MODELLO ORGANIZZATIVO
A TUTELA DEI DATI PERSONALI AI SENSI DEL REGOLAMENTO UE 2016/679 (GDPR).

Sommario

1. PREMESSA 2
2. PARTE I - NORME E PRINCIPI GENERALI 3
3. PARTE II - PROFILO ORGANIZZATIVO 6
   3.1. Profilo strutturale 6
   3.2. Il Titolare del trattamento 6
   3.3. IL Responsabile della Protezione dei Dati personali (DPO) 7
   3.4. Addetti al trattamento e designati ai sensi dell'art.2-quaterdecis (Codice Privacy). 7
   3.5. Il Contitolare del trattamento e i titolari autonomi 8
   3.6. Il Responsabile del trattamento 9
4. PARTE III - ADEMPIMENTI E PROCEDURE 10
   4.1. Misure per la sicurezza dei dati personali 10
   4.2. Violazione dei dati personali 10
5. PARTE IV - DIRITTI DELL'INTERESSATO 13
   5.1. Informativa e modalità per l'esercizio dei diritti dell'interessato 13

1. PREMESSA

Il Regolamento UE 2016/679, denominato GDPR (in italiano RGPD, acronimo di "Regolamento GeneraleProtezione dei Dati), detta una complessa disciplina di carattere generale in materia di protezione dei dati personali concernenti persone fisiche. Le sue disposizioni sono state ulteriormente specificate dalla normativa nazionaleattraverso il Decreto Legislativo 101/2018 il quale, modificando il D.Lgs 196/2003, definisce il "Codice della privacy" italiano. I Provvedimenti di carattere generale emanati dal Garante per la protezione dei dati personali (di seguito solo "Garante") completano il complesso normativo dedicato alla protezione dei dati personali.

L'adeguamento alla normativa vigente impone al Titolare di trattamento pubblico di prestare grande attenzione al fattore organizzativo. Per questo, il presente atto organizzativo individua le politiche, gli obiettivi strategici e gli standard di sicurezza per garantire la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati personali. Il modello che si intende delineare individua i soggetti che intervengono nel trattamento dei dati, assieme alle loro funzioni e responsabilità, e definisce il quadro delle misure di sicurezza informatica, logiche, fisiche, organizzative e procedurali da adottare e da applicare per attenuare e, ove possibile, eliminare il rischio di violazione dei dati derivante dal trattamento.

Al fine di garantire la migliore e più puntuale attuazione del principio di accountability, il presente modello organizzativo del dirigente scolastico contiene disposizioni regolamentari minime la cui concreta attuazione è demandata all'organizzazione del personale operante all'interno dell'Ente, nelle sue articolazioni gerarchiche.

2. PARTE I - NORME E PRINCIPI GENERALI

L'istituto, in funzione delle attività che è chiamato a svolgere, effettua molteplici trattamenti di un'ampia categoria di dati personali, compresi quelli appartenenti a categorie particolari (di seguito definiti per brevità "dati particolari"): dati sulla salute, dati giudiziari, dati che rivelano l'origine razziale o etnica, le convinzioni religiose e la vita e l'orientamento sessuale. Essi si svolgono sempre nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, tenendo conto dei seguenti principi:

a) «liceità, correttezza e trasparenza»: i dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;

b) «limitazione delle finalità»: i dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;

c) «minimizzazione dei dati»: i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

d) «necessità»: è ridotta al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità possano essere perseguite mediante dati anonimi o con l'uso di opportune modalità che permettono di identificare l'interessato solo un caso di necessità;

e) «esattezza»: i dati personali sono esatti e, se necessario, aggiornati; sono adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;

f) «limitazione della conservazione»: i dati personali sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'art. 89, prf. 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste a tutela dei diritti e delle libertà dell'interessato;

g) «integrità e riservatezza»: i dati personali sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;

h) «responsabilizzazione»: il titolare del trattamento è competente per il rispetto dei principi di cui al comma 1 e deve essere in grado di comprovarlo.

Entrando più nello specifico, si indicano nel seguito le finalità e la base giuridica per i trattamenti effettuati.

Finalità dei trattamenti: tutti i trattamenti dei dati sono effettuati dall'istitutoper l'esecuzione di un compito di interesse pubblico o comunque connesso all'esercizio di pubblici poteri. In particolare, i trattamenti di categorie particolari di dati personali sono effettuati solo ove necessario per motivi di interesse pubblico rilevante e, comunque, ove siano previsti da disposizioni di legge (o di regolamento, in tutti quei casi previsti dalla legge) che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Base giuridica dei trattamenti: in linea con gli articoli 2-ter e 2-sexies del Codice privacy, che specificano l'applicazione rispettivamente dell'art. 6 e dell'art.9 del Regolamento UE 679/2016 (GDPR), la base giuridica per ogni trattamento è costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento. Pertanto il consenso esplicito non è mai richiesto.

CIRCOLAZIONE DEI DATI PERSONALI

Le operazioni di trattamento possono avvenire esclusivamente ad opera dei soggetti all'uopo delegati, designati ed autorizzati secondo quanto previsto infra nel presente documento. Non è consentito il trattamento da parte di persone non puntualmente autorizzate ed istruite in tal senso.

Fatto salvo il rispetto di specifiche e puntuali disposizione normative che lo vietino, l'istituto favorisce la circolazione all'interno dei propri uffici dei dati personali dei cittadini il cui trattamento sia necessario ai sensi degli articoli 6, 9 e 10 del GDPR.La circolazione, ove possibile, è assicurata mediante l'accessibilità diretta delle banche dati informative detenute da ciascun ufficio, previa creazione di appositi profili di utenza che tengano conto dei profili di autorizzazione conferiti.

Forme similari di accessibilità sono garantite in favore di contitolari e responsabili del trattamento, limitatamente ai dati personali diversi da quelli contemplati dagli articoli 9 e 10 del GDPR.

Al fine di garantire la correttezza delle operazioni di trattamento l'istituto provvede alla ricognizione di tutti i trattamenti di dati personali effettuati nell'ambito dei processi e procedimenti svolti, finalizzata alla compilazione ed aggiornamento del Registro delle attività di trattamento di cui al GDPR.

COORDINAMENTO DI NORME

Questa Amministrazione intende perseguire l'obiettivo di assicurare le forme più estese di accessibilità e trasparenza sul proprio operato ad opera dei cittadini, nelle varie forme in cui il diritto di accesso è riconosciuto, quali quella prevista dalla Legge 241/90 e s.m.i.e quelle previste dal D.Lgs. 33/2013 e s.m.i.

A tale proposito - fermo restando che i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso ai documenti amministrativi e del diritto di accesso civico, semplice e generalizzato e la relativa tutela giurisdizionale, così come gli obblighi di pubblicità e pubblicazione restano disciplinati dalla normativa di settore – gli Uffici dovranno interpretare la vigente normativa in materia di trasparenza ed accesso in modo da garantire la più rigorosa tutela dei dati personali degli interessati, anche tenendo in considerazione le motivazioni addotte dal soggetto (eventualmente, in caso di accesso) controinteressato.

In attuazione dei principi contenuti nella normativa nazionale e comunitaria vigente, l'istituto, nel dare riscontro alle richieste di accesso ovvero nel pubblicare i provvedimenti, dovrebbe in linea generale scegliere le modalità meno pregiudizievoli per i diritti dell'interessato, privilegiando l'ostensione di documenti con l'omissione dei «dati personali» in esso presenti, laddove l'esigenza informativa, alla base dell'accesso o della trasparenza e pubblicazione, possa essere raggiunta senza implicare il trattamento dei dati personali.

SENSIBILIZZAZIONE E FORMAZIONE

Dall'esame della materia emerge come sia oramai imprescindibile un cambiamento di mentalità che porti alla piena tutela della privacy, da considerare non solo come un oneroso rispetto di adempimenti burocratici, ma soprattutto come garanzia, per il cittadino che si rivolge alle pubbliche amministrazioni, di una riservatezza totale dal punto di vista reale e sostanziale.

Ai fini della corretta e puntuale applicazione della disciplina relativa ai principi, alla liceità del trattamento, all'informativa e, più in generale, alla protezione dei dati personali, l'istituto sostiene e promuove, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione che possa consolidare la consapevolezza del valore della riservatezza dei dati, e migliorare la qualità del servizio.

A tale riguardo, questa Amministrazione riconosce che uno degli strumenti essenziali di sensibilizzazione sia rappresentato dall'attività formativa del personale. Al fine di garantire la conoscenza capillare delle disposizioni normative vigenti, al momento dell'ingresso in servizio è data ad ogni dipendente una specifica comunicazione, con apposita clausola inserita nel contratto di lavoro, contenente il richiamo ai principi ed alle norme di cui al presente Modello organizzativo, oltre che alle vigenti disposizioni nazionali e comunitarie e alle dettagliate istruzioni relative ai trattamenti che lo stesso dipendente sarà autorizzato ad effettuare.

Ma la consegna di istruzioni all'atto dell'ingresso in servizio non vuole essere l'unico momento formativo che l'istituto organizza verso i propri dipendenti: nell'ambito della formazione continua e obbligatoria del

personale si intende organizzare, infatti, specifici interventi di aggiornamento in materia di protezione dei dati personali, finalizzati alla conoscenza delle norme, alla prevenzione di fenomeni di abuso e illegalità nell'attuazione della normativa, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza delle misure di sicurezza per il trattamento e la conservazione dei dati, dei rischi individuati e dei modi per prevenire danni agli interessati.

La formazione in materia di prevenzione dei rischi di violazione dei dati personali viene integrata e coordinata con la formazione in materia di trasparenza e di accesso, con particolare riguardo ai rapporti tra protezione dei dati personali, trasparenza accesso ai documenti amministrativi e accesso civico, semplice e generalizzato, nei diversi ambiti in cui opera l'istituto.

La partecipazione dei dipendenti agli interventi formativi viene considerata quale elemento di misurazione e valutazione della performance organizzativa ed individuale.

3. PARTE II - PROFILO ORGANIZZATIVO

3.1. Profilo strutturale

La struttura organizzativa dell'istituto scolastico si articola in: ufficio del Dirigente scolastico, ufficio di segreteria, consiglio di istituto, collegio dei docenti, dipartimenti del collegio, consigli di classe, interclasse e intersezione. Il Dirigente scolastico esercita il coordinamento degli organi collegiali e definisce l'assetto organizzativo dell'ufficio di segreteria.

3.2. Il Titolare del trattamento

L'art. 4 n. 7 del GDPR precisa che il titolare del trattamento (interpretando la norma rispetto all'Ente locale) è "*l'autorità pubblica*" che "*determina le finalità e i mezzi del trattamento di dati personali*". Ai sensi di tale articolo, e dell'art. 24 del Regolamento, il Titolare è l'istituto scolastico e, per suo conto, il Dirigente scolastico pro tempore, cui spetta l'adozione di misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento.

Le competenze e le responsabilità che il GDPR assegna al Titolare del trattamento possono così essere riassunte:

a) determinare le finalità ed i mezzi del trattamento dei dati personali: in considerazione del carattere pubblico che contraddistingue questa Amministrazione, le finalità sono determinate e circoscritte in quelle necessarie a garantire il corretto svolgimento delle funzioni istituzionali e dei compiti di interesse pubblico (art. 4);

b) mettere in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR (c.d. accountability) (art. 24);

c) garantire che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali non tratti tali dati se non è adeguatamente istruito in tal senso (artt. 29 e 32);

d) individuare i responsabili del trattamento, controllarne e garantirne l'operato (art. 28);

e) agevolare l'esercizio dei diritti dell'interessato (art. 12) e fornire agli interessati le informazioni previste dal GDPR (art. 13);

f) designare il Responsabile della protezione dei dati (art. 37) ponendolo in grado di svolgere adeguatamente l'attività (art. 38);

g) istituire e tenere aggiornato un registro delle attività di trattamento svolte sotto la propria responsabilità (art. 30);

h) nei casi ove ciò sia necessario e prima di procedere al trattamento, effettuare una valutazione dell'impatto sulla protezione dei dati personali (art. 35);

i) comunicare all'autorità di controllo (art. 33) ed all'interessato (art. 34) eventuali violazioni dei dati;

j) ricevere ed osservare provvedimenti, notifiche e ingiunzioni dell'autorità di controllo (art. 58);

k) rispondere per il danno cagionato dal trattamento che violi il GDPR (art. 82);

l) rispondere delle violazioni amministrative ai sensi del GDPR (art. 83)

3.3. IL Responsabile della Protezione dei Dati personali (DPO)

L'istituto si avvale obbligatoriamente di un Responsabile della protezione dei dati (DPO), in possesso delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di competenza.

Il Responsabile della protezione è individuato con regolare determina dirigenziale tra soggetti esterni, persone fisiche o soggetti giuridici.L'assenza di conflitti di interesse anche potenziali con l'esercizio dei propri compiti è strettamente connessa agli obblighi di indipendenza del DPO.

I dati identificativi e di contatto del Responsabile della protezione dei dati sono pubblicati nel sito web istituzionale dell'Ente, rendendoli accessibili da un apposito link, comunicato all'Autorità di controlloe inclusio in tutte le informative rese agli interessati ai sensi degli articoli 13 e 14 del GDPR.

I compiti e le funzioni demandate al Responsabile della protezione dei dati sono quelli indicati nell'art. 28 del Regolamento (UE) 2016/679 ed elencati di seguito:

a) informare e fornire consulenza all'istituto in merito agli obblighi derivanti dalla normativa in materia di protezione dei dati personali, con la collaborazione della struttura di supporto e dell'eventuale Referente nominato dal titolare (si veda il paragrafo dedicato);

b) sorvegliare l'osservanza della normativa in materia di protezione dei dati personali, nonché delle politiche dell'istituto in materia di protezione dei dati personali;

c) cooperare con il Garante per la protezione dei dati personali, facilitando l'accesso documenti ed informazioni necessari per l'adempimento dei compiti dell'Autorità di controllo;

d) fungere da punto di contatto per il garante per questioni connesse al trattamento;

e) fungere da punto di contatto per gli interessati per questioni attinenti al trattamento dei propri dati personali e all'esercizio dei loro diritti;

f) promuovere la formazione di tutto il personale dell'istituto in materia di protezione di dati personali e di sicurezza informatica;

g) partecipare alla gestione degli incidenti di sicurezza nelle modalità previste da specifica policy dell'istituto;

h) formulare gli indirizzi e monitorare la realizzazione del registro delle attività del trattamento di cui all'art. 30 del Regolamento

i) fornire i pareri obbligatori e facoltativi richiesti dal Dirigente scolastico titolare del trattamento.

3.4. Addetti al trattamento e designati ai sensi dell'art.2-quaterdecis (Codice Privacy).

Addetti autorizzati al trattamento

All'interno della struttura organizzativadel GDPR non è espressamente prevista la figura degli "incaricati", bensì lo stesso Regolamento impone che chiunque agisca, avendo accesso ai dