Autore:
Dott.ssa M. P. Teresa Useri
Redattore:
Ing. Antonio Vargiu
Validatore:
Dr. Mario Mureddu

Titolo: DPIA per le attività di prevenzione e gestione dei fenomeni di Cyberbullismo

Richiesta del parere degli interessati
Non è stato chiesto il parere degli interessati.
Motivazione della mancata richiesta del parere degli interessati
Non si è ritenuto necessario richiedere un parere agli interessati, trattandosi di un trattamento necessario ai fini di legge.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?
Il trattamento consiste nella raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, e la comunicazione mediante trasmissione dei dati personali degli interessati, a fini di prevenzione ed eventuale gestione dei fenomeni di cyberbullismo connessi con le attività della scuola.
Quali sono le responsabilità connesse al trattamento?
Il titolare del trattamento è l'amministrazione scolastica. Si prevede la condivisione dei dati con l'autorità giudiziaria, su richiesta esplicita della stessa. I dati relativi ad episodi di cyberbullismo di cui la scuola viene a conoscenza potrebbero, qualora fosse necessario e ai fini delle indicazioni dell'Art. 5 della Legge 71/2017, essere condivisi con gli interessati o con i genitori degli stessi.

Responsabile del trattamento è il gestore del software e del server di conservazione connesso al servizio di segreteria digitale scolastico.
Ci sono standard applicabili al trattamento?
Non si è a conoscenza di standard applicabili al trattamento.

Dati, processi e risorse di supporto

Quali sono i dati trattati?
Dati anagrafici di alunni, genitori e dipendenti della scuola. Eventuali dati personali degli esperti che prestano attività formativa in materia.
Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?
I dati di alunni, genitori e dipendenti provengono dagli archivi scolastici, e vengono conservati per la durata dell'evento o per i relativi adempimenti di legge. Le eventuali chat o post su social network dei

quali l'amministrazione viene messa a conoscenza, relativi ad episodi di cyberbullismo, vengono acquisiti dalla scuola ai fini dell'adempimento agli obblighi relativi alla normativa vigente,e mantenuti nella esclusiva disponibilità del Dirigente Scolastico (D.S.) o di un suo eventuale delegato (ad es., a discrezione del D.s., il referente scolastico per il cyberbullismo così come introdotto nell'Art. 4, comma 3 della Legge 71/2017).
I dati degli esperti esterni incaricati delle attività formative in materia vengono trattai secondo le modalità descritte nel registro dei trattamenti, relative al trattamento di dati personali di esperti esterni alla scuola.

Quali sono le risorse di supporto ai dati?

I dati di alunni, genitori, dipendenti ed esperti esterni vengono trattati facendo uso delle risorse informatiche della scuola. L'hardware utilizzato consiste nelle risorse hardware scolastiche (PC del D.S., ed eventualmente del referente per il cyberbullismo o della segreteria per le attività di protocollo), il software utilizzato consiste nella suite di segretria digitale scolastica. Le eventuali chat o post inerenti atti di cyberbullismo vengono acquisiti dalla scuola e conservati con accesso riservato al D.S. e al suo eventuale delegato (referente per il cyberbullismo).

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Il trattamento viene effettuato ai fini del perseguimento di un obbligo legale dell'amministrazione, orientato specificamente alla prevenzione e/o gestione degli episodi di cyberbullismo.

Quali sono le basi legali che rendono lecito il trattamento?

Le basi legali sono da ricercarsi nella Legge 71/2017 (Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo). Il trattamento si profila inoltre come attività di interesse pubblico rilevante, di istruzione e formazione in ambito scolastico, professionale, superiore o universitario, come previsto dall'Art. 2-sexies, comma 2bb del D.Lgs. 196/2003.
Inoltre, le modalità di archiviazione sono definite da:

il DPR 445/2000;
Decreto Legislativo 22 gennaio 2004 n. 42, Codice dei beni culturali e del paesaggio
Legge 6 luglio 2002, n. 137, art 10 (G.U. n. 45 del 24 febbraio 2004, s.o. n. 28).

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

Per la realizzazione delle attività di formazione e prevenzione non vengono utilizzati dati in eccesso rispetto a quelli già esistenti negli archivi scolastici. Qualora venissero individuati atti di cyberbullismo all'interno del campo di influenza dell'amministrazione scolastica, si prevede di acquisire le informazioni minime per l'esercizio degli obblighi legali, limitando al tempo stesso l'accesso alle stesse al D.S. o ai suoi delegati.

