Data Breach Policy

Procedura di notifica di violazione dei dati personali

Data di ultima revisione della policy: 01/02/2023

INDICE

1. PREMESSE

La **Libera Università di Lingue e Comunicazione IULM**, ai sensi del Regolamento Europeo 2016/679 (da qui in avanti GDPR), è tenuta a mantenere sicuri i dati personali trattati nell'ambito delle proprie attività istituzionali e ad agire senza ingiustificato ritardo in caso di violazione dei dati stessi (incluse eventuali notifiche all'Autorità Garante competente ed eventuali comunicazioni agli interessati).
È di fondamentale importanza predisporre azioni da attuare nell'eventualità in cui si presentino violazioni concrete, potenziali o sospette di dati personali, ciò al fine di evitare rischi per i diritti e le libertà degli interessati, nonché danni economici all'Ateneo e per poter riscontrare nei tempi e nei modi previsti dalla normativa europea l'Autorità Garante e/o gli interessati.
Le sanzioni previste dal GDPR per omessa notifica di Data Breach all'Autorità di Controllo o omessa comunicazione agli interessati o entrambi gli adempimenti, nei casi in cui siano soddisfatti i requisiti di cui agli artt. 33 e 34 GDPR, può comportare l'applicazione in capo alla Libera Università di Lingue e Comunicazione IULM di una sanzione amministrativa pecuniaria fino a 10 milioni di euro o fino al 2% del "fatturato" annuo totale dell'esercizio precedente, anche accompagnata da una misura correttiva ai sensi dell'art. 58 c. 2.

2. SCOPO

Lo scopo di questa procedura è:

- sensibilizzare i dipendenti riguardo le responsabilità in materia di protezione dei dati personali e riguardo all'importanza della tempestiva segnalazione di un incidente sulla Sicurezza
- di disegnare un flusso comunicativo per la gestione delle violazioni dei dati personali trattati da Libera Università di Lingue e Comunicazione IULM in qualità di Titolare del trattamento (di seguito "**Titolare del trattamento**").

3. COS'È UNA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

Una violazione di dati personali è ogni infrazione alla sicurezza degli stessi 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.

Le violazioni di dati personali possono accadere per un ampio numero di ragioni che possono includere:

- divulgazione di dati confidenziali a persone non autorizzate;
- perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
- perdita o furto di documenti cartacei;
- infedeltà aziendale (ad esempio: data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico);
- accesso abusivo (ad esempio: data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
- casi di pirateria informatica;
- banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo "owner";
- virus o altri attacchi al sistema informatico o alla rete aziendale;
- violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);
- smarrimento di pc portatili, devices o attrezzature informatiche aziendali;
- invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

4. A CHI SONO RIVOLTE QUESTE PROCEDURE?

Queste procedure sono rivolte a tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del **Titolare del trattamento** (meglio descritti al punto 5 della presente procedura) quali:

- i lavoratori dipendenti, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto intercorrente - abbiano accesso ai dati personali trattati nel corso del proprio impiego per conto del Titolare del trattamento (di seguito genericamente denominati Destinatari interni);
- qualsiasi soggetto (persona fisica o persona giuridica) diverso dal Destinatario interno 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 (di seguito genericamente denominati Destinatari esterni);

di seguito, genericamente denominati "Destinatari".

Tutti i Destinatari devono essere debitamente informati dell'esistenza della presente procedura, mediante metodi e mezzi che ne assicurino la comprensione.

Il rispetto della presente 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 terze parti inadempienti, secondo le normative vigenti in materia.

5. A QUALI TIPI DI DATI SI RIFERISCONO QUESTE PROCEDURE

Queste procedure si riferiscono a:

- dati personali trattati "da "e "per conto" del Titolare del trattamento, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo;
- dati personali conservati o trattati a mezzo di qualsiasi altro sistema aziendale.

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.

6. GESTIONE COMUNICAZIONE DI DATA BREACHES

Le violazioni di dati personali sono gestite dal Titolare del trattamento o da un suo delegato, sotto la supervisione del DPO.

