ATENEO INTERNAZIONALE
Università per Stranieri di Siena

Procedura da adottare in caso di violazione dei dati personali

Art. 4, 33, 34 del Regolamento UE 679/2016

1. Premessa

Il presente documento è redatto in adempimento a quanto previsto dal Regolamento UE 679/2016 (GDPR) in materia di violazione dei dati personali.

Per «**dato personale**» si intende *qualsiasi informazione riguardante una persona fisica identificata o identificabile («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.*

Il GDPR definisce violazione del dato personale o ***DATA BREACH*** ogni "*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*" dal Titolare del trattamento.

2. Scopo e ambito di applicazione

La presente procedura è predisposta al fine di tutelare le persone, i dati e le informazioni e documentare i flussi per la gestione delle violazioni dei dati personali trattati dall'Università per Stranieri di Siena, nella sua qualità di Titolare del trattamento.

La procedura definisce le modalità e le responsabilità per:

- identificare la violazione,
- analizzare le cause della violazione,
- definire le misure da adottare per rimediare alla violazione dei dati personali e attenuarne i possibili effetti negativi,
- registrare le informazioni relative alla violazione, le misure identificate e l'efficacia delle stesse,

- notificare una violazione di dati personali al Garante, nel caso in cui la violazione comporti un rischio per i diritti e la libertà delle persone fisiche,
- comunicare una violazione dei dati personali all'interessato nel caso in cui il rischio fosse elevato.

La procedura si applica a qualunque attività svolta dal Titolare del trattamento con particolare riferimento a tutti gli archivi e/o documenti cartacei e a tutti i sistemi informativi attraverso cui sono trattati dati personali, anche con il supporto di fornitori esterni.

L'Università per Stranieri di Siena, quale Titolare del trattamento dei dati, ad integrazione delle procedure già adottate in materia di protezione dei dati personali, ha predisposto azioni da attuare nelle ipotesi in cui dovessero presentarsi violazioni concrete, potenziali o sospette di dati personali trattati dall'Ateneo in qualità di Titolare, al fine di:

- evitare rischi per i diritti e le libertà degli interessati,
- evitare danni economici all'Ateneo,
- notificare la violazione (Data Breach) al Garante e/o agli interessati, nei tempi e nei modi previsti dalla normativa di riferimento,
- non incorrere nelle sanzioni previste dal GDPR per omessa notifica,
- minimizzare l'impatto della violazione e prevenire che si ripeta.

3. Verso chi si rivolge la procedura

La procedura è rivolta a tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del Titolare del trattamento, in qualsiasi formato e con qualsiasi mezzo, quali:

• i dipendenti, nonché coloro che a qualsiasi titolo (a prescindere pertanto dal tipo di rapporto intercorrente con l'Università per Stranieri di Siena) abbiano accesso ai dati personali trattati nel corso del proprio impiego per conto del Titolare del trattamento;

• qualsiasi soggetto (persona fisica o persona giuridica) che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento, abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento *ex* art. 28 GDPR o di autonomo Titolare.

Il rispetto della predisposta procedura **è obbligatorio** per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste dalla stessa potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con le terze parti inadempienti, secondo le normative vigenti in materia.

4. La procedura di *Data Breach*

Nel caso in cui uno dei soggetti in precedenza indicati venga a conoscenza di una concreta, o solo potenziale o anche meramente sospetta violazione di dati personali, **dovrà attivare** il flusso di adempimenti più avanti descritti.

La gestione della violazione concreta, potenziale o sospetta prevede l'attuazione delle seguenti attività:

1. rilevazione e segnalazione della violazione dei dati personali,
2. raccolta delle informazioni sulla violazione e comunicazione della violazione,
3. valutazione del rischio,
4. individuazione delle possibili azioni correttive,
5. comunicazione delle valutazioni effettuate e delle azioni da intraprendere,
6. notifica della violazione (qualora necessaria),
7. documentazione delle violazioni (Registro dei *data breach*).

