LISEA S.C.A.R.L.
Via Nicola Pende 19 - 70124 Bari
P.IVA 08415070724 | Numero REA: BA-62
www.liseabari.it | info@liseabari.it
Tel. +39 080 404.63.37

La Procedura Per La Gestione Dei Data Breach

"ISTITUTO SCOLASTICO JAPIGIA 1 - VERGA

LISEA S.C.A.R.L.
Via Nicola Pende 19 - 70124 Bari
P.IVA 08415070724 | Numero REA: BA-62
www.liseabari.it | info@liseabari.it
Tel. +39 080 404.63.37

SOMMARIO

LISEA S.C.A.R.L.
Via Nicola Pende 19 - 70124 Bari
P.IVA 08415070724 | Numero REA: BA-62
www.liseabari.it | info@liseabari.it
Tel. +39 080 404.63.37

Premessa

Secondo le disposizioni degli **Artt.33 e 34 del GDPR**, il Titolare del Trattamento che subisce una violazione dei dati personali (dei suoi clienti, dipendenti o fornitori) deve assolutamente valutare, nel giro di **72 ore**, l'entità del danno, le cause che hanno fatto si che l'evento si verificasse, l'efficacia delle misure di sicurezza implementate e se è necessario, segnalare al Garante e agli interessati ciò che è accaduto, in modo che il primo possa condurre le opportune indagini al fine di ben comprendere se vi siano pericoli per la libertà e i diritti dei secondi e costoro possano, quanto meno, correre ai ripari per evitare ulteriori problemi (es. cambiare la password, bloccare la carta di credito, ecc.…).

Un **Data Breach** può dipendere essenzialmente dal verificarsi di un rischio, evento che, per sua stessa definizione, non può essere evitato, ma mitigato con l'implementazione delle misure di sicurezza adeguate al trattamento, alle finalità perseguite e alla qualità dei dati trattati. Dunque, va da sé, se si è svolta un'ottima attività dell'analisi dei rischi e siano state implementate le opportune ed adeguate misure di sicurezza al fine di prevenire il verificarsi di un Data Breach, comunicare al Garante e ai propri clienti, dipendenti e fornitori che v'è stata una violazione, non potrà costituire un valido motivo per l'irrogazione di qualsivoglia sanzione.

Al contrario, il non aver implementato le adeguate misure di sicurezza e l'aver subito un Data Breach, può comportare l'irrogazione delle passate sanzioni previste dal Regolamento Europeo, sanzioni che potrebbero essere anche maggiorate se il Titolare non abbia comunicato la violazione al Garante e ai propri interessati.

Il modello di analisi e gestione del Data Breach è fondamentale per valutare la necessità o meno di effettuare la notifica al Garante per la Protezione dei Dati Personali e agli interessati, qualora il rischio per i loro diritti e le loro libertà risulti elevato. Esso, però, non rappresenta l'unico elemento da considerare per una risposta efficace in caso del verificarsi di una violazione.

Detta risposta, infatti è da considerarsi come un vero e proprio processo aziendale, con la designazione di referenti specifici, fasi ben delineate, metodologie di analisi che devono essere testate all'interno dell'organizzazione, di modo che sia possibile valutare nell'arco di 72 ore se

LISEA S.C.A.R.L.
Via Nicola Pende 19 - 70124 Bari
P.IVA 08415070724 | Numero REA: BA-62
www.liseabari.it | info@liseabari.it
Tel. +39 080 404.63.37

notificare il verificarsi dell'evento dannoso o no, ma anche di valutare quali possano essere le misure di mitigazione da porre in essere per l'azienda e l'interessato, al fine di ridurre il rischio e le conseguenze della violazione delle informazioni.

Proprio per questo, è necessario implementare il processo aziendale per la gestione di violazione dei dati, così come illustrato nella guida che segue.

Prima dell'implementazione del modello di gestione del Data Breach

L'analisi dei rischi è la fase di maggior importanza nel processo di adeguamento dell'organizzazione al GDPR: sapere quali strumenti sono utilizzati per il trattamento e l'archiviazione dei dati, a quali rischi sono esposti e quali misure di sicurezza implementare per la tutela delle informazioni è un aspetto essenziale per poter valutare come intervenire nel caso di violazione dei dati.

Si badi bene: il GDPR non si riferisce solo ed esclusivamente alle informazioni che sono trattate con l'ausilio di strumenti informatici, ma anche a tutti i trattamenti di dati che possono essere svolti con strumenti analogici o, ancora, all'archiviazione in armadi o altri locali di pertinenza del Titolare di Trattamento.