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, dovrà immediatamente **informare dell'incidente il superiore gerarchico** il quale si occuperà, con il supporto dei Destinatari stessi, di informare il Titolare del trattamento o un suo delegato mediante la compilazione dell'**Allegato A – Modulo di comunicazione interna di Data Breach** da inviare a mezzo mail all'indirizzo databreach@iulm.it

7. GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI

Per gestire una violazione dei dati personali è necessario seguire i seguenti quattro step:

Step 1: Identificazione e indagine preliminare

Step 2: Contenimento, recovery e risk assessment

Step 3: Eventuale notifica all'Autorità Garante

Step 4: Eventuale comunicazione agli interessati

Step 5: Documentazione della violazione

Step 1: Identificazione e indagine preliminare

L'**Allegato A**, debitamente compilato, permetterà al Titolare del trattamento o un suo delegato, di condurre una valutazione iniziale riguardante la notizia dell'incidente occorso, ciò al fine di stabilire se si sia effettivamente verificata un'ipotesi di Data Breach (violazione) e se sia necessaria un'indagine più approfondita dell'accaduto, procedendo con il risk assessment (step 2) e con il coinvolgimento del DPO.

Nel caso in cui si tratti di violazione di dati contenuti in un sistema informatico, il Titolare del trattamento o un suo delegato **dovrà coinvolgere in tutta la procedura indicata nel presente documento anche il Responsabile dell'Ufficio IT o un suo delegato in caso di assenza.**

Detta valutazione iniziale sarà effettuata attraverso l'esame delle informazioni riportate nell'Allegato A, quali:

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

Step 2: Contenimento, Recovery e risk assessment

Una volta stabilito che un Data Breach è avvenuto, il Titolare del trattamento o un suo delegato insieme al DPO dovranno stabilire:

- se esistono azioni che possano limitare i danni che la violazione potrebbe causare (i.e. 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… ecc.);
- una volta identificate tali azioni, quali siano i soggetti che devono agire per contenere la violazione;
- se sia necessario notificare la violazione all'Autorità Garante per la Protezione dei dati personali (ove sia probabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche);
- se sia necessario comunicare la violazione agli interessati (ove la violazione presenti un elevato rischio per i diritti e le libertà delle persone fisiche).

Al fine di individuare la necessità di notificazione all'Autorità Garante e di comunicazione agli interessati, il Titolare del trattamento e il DPO valuteranno la gravità della violazione utilizzando l'**Allegato B - Modulo di valutazione del Rischio connesso al Data Breach** che dovrà essere esaminato unitamente all'Allegato A, tenendo, altresì, in debita considerazione i principi e le indicazioni di cui all'art. 33 GDPR .

Se, infatti, gli obblighi di notifica all'Autorità di Controllo scaturiscono dal superamento di una soglia di rischio *semplice*, l'art. 34 GDPR prevede, invece, che l'obbligo di comunicazione agli interessati sia innescato dal superamento di un rischio *elevato*.

Step 3: Eventuale notifica all'Autorità Garante competente

Una volta valutata la necessità di effettuare notifica della violazione dei dati subita sulla base della procedura di cui allo step 2, secondo quanto prescritto dal Regolamento (UE) 2016/679, la **Libera Università di Lingue e Comunicazione IULM** dovrà provvedervi, senza ingiustificato ritardo e, ove possibile entro 72 ore dal momento in cui ne è venuta a conoscenza.

Pertanto, il Titolare del trattamento e il DPO individueranno l'Autorità di Controllo competente sulla base delle informative e/o della valutazione d'impatto sulla protezione dei dati già in essere presso la **Libera Università di Lingue e Comunicazione IULM** in relazione ai dati oggetto di violazione (in mancanza di tale documentazione che abbia preventivamente individuato l'Autorità Garante competente, la stessa sarà da individuare in quella dello Stato in cui è ubicato lo stabilimento principale o lo stabilimento unico del Titolare del trattamento, anche per i trattamenti transfrontalieri eventualmente effettuati).

Una volta determinata l'Autorità di Controllo competente, il Titolare del trattamento e il DPO individueranno la corretta modulistica da utilizzare per effettuare la notificazione e vi provvederanno.

Step 4: Eventuale comunicazione agli interessati

Una volta valutata la necessità di effettuare la comunicazione della violazione dei dati a coloro dei cui dati si tratta, sulla base della procedura di cui allo step 2, secondo quanto prescritto dal Regolamento (UE) 2016/679, la **Libera Università di Lingue e Comunicazione IULM** dovrà provvedervi, senza ingiustificato ritardo.

Quanto al contenuto di tale comunicazione, il Titolare del trattamento o da un suo delegato e il DPO dovranno:

- comunicare il nome e i dati di contatto del Responsabile della protezione dei dati (DPO);
- descrivere le probabili conseguenze della violazione dei dati personali;
- 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, se del caso, per attenuarne i possibili effetti negativi.