Schema di sintesi

	Attività	Interessati	Destinatari	Quando	Modalità
1	***Rilevazione e segnalazione***	- personale dipendente - collaboratori - fornitori	- Responsabile della struttura - Responsabile per la sicurezza informatica - Responsabile per la transizione al digitale - RPD/DPO	Non appena ne viene a conoscenza	Modalità più veloci (telefono, e-mail, ecc.)
2	***Raccolta delle informazioni***	Colui che ha rilevato la violazione	- Responsabile della struttura - Responsabile per la sicurezza informatica - Responsabile per la transizione al digitale - RPD/DPO	Entro 24 ore	Modulo per la raccolta delle informazioni (allegato)
3	***Valutazione del rischio***	- RPD/DPO - Responsabile per la sicurezza informatica - Responsabile per la transizione al digitale		Non appena ne viene a conoscenza	Relazione cartacea
4	***Azioni correttive***	- RPD/DPO - Responsabile per la sicurezza informatica - Responsabile per la		Dopo ogni revisione della DPIA	Integrazione della DPIA

		transizione al digitale			
5	***Comunicazione delle valutazioni e delle azioni***	- RPD/DPO - Responsabile per la sicurezza informatica - Responsabile per la transizione al digitale - Responsabili di struttura	Titolare		Relazione cartacea
6	***Notifica della violazione***	Titolare	Garante della *Privacy*		Modello predisposto dal Garante
7	***Comunicazione agli interessati***	Titolare	Persone fisiche coinvolte		
8	***Documentazione***	- RPD/DPO - Responsabile per la sicurezza informatica - Responsabile per la transizione al digitale - Responsabili di struttura		Non appena completate le sottostanti fasi	Inserimento dei dati nel Registro dei *Data Breach*

5. Violazione in caso di trattamenti di dati esternalizzati

Nel caso di trattamenti di dati esternalizzati, i Responsabili esterni del trattamento sono tenuti a comunicare al Titolare del trattamento (utilizzando l'allegato Modulo per la raccolta delle informazioni sulla violazione dei dati), per il tramite del Responsabile della Protezione dei Dati (RPD/DPO), l'avvenuta violazione **entro e non oltre 24 ore** dalla scoperta, al fine di consentire al Titolare di effettuare l'eventuale notifica al Garante e la comunicazione agli interessati entro i termini stabiliti dal Regolamento UE 679/2016.

Chiunque riceva segnalazioni di avvenute violazioni da parte di soggetti esterni, compresi i Responsabili esterni del trattamento, è tenuto a darne immediata comunicazione via mail al Responsabile della struttura di afferenza, al Responsabile per la Sicurezza informatica, al Responsabile della Transizione al digitale e al Responsabile per la Protezione dei Dati di Ateneo.

In tema il Garante, con Provvedimento del 30 luglio 2019 (Registro dei provvedimenti n. 157 del 30 luglio 2019) ha predisposto il modello di notifica delle violazioni dei dati personali (data breach), come riportato a pag. 7.

Allegato: Modulo per la raccolta di informazioni sulla violazione dei dati

Data della segnalazione:
Nome e cognome del segnalante:
Struttura di afferenza, funzione e dati di contatto del segnalante (tel., e-mail ecc.):

_____

1. Breve descrizione della violazione di dati personali

_____

_____

_____

2. 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 _____

3. Luogo 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. Tipologia 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
• Dispositivo mobile (specificare)
• Documento cartaceo (specificare)
• File o parte di un file
• Strumento di *backup*
• Rete
• Altro _____

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

_____

_____

_____

_____

8. Persone che sono state colpite dalla violazione di dati personali

- N. ____
- Circa _____ persone
- Un numero (ancora) sconosciuto di persone

9. Tipologia di dati coinvolti nella violazione

- Dati anagrafici
- Numero di telefono (fisso o mobile)
- Indirizzo di posta elettronica
- Dati di accesso e di identificazione (user name, password, customer ID, altro)
- Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro) _____
- Altri dati personali (sesso, data di nascita, età, ...), dati sensibili e giudiziari
- Dato non ancora conosciuto

10. Livello di gravità della violazione dei dati personali

(secondo le valutazioni dell'Area/Struttura)

- Basso
- Medio
- Alto
- Molto alto

11. Misure tecniche e organizzative applicate ai dati colpiti dalla violazione

_____

_____

_____

_____

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Notifica di una violazione dei dati personali

(art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del d.lgs. 51/2018)

Tipo di notifica

○ Preliminare[1] ○ Completa ◉ Integrativa [2] rif.

