 00163 Roma (Italia) - Tel. (+39) 06-665431 - Fax (+39) 06-66543840
E-mail: rettorato@unier.it - Website: http://www.universitaeuropeadiroma.it

- descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare per porre rimedio alla violazione dei dati personali e, se del caso, per attenuarne i possibili effetti negativi.

La suddetta comunicazione deve avvenire con modalità dirette, ad esempio posta elettronica, SMS o messaggi diretti. Il messaggio dovrà essere comunicato in maniera evidente e trasparente, evitando quindi di inviare le informazioni nel contesto di update generali o newsletter, che potrebbero essere facilmente fraintese dai lettori.

Nel caso in cui la segnalazione diretta richieda uno sforzo ritenuto sproporzionato, allora si potrà utilizzare una comunicazione pubblica, che dovrà essere ugualmente efficace nel contatto diretto con l'interessato.

6. DOCUMENTAZIONE DELLA PROCEDURA

Ogni segnalazione viene annotata nel Registro dei Data Breach, tenuto dal DPO, nel quale sono ripotate le seguenti informazioni: (*i*) n. violazione; (*ii*) data violazione; (*iii*) natura della violazione; (*iv*) categoria di interessati; (*v*) categoria di dati personali coinvolti; (*vi*) numero approssimativo di registrazioni dei dati personali; (*vii*) conseguenze della violazione; (*viii*) contromisure adottate; (*ix*) se sia stata effettuata notifica al Garante Privacy; (*x*) se sia stata effettuata comunicazione agli interessati.

Il Registro dei Data Breach deve essere continuamente aggiornato e messo a disposizione del Garante qualora chieda di accedervi.

Università Europea di Roma
Via degli Aldobrandeschi, 190 - 00163 Roma (Italia) - Tel. (+39) 06-665431 - Fax (+39) 06-66543840
E-mail: rettorato@unier.it - Website: http://www.universitaeuropeadiroma.it

ALLEGATO A – MODULO PER LA SEGNALAZIONE DI SOSPETTA VIOLAZIONE DEI DATI PERSONALI

Qualora un Destinatario si accorga di una concreta, potenziale o sospetta violazione dei dati personali, c.d. *data breach*, deve immediatamente informare dell'incidente il Responsabile della Protezione dei Dati personali e il suo superiore gerarchico, riempiendo il presente modulo, entro e non oltre 24 ore dalla conoscenza, anche generica, della violazione, che dovrà poi essere inviato a databreach@unier.it.

COMUNICAZIONE DI DATA BREACH	NOTE
Data scoperta violazione:	
Data dell'incidente:	
Luogo della violazione (specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili):	
Nome e ruolo della persona che riferisce della violazione e compila il modulo:	
Dati di contatto della persona che riferisce della violazione (indirizzo e-mail, numero telefonico): In caso di soggetto esterno indicare la denominazione o la ragione sociale:	
Denominazione della/e banca/che dati oggetto di Data Breach e breve descrizione della violazione dei dati personali ivi trattati:	
Categorie e numero approssimativo di interessati coinvolti nella violazione:	
Breve descrizione di eventuali azioni poste in essere al momento della scoperta della violazione:	
Responsabile dell'area o dipartimento interessato dalla violazione:	
Data:	
N. Scheda (a cura del DPO)	

Università Europea di Roma
Via degli Aldobrandeschi, 190 - 00163 Roma (Italia) - Tel. (+39) 06-665431 - Fax (+39) 06-66543840
E-mail: rettorato@unier.it - Website: http://www.universitaeuropeadiroma.it