I dati sono esatti e aggiornati?

I dati vengono tenuti esatti e aggiornati per tutta la durata del trattamento, essendo quelli derivanti dagli archivi scolastici. In caso di episodi rilevati di cyberbullismo, verranno verificate le fonti di provenienza di eventuali prove documentali relative agli stessi.

Qual è il periodo di conservazione dei dati?

Per le finalità di prevenzione, i dati vengono conservati seguendo le indicazioni dell'archivio di stato, relativamente alle attività di istruzione e formazione (illimitato). Per le attività di constrasto e gestione degli atti di cyberbullismo, gli eventuali dati acquisiti vengono conservati dalla scuola per il tempo necessario a svolgere le attività previste dalla normativa di riferimento.

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Gli interessati vengono informati del trattamento tramite apposita informativa fornita dalla scuola.

Ove applicabile: come si ottiene il consenso degli interessati?

Non è previsto.

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

La scuola mette a disposizione degli interessati un modulo di esercizio dei propri diritti. Gli interessati posso sempre rivolgersi all'amministrazione tramite la modalità da loro preferita per l'esercizio degli stessi.

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

La scuola mette a disposizione degli interessati un modulo di esercizio dei propri diritti. Gli interessati posso sempre rivolgersi all'amministrazione tramite la modalità da loro preferita per l'esercizio degli stessi.

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

La scuola mette a disposizione degli interessati un modulo di esercizio dei propri diritti. Gli interessati posso sempre rivolgersi all'amministrazione tramite la modalità da loro preferita per l'esercizio degli stessi.

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

Il gestore del servizio cloud di segreteria digitale è stato nominato Responsabile del Trattamento ai sensi degli Artt. 28 e 29 del Reg. UE 679/2016.

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

Non sono previsti trasferimenti di dati al di fuori dell'U.E.

Rischi

Misure esistenti o pianificate

Crittografia
I dati sono trattati tramite l'utilizzo di meccanismi di conservazione e comunicazione cifrati, ai fini di garantire la minimizzazione del rischio di acceso agli stessi.

Controllo degli accessi logici
L'accesso alle funzionalità del sistema di segreteria digitale è regolato da un sistema di attivazione di account con permessi specifici, protetti da password, attivabili e disattivabili dall'amministratore del software (il D.S. o un suo delegato).

Archiviazione
Tutta la documentazione relativa all'attività Istituzionale dell'Amministrazione è regolata dalla normativa vigente in materia di archiviazione nella pubblica amministrazione, contenente indicazioni specifiche per la pubblica istruzione.

Minimizzazione dei dati
I dati vengono trattati e archiviati in forma minima, per quanto previsto dalla normativa vigente

Lotta contro il malware
I sistemi scolastici sono protetti da malware con modalità di protezione sia hardware che software (firewall e antivirus).

Backup
I sistemi di segreteria digitale utilizzati per il trattamento sono provvisti di una modalità di backup.

Manutenzione
Viene effettuata regolarmente una attività di manutenzione nei confronti dei sistemi hardware scolastici. Il responsabile del trattamento garantisce inoltre il corretto funizonamento del software di segreteria.

Contratto con il responsabile del trattamento
Il responsabile del trattamento è stato nominato tale tramite la stipula di un contratto, ai sensi degli Artt. 28 e 29 del Reg. Ue 679/2016

Sicurezza dei canali informatici
I canali interni della scuola cono protetti da firewall. Tutti i protocolli di comunicazione utilizzati dal software di segreteria digitale sono cifrati.

Sicurezza dell'hardware
Le postazioni hardware sono conservate all'interno di locali che vengono chiusi a chiave durante i periodi di chiusura della scuola, protetti tramite sistema di allarme. Durante i periodi di apertura al pubblico della scuola, viene garantita la custodia degli stessi tramite istruzioni scritte al personale interessato.

Politica di tutela della privacy
L'amministrazione ha messo in atto una serie di misure orientate all'adeguamento della stessa alla normativa vigente.

Gestire gli incidenti di sicurezza e le violazioni dei dati personali
L'amministrazione ha emesso un regolamento interno per la gestione dei data breach, al cui interno sono specificate le modalitàdi gestieone di tali fenomeni.

Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Per le attività di prevenzione, non si ravvedono particolari impatti sugli interessati., Per le attività di intervento e gestione degli atti di cyberbullismo, è possibile che vengano rese pubbliche le prove degli atti, il che potrebbe portare ad una limitazione dei diritti e delle libertà degli interessati.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Accesso illecito ai dati, Pubblicazione dei dati

Quali sono le fonti di rischio?

Errore umano, Mancato inserimento dei dati all'interno di una modalità di conservazione riservata

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Controllo degli accessi logici, Minimizzazione dei dati, Lotta contro il malware, Backup, Manutenzione, Contratto con il responsabile del trattamento, Sicurezza dei canali informatici, Sicurezza dell'hardware, Politica di tutela della privacy, Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Importante, Gli interessati potrebbero subire conseguenze significative, che dovrebbero essere in grado di superare, ma con difficoltà reali e significative :

- psicologici: grave disturbo psicologico (depressione, fobie), senso di violazione della privacy e di un danno irreparabile, esposizione a ricatti, cyberbullismo e molestie psicologiche, ecc.

In particolare, l'accesso e la potenziale pubblicazione dei dati comprovanti l'atto di cyberbullismo potrebbe comportare un aggravamento o una mala gestione del problema.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile, Appare impossibile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti (ad esempio: accesso e copia di un documento comprovante atti di cyberbullismo, conservato con modalità che permettano l'accesso al solo D.S.).

Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Potrebbe limitare le possibilità di intervento dell'amministrazione o dell'autorità giudiziaria.

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Accesso illecito ai dati e modifica degli stessi

Quali sono le fonti di rischio?

Errore umano, Fonti umane interne, che intervengano nella modifica dei dati

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Crittografia, Controllo degli accessi logici, Archiviazione, Minimizzazione dei dati, Backup, Lotta contro il malware, Manutenzione, Contratto con il responsabile del trattamento, Sicurezza dei canali informatici, Sicurezza dell'hardware, Politica di tutela della privacy, Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

Importante, Gli interessati potrebbero subire conseguenze significative, che dovrebbero essere in grado di superare, ma con difficoltà reali e significative :

- psicologici: grave disturbo psicologico (depressione, fobie), senso di violazione della privacy e di un danno irreparabile, esposizione a ricatti, cyberbullismo e molestie psicologiche, ecc.

In particolare, la modifica dei dati comprovanti l'atto di cyberbullismo potrebbe comportare un aggravamento o una mala gestione del problema.

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?

Trascurabile, Le modalità di protezione dei dati rendono improbabile una azione del genere. L'esistenza di un backup e del tracciamento delle attività, inoltre, rende possibile il recupero delle informazioni originali e l'identificazione delle finti di modifica dei dati stessi.

Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

Perdita dei dati relativi ad atti di cyberbullismo, che essi possano costituire o no reato

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

Distruzione dei server di segreteria digitale, Perdita dell'accesso ai documenti

Quali sono le fonti di rischio?

Fonti umane interne, Fonti umane esterne (incaricati del responsabile del trattamento o dei sub-responsabili), Eventi naturali che possano influire sui dispositivi fisici di archiviazione.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Crittografia, Controllo degli accessi logici, Contratto con il responsabile del trattamento, Archiviazione, Minimizzazione dei dati, Lotta contro il malware, Backup, Sicurezza dei canali informatici, Manutenzione, Sicurezza dell'hardware, Politica di tutela della privacy, Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Importante, Gli interessati potrebbero subire conseguenze significative, che dovrebbero essere in grado di superare, ma con difficoltà reali e significative :

- psicologici: grave disturbo psicologico (depressione, fobie), senso di violazione della privacy e di un danno irreparabile, esposizione a ricatti, cyberbullismo e molestie psicologiche, ecc.

In particolare, la perdita dei dati comprovanti l'atto di cyberbullismo potrebbe comportare un aggravamento o una mala gestione del problema.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile, Le modalità di protezione dei dati rendono improbabile una azione del genere. L'esistenza di un backup e del tracciamento delle attività, inoltre, rende possibile il recupero delle informazioni originali e l'identificazione delle fonti di modifica dei dati stessi.