Effettuata ai sensi del ◉ art. 33 RGPD ○ art. 26 d.lgs 51/2018

Sez. A - Dati del soggetto che effettua la notifica

Cognome Nome
E-mail:
Recapito telefonico per eventuali comunicazioni:
Funzione rivestita:

Sez. B - Titolare del trattamento

Denominazione[3]:
Codice Fiscale/P.IVA: Soggetto privo di C.F./P.IVA ☐
Stato:
Indirizzo:
CAP : Città: Provincia:
Telefono:
E-mail:
PEC:

1 Il titolare del trattamento avvia il processo di notifica pur in assenza di un quadro completo della violazione con riserva di effettuare una successiva notifica integrativa. E' obbligatoria la compilazione delle sezioni A, B, B1 e C.
2 Il titolare del trattamento integra una precedente notifica (inserire il numero di fascicolo assegnato alla precedente notifica, se noto)
3 Indicare nome e cognome nel caso di persona fisica

Sez. B1- Dati di contatto per informazioni relative alla violazione

Indicare i riferimenti del soggetto da contattare per ottenere maggiori informazioni circa la violazione

◉ Responsabile della protezione dei dati[4] - prot. n.

○ Altro soggetto[5]

Cognome Nome
E-mail:
Recapito telefonico per eventuali comunicazioni:
Funzione rivestita:

Sez. B2- Ulteriori soggetti coinvolti nel trattamento

Indicare i riferimenti di ulteriori soggetti coinvolti ed il ruolo svolto (contitolare o responsabile del trattamento[6], rappresentante del titolare non stabilito nell'Ue)

Denominazione[7] *:
Codice Fiscale/P.IVA: Soggetto privo di C.F./P.IVA ☐
Ruolo: ○ Contitolare ○ Responsabile ○ Rappresentante

Denominazione *: .....
Codice Fiscale/P.IVA: ..... Soggetto privo di C.F./P.IVA ☐
Ruolo: ○ Contitolare ○ Responsabile

Denominazione *: .....
Codice Fiscale/P.IVA: ..... Soggetto privo di C.F./P.IVA ☐
Ruolo: ○ Contitolare ○ Responsabile

Denominazione *: .....
Codice Fiscale/P.IVA: ..... Soggetto privo di C.F./P.IVA ☐
Ruolo: ○ Contitolare ○ Responsabile

[4] Qualora designato, indicare il numero di protocollo assegnato alla comunicazione dei dati di contatto del RPD
[5] In assenza di un RPD, indicare i riferimenti di un punto di contatto designato per la notifica in questione
[6] In tale tipologia rientra anche il Responsabile individuato ai sensi art. 28, par. 4
[7] Indicare nome e cognome nel caso di persona fisica

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Sez. C - Informazioni di sintesi sulla violazione

1. **Indicare quando è avvenuta la violazione**

- (•) Il
- ( ) Dal (la violazione è ancora in corso)
- ( ) Dal al
- ( ) In un tempo non ancora determinato

Ulteriori informazioni circa le date in cui è avvenuta la violazione

2. **Momento in cui il titolare del trattamento è venuto a conoscenza della violazione**

Data: Ora:

3. **Modalità con la quale il titolare del trattamento è venuto a conoscenza della violazione**

- ( ) Il titolare è stato informato dal responsabile del trattamento
- ( ) Altro[8]

4. **In caso di notifica oltre le 72 ore, quali sono i motivi del ritardo?[9]**

5. **Breve descrizione della violazione**

[8] Ad esempio: Segnalazione da parte di un interessato, comunicazione da parte di terzi, ecc.

[9] Da compilare solo per notifiche tardive.

