Procedura per la gestione dei Data Breach (artt. 33 e 34 Reg. UE 2016/679)

Versione 1.3

Aggiornata in data 31/01/2025

UNIVERSITÀ DEGLI STUDI DI TRIESTE

Sommario

Università degli Studi di Trieste
Area dei Servizi ICT
Via Alfonso Valerio 12
I - 34127 Trieste

1. Premesse

Una violazione di dati personali (c.d. *Data Breach*) può comportare per le persone fisiche interessate dei danni considerevoli di natura morale, fisica e patrimoniale. Conseguentemente, l'organizzazione che subisce un Data Breach, se non gestito in maniera tempestiva ed efficace, può subire danni ingenti alla propria immagine, nonché danni patrimoniali anche molto elevati.

Con l'entrata in vigore del Reg. UE 2016/679 (GDPR), è stato introdotto l'obbligo per ogni organizzazione di gestire i Data Breach, annotarli in un apposito registro e, ove necessario, notificarli all'Autorità Garante e comunicarli alle persone fisiche interessate. Il mancato rispetto delle disposizioni in materia di Data Breach può portare l'organizzazione a subire importanti sanzioni.

Poiché l'eliminazione totale del rischio è per definizione impossibile, anche l'organizzazione più attenta può subire un Data Breach. Pertanto, le violazioni o potenziali violazioni non vanno mai nascoste o trascurate ma comunicate ai soggetti incaricati della loro gestione. Infatti, ogni violazione è utile all'organizzazione per individuare le proprie vulnerabilità e migliorarsi.

Il presente documento è redatto a cura del gruppo di supporto al RPD con la consulenza del RPD stesso, e viene aggiornato periodicamente. Nella procedura di seguito esposta, vengono individuati i criteri per riconoscere un Data Breach e le regole per gestirlo. Tutto il personale è tenuto a leggere, conoscere e rispettare, secondo i compiti affidati, la presente procedura che **sarà oggetto di specifica circolare interna all' Ateneo.**

Le denominazioni riferite a persone, riportate solo nella forma maschile, si riferiscono indistintamente a persone di genere maschile e femminile.

2. Riconoscere un Data Breach

Rappresenta un Data Breach o violazione di sicurezza qualsiasi evento in conseguenza del quale si verifica una violazione di dati personali. Più precisamente, qualsiasi evento 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, secondo l'articolo 4, punto 12 del Regolamento Ue 679/2016.

Si ha un Data Breach ogniqualvolta si verifica una:

1) violazione della **riservatezza** dei dati (in caso di divulgazione di dati personali o accesso agli stessi non autorizzati o accidentali);
2) violazione dell'**integrità** dei dati (in caso di modifica non autorizzata o accidentale di dati personali);

Università degli Studi di Trieste
Area dei Servizi ICT
Via Alfonso Valerio 12
I - 34127 Trieste

3) violazione della **disponibilità** dei dati (in caso di perdita, impossibilità di accesso o distruzione accidentali o non autorizzate di dati personali).

Sono Data Breach le violazioni che riguardano **dati personali**, ovvero: 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.

I Data Breach possono avere sia natura informatica (es. un malware o un attacco hacker) che analogica (es. lo smarrimento di documentazione cartacea contenente dati personali).

Per aiutare il personale a riconoscerli, vengono forniti di seguito alcuni esempi di Data Breach (informatico) più comuni.

- smarrimento o furto di un dispositivo informatico contenente dati personali (laptop, tablet, smartphone, chiavi USB, Hard Disk esterni etc.) (perdita di disponibilità e riservatezza);
- guasto o non corretto funzionamento di un dispositivo informatico contenente dati personali (perdita di disponibilità);
- azione di un virus informatico o malware (perdita di riservatezza, disponibilità ed integrità);
- accesso non autorizzato ad un database o ad un dispositivo informatico (perdita di riservatezza e potenzialmente integrità);
- compromissione di una password utilizzata per accedere a dati aziendali (perdita di riservatezza, potenziale integrità e disponibilità);
- divulgazione su Internet di informazioni, dati, immagini senza autorizzazione (perdita di riservatezza);
- cancellazione accidentale di dati personali non recuperabili (perdita di disponibilità);
- invio di dati personali riservati ad un destinatario sbagliato (perdita di riservatezza);

Di seguito si riportano invece alcuni casi di Data Breach (analogico) più comuni.

- accesso non autorizzato a locali aziendali riservati o ad un archivio cartaceo (perdita di riservatezza, potenziale integrità e disponibilità);
- distruzione o perdita di un archivio cartaceo, schede o formulari contenenti dati personali (perdita di riservatezza e disponibilità);
- invio in modo analogico di dati personali riservati ad un destinatario sbagliato (perdita di riservatezza);

In caso di dubbio, è sempre necessario rivolgersi immediatamente al gruppo di supporto RPD, gruppodpo@units.it:

Università degli Studi di Trieste
Area dei Servizi ICT
Via Alfonso Valerio 12
I - 34127 Trieste

Si ha un Data Breach anche quando la violazione riguarda un fornitore che tratta dati personali per conto dell'Università di Trieste (ad esempio un fornitore di servizi informatici, un partner in un progetto, un'agenzia etc.).

3. Segnalazione del Data Breach

Quando si riconosce o si sospetta che si sia verificato un Data Breach, questo deve essere comunicato senza ingiustificato ritardo al Titolare che dovrà avviare le procedure previste dagli articoli 33 e 34 del Regolamento UE 679/2016.

La comunicazione di un Data Breach può arrivare dai seguenti soggetti:

INTERNAMENTE

- da personale dipendente;
- da personale studentesco;
- da personale convenzionato/stagisti/tirocinanti etc;

ESTERNAMENTE

- da parte degli interessati;
- da parte degli organi pubblici (Agid, Polizia, giornalisti etc.);
- da parte dei responsabili del trattamento (fornitori);
- da parte di altri soggetti;

4. Soggetti autorizzati alla gestione del Data Breach

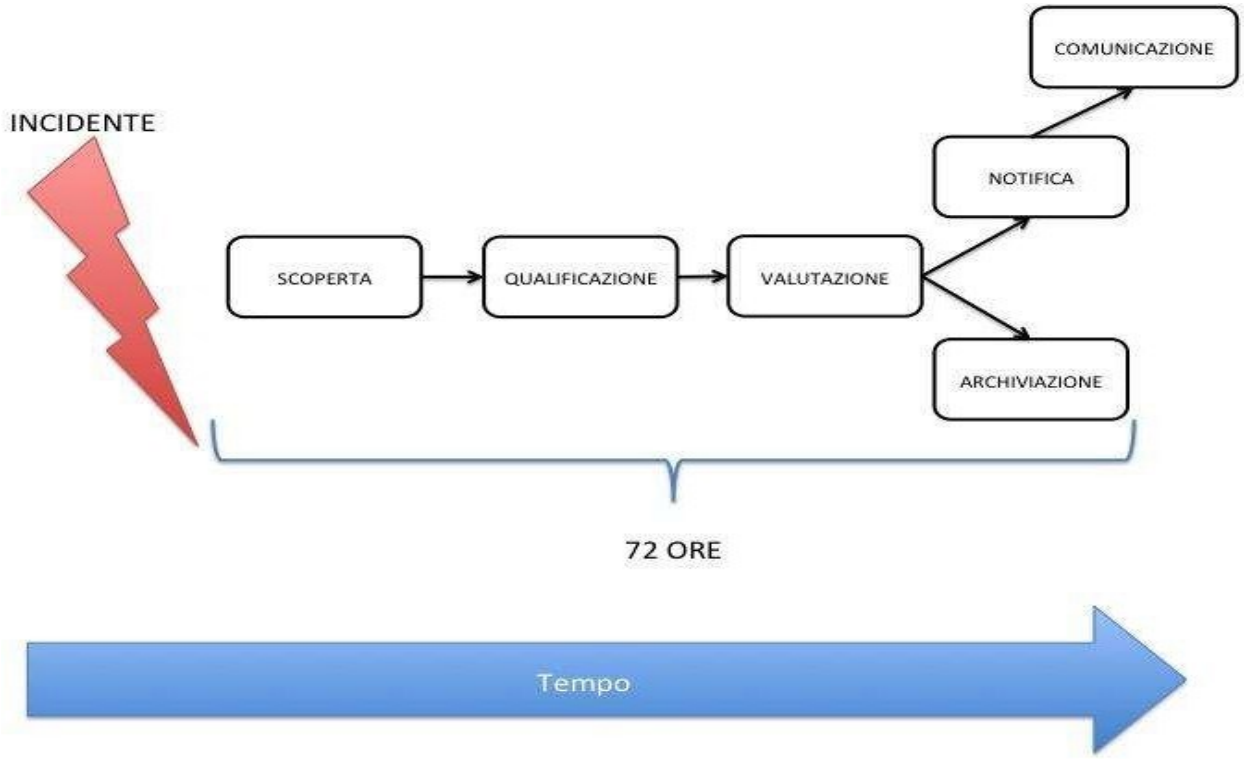
I soggetti destinatari delle segnalazioni di cui al punto 3 devono prendere immediatamente in carico la gestione dell'incidente.

