Manuale di Gestione della Privacy

dell'Istituto

prot. _____ del _____

Sommario

Il presente documento ha l'obiettivo di descrivere il modello generale di gestione della privacy all'interno dell'Istituto Scolastico in accordo ai requisiti del nuovo regolamento europeo in materia di protezione dei dati personali (*REGOLAMENTO - UE 2016/679*, noto anche come *GDPR – General Data Protection Regulation*).

Premessa

L'Istituto Scolastico, ai sensi e nelle forme dell'art. 35 del GDPR, a mezzo del presente documento ha ritenuto opportuno e utile dotarsi di un'adeguata mappatura dei processi organizzativi e amministrativi coinvolti dalla normativa sulla privacy.
Il presente documento costituisce dunque uno strumento finalizzato alla rappresentazione del complesso di misure poste in essere al fine di adempiere rigorosamente a quanto prescritto dalla normativa vigente in materia di Protezione dei Dati Personali.

1 RIFERIMENTI NORMATIVI E TERMINOLOGIA UTILIZZATA

1. Nuovo Regolamento Europeo in materia di Protezione dei Dati Personali (REGOLAMENTO (UE) 2016/679 detto anche GDPR – General Data Protection Regulation).
2. D.Lgs. 30 giugno 2003 n. 196 - Codice in materia di protezione dei dati personali
3. D.Lgs. 10 agosto 2018 n. 101 – Modifiche al Codice in materia di protezione dei dati personali
4. Provvedimenti deliberati dal Garante per la Protezione dei Dati Personali
5. Provvedimenti deliberati dalle autorità dell'Unione Europea in materia di Trattamento dei dati personali

Glossario Privacy

AMMINISTRATORE DI SISTEMA
La figura professionale dedicata alla gestione e alla manutenzione degli impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali.

ARCHIVIO
Qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

BASE GIURIDICA DEL TRATTAMENTO
Base normativa che autorizza l'ente al trattamento dei dati personali, con riferimento alle attribuzioni e competenze.

CATEGORIE DI DATI PERSONALI
1. DATI IDENTIFICATIVI COMUNI. Cognome e nome, residenza, domicilio, nascita, identificativo online (username, password), situazione familiare, immagini, elementi caratteristici della sua identità.

2- DATI PERSONALI APPARTENENTI A CATEGORIE PARTICOLARI (anche definiti come dati sensibili o giudiziari):
- **Dati relativi all'origine e allo stile di vita personale**

I dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, o relativi alla vita sessuale o all'orientamento sessuale della persona.

- **Dato personale biometrico**
  I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.
- **Dato personale genetico**
  I dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.
- **Dati personali relativi alla salute**
  I dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

3 - DATI PERSONALI RELATIVI ALLA SITUAZIONE ECONOMICA, FINANZIARIA, PATRIMONIALE O FISCALE

4 - DATI PERSONALI APPARTENENTI AD ALTRE CATEGORIE PARTICOLARI (cd giudiziari)

Dati personali che rivelano l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (quali, ad es., i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione). Rientrano in questa categoria anche la qualità di imputato o di indagato.

CATEGORIE DI INTERESSATI

In via esemplificativa e non esaustiva: cittadini, residenti, minori, elettori, contribuenti, utenti, partecipanti al procedimento, dipendenti, amministratori, etc.. (vedi anche "Interessato")

CATEGORIE DI TRATTAMENTO

Si intende per trattamento 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:

1. la raccolta;
2. la registrazione;
3. l'organizzazione;
4. la strutturazione;
5. la conservazione;
6. l'adattamento o la modifica;
7. l'estrazione;
8. la consultazione;
9. l'uso;
10. la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma messa a disposizione;
11. il raffronto e l'interconnessione;
12. la limitazione;
13. la cancellazione;
14. la distruzione.

COMUNICAZIONE DI DATI PERSONALI
Far conoscere dati personali a uno o più soggetti determinati (che non siano l'interessato, il responsabile, il soggetto autorizzato al trattamento), in qualunque forma, anche attraverso la loro messa a disposizione o consultazione.

DATO PERSONALE
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;

DESTINATARIO
La persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazioni di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione Europea o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.

DIFFUSIONE
Divulgare dati personali al pubblico o, comunque, ad un numero indeterminato di soggetti (*ad esempio*, è diffusione la pubblicazione di dati personali su un quotidiano o su una pagina *web*).

FINALITA' DEL TRATTAMENTO
Esecuzione dei compiti e delle attività connesse alla funzione istituzionale.
Adempimento di un obbligo legale o di contrattazione collettiva a cui è soggetta l'amministrazione.
Esecuzione di un contratto con i soggetti interessati.
Altre specifiche e diverse finalità.

INTERESSATO
La persona fisica cui si riferiscono i dati personali

MISURE TECNICHE ED ORGANIZZATIVE
Pseudonimizzazione, anonimizzazione, cifratura, misure specifiche per assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano dati personali; procedure specifiche per provare, verificare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; altre misure specifiche adottate per il trattamento di cui trattasi.
Sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus, firewall, antintrusione, altro) – adottati per il trattamento di cui trattasi ovvero dal Servizio/Ente nel suo complesso.
Misure antincendi; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi, contenitori dotati di serratura; sistemi di copiatura e conservazione archivi elettronici; altre misure per ripristinare tempestivamente la

disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico – adottati per il trattamento di cui trattasi.
Procedure per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento.

PROFILAZIONE
Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

PSEUDONIMIZZAZIONE E ANONIMIZZAZIONE DEI DATI PERSONALI
Il trattamento dei dati personali in modo tale che i dati personali non possano essere più attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile. A differenza dell'anonimizzazione, questa tecnica non compromette irreversibilmente la identificazione o identificabilità dell'interessato.

RESPONSABILE (INTERNO/ESTERNO) DEL TRATTAMENTO
La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

SOGGETTO AUTORIZZATO AL TRATTAMENTO (Sub-responsabile)
Il soggetto incaricato del trattamento di dati personali per l'esecuzione di specifiche attività di trattamento per conto del Titolare del trattamento (elabora o utilizza materialmente i dati personali)

TITOLARE DEL TRATTAMENTO
La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

TRATTAMENTO
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;

2 ORGANIGRAMMA PRIVACY

Si riporta di seguito l'organigramma adottato in ambito privacy, con l'indicazione delle Unità Organizzative di competenza

Unità organizzativa	Compiti
Collaboratori del DS	Trattamento di tutti i dati dell'Istituto quando svolge i compiti delegati dal DS o in sua sostituzione
Personale Docente	Trattamento dati alunni
Personale di Segreteria	Trattamento dati dipendenti, alunni, collaboratori e fornitori
Personale ausiliario	Trattamento dati alunni e dipendenti

3 PIANIFICAZIONE

3.1 Azioni per affrontare rischi ed opportunità

L'analisi dei rischi e delle opportunità insite nei processi di trattamento di dati personali rappresenta un aspetto importante per la conformità alle normative vigenti in materia di Protezione dei Dati Personali che viene considerato in molteplici momenti di controllo:

- in fase di procedura di valutazione dei rischi;
- in fase di revisione periodica dei processi di trattamento di dati personali.

L'Istituzione scolastica, prima ancora di procedere alla predisposizione del presente manuale e di tutto il sistema di protezione dei dati, ha correttamente avviato una accurata analisi e valutazione dei rischi i cui esiti vengono riportati del Documento di Valutazione dei Rischi.

3.2 Obiettivi per la privacy e pianificazione per il loro raggiungimento

Con cadenza annuale, il RdT, in accordo con il Titolare definisce gli obiettivi privacy da raggiungere e da monitorare nel corso dell'anno.

Il monitoraggio dell'andamento di tali obiettivi viene effettuato in occasione di riunioni, da effettuarsi con cadenza almeno annuale.

Di seguito gli obiettivi previsti per l'anno scolastico 2018/2019:

- Analisi dei Rischi e predisposizione del Documento di Valutazione dei Rischi
- Approvazione ed emissione del Manuale Privacy
- Approvazione ed emissione di una prima versione del Registro dei Trattamenti
- Approvazione ed emissione del Regolamento utilizzo sistemi informatici
- Approvazione ed emissione della Procedura di Data Breach

4 SUPPORTO

4.1 Risorse (Persone, Infrastrutture e Conoscenza Organizzativa)

L'Istituto scolastico garantisce la disponibilità di adeguate risorse in termini di persone, infrastrutture e conoscenza organizzativa per poter gestire in maniera efficace ed efficiente gli adempimenti privacy applicabili al contesto scolastico, sempre tenendo in considerazione i limiti conseguenti alle risorse economiche a disposizione dell'istituzione.
L'utilizzo delle risorse ai fini dell'implementazione delle misure di sicurezza è inevitabilmente vincolato dalle normative in materia di utilizzo delle risorse e nei limiti del loro stanziamento.

4.2 Competenza, Consapevolezza e Comunicazione

L'Istituto scolastico è consapevole dell'importanza di presidiare i requisiti di formazione sui temi riguardanti la tutela dei dati personali, a presidio degli aspetti di competenza, consapevolezza del personale e di comunicazione dei corretti comportamenti da adottare
A tale scopo, ogni dipendente della scuola ha l'obbligo di seguire un corso di base sui concetti della privacy, che verrà effettuato personalmente dal DPO nominato.
Nel corso dell'erogazione delle iniziative formative previste, il Titolare del trattamento ha il compito di raccogliere e archiviare le relative evidenze documentali che ne provino l'effettiva attuazione a beneficio dei destinatari indicati.

4.3 Informazioni Documentali

La documentazione adottata dall'amministrazione ai fini della privacy è suddivisa in:

- Documentazione descrittiva del Sistema di Gestione della privacy:
    1. Documento della Valutazione dei Rischi
    2. Manuale del Sistema di Gestione della Privacy
    3. Registro dei trattamenti
    4. Regolamento utilizzo sistemi informatici
    5. Procedure di Data Breach
- Documentazione relativa al conferimento di incarichi in materia privacy:
    1. Documentazione di nomina del DPO
    2. Documentazione di nomina del Responsabile del Trattamento
    3. Documentazione di nomina degli autorizzati al trattamento
- Documentazione ai fini della tutela dell'utenza:
    1. Informativa dipendenti
    2. Informativa studenti e utenti della scuola

4.4 Canale di comunicazione dedicato

Al fine di agevolare lo scambio di comunicazioni, la tenuta sotto controllo e la gestione degli eventi inerenti e/o con impatto sul sistema di gestione della privacy può essere utilizzato il seguente indirizzo mail _____@_____ a cui ha accesso il titolare del trattamento e il RdT e persone di loro fiducia formalmente delegate.

5 VALUTAZIONE DELLE PRESTAZIONI

5.1 Monitoraggio, misurazione, analisi e valutazione

Con cadenza annuale, il Titolare, in accordo con il RdT, definisce gli obiettivi privacy da raggiungere e da monitorare nel corso dell'anno.
Il monitoraggio dell'andamento di tali obiettivi viene effettuato in occasione di riunioni, da effettuarsi con cadenza almeno annuale alla presenza del Titolare e del DPO.
In base all'esito delle valutazioni sul raggiungimento degli obiettivi, in tale sede possono essere definite delle opportune azioni correttive e/o di miglioramento ai fini della conformità dei processi di trattamento dei dati personali.

5.2 Revisione periodica del sistema di gestione della privacy

L'Istituto Scolastico esegue periodicamente, ed almeno con cadenza annuale o in occasione di importanti eventi o cambiamenti che impattano sul Sistema di Gestione della Privacy, audit interni allo scopo di:

- verificare se i vari procedimenti sono svolti in accordo alle procedure che le regolamentano;
- definire le eventuali azioni correttive da attuare e misurarne l'efficacia.

È compito del RdT coordinare le varie fasi del processo di verifica secondo le seguenti indicazioni:

- Ogni processo riportato nel registro dei trattamenti deve essere verificato annualmente, secondo quanto definito nel piano di audit interno;
- I temi da sottoporre a verifica devono riguardare i processi riportati nel registro dei trattamenti e la loro conformità rispetto alla normativa vigente in materia di privacy ed alle relative procedure aziendali;
- La verifica deve essere rivolta al controllo della corretta applicazione delle procedure anche allo scopo di verificarne l'efficacia, mediante l'uso di una opportuna check-list;
- Il RdT può avvalersi di un Consulente esterno e del DPO per l'esecuzione degli audit interni.

Firma del Titolare del Trattamento