PROCEDURA OPERATIVA PRIVACY: GESTIONE DATA BREACH

Istituto d'Istruzione Secondaria "Leopoldo Nobili"

INDICE

1 SCOPO/OBIETTIVO

La procedura operativa oggetto del presente documento ha lo scopo di regolamentare le azioni da attuare nel momento di un episodio di data breach, nel pieno rispetto delle prescrizioni contenute nel Regolamento Europeo sulla Protezione dei Dati Personali (GDPR) e dai provvedimenti espressi dal Garante per la Protezione dei Dati Personali.

Gli obiettivi che si intende perseguire sono i seguenti:

1. **acquisizione** delle informazioni riguardanti il data breach, in maniera tempestiva, da parte del referente interno;
2. **valutazione dell'episodio e dei rischi** che i soggetti interessati potrebbero subire a seguito del data breach;
3. **valutazione delle eventuali misure di sicurezza**, tecniche e/o organizzative, da realizzare per ridurre i rischi;
4. **valutazione dell'obbligatorietà delle comunicazioni** del data breach nei confronti del Garante e/o degli interessati coinvolti;
5. **effettuazione** della eventuale comunicazione;
6. **registrazione** dell'episodio nel registro delle violazioni;
7. **archiviazione** della documentazione prodotta, inviata e/o ricevuta.

Dal punto 1, quindi dal momento dell'attivazione della procedura, al punto 5 (eventuale comunicazione) dovranno trascorrere necessariamente al **massimo 72 ore**.

2 CAMPO DI APPLICAZIONE

La procedura operativa oggetto del presente documento dovrà essere attivata, dunque si applicherà, ogniqualvolta si presenti una violazione dei dati personali, dunque un data breach. Per semplicità si riporta un elenco non esaustivo delle ipotesi di violazioni:

- perdita, furto o distruzione di documenti, fascicoli o raccoglitori;
- danneggiamento irreversibile degli archivi;
- furto o smarrimento di strumenti elettronici contenenti dati personali;
- accesso non autorizzato nei locali deputati all'archiviazione;
- accesso non autorizzato nella sala CED (o comunque nella stanza in cui si trova/trovano i/il server);
- accesso non autorizzato nel proprio dispositivo elettronico;
- comportamento anomalo del proprio PC o dispositivo informatico;
- invio erroneo di dati personali a destinatari non autorizzati a riceverli.

3 MODIFICHE ALLE REVISIONI PRECEDENTI

Il presente documento rappresenta la prima revisione.

4 DEFINIZIONI

Nel presente documento sono/potranno essere utilizzati le seguenti parole, sigle, acronimi, abbreviazioni:

- **GDPR**: General Data Protection Regulation, regolamento europeo per la protezione dei dati personali.
- **Data Breach**: violazione dei dati personali 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 oppure trattati.
- **Dato personale**: qualunque informazione riferita o riferibile ad una persona fisica.
- **Dato particolare**: dato idoneo a rivelare le origini razziali o etniche, le condizioni politiche o religiose, l'appartenenza a partiti o sindacati, lo stato di salute o le preferenze sessuali di un interessato.
- **Interessato**: persona fisica a cui si riferiscono i dati personali.
- **Titolare del Trattamento**: persona fisica o giuridica, ente, associazione o pubblica amministrazione che determina le finalità e le modalità di trattamento.
- **Garante per la protezione dei dati personali**: autorità indipendente che si occupa di regolamentare e sorvegliare il rispetto del GDPR e delle normative inerenti il trattamento dei dati personali.
- **Trattamento di dati personali**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
- **Procedura operativa**: documento che disciplina, in ogni singola fase, un flusso di operazioni volte alla gestione di un processo, in questo caso dei curricula.

5 MATRICE DI RESPONSABILITÀ/ATTIVITÀ

5.1 Operazioni preliminari

Il Titolare individua, per la gestione del data breach, il Sig. Filippo Piccinini, n. tel. 0522.921433, indirizzo email filippo.piccinini@iisnobili.edu.it dandone comunicazione a tutto il personale scolastico, qualificandosi come **referente data breach scolastico**.

Il Titolare individua inoltre un **Nucleo di Crisi** da convocare in caso di data breach che comportino rischi considerevoli per gli interessati. Il Nucleo di Crisi è composto da:

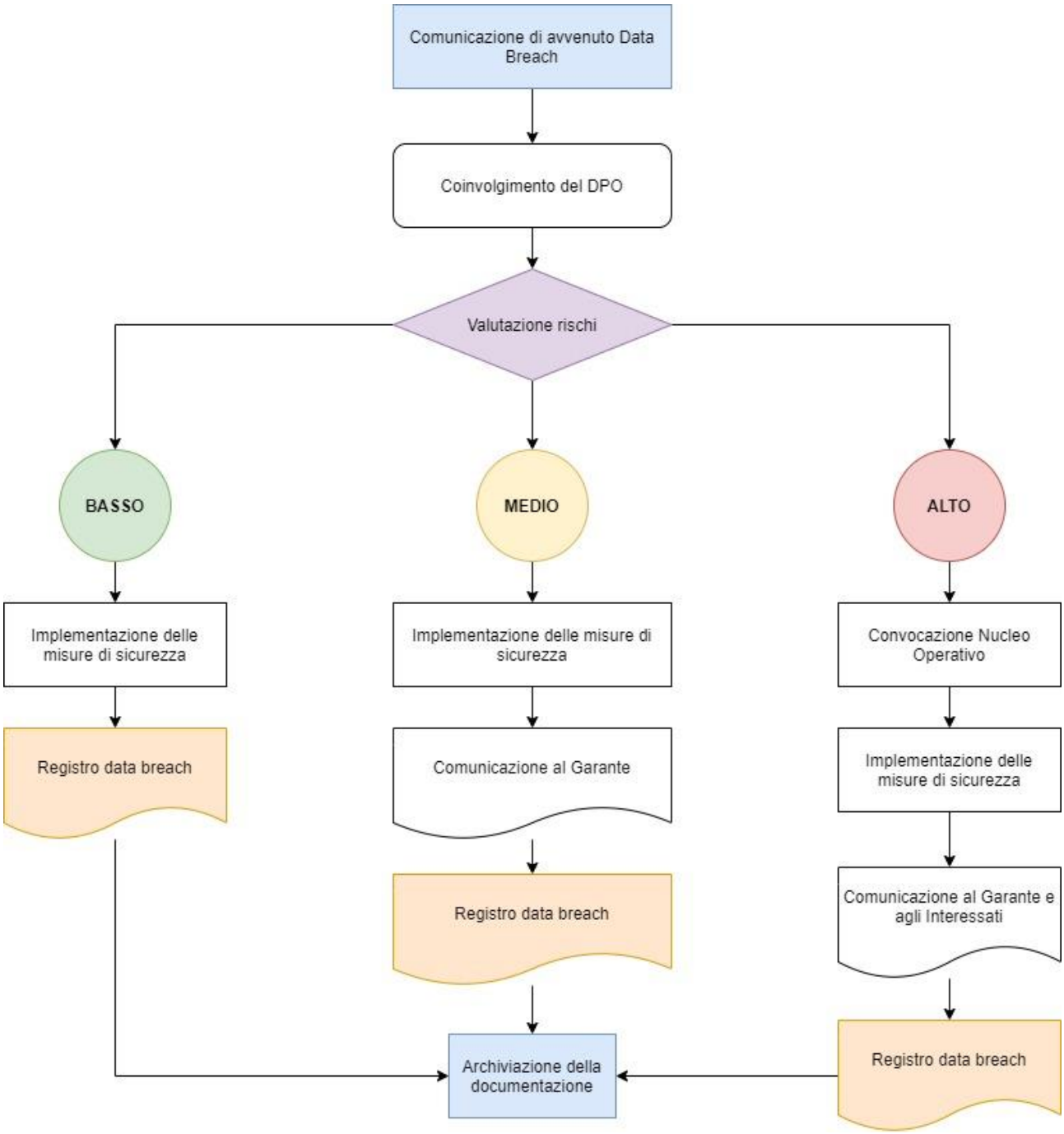
a. Dirigente scolastico nella persona di Elena Guidi e-mail presidenza@iisnobili.edu.it – tel. 0522.921433
b. DSGA nella persona di Angela Russolillo e-mail angela.russolillo@iisnobili.edu.it – tel. 0522.921433
c. Referente data breach: Filippo Piccinini e-mail filippo.piccinini@iisnobili.edu.it – tel. 0522.921433
d. Referente IT: Francesco Le Pera e-mail francesco.lepera@iisnobili.edu.it – tel. 0522.921433 (da convocare solo se il data breach coinvolge strumenti informatici)

e. DPO – Data Protection Officer: Emanuele Solombrino - e-mail solombrino@01privacy.it - tel. 3703522902

f. Soggetto che ha attivato la procedura – Dati di contatto rinvenibili tramite Modello A

ATTIVITÀ	UFFICIO RESPONSABILE	NOTE
1. **Segnalazione al referente**	*Soggetto interno che ha subito/individuato la violazione*	**La segnalazione dovrà essere tempestiva**
2. **Valutazione episodio**	*Referente data breach*	Congiuntamente al DPO
3. **Implementazione misure di sicurezza**	*Referente data breach*	Congiuntamente al DPO
4. **Valutazione comunicazione a Garante e/o soggetti interessati**	*Referente data breach*	Congiuntamente al DPO
5. **Eventuale comunicazione**	*Titolare*	Congiuntamente al DPO
6. **Registrazione episodio**	*Consulente privacy e/o DPO*	
7. **Firma/accettazione del registro delle violazioni**	*Titolare*	
8. **Archiviazione della documentazione prodotta**	*Referente Data Breach*	

6 DIAGRAMMA DI FLUSSO



- *Il rettangolo identifica un'attività, una tappa della procedura;*
- *Il rettangolo con il lato inferiore ondulato rappresenta un documento;*
- *Il rombo indica uno stato decisionale: definisce la condizione in cui deve trovarsi un'azione perché possa essere effettuata;*
- *Le frecce indicano il flusso del processo, cioè la sequenza logica delle attività;*
- *Le frecce uscenti verso un documento indicano che tale documento è il risultato dell'attività descritta nel riquadro;*
- *Le frecce entranti da un documento verso l'attività descritta nel riquadro indicano che tale documento è utile per svolgere l'attività stessa.*

7 DESCRIZIONE DELLE ATTIVITÀ

7.1 Ricezione del modello A

A tutti i soggetti autorizzati dovrà essere inviato il Modello A "*Comunicazione avvenuto Data Breach*", al cui interno dovrà essere riportato il nominativo e i recapiti del referente interno atto alla gestione dei data breach.

In caso di violazione o sospetto di violazione il soggetto autorizzato dovrà comunicare, tramite eventualmente il Modello A, la comunicazione dell'avvenuto data breach.

Nel momento della ricezione del modello o della comunicazione diretta da parte del soggetto che ha subito il data breach, il referente interno dovrà raccogliere il maggior numero di informazioni utili alla comprensione e gestione del data breach.

Dopo aver raccolto le informazioni il referente interno dovrà necessariamente coinvolgere il DPO (e-mail solombrino@01privacy.it - tel. 3703522902) per una prima valutazione dell'incidente e dei rischi che gli interessati potrebbero subire.

7.2 Comprensione del Data Breach

Dopo aver raccolto tutte le informazioni il referente interno dovrà coinvolgere i soggetti interni/esterni indispensabili alla comprensione del data breach (ad esempio consulente registro elettronico, consulente informatico, manutentore del gestionale, etc.).

In questa fase risulta necessario comprendere appieno la portata della violazione, la natura e la quantità dei dati personali esposti alla violazione stessa.

7.3 Valutazione dei rischi

Dopo aver raccolto tutte le informazioni il referente interno, con il coinvolgimento del DPO, potrà procedere alla valutazione dei rischi che corrono gli interessati. In base alla valutazione effettuata le linee di azione possono essere di tre tipi:

7.3.1 Rischio basso

In caso di rischio basso o nullo per gli interessati si procede ad una valutazione delle misure di sicurezza da implementare per evitare futuri episodi di violazioni. Successivamente si riporta l'episodio sul registro delle violazioni e si procede con l'archiviazione della documentazione eventualmente prodotta/inviata/ricevuta.

7.3.2 Rischio medio

Quando i rischi rilevati per gli interessati possono risultare importanti si procede con urgenza al coinvolgimento del DPO per procedere alla valutazione delle misure di sicurezza da implementare per ridurre gli eventuali rischi degli interessati. **Entro 72 ore** occorre necessariamente comunicare il data breach al Garante per la protezione dei dati personali tramite il DPO. Successivamente si può procedere con l'archiviazione della documentazione prodotta/inviata/ricevuta.

7.3.3 Rischio alto

Quando i rischi rilevati per gli interessati sono considerevoli si procede con urgenza alla convocazione del **Nucleo Operativo**. Il Nucleo Operativo dovrà valutare le misure di sicurezza da implementare per ridurre, se possibile, i rischi e le misure da adottare per evitare il ripetersi di simili episodi. Con urgenza il Nucleo Operativo dovrà comunicare, nel modo più efficace, l'episodio a tutti i soggetti interessati coinvolti. **Entro 72 ore** occorre necessariamente comunicare il data breach al

Garante per la protezione dei dati personali tramite il DPO. Successivamente si può procedere con l'archiviazione della documentazione prodotta/inviata/ricevuta.

8 RIFERIMENTI E ALLEGATI

8.1 Riferimenti normativi

- Regolamento Europeo 2016/679
- D. Lgs. 196/2003 così come novellato dal D. Lgs. 101/2018
- Provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach) - 30 luglio 2019 [9126951]

8.2 Allegati

- Modello A "Comunicazione avvenuto Data Breach"

9 INDICATORI/PARAMETRI DI CONTROLLO

Gli indicatori di controllo sono i seguenti:

- Numero di violazioni subite
- Numero di violazioni correttamente gestite
- Comunicazioni del Garante

10 MODALITÀ DEI CONTROLLI

Annualmente si procederà ad un controllo della corretta applicazione della presente procedura operativa.

Il controllo, effettuato dal consulente esterno/DPO, dovrà evidenziare la **corretta diffusione della procedura a tutti i soggetti autorizzati**, andando a verificarne l'invio al nuovo personale del Modello A "Comunicazione avvenuto Data Breach".

Dovrà inoltre essere verificata la corretta applicazione della procedura negli eventuali casi di violazioni, andando a verificare il **numero di violazioni subite rapportandolo al numero di violazioni correttamente gestite**.

Andranno infine verificate le eventuali comunicazioni del Garante e la **corretta applicazione** degli eventuali suggerimenti/prescrizioni.

11 ELENCO DEI CONTROLLI

Data	**Numero di violazioni subite nell'anno**	**Numero di violazioni correttamente gestite**	**Comunicazioni del Garante**	Controllo effettuato da	
				Nome e Cognome	Firma

Il dettaglio delle violazioni subite, delle modalità di intervento sono riportati nel registro delle violazioni o in un documento allegato alla presente procedura