Gli stessi sono selezionati dal Titolare secondo le competenze della struttura di appartenenza e sono individuabili nel:

- Il Gruppo RPD;
- Il Gruppo di lavoro competente in materia di Cybersicurezza.

5. Procedura in caso di Data Breach

Università degli Studi di Trieste
Area dei Servizi ICT
Via Alfonso Valerio 12
I - 34127 Trieste



Nell'eventualità in cui si constati o si sospetti un evento di Data Breach **Informatico** (***SCOPERTA***) è necessario inviare tempestivamente una notifica all'indirizzo sicurezzainformatica@units.it al quale risponde il SOC (come da organigramma della sicurezza informatica) nella quale si indicano gli elementi utili ad avviare gli approfondimenti del caso.

Sarà necessario compilare l'**ALLEGATO A) scheda rilevazione evento critico di sicurezza.**

Il SOC **entro 12 ore informa** il RPD (dpo@units.it), il CISO/CIO (rtd@units.it), il RSGSI (ict.sgsi@units.it) ed il gruppo di supporto al RPD (gruppodpo@units.it), che contatta i responsabili e/o le persone coinvolte dell'Area dei Servizi ICT, dei Dipartimenti o altra struttura periferica nonché,

se del caso, dell'Amministrazione Centrale per la gestione dell'incidente e la continuità operativa e, **in caso di accertata gravità, preavvisa il Titolare**.

Nell'eventualità in cui si constati o si sospetti un evento di Data Breach **analogico** (***SCOPERTA***) è necessario inviare tempestivamente una notifica al gruppo di supporto al RPD (gruppodpo@units.it), che **entro 12 ore informa** il RPD (dpo@units.it), il CISO/CIO (rtd@units.it), il RSGSI (ict.sgsi@units.it), e contatta i responsabili e/o le persone coinvolte dell'Amministrazione Centrale/Dipartimenti o altra struttura periferica per la gestione dell'incidente e la continuità operativa e, **in caso di accertata gravità, preavvisa il Titolare**.

5.1 Qualificazione

Una volta ricevuta la segnalazione di un Data Breach, devono essere attivate immediatamente le procedure necessarie a contenere l'impatto della violazione. Quando l'evento ha natura informatica, l'Area dei Servizi ICT deve porre in essere le operazioni necessarie a mitigare, per quanto possibile, gli effetti delle violazioni (es. decidere lo spegnimento dei dispositivi coinvolti, reset delle password, cancellazione da remoto dei dati contenuti su dispositivi mobili, messa in sicurezza dei back-up etc.).

Una volta poste in atto le misure urgenti, devono essere raccolte tutte le informazioni (***QUALIFICAZIONE***) necessarie alla valutazione dell'evento, in modo da poter valutare l'opportunità di effettuare la notifica all'Autorità Garante. Solo qualora non sia possibile fornire tutte le informazioni contestualmente alla prima notifica o alla prima comunicazione, esse potranno essere integrate in fasi successive senza ulteriore ingiustificato ritardo (artt. 33 e 34 Reg. UE 2016/679).

Ove il Data Breach sia occorso ad un fornitore dell'Università di Trieste, le informazioni necessarie devono essere fornite al Titolare, senza ingiustificato ritardo dopo esserne venuto a conoscenza.

L'analisi dell'evento dovrà comprendere le seguenti informazioni:

☐ la natura della violazione (perdita di riservatezza, integrità o disponibilità);

☐ l'identificazione dei dati compromessi e dei trattamenti coinvolti;

☐ l'identificazione degli interessati i cui dati sono stati violati;

☐ le misure attuate o da attuare per la mitigazione del danno (limitazioni degli effetti, raccolta di prove, azioni e tempi di ripristino);

☐ individuazione delle vulnerabilità sfruttate dalla violazione;

☐ le possibili azioni di miglioramento per eliminare o ridurre la vulnerabilità.