Analizzare il livello di rischio dei trattamenti attuati dall'organizzazione è, quindi, presupposto essenziale per l'implementazione del protocollo per la gestione del Data Breach, visto che, quando il processo sarà messo alla prova, non ci sarà sicuramente il tempo per poterla effettuare per poter capire cosa non abbia funzionato.

Il vecchio adagio nazional-popolare "prevenire è meglio che curare" è valido anche in questa situazione: investire in prevenzione, infatti significa ridurre il rischio di costi esorbitanti connessi ai danni prodotti dalla violazione subita dall'organizzazione, visto che da un lato il Garante potrebbe irrogare le sanzioni, dall'altro invece, gli interessati avrebbero il diritto di adire l'Autorità Giudiziaria per ottenere un risarcimento proporzionato all'entità del danno subito e della natura dei dati oggetto della violazione. Inoltre, l'immagine dell'organizzazione potrebbe essere seriamente compromessa: recenti studi dimostrano che i consumatori/clienti preferiscono rivolgersi a chi tutela le proprie informazioni personali.

LISEA S.C.A.R.L.
Via Nicola Pende 19 - 70124 Bari
P.IVA 08415070724 | Numero REA: BA-62
www.liseabari.it | info@liseabari.it
Tel. +39 080 404.63.37

Dunque, durante l'analisi, dovrà essere valutata l'adeguatezza tanto delle misure di sicurezza fisiche contro i rischi di natura fisica e/o naturale, quanto quelle delle misure di sicurezza informatica. Nei casi più complessi, o se il Titolare del Trattamento lo ritiene opportuno, può svolgersi un c.d. "penetration test", ossia una simulazione di un attacco hacker volto a sottrarre o distruggere i dati aziendali.

L'analisi dei rischi, peraltro, è fondamentale per completare il registro dei trattamenti che elenca i trattamenti svolti dal Titolare del Trattamento, la tipologia dei dati trattati, i soggetti interessati, le finalità del trattamento, e, per l'appunto, le misure di sicurezza atte a prevenire il verificarsi di un Data Breach.

Il Comitato per la Gestione del Data Breach

Composizione

Come già evidenziato in precedenza, il Titolare del Trattamento ha solo 72 ore per poter comunicare al Garante e agli interessati di aver subito un Data Breach. Ovviamente una simile analisi non può essere svolta da una singola persona o, nelle organizzazioni più complesse, da un solo dipartimento. Pertanto, è opportuno, costituire un comitato per la gestione del Data Breach, ossia un gruppo di persone costituito da:

- ✓ Titolare del Trattamento dei Dati o suo delegato;
- ✓ Data Protection Office (DPO);
- ✓ Referente Privacy Interno se nominato;
- ✓ Direttore dei Servizi Generali e Amministrativi;
- ✓ I responsabili del trattamento dei dati o loro delegati che trattano i dati in nome e per conto del Titolare del Trattamento (es. fornitore dei servizi IT, amministratore di Sistema, Responsabile del Software Gestionale, ecc.);
- ✓ Amministratore di Sistema se interno;
- ✓ Animatore Digitale;

LISEA S.C.A.R.L.
Via Nicola Pende 19 - 70124 Bari
P.IVA 08415070724 | Numero REA: BA-62
www.liseabari.it | info@liseabari.it
Tel. +39 080 404.63.37

Ruoli

All'interno del comitato andranno poi stabiliti i ruoli di ciascun suo componente: il coordinamento è opportuno sia affidato al DPO, di modo che possa immediatamente attivarsi per la raccolta delle informazioni necessarie per stabilire gravità del danno e per la stesura della segnalazione al Garante della Protezione dei Dati Personali in collaborazione con il DSGA o Delegato del Titolare del Trattamento.

Il responsabile IT (o manutentore dei servizi informatici esterno), l'Amministratore di Sistema e le ulteriori figure interessate, devono, invece, ricostruire la causa dell'evento dannoso e, di concerto con il DPO, attivare tutte quelle misure di mitigazione del rischio già implementate per risolvere il problema e ripristinare immediatamente la situazione precedente. Il loro compito è anche quello di recuperare i dati persi e verificare quali interessati siano stati coinvolti dal Data Breach e, soprattutto determinare se l'evento ha riguardato anche i loro dati particolari (ex dati sensibili).

Il tempo di reazione dell'IT e la corretta implementazione delle misure adeguate alla mitigazione del rischio di perdita o di furto dei dati sono due parametri che l'Autorità Garante valuterà per l'eventuale irrogazione di sanzioni: se, infatti, il Titolare del Trattamento dei Dati dimostra che ha fatto tutto quanto possibile per arginare il rischio e l'evento, imprevedibile o comunque non risolvibile con nessun'altra misura, non vi sarà alcuna sanzione. Se, invece, dovesse verificarsi il contrario, la sanzione è quasi inevitabile.

Al Dirigente Scolastico toccherà l'arduo compito di informare, con un linguaggio chiaro e semplice, tutti gli interessati i cui dati siano stati oggetto del Data Breach, consigliando loro cosa fare e come comportarsi per tutelare i propri diritti e proteggere le proprie informazioni.

La procedura da adottare in caso di violazione dei dati personali

Finalità e ambito di applicazione

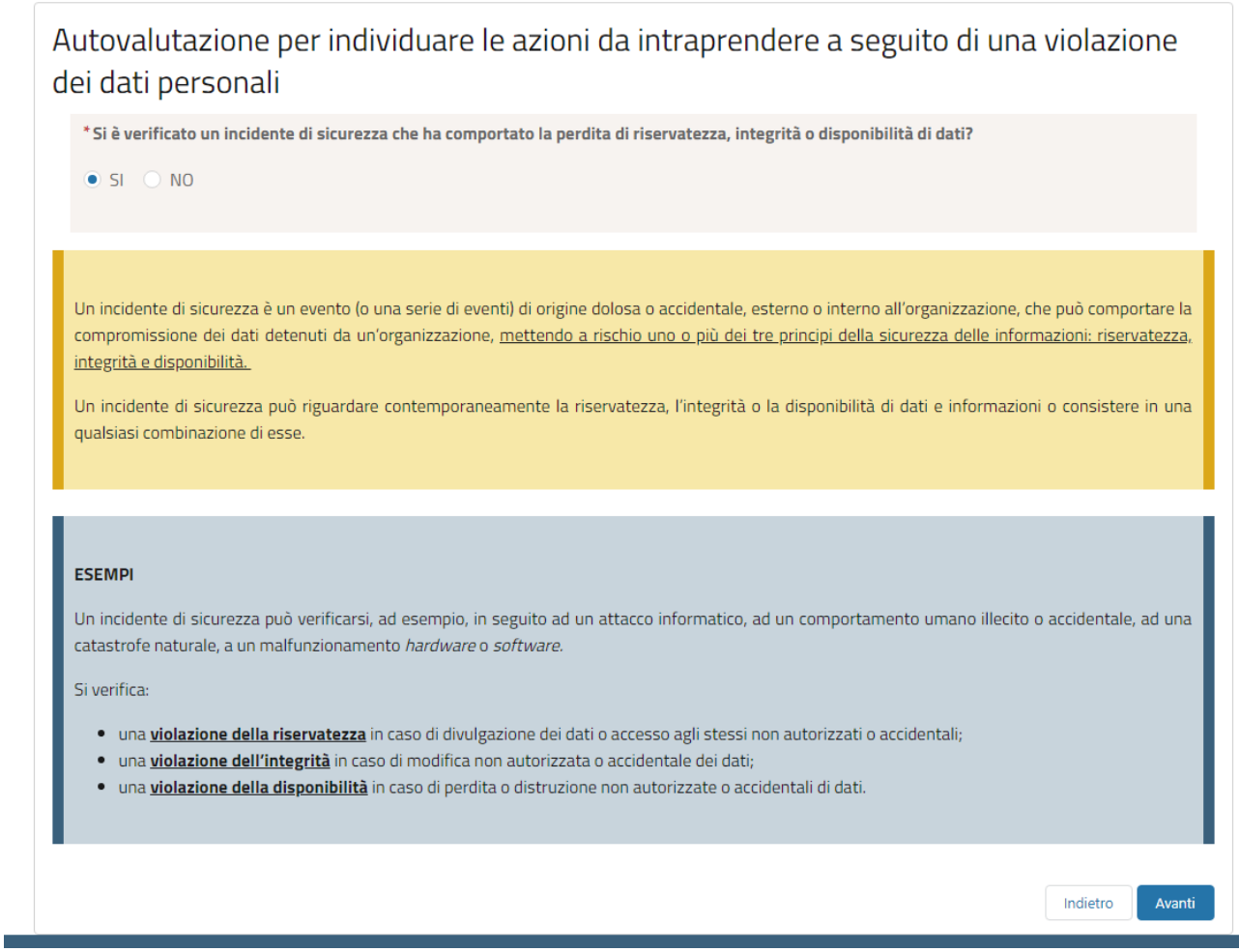
La presente procedura da attuare in caso di violazione dei dati personali (c.d. Data Breach) è redatta nel rispetto degli Artt. 4, 33 e 34 del Regolamento UE 679/2016 (GDPR) ed è stata adottata

dall'istituto Comprensivo Japigia 1 - Verga, quale Titolare del Trattamento dei Dati, al fine di tutelare i dati degli interessati cui si riferiscono.

Scopo principale della Policy è quello di documentare i flussi per la gestione dei Data Breach, definendo le modalità e le responsabilità per:

1. identificare la violazione;
2. analizzare le cause e le concause che hanno portato al verificarsi dell'evento dannoso;
3. definire le misure da adottare per rimediare, o quanto meno, mitigare le conseguenze negative di un Data Breach;
4. tenere traccia delle informazioni relative alle violazioni, alle misure applicate per mitigarle e alla loro efficacia nel c.d. registro delle violazioni;
5. valutare se sia il caso di notificare la violazione all'Autorità Garante per la Protezione dei Dati Personali, nel caso in cui il Data Breach comporti un rischio per le libertà e i diritti delle persone fisiche; Utilizzare il servizio https://servizi.gpdp.it/databreach/s/self-assessment

LISEA S.C.A.R.L.
Via Nicola Pende 19 - 70124 Bari
P.IVA 08415070724 | Numero REA: BA-62
www.liseabari.it | info@liseabari.it
Tel. +39 080 404.63.37



6. comunicare con un linguaggio chiaro, semplice e immediato la violazione dei dati personali all'interessato e le eventuali misure da adottare, qualora il rischio per le sue libertà e i suoi diritti si riveli elevato.

La procedura definita dall'Istituto Comprensivo Japigia 1 – Verga si applica ovviamente, tanto agli archivi cartacei quanto a quelli logici e ai sistemi informativi con cui sono stati trattati i dati.

I soggetti coinvolti dalla procedura

La procedura per la gestione delle violazioni dei dati personali proposta dall'Istituto Comprensivo Japigia 1 - Verga si applica a tutti i soggetti autorizzati al trattamento dei dati personali e a tutti i propri responsabili esterni del trattamento dei dati. Per questo, sarà trasmessa e comunicata a:

- ✓ tutti i dipendenti e a tutti i collaboratori esterni che, a qualsiasi titolo, trattino i dati personali di cui l'Istituto_Comprensivo Japigia 1 - Verga è Titolare;
- ✓ tutte le persone, fisiche o giuridiche, e gli enti che, in ragione del rapporto contrattuale in essere con il Titolare del Trattamento, abbiano accesso ai dati personali e agiscano in qualità di Responsabili del Trattamento, di Titolari Autonomi o di Contitolari.

Il rispetto della procedura è obbligatorio per tutti i soggetti indicati e, come già contrattualmente previsto o comunicato con ordine di servizio, la sua inosservanza darà luogo a provvedimenti disciplinari a carico dei dipendenti o a responsabilità di natura contrattuale per i Responsabili del Trattamento, cosa che potrebbe comportare anche la risoluzione per inadempimento degli accordi in essere.

Perché rispettare la procedura

Oltre alle sanzioni indicate già precedentemente, i dipendenti, i collaboratori e i fornitori dell'Istituto Comprensivo Japigia 1 – Verga sono tenuti a rispettare (e a far rispettare ai propri dipendenti e collaboratori) la procedura per:

- ✓ evitare, in primis, rischi per i diritti e le libertà degli interessati;
- ✓ evitare danni economici e di reputazione per il Titolare del Trattamento, che si riserva comunque il diritto di agire in rivalsa, e per se stessi;
- ✓ notificare all'Autorità Garante per la Protezione dei Dati Personali l'evento dannoso nelle 72 ore successive al suo verificarsi o alla sua scoperta ed evitare così le sanzioni per omessa notifica;
- ✓ evitare l'irrogazione delle pesanti sanzioni previste dal GDPR e dal Codice Privacy, con espressa riserva di agire in rivalsa dei propri soggetti autorizzati e dei propri responsabili qualora la violazione dipenda da loro dolo o colpa;
- ✓ minimizzare gli effetti negativi del Data Breach.

LISEA S.C.A.R.L.
Via Nicola Pende 19 - 70124 Bari
P.IVA 08415070724 | Numero REA: BA-62
www.liseabari.it | info@liseabari.it
Tel. +39 080 404.63.37

Cosa fare passo per passo

La procedura consiste nei seguenti passaggi:

1. rilevazione e segnalazione della violazione dei dati al Titolare del Trattamento e al suo Data Protection Officer;
2. raccolta delle informazioni sulla violazione;
3. valutazione del rischio e degli effetti dannosi del Data Breach, tenendo conto delle misure di sicurezza già in essere;
4. individuazione delle azioni correttive onde minimizzare gli effetti dell'evento dannoso;
5. se necessario, notifica della violazione all'Autorità Garante Privacy;
6. documentazione della violazione nel registro dei Data Breach.

Nel caso in cui si verifichi un Data Breach e uno dei soggetti indicati al precedente punto ("i soggetti coinvolti nella procedura) ne venga a conoscenza o ne abbia semplicemente sospetto, costui dovrà attivarsi compilando il modulo per la raccolta delle informazioni sui Data Breach, disponibile in segreteria e/o sul sito web della scuola nella sezione Privacy, comunicarlo al Titolare del Trattamento e al DPO e seguire i passaggi indicati nella tabella seguente in ragione della propria mansione o del rapporto contrattuale che lo lega all'istituto scolastico.

STEP	ATTIVITA'	CHI	DESTINATARI	QUANDO	COME
1	Rilevazione e segnalazione di un Data Breach o di un potenziale Data Breach	tutti i dipendenti tutti i collaboratori tutti i fornitori tutti i responsabili	il Titolare del Trattamento il Data Protection Officer DPO	Non appena si è a conoscenza della violazione o del presunto Data Breach	Avvertire subito per le vie brevi (telefono, e-mail)
2	Raccolta delle informazioni sulla violazione e comunicazione del Data Breach	Il soggetto autorizzato o responsabile che è venuto a conoscenza del Data Breach o del presunto tale	il Titolare del Trattamento il Data Protection Officer DPO	Entro 24 ore dalla scoperta	Compilazione del modulo per la raccolta delle informazioni sul data breach *(disponibile in segreteria o sul sito web della scuola nella sezione privacy)*
3	Valutazione dell'evento e delle conseguenze dannose del Data Breach	il Titolare del Trattamento il Data Protection Officer DPO		Appena ricevuta la comunicazione di cui allo step n°1	Valutazione del rischio utilizzando il servizio messo a disposizione dal Garante https://servizi.gpdp.it/databreach/s/self-assessment
4	Individuazione delle azioni correttive	il Titolare del Trattamento il Data Protection Officer DPO		Appena conclusa la valutazione di cui al punto precedente	Analisi dei risultati della valutazione dell'evento dannoso e delle sue conseguenze
5	Redazione della relazione sul Data Breach e pianificazione delle azioni da intraprendere per la mitigazione delle	il Titolare del Trattamento il Data Protection Officer DPO			Stesura della relazione sul Data Breach ed eventuale compilazione della modulistica

LISEA S.C.A.R.L.
Via Nicola Pende 19 - 70124 Bari
P.IVA 08415070724 | Numero REA: BA-62
www.liseabari.it | info@liseabari.it
Tel. +39 080 404.63.37

	conseguenze dannose				predisposta dal Garante per la Protezione dei Dati Personali
6	Notifica della violazione (se necessaria)	il Titolare del Trattamento il Data Protection Officer DPO	L'Autorità Garante per la Protezione dei Dati Personali	Entro 72 ore dal verificarsi dell'evento dannoso o da quando se n'è avuta effettiva conoscenza	Compilazione della modulistica predisposta dal Garante per la Protezione dei Dati Personali
7	Comunicazione agli interessati **(se necessaria)**	Il Titolare del Trattamento	Gli interessati i cui dati sono stati coinvolti nel Data Breach	Non appena concluso lo step 4	Per e-mail o per telefono. Se la segnalazione richiede uno sforzo sproporzionato, allora si potrà ricorrere ad una comunicazione pubblica, che però, deve essere efficace parimenti alla comunicazione personale
8	Documentazione del Data Breach	il Titolare del Trattamento il Data Protection Officer DPO		Non appena concluse tutte le fasi precedenti	Compilazione del registro dei Data Breach

LEGENDA

- *STEP: ordine in cui eseguire le operazioni*
- *ATTIVITA': cosa fare nel caso in cui si verifichi un Data Breach*
- *CHI: soggetto coinvolto in ragione della sua mansione o del rapporto contrattuale che lo lega al Titolare;*
- *DESTINATARI: destinatario dell'attività svolta dai soggetti autorizzati o dai responsabili del trattamento*
- *QUANDO: le tempistiche da rispettare per l'esecuzione dell'attività*
- *COME: le modalità con cui svolgere il compito.*

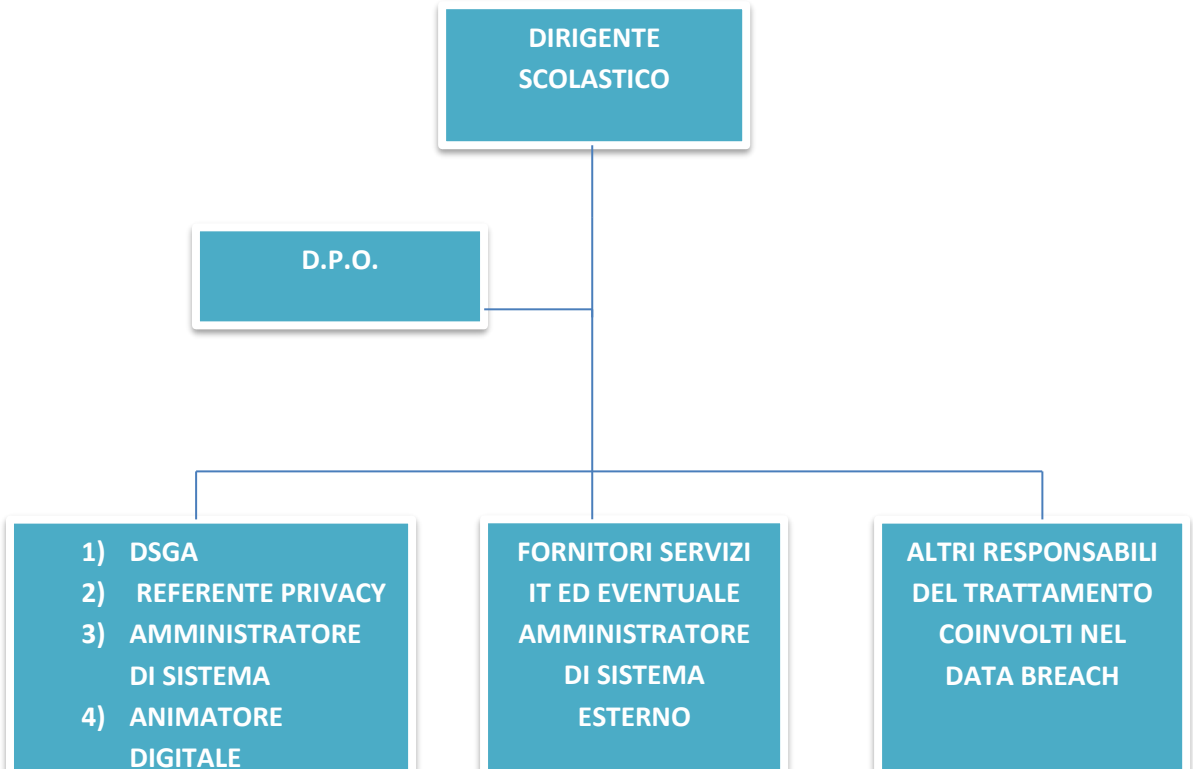
Cosa inserire nel registro delle violazioni

LISEA S.C.A.R.L.
Via Nicola Pende 19 - 70124 Bari
P.IVA 08415070724 | Numero REA: BA-62
www.liseabari.it | info@liseabari.it
Tel. +39 080 404.63.37

Per ogni Data Breach accertato, il Titolare del Trattamento e il Data Protection Officer dovranno compilare il registro delle violazioni, che dovrà contenere le seguenti informazioni:

- ✓ codice progressivo ed univoco delle violazioni;
- ✓ data di rilevamento;
- ✓ settore o processo interessato alla violazione;
- ✓ descrizione del Data Breach;
- ✓ categorie di interessati coinvolti;
- ✓ numero approssimativo degli stessi;
- ✓ categorie di dati personali e particolari coinvolti;
- ✓ numero approssimativo delle registrazioni dei suddetti dati;
- ✓ cause dell'evento dannoso;
- ✓ conseguenze del Data Breach;
- ✓ contromisure adottate;
- ✓ valutazione sulla notifica del Garante per la Protezione dei Dati Personali;
- ✓ valutazione sulla notifica agli interessati e data e ora della stessa, qualora sia possibile determinarla.