6. **Natura della violazione**
   - ☐ a) Perdita di confidenzialità[10]
   - ☐ b) Perdita di integrità[11]
   - ☐ c) Perdita di disponibilità[12]

7. **Causa della violazione**
   - ☐ Azione intenzionale interna
   - ☐ Azione accidentale interna
   - ☐ Azione intenzionale esterna
   - ☐ Azione accidentale esterna
   - ☐ Sconosciuta
   - ☐ Altro (specificare)

8. **Categorie di dati personali oggetto di violazione**
   - ☐ Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale, altro...)
   - ☐ Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
   - ☐ Dati di accesso e di identificazione (username, password, customer ID, altro…)
   - ☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…)
   - ☐ Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro…)
   - ☐ Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza o di prevenzione
   - ☐ Dati di profilazione
   - ☐ Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…)
   - ☐ Dati di localizzazione
   - ☐ Dati che rivelino l'origine razziale o etnica
   - ☐ Dati che rivelino opinioni politiche
   - ☐ Dati che rivelino convinzioni religiose o filosofiche
   - ☐ Dati che rivelino l'appartenenza sindacale
   - ☐ Dati relativi alla vita sessuale o all'orientamento sessuale
   - ☐ Dati relativi alla salute
   - ☐ Dati genetici
   - ☐ Dati biometrici
   - ☐ Categorie ancora non determinate
   - ☐ Altro

[10] Diffusione/ accesso non autorizzato o accidentale
[11] Modifica non autorizzata o accidentale
[12] Impossibilità di accesso,perdita, distruzione non autorizzata o accidentale

9. Indicare il volume (anche approssimativo) dei dati personali oggetto di violazione[13]

◯ N.
◯ Circa n.
◯ Un numero (ancora) non definito di dati

10. Categorie di interessati coinvolti nella violazione

☐ Dipendenti/Consulenti
☐ Utenti/Contraenti/Abbonati/Clienti (attuali o potenziali)
☐ Associati,soci, aderenti, simpatizzanti, sostenitori
☐ Soggetti che ricoprono cariche sociali
☐ Beneficiari o assistiti
☐ Pazienti
☐ Minori
☐ Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
☐ Categorie ancora non determinate
☐ Altro (specificare)

☐ Ulteriori dettagli circa le categorie di interessati

11. Numero (anche approssimativo) di interessati coinvolti nella violazione

◯ N. interessati
◯ Circa n. interessati
◯ Un numero (ancora) sconosciuto di interessati

[13] Ad esempio numero di referti, numero di record di un database, numero di transazioni registrate.

Sez. D - Informazioni di dettaglio sulla violazione

1. **Descrizione dell'incidente di sicurezza alla base della violazione**[14]

2. **Descrizione delle categorie di dati personali oggetto della violazione**[15]

3. **Descrizione dei sistemi e delle infrastrutture IT coinvolti nell'incidente, con indicazione della loro ubicazione**

4. **Misure di sicurezza tecniche e organizzative adottate per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture IT coinvolti**[16]

[14] Segue punto 5, 6 e 7 della sez. C
[15] Segue punto 8 della sez. C
[16] Indicare le misure in essere al momento della violazione

Sez. E - Possibili conseguenze e gravità della violazione

1. Possibili conseguenze della violazione sugli interessati

a) In caso di perdita di confidenzialità: [17]

- ☐ I dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento
- ☐ I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati
- ☐ I dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito
- ☐ Altro (specificare)

b) In caso di perdita di integrità: [18]

- ☐ I dati sono stati modificati e resi inconsistenti
- ☐ I dati sono stati modificati mantenendo la consistenza
- ☐ Altro (specificare)

c) In caso di perdita di disponibilità: [19]

- ☐ Mancato accesso a servizi
- ☐ Malfunzionamento e difficoltà nell'utilizzo di servizi
- ☐ Altro (specificare)

Ulteriori considerazioni sulle possibili conseguenze

[17] Da compilare solo nel caso in cui è stata selezionata l'opzione a) del punto 6, Sez. C
[18] Da compilare solo nel caso in cui è stata selezionata l'opzione b) del punto 6, Sez. C
[19] Da compilare solo nel caso in cui è stata selezionata l'opzione c) del punto 6, Sez. C