Le suddette operazioni dovranno essere svolte dai soggetti autorizzati individuati dal Titolare.

Il tempo consigliato per il completamento delle suddette operazioni è di **24 ore dalla conoscenza** evento.

5.2 Valutazione

Non sussiste l'obbligo di notifica della violazione all'Autorità Garante quando è "improbabile" che questa comporti un rischio per i diritti e le libertà delle persone fisiche (art. 33 Reg. UE 2016/679). Occorre quindi effettuare una valutazione dell'evento per decidere se sia necessario notificare il Data Breach.

Per poter valutare l'impatto della violazione sui diritti e le libertà delle persone fisiche, occorre prendere in considerazione i seguenti fattori:

- Natura dai dati coinvolti (una maggiore attenzione deve essere posta per i dati appartenenti alle categorie particolari di cui agli artt. 9 e 10 Reg. UE 2016/679, ed a tutti quei dati la cui compromissione potrebbe causare danni fisici, morali o patrimoniali per i soggetti interessati);
- il numero degli interessati coinvolti;
- la durata della violazione;
- le misure di contenimento applicate (se è stata adottata la criptazione dei dati e mantenuta segreta la password di decriptazione ne consegue l'improbabilità di una compromissione della riservatezza).

Sotto il coordinamento del Gruppo di lavoro Cybersicurezza, tutti i settori operativi coinvolti effettuano un'analisi relativa all'incidente e forniscono al RPD gli elementi utili a descriverlo ai fini della sua valutazione.

Nel caso permanga un dubbio considerevole sulla probabilità o meno del rischio, la notifica deve essere effettuata.

La decisione relativa alla notifica spetta al Titolare, il quale si avvale del Gruppo di Supporto RPD. Nell'ipotesi in cui si decida di non notificare il Data Breach, questo deve comunque essere appuntato nel Registro delle violazioni, secondo quanto indicato nel punto 5.4.

Università degli Studi di Trieste
Area dei Servizi ICT
Via Alfonso Valerio 12
I - 34127 Trieste

5.3 Notifica

La notifica all'Autorità Garante deve essere effettuata entro il **termine massimo di 72 ore** dalla conoscenza della violazione e comunque senza ingiustificato ritardo. Qualora la notifica non venga effettuata nel termine di 72 ore, deve essere corredata dei motivi del ritardo. Qualora sia necessario integrare le informazioni fornite con la prima notifica, sarà possibile fornirle in momenti successivi, senza ingiustificato ritardo.

La notifica deve essere effettuata compilando il modulo predisposto dall'Autorità Garante e disponibile per il download presso il suo sito web utilizzando la firma digitale del Rappresentante legale del centro.

La notifica deve perlomeno:

1. descrivere la natura della violazione dei dati personali 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;
2. comunicare il nome e i dati di contatto del RPD;
3. descrivere le probabili conseguenze della violazione dei dati personali;
4. descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

5.4 Comunicazione agli interessati

In caso di elevato rischio per la libertà e i diritti degli individui, oltre alla notifica della violazione all' Autorità, è necessario informare gli interessati sul fatto avvenuto, sui dati violati e sugli accorgimenti necessari a ridurre il rischio.

La comunicazione agli interessati non è richiesta nei seguenti casi:

- quando 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, quali la cifratura;
- quando 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;

Università degli Studi di Trieste
Area dei Servizi ICT
Via Alfonso Valerio 12
I - 34127 Trieste

- la comunicazione richiederebbe sforzi spropositati ed in tal caso si ritiene opportuno adottare il metodo della comunicazione pubblica.

La comunicazione avviene ad opera dell'ufficio individuato in relazione all'interessato/i coinvolto/i e descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali. A tale scopo è possibile utilizzare l'**ALLEGATO B) schema di comunicazione al soggetto interessato**.

La comunicazione agli interessati deve contenere le seguenti informazioni:

- i dati di contatto dell'RPD per rivolgersi all' Università di Trieste ed ottenere informazioni riguardanti il Data Breach;
- descrivere le probabili conseguenze della violazione dei dati personali;
- la descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

La necessità circa la comunicazione agli interessati deve essere valutata prima della notifica al Garante. La decisione di non procedere alla comunicazione agli interessati deve essere idoneamente motivata e annotata nel registro delle violazioni.