ALLEGATO B - MODULO DI VALUTAZIONE DEL RISCHIO CONNESSO AL DATA BREACH

ASSESSMENT DI GRAVITÀ	A CURA DEL DPO, CON IL SUPPORTO DEL DESIGNATO E DELL'AdS
Dispositivi oggetto del Data Breach	Esempi: computer, service cloud, server, rete dispositivo mobile, file o parte di un file, strumento di back up, archivio cartaceo, altro
Modalità di esposizione al rischio (tipo di violazione):	Esempi: 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 presenti 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.
Breve descrizione dei sistemi di elaborazione o di memorizzazione dati coinvolti, con indicazione della loro ubicazione.	
Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati violata?	
La violazione può avere conseguenze negative in una delle seguenti unità organizzative:	Rettorato Segreteria Dipartimenti Ricerca Promozione Post lauream Altro
Qual è la natura dei dati coinvolti?	• Dati anagrafici (nome, cognome, numero di telefono, email, CF, indirizzo etc.) • Dati di accesso e di identificazione (user name, password, customer ID, altro) • Dati personali idonei a rivelare l'origine razziale ed etnica • Dati personali idonei a rivelare le convinzioni religiose • Dati personali idonei a rivelare le convinzioni filosofiche o di altro genere

Università Europea di Roma
Via degli Aldobrandeschi, 190 - 00163 Roma (Italia) - Tel. (+39) 06-665431 - Fax (+39) 06-66543840
E-mail: rettorato@unier.it - Website: http://www.universitaeuropeadiroma.it

	• Dati personali idonei a rivelare le opinioni politiche • Dati personali idonei a rivelare l'adesione a partiti • Dati personali idonei a rivelare l'adesione a sindacati, • Dati personali idonei a rivelare l'adesione ad associazioni od organizzazioni a carattere religioso, • Dati personali idonei a rivelare l'adesione ad associazioni od organizzazioni a carattere filosofico, • Dati personali idonei a rivelare l'adesione ad associazioni od organizzazioni a carattere politico • Dati personali idonei a rivelare l'adesione ad associazioni od organizzazioni a carattere sindacale • Dati personali idonei a rivelare lo stato di salute • Dati personali idonei a rivelare la vita sessuale • Dati giudiziari • Dati genetici • Dati biometrici • Copia per immagine su supporto informatico di documenti analogici • Informazioni che possono essere utilizzate per commettere furti d'identità (i.e. dati di accesso e di identificazione, codice fiscale e copie di carta d'identità, passaporto o carte di credito); • Informazioni personali relative a soggetti fragili (i.e. anziani, disabili, minori); • Profili individuali che includono informazioni relative a performance lavorative, salario o stato di famiglia, sanzioni disciplinari, che potrebbero causare danni significativi alle persone.
Gli interessati rischiano di essere privati dell'esercizio del controllo sui dati personali che li riguardano?	
Quali misure tecniche e organizzative sono adottate ai dati oggetto di violazione?	Esempi: pseudonimizzazione; cifratura dei dati
Il Responsabile/Contitolare aderisce ad un codice di condotta approvato ai sensi dell'art.	

Università Europea di Roma
Via degli Aldobrandeschi, 190 - 00163 Roma (Italia) - Tel. (+39) 06-665431 - Fax (+39) 06-66543840
E-mail: rettorato@unier.it - Website: http://www.universitaeuropeadiroma.it

40 Regolamento (UE) o un meccanismo di certificazione di cui all'art. 42 Regolamento (UE)?	
Il Titolare ha adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati successivamente alla violazione?	
Classificazione della violazione e motivazioni:	Nullo Basso Medio Alto In quanto è possibile che si verifichi una delle seguenti condizioni a danno degli interessati, a causa della violazione: 1. discriminazioni 2. furto o usurpazione d'identità 3. perdite finanziarie 4. pregiudizio alla reputazione 5. perdita di riservatezza dei dati personali protetti da segreto professionale 6. decifratura non autorizzata della pseudonimizzazione 7. danno economico o sociale significativo 8. privazione o limitazione di diritti o libertà 9. impedito controllo sui dati personali all'interessato 10. danni fisici, materiali o immateriali alle persone fisiche.
Notificazione del Data Breach al Garante	SI/NO Se sì, notificato in data: Dettagli:
Comunicazione del Data Breach agli interessati	SI/NO Se sì, notificato in data: Dettagli:
Comunicazione del Data Breach ad altri soggetti	SI/NO Se sì, notificato in data: Dettagli:

Università Europea di Roma
Via degli Aldobrandeschi, 190 - 00163 Roma (Italia) - Tel. (+39) 06-665431 - Fax (+39) 06-66543840
E-mail: rettorato@unier.it - Website: http://www.universitaeuropeadiroma.it