Composizione del Comitato per il Data Breach dell'istituto Scolastico




ISTITUTO COMPRENSIVO JAPIGIA I- VERGA
Plesso San Francesco Via Peucetia n. 50 BARI – tel. 080553 0943/5541991 fax 080 5524042
Plesso Verga via Carabellese n. 34 – tel/fax 080 5586758
Plesso Don Orione Viale Japigia n.140 BARI – tel./Fax 0805537467
baic88400x@istruzione.it baic88400x@pec.istruzione.it www.icjapigia1verga.it
C.M. BAIC88400X
Con l'Europa investiamo nel vostro futuro!
C.F. 93437840726

Modulo per la raccolta delle informazioni sul data breach

Data della segnalazione	
Nome e Cognome o Denominazione del soggetto che effettua la segnalazione	
in qualità di	☐ Responsabile del trattamento ☐ Soggetto autorizzato al trattamento

Descrizione sommaria dell'evento

_____

_____

_____

_____

_____

_____

Quando si è verificato il Data Breach?

- ☐ In data _____
- ☐ Tra il _____ e il _____
- ☐ In un periodo di tempo non ancora determinato _____
- ☐ E' ancora in corso_____

In caso di smarrimento di dispositivi, supporti portatili, faldoni, fascicoli o documenti, dove si è verificato il Data Breach?

LISEA S.C.A.R.L.
Via Nicola Pende 19 - 70124 Bari
P.IVA 08415070724 | Numero REA: BA-62
www.liseabari.it | info@liseabari.it
Tel. +39 080 404.63.37

_____

_____

_____

_____

_____

_____

_____

Indicare il tipo di violazione

- ☐ Sola lettura (i dati sono stati letti, ma non copiati)
- ☐ Copia (i dati sono stati copiati)
- ☐ Alterazione (i dati presenti nei sistemi o negli archivi fisici sono stati alterati o modificati)
- ☐ Cancellazione (i dati sono stati cancellati dai sistemi e non sono più nella disponibilità del Titolare del Trattamento)
- ☐ Furto (i dati non sono più presenti sui sistemi del titolare o nei suoi archivi e sono in possesso dell'autore del Data Breach
- ☐ Crittografia (i dati sono ancora presenti sui sistemi del titolare, ma sono crittografati dall'autore del Data Breach)
- ☐ Altro (specificare)

_____

_____

Dispositivo o assett oggetto della violazione

- ☐ Computer fisso
- ☐ Computer portatile aziendale
- ☐ Computer portatile personale
- ☐ Dispositivo mobile aziendale
- ☐ Dispositivo mobile personale
- ☐ Documento cartaceo
- ☐ File o parte di esso
- ☐ Unità di backup
- ☐ Asset di rete

LISEA S.C.A.R.L.
Via Nicola Pende 19 - 70124 Bari
P.IVA 08415070724 | Numero REA: BA-62
www.liseabari.it | info@liseabari.it
Tel. +39 080 404.63.37

☐ Altro (specificare)

_____

_____

Descrizione sintetica degli asset coinvolti, della loro ubicazione, indicazione del nominativo del loro responsabile

_____

_____

_____

Quanti interessati sono stati coinvolti dal Data Breach?

☐ N.° _____ di interessati
☐ Circa _____ di interessati
☐ Un numero imprecisato di interessati

Quali sono le categorie di dati coinvolte dal Data Breach?

☐ Dati anagrafici
☐ Dati di pagamento
☐ Dati di contatto
☐ Dati di identificazione e di accesso
☐ Dati sanitari
☐ Dati relativi alla confessione religiosa
☐ Dati relativi all'orientamento filosofico
☐ Dati relativi all'appartenenza sindacale
☐ Dati relativi all'appartenenza politica
☐ Dati sull'orientamento o sulla vita sessuale
☐ Dati sull'origine razziale o etnica
☐ Dati genetici
☐ Dati biometrici
☐ Dati giudiziari

Qual è il livello di gravità del Data Breach?