5.5 Archiviazione sul Registro delle violazioni

Ai sensi dell'art. 33, paragrafo 5 Reg. UE 2016/679, ciascuna violazione deve essere documentata ed annotata nell'apposito registro delle violazioni.

L'annotazione deve essere effettuata anche nell'eventualità in cui sia stato deciso di omettere la notifica all'Autorità Garante. In questo caso, deve essere annotata la motivazione per la quale la notifica è stata ritenuta non necessaria. Allo stesso modo, deve essere annotata nel registro la motivazione per la quale non si è ritenuta necessaria la comunicazione agli interessati.

L'annotazione deve contenere tutte le informazioni di cui al punto 5 della presente procedura. A ciò dovranno aggiungersi le informazioni relative alla notifica effettuata al Garante ed alla comunicazione agli interessati, oppure le motivazioni per le quali non si è ritenuto procedere a notificare all'Autorità.

6. Piano di miglioramento

Università degli Studi di Trieste
Area dei Servizi ICT
Via Alfonso Valerio 12
I - 34127 Trieste

Il Data Breach, anche quando non si sia tradotto in un danno per dati personali o informazioni aziendali, costituisce un'opportunità per il miglioramento continuo dell'organizzazione. Il Data Breach può essere utilizzato per individuare delle vulnerabilità e contrastarle, riducendo così il rischio che violazioni identiche o simili si verifichino nuovamente.

L'Ateneo ha adottato un insieme di regolamenti, volti a prevenire i rischi di Data Breach (vedi Normativa di Ateneo - Regolamenti area informatica):

- Accesso al Sistema Integrato di Reti dell'Ateneo - SIRA
- Regolamento in materia di utilizzo della posta elettronica e della rete internet messi a disposizionedall'Università di Trieste
- Regolamento per i servizi web di Ateneo.

Il presente piano di gestione della sicurezza è pubblicato nella pagina *Sicurezza informatica* presente nella sezione *intranet* del portale di Ateneo.

Il personale dell'Ateneo viene sensibilizzato sul tema della sicurezza informatica attraverso periodici appuntamenti formativi ed attraverso una pagina dedicata presente sul portale di Ateneo in *intranet, Sicurezza informatica* e può contare sull'indirizzo mail di supporto sicurezzainformatica@units.it.

Al fine di contenere la portata dei Data Breach, il titolare valuta l'opportunità di impartire apposite indicazioni e istruzioni operative, avvalendosi anche del supporto del RPD.

Periodicamente l'Ateneo aggiorna il rapporto relativo ai controlli previsti dalle "Misure minime di sicurezza ICT per le pubbliche amministrazioni", in ottemperanza a quanto previsto dalla circolare 18 aprile 2017, n. 2/2017 dall'AGID – Agenzia per l'Italia Digitale:

- analisi e ricognizione della situazione attuale in termini di architettura hardware e software
- elenco dei software autorizzati e regolamenti operativi in tal senso
- esecuzione periodica di scansioni sui sistemi per la rilevazione di software non autorizzato/aggiornato
- definizione configurazioni sicure standard per la protezione dei sistemi operativi
- verifica e certificazione che le operazioni di amministrazione di sistema remote di server, workstation e dispositivi di rete siano effettuate per mezzo di connessioni sicure
- scansione di vulnerabilità ai sensi del punto 4.1.1 della circolare AGID
- limitazione dei privilegi di administrator ai soli utenti che abbiano competenze adeguate e la necessità operativa dimostrabile di modificare la configurazione dei sistemi
- censimento account di administrator
- individuazione e inventariazione dei soggetti che operano con qualifica o comunque profilo diadministrator
- nomina ad amministratore di sistema (soggetti sia interni che esterni)

I controlli sono descritti ed eseguiti dalle strutture dell'Area dei Servizi ICT per l'Amministrazione Centrale ed i sistemi gestiti centralmente, nonché dai Direttori di Dipartimento e dal Settore Servizi per il Trasferimento delle Conoscenze – SBA per i sistemi periferici.