2. Potenziali effetti negativi per gli interessati

☐ Perdita del controllo dei dati personali
☐ Limitazione dei diritti
☐ Discriminazione
☐ Furto o usurpazione d'identità
☐ Frodi
☐ Perdite finanziarie
☐ Decifratura non autorizzata della pseudonimizzazione
☐ Pregiudizio alla reputazione
☐ Perdita di riservatezza dei dati personali protetti da segreto professionale
☐ Conoscenza da parte di terzi non autorizzati
Qualsiasi altro danno economico o sociale significativo (specificare)

3. Stima della gravità della violazione

○ Trascurabile
○ Basso
○ Medio
○ Alto

Indicare le motivazioni

Sez. F – Misure adottate a seguito della violazione

1. **Misure tecniche e organizzative adottate (o di cui si propone l'adozione[20]) per porre rimedio alla violazione e ridurne gli effetti negativi per gli interessati**

2. **Misure tecniche e organizzative adottate (o di cui si propone l'adozione) per prevenire simili violazioni future**

[20] Nella descrizione distinguere le misure adottate da quelle in corso di adozione

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Sez. G - Comunicazione agli interessati

1. La violazione è stata comunicata agli interessati?

◯ Sì, è stata comunicata il
◯ No, sarà comunicata
il
in una data da definire
◯ No, sono tuttora in corso le dovute valutazioni[21]
◉ No e non sarà comunicata perché:

a) il titolare del trattamento ritiene che la violazione dei dati personali non presenti un rischio elevato per i diritti e le libertà delle persone fisiche;
Spiegare le motivazioni

b) il titolare del trattamento ha messo in atto 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 personali incomprensibili a chiunque non sia autorizzato ad accedervi;

Descrivere le misure applicate

▪ c) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

Descrivere le misure adottate

d) detta comunicazione richiederebbe sforzi sproporzionati.
Descrivere la modalità (comunicazione pubblica o misura simile) tramite la quale gli interessati sono stati informati

[21] Selezionando questa opzione, il titolare del trattamento si impegna a effettuare una integrazione alla presente notifica

2. **Numero di interessati a cui è stata comunicata la violazione**[22]

   N. interessati

3. **Contenuto della comunicazione agli interessati**

4. **Canale utilizzato per la comunicazione agli interessati**
   - ☐ SMS
   - ☐ Posta cartacea
   - ☐ Posta elettronica
   - ☐ Altro (specificare)

[22] Da compilare solo nel caso in cui al punto 1 venga scelta una delle prime due opzioni.

Sez. H - Altre informazioni

1. **La violazione coinvolge interessati di altri Paesi dello Spazio Economico Europeo[23]?**

   ◉ SI (indicare quali):

   ○ NO

2. **La violazione coinvolge interessati di Paesi non appartenenti allo Spazio Economico Europeo?**

   ○ SI (indicare quali):

   ○ NO

3. **La violazione è stata notificata ad altre autorità di controllo[24]?**

   ○ SI (indicare quali):

   ○ NO

4. **La violazione è stata notificata ad altri organismi di vigilanza o di controllo in virtù di ulteriori disposizioni normative[25]?**

   ○ SI (indicare quali):

   ○ NO

5. **E' stata effettuata una segnalazione all'autorità giudiziaria o di polizia?**

   ○ SI
   ○ NO

[23] Fanno parte dello Spazio Economico Europeo tutti gli Stati membri della Unione Europea, nonchè l'Islanda, il Liechtenstein e la Norvegia
[24] Autorità di controllo così come definite ex art. 51 del Regolamento (UE) 2016/679
[25] Ad esempio: Regolamento (UE) 910/2014 (eIDAS), d.lgs. 65/2018 attuativo della Direttiva (UE) 2016/1148 (NIS)

Metodologia di valutazione del rischio connesso alla violazione

Per identificare le modalità di gestione di una violazione e gli eventuali obblighi di notifica e/o di comunicazione, il Responsabile della Protezione dei Dati, con il supporto del Responsabile per la Sicurezza informatica e del Responsabile per la Transizione al digitale di Ateneo nel caso di dati digitalizzati, effettua la valutazione del rischio, come di seguito indicato.