☐ Basso

LISEA S.C.A.R.L.
Via Nicola Pende 19 - 70124 Bari
P.IVA 08415070724 | Numero REA: BA-62
www.liseabari.it | info@liseabari.it
Tel. +39 080 404.63.37

☐ Medio
☐ Alto

Misure tecniche e organizzative già in essere per la mitigazione o il contrasto del rischio verificatosi

_____

_____

_____

Alcuni esempi di Data Breach

A titolo esemplificativo, ma non esaustivo, si elencano qui alcuni episodi di Data Breach che potrebbero verificarsi nel corso della normale attività. Pertanto, è opportuno che **tutti i dipendenti** e **collaboratori,** qualora ravvisino situazioni similari alle seguenti, attivino immediatamente la procedura, seguendo i passaggi precedentemente elencati.

1) Smarrimento o furto di un dispositivo

Può verificarsi l'eventualità che un dispositivo (pc, pc portatile, smartphone, tablet ecc.) sul quale sono memorizzati i dati del Titolare del Trattamento (dati degli alunni, del personale scolastico, e-mail, altri documenti ecc) possa essere smarrito, o peggio, possa essere oggetto di furto. In tal caso:

- è necessario segnalare immediatamente il furto o lo smarrimento del dispositivo;
- nella segnalazione, è necessario indicare se qualcuno abbia la possibilità di accedere ai dati trattati del Titolare o se, invece, il dispositivo era protetto nel rispetto delle misure di sicurezza già comunicate.

2) Forzatura di un archivio o della porta di accesso a un locale del Titolare del Trattamento

Può accadere che qualcuno noti che la serratura di un archivio o di un locale del Titolare del Trattamento risulti forzata. In tal caso:

- Segnalare immediatamente l'accaduto, anche se sembra che non manchi nulla.

LISEA S.C.A.R.L.
Via Nicola Pende 19 - 70124 Bari
P.IVA 08415070724 | Numero REA: BA-62
www.liseabari.it | info@liseabari.it
Tel. +39 080 404.63.37

3) Chiave dimenticata all'interno della serratura degli armadi o schedari

Spesso, chi utilizza uno schedario o un archivio, "dimentica" la chiave per aprirlo all'interno della serratura. In tal caso:

- Segnalare immediatamente l'accaduto, anche se sembra che non manchi nulla;
- Chiudere l'armadio o lo schedario e consegnare le chiavi all'impiegato amministrativo.

4) Azione di virus o malware

Nonostante i sistemi antivirus debbano essere sempre mantenuti aggiornati, può capitare che qualche virus o, più in generale, malware, riesca a cancellare, modificare, copiare abusivamente, alterare o crittografare i file su un dispositivo. In tal caso:

- Segnalare immediatamente senza indugio alcuno l'accaduto.

5) Abbandono di fascicoli e faldoni

Alcuni fascicoli o documenti contenenti dati personali e particolari trattati dal Titolare sono stati lasciati incustoditi sulla scrivania, in un luogo aperto all'utenza. In tal caso:

- Segnalare immediatamente l'accaduto, avendo cura di precisare a chi sia assegnata la postazione di lavoro;
- Riporre documenti, fascicoli e faldoni nello schedario o nell'archivio.

6) Distruzione dei documenti o dei dispositivi di memorizzazione non a norma

E' necessario distruggere documenti cartacei o dispositivi di memorizzazione non più utili, ma questi vengono semplicemente buttati nella spazzatura. In tal caso:

- Segnalare immediatamente l'accaduto;
- Recuperare i documenti e i dispositivi cestinati;
- Procedere alla loro distruzione a norma tramite fornitori specializzati.

7) Blocco temporaneo, ma prolungato, dei sistemi

Può accadere che alcuni PC o alcuni software in uso al Titolare possano non funzionare correttamente per un periodo di tempo. In tal caso:

- Segnalare immediatamente l'accaduto;

LISEA S.C.A.R.L.
Via Nicola Pende 19 - 70124 Bari
P.IVA 08415070724 | Numero REA: BA-62
www.liseabari.it | info@liseabari.it
Tel. +39 080 404.63.37

- Allertare l'amministrazione di modo che possa far intervenire senza indugio i servizi di assistenza tecnica.

Bari, il 01/07/2021

IL DPO

Firmato digitalmente da
ANTONIO GABRIELE ARMENISE
C = IT

IL TITOLARE DEL TRATTAMENTO

ROSSINI PATRIZIA
01.07.2021
07:59:17 UTC