Quanto alle modalità di comunicazione, caso per caso, il Titolare del trattamento o da un suo delegato e il DPO dovranno sempre privilegiare la modalità di comunicazione diretta con i soggetti interessati (quali e- mail, 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 fraintesi 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.

Step 5: Documentazione della violazione

Indipendentemente dalla valutazione circa la necessità di procedere a notificazione e/o comunicazione della violazione di Data Breach, ogni qualvolta si verifichi un incidente comunicato dai Destinatari attraverso l'Allegato A, la Libera Università di Lingue e Comunicazione IULM sarà tenuta a documentarlo.

Tale documentazione sarà affidata al Titolare del trattamento o da un suo delegato con l'ausilio del Responsabile dell'Ufficio IT (qualora la violazione riguardi dati contenuti in sistemi informatici) vi provvederà mediante la tenuta dell'**Allegato C - Registro dei Data Breach**, secondo le informazioni ivi riportate: (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 all'Autorità 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 l'Autorità chieda di accedervi.

ALLEGATO A – MODULO DI COMUNICAZIONE DATA BREACH

Qualora scopra un Data Breach, è pregato di informare immediatamente il Suo superiore gerarchico, il quale, a sua volta, dovrà compilare la modulistica a seguire e inviarla a mezzo e-mail al seguente indirizzo email: databreach@iulm.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 della persona che ha riferito della violazione:	
Dati di contatto della persona che ha riferito della violazione (indirizzo e-mail, numero telefonico): *In caso di destinatario esterno indicare 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 del dipartimento:	
data:	

ALLEGATO B – MODULO DI VALUTAZIONE DEL RISCHIO CONNESSO AL DATA BREACH
secondo le linee guida ENISA

Questa sezione è a cura del Team Privacy dell'Ateneo, sentito il DPO, l'Ufficio IT e il Responsabile dell'ufficio coinvolto dalla violazione.

CONTESTO DEL TRATTAMENTO		PUNTEGGIO
DATI COMUNI	Es. Dati anagrafici, dati di contatto, dati sulla vita della famiglia, esperienze professionali, dati sulla formazione	
	Punteggio preliminare: quando la violazione coinvolge dati comuni e il Titolare non è consapevole dei fattori aggravanti	**1**
	Il punteggio potrebbe essere **incrementato di 1** quando il volume dei dati, le caratteristiche del Titolare ed il profilo dell'interessato possono permettere di fare ipotesi e/o identificare lo status sociale/finanziario	**2**
	Il punteggio potrebbe essere **incrementato di 2** quando i dati comuni o le caratteristiche del Titolare possono portare a fare ipotesi sulla salute dell'interessato, l'orientamento sessuale, le idee politiche o religiose.	**3**
	Il punteggio potrebbe essere **incrementato di 3** per certe caratteristiche dell'interessato (vulnerabilità, minore età). In questo caso i dati sono critici per la sicurezza personale o le condizioni fisiche/ psicologiche	**4**
DATI COMPORTAMENTALI	Es. residenza, dati di traffico, dati sulle preferenze abituali o le abitudini, etc.	
	Punteggio preliminare: quando la violazione coinvolge dati comuni e il Titolare non è consapevole dei fattori aggravanti o attenuanti	**2**
	Il punteggio potrebbe **essere diminuito di 1** quando la natura dei dati non permette una notevole comprensione delle informazioni riguardanti il comportamento dell'interessato, oppure i dati possono essere evinti facilmente (indipendentemente dalla violazione) attraverso fonti pubblicamente disponibili (es. combinazioni di informazioni dalle ricerche web)	**1**
	Il punteggio potrebbe essere **incrementato di 1** quando il volume dei dati comportamentali e/o le caratteristiche del Titolare sono tali che può essere creato un profilo dell'interessato, svelando informazioni circa le sue abitudini quotidiane	**3**
	Il punteggio potrebbe essere **incrementato di 2** (es. se può essere creato un profilo basato su dati particolari)	**4**

DATI FINANZIARI	Qualsiasi tipo di dato finanziario (es. reddito, transazioni finanziarie, estratto conto bancario, investimenti, carte di credito, fatture, ecc.)	
	Punteggio preliminare: quando la violazione coinvolge dati finanziari e il Titolare non è consapevole dei fattori aggravanti o attenuanti	**3**
	Il punteggio potrebbe essere **diminuito di 2** quando la natura dei dati non permette una comprensione delle informazioni finanziarie dell'interessato (es. il fatto che una persona è cliente di una certa banca senza ulteriori dettagli)	**1**
	Il punteggio potrebbe essere **diminuito di 1**, quando i dati includono informazioni finanziarie ma non permettono una comprensione della situazione/stato finanziario dell'interessato (es. semplice numero di conto corrente senza altri dati)	**2**
	Il punteggio potrebbe essere **incrementato di 1** quando la natura e/o il volume dei dati le informazioni finanziarie sono svelate (es. carta di credito) e ciò potrebbe permettere una frode o potrebbe essere creato un profilo sociale/finanziario	**4**
DATI PARTICOLARI	Qualsiasi tipo di dato sensibile (es. opinioni politiche, dati sanitari, vita sessuale/orientamento sessuale)	
	Punteggio preliminare: quando la violazione Coinvolge dati sensibili e il Titolare non è consapevole dei fattori aggravanti o attenuanti	**4**
	Il punteggio potrebbe essere **diminuito di 3** quando la natura dei dati non permette una comprensione dei comportamenti degli individui oppure i dati possono essere raccolti facilmente (indipendentemente dalla violazione) attraverso fonti pubbliche disponibili (es. combinazioni di informazioni dalle ricerche web)	**1**
	Il punteggio potrebbe essere **diminuito di 2**, quando la natura dei dati può portare ad una deduzione/ipotesi generale	**2**
	Il punteggio potrebbe essere **diminuito di 1** quando la natura dei dati può portare ad ipotesi circa informazioni particolari	**3**

Fattori incrementali

- **Volume di dati violati (per lo stesso individuo):** il volume deve essere considerato sia in termini di tempo (es. stesso tipo di dati violati per un certo periodo di tempo) ed il contenuto (es. tutti i dati di un file);
- **Speciali caratteristiche del Titolare**;
- **Speciali caratteristiche dell'interessato** (es. minori, interessati vulnerabili).

Fattori attenuanti

- **Dati non aggiornati e/o inaccurati:** il valore del dato è inferiore perché i dati non sono aggiornati e quindi perdono di significato;
- **Dati disponibili pubblicamente:** i dati violati erano già disponibili pubblicamente;
- **Natura dei dati:** la natura dei dati che può avere un valore più basso di quello assegnato (es. certificato medico che rivela il buono stato di salute dell'individuo senza altre informazioni, non impatta sulla vita dell'interessato).

FACILITA' DI IDENTIFICAZIONE	
Livello di identificabilità	**Moltiplicatore**
Trascurabile	0,25
Limitato	0,5
Significativo	0,75
Massimo	1,00

La facilità di identificazione valuta quanto può essere facile per una persona che ha accesso ai dati collegarli in maniera univoca ad una certa persona.
Il **punteggio più basso** è dato quando la possibilità di identificare l'interessato è trascurabile perché è estremamente difficile collegare i dati ad una particolare persona, ma a certe condizioni potrebbe essere comunque possibile.
Il **punteggio più alto** si ha quando è possibile l'identificazione diretta dai dati violati senza bisogno di particolari ricerche per scoprire l'identità dell'interessato.
Quando si definisce questo fattore deve essere preso in considerazione il fatto che l'identificazione può essere possibile direttamente (es. sulla base di un nome) o indirettamente (es. sulla base di un numero ID) sulla base della violazione ma può anche dipendere dallo specifico contesto della violazione. Così certi identificatori possono portare a differenti punteggi di Facilità di identificazione a seconda della tipologia di violazione.
Devono essere presi in considerazione i mezzi ragionevolmente possibili per identificare gli interessati (es. informazione ottenuta tramite internet, collegando più dati).

CIRCOSTANZE DELLA VIOLAZIONE	
Circostanza	**Correzione**
Perdita di riservatezza	Da +0 a + 0.50
Perdita di integrità	Da +0 a + 0.50
Perdita di disponibilità	Da +0 a + 0.50
Intenzioni malevole	+ 0.50

Gli elementi che devono essere considerati sono:

- **Perdita di riservatezza**: avviene quando l'accesso alle informazioni è compiuto da persone che non sono autorizzate o non hanno uno scopo legittimo. La gravità della perdita di riservatezza varia a seconda dello scopo dell'accesso, del numero potenziale e della tipologia dei soggetti che hanno subito la violazione dei dati.

- **Perdita di integrità**: avviene quando i dati sono alterati e sostituiti da dati che possono arrecare un pregiudizio alla persona. La situazione più grave si ha quando ci sono serie possibilità che i dati alterati possono essere usati in un modo che possa arrecare danno agli interessati.

- **Perdita di disponibilità**: avviene quando i dati non sono disponibili in caso di necessità. Può essere sia temporanea (i dati sono recuperabili ma ci vuole tempo e questo può essere dannoso per l'interessato) che permanente (i dati non sono più recuperabili).

- **Intenzioni malevole**: è necessario valutare se la violazione è dovuta ad uno sbaglio umano o tecnico oppure è causata da intenzioni malevole.
  Le **violazioni non malevole** includono perdite accidentali, cancellazione accidentale, errore umano, virus o non corretta configurazione.
  Gli **Intenti malevoli** includono casi di furto o hackeraggio con l'intento di arrecare danno all'interessato (es. divulgando dati personali a persone non autorizzate), trasferimento di dati a terzi per profitto (es. vendita di elenchi di dati), azioni per danneggiare il Titolare (es. attraverso il furto e la divulgazione di dati personali a persone non autorizzate).
  L'intento malevolo è un fattore che incrementa la probabilità che i dati siano usati in modo dannoso, dal momento che questo è lo scopo della violazione.

La **gravità di una violazione di dati personali** viene calcolata attraverso la formula:

Gravità = (Contesto x Facilità di identificazione) + Circostanze

Valutando, infine, il risultato ottenuto secondo quanto riportato nelle seguente tabella.

GRAVITA'	RISCHIO	DESCRIZIONE
Minore di 2 (A)	**Basso**	Gli interessati non incontreranno inconvenienti o potrebbero incontrare alcuni inconvenienti che supereranno senza alcun problema (tempo passato a reinserire informazioni, fastidio, irritazione, ecc.).
Compreso tra 2 e 3 (B)	**Medio**	Gli interessati potranno incontrare inconvenienti significativi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici lievi, ecc.)
Compreso tra 3 e 4 (C)	**Alto**	Gli interessati possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, lista nera da parte di banche, danni alla proprietà, perdita di posti di lavoro, citazione, peggioramento della salute, ecc.).
Maggiore di 4 (D)	**Molto alto**	Gli interessati possono incontrare conseguenze significative o addirittura irreversibili che non possono superare (difficoltà finanziarie come debito sostanziale o incapacità al lavoro, disturbi psicologici a lungo termine o disturbi fisici, morte, ecc.).

Una volta che è stata stabilita la gravità della violazione, devono essere tenuti presenti i seguenti due indicatori, sebbene non abbiano influenzato il punteggio a priori, perché ritenuti importanti per la valutazione del rischio:

- **Numero di individui violati superiore a 100:** i dati di un individuo violati nel contesto di un incidente più grave, possono potenzialmente essere più facilmente divulgati, mentre allo stesso tempo un alto numero di individui colpiti influenza la portata complessiva della violazione dei dati;
- **Dati inintelligibili:** la crittografia, senza chiave compromessa, diminuisce la possibilità dell'accesso ai dati da parte di persone non autorizzate.

Il risultato del calcolo del rischio deve essere interpretato come segue:

A. **Valore data breach < 2 = nessun rischio** – MISURE: non fare NOTIFICA all'Autorità di controllo e COMUNICAZIONE agli interessati e valutare eventuale AC (vedi **Sezione S8** del MODULO Gestione del Data Breach);
B. **Valore data breach tra 2 e 3 = rischio** - MISURE: non fare NOTIFICA all'Autorità di controllo e COMUNICAZIONE agli interessati, effettuare il trattamento dell'evento (vedi **Sezione S7)** ed eventuale AC (vedi **Sezione S8** del MODULO Gestione del Data Breach);
C. **Valore data breach tra 3 e 4 = rischio** MISURE: fare NOTIFICA all'Autorità di controllo, non fare la COMUNICAZIONE agli interessati, effettuare il trattamento dell'evento (vedi **Sezione S7**) ed eventuale AC (vedi **Sezione S8** del MODULO Gestione del Data Breach);
D. **Valore data breach > 4 = rischio elevato** – MISURE: implica quanto previsto al caso e anche la COMUNICAZIONE obbligatoria agli interessati coinvolti.