Il livello di rischio è definito sulla base di due parametri: gravità e probabilità.

Gravità: rilevanza degli effetti dannosi che la violazione è in grado di produrre sui diritti e le libertà delle persone coinvolte (es. impedendo il controllo da parte dell'interessato sulla diffusione dei propri dati).

Probabilità: grado di possibilità che si verifichino uno o più eventi temuti (es. la perdita di ogni traccia dei dati).

Ai fini della identificazione dei valori da attribuire ai due parametri per la valutazione del rischio, sono considerati i seguenti fattori:

- tipo di violazione (violazione della riservatezza, violazione dell'integrità, violazione della disponibilità);
- natura, sensibilità e volume dei dati personali;
- facilità nella identificazione degli interessati;
- gravità delle conseguenze per gli interessati;
- particolarità degli interessati;
- particolarità dei responsabili del trattamento;
- numero degli interessati.

GRAVITA'	• Basso: nessun impatto • Medio: impatto poco significativo, reversibile • Alto: impatto significativo, irreversibile
PROBABILITA'	• Basso: l'evento temuto non si manifesta • Medio: l'evento temuto potrebbe manifestarsi • Alto: l'evento temuto si è manifestato

Rischio

DESCRIZIONE RISCHIO	NOTIFICA	COMUNICAZIONE
Basso: assenza di pregiudizio sui diritti e sulle libertà degli interessati e sulla sicurezza dei dati personali utilizzati	**NO**	**NO**
Medio: possibile pregiudizio sui diritti e sulle libertà degli interessati e sulla sicurezza dei dati personali utilizzati	**SI**	**NO**
Alto: pregiudizio concreto e reale sui diritti e sulle libertà degli interessati e sulla sicurezza dei dati personali utilizzati	**SI**	**SI**

Comunicazione della violazione all'interessato

Gentilissimo/a

_____

La informiamo che in data ..... siamo venuti a conoscenza di un evento che potrebbe aver coinvolto i suoi dati personali.

Presumiamo infatti che il _____, alle ore _____, un soggetto terzo non autorizzato abbia acquisito i seguenti dati personali relativi alla sua posizione:

- _____
- _____
- _____

Le possibili conseguenze dell'evento sono le seguenti:

Quale immediata reazione all'evento le confermiamo di aver adottato le seguenti misure di sicurezza:

Per maggiore garanzia e per ogni altra utilità, la invitiamo a:

Per qualsiasi informazione o chiarimento, potrà contattare il Responsabile della Protezione dei Dati (RPD/DPO) dell'Ateneo, _____, ai seguenti recapiti:

- Tel...
- E-mail rpd@unistrasi.it
- Pec: rpd.unistrasi@pec.it

Registro delle violazioni

Per ogni violazione di cui sia accertata l'esistenza, il personale individuato dal Centro Servizi Informatici dell'Università per Stranieri di Siena (qualora la violazione riguardi dati contenuti in sistemi informatici centralizzati) e il Responsabile di Area/Struttura o suo Referente, compilano il **"Registro delle violazioni"**, che riporta:

- numerazione progressiva della violazione;
- data di rilevazione dell'evento;
- natura dell'evento;
- descrizione della violazione;
- soggetti coinvolti;
- conseguenze della violazione;
- misure intraprese: notifica alla Autorità/comunicazione interessati;
- misure da intraprendere: azioni intraprese/azioni da intraprendere.

Il Registro delle violazioni deve essere continuamente aggiornato, consultabile dal Responsabile della Protezione dei Dati (RPD/DPO) e reso disponibile in caso di richiesta del Garante.

Ad integrazione di quanto riportato nel Registro, il RPD/DPO raccoglie e conserva tutti i documenti relativi ad ogni violazione, compresi quelli inerenti le circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Tale documentazione è resa disponibile al Garante per le verifiche di competenza.

per il Titolare del trattamento	**Il Responsabile della Protezione dei Dati**
Il Rettore	**(RPD/DPO)**
f.to Prof. Pietro Cataldi	**f.to Avv. Luigi Pelliccia**