Anche in base all'esito dei controlli di cui sopra, vengono aggiornate con continuità le configurazioni dei dispositivi hardware ed i sistemi software rivolti a ridurre i rischi informatici (firewall perimetrali, dispositivi di accesso VPN, antispam ed antivirus per postazioni di lavoro e posta elettronica, misure infrastrutturali di isolamento fisico e logico di determinate categorie di dispositivi, dispositivi di backup, sistemi di cifratura e pseudonimizzazione, ecc…)

Ad opera delle strutture dell'Area dei Servizi ICT, prima fra tutte l'Ufficio Reti di Ateneo, con cadenza almeno semestrale, vengono eseguite scansioni sull'intera infrastruttura di rete di Ateneo, utilizzando sistemi di vulnerability assessment, per rilevare programmi e sistemi operativi non aggiornati o non più supportati. Tali vulnerabilità sono riportate ai rispettivi amministratori.

Specifici canali e modalità di comunicazione sono adottati per inviare e ricevere notifiche riguardo le problematiche di sicurezza informatica:

- internamente, attraverso le liste di distribuzione dei referenti di rete (refrete@units.it) e deitecnici informatici (tecsia@units.it),
- internamente, attraverso le liste di distribuzione a tutto il personale di Ateneo e/o ad un sotto-insieme (es. Responsabili di Struttura, Personale Docente, ecc…),
- con il GARR-CERT - Computer Emergency Response Team della comunità dell'istruzione e dellaricerca nazionale,
- con il CERT-Agid - Computer Emergency Response Team Pubblica Amministrazione,
- con il CSIRT – "Computer Security Incident Response Team" dell'Agenzia per la Cybersicurezza Nazionale
- con il Compartimento Polizia Postale e delle Comunicazioni per il Friuli V.G.

Per gli aspetti relativi alla protezione dei dati, in particolare il Data Breach, sono attivi gli indirizzi gruppodpo@units.it – dpo@units.it con cui è possibile contattare l'RPD - Responsabile della Protezione dei Dati dell'Ateneo.

UNIVERSITÀ DEGLI STUDI DI TRIESTE

ALLEGATO A) SCHEDA RILEVAZIONE EVENTO CRITICO DI SICUREZZA

n° Codice Scheda Rilevazione Evento (Incidente di Sicurezza):
_____

Data avvio compilazione:
_____

Ora avvio compilazione:
_____

Segnalazione Incidente di Sicurezza (riportare i dati personali del segnalante):

☐ SOGGETTO INTERNO

Cognome:
_____

Nome:_____

email: _____

☐ Autorizzato

Funzione rivestita (es. Personale dipendente, studente, stagista ecc.):
_____

Dipartimento di cui fa parte:
_____

☐ SOGGETTO ESTERNO

Cognome:
_____

Nome:_____

email: _____

☐ Interessato
☐ Responsabile del Trattamento (indicare il fornitore dell'Università)

_____

☐ Organo Pubblico (indicare quale)

_____

☐ Altro soggetto (indicare il proprio ruolo)

_____

Descrizione sintetica evento critico (indicare eventuale database o software coinvolti):
_____

Università degli Studi di Trieste
Area dei Servizi ICT
Via Alfonso Valerio 12
I - 34127 Trieste

Università degli Studi di Trieste
Area dei Servizi ICT
Via Alfonso Valerio 12
I - 34127 Trieste

UNIVERSITÀ DEGLI STUDI DI TRIESTE

ALLEGATO B) SCHEMA DI COMUNICAZIONE AL SOGGETTO INTERESSATO

Al Sig./Sig.ra_____

email _____

Oggetto: **Comunicazione di una violazione di dati personali all'interessato ai sensi dell'art. 34 del Regolamento UE 2016/679.**

Egregio Sig./Gentile Sig.ra,

L'Università di Trieste con sede in p.le Europa 1 (TS), in qualità di Titolare del trattamento dei dati personali, ai sensi e per gli effetti di cui all'art. 34 del Regolamento Europeo 2016/679 in materia di protezione dei dati personali

COMUNICA

Il seguente evento che ha riguardato una violazione di sicurezza relativa ai Suoi dati personali

[completare inserendo le informazioni relative ai seguenti campi:

- *Descrizione della natura della violazione*
- *Descrizione delle probabili conseguenze della violazione*
- *Descrizione delle misure adottate o in corso di adozione da parte dell'Università di Trieste, per porre rimedio alla violazione e, se del caso, per attenuarne i possibili effetti negativi*
- *Dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto]*

Nel rimanere a disposizione per eventuali ulteriori informazioni, si porgono Distinti Saluti

Il Titolare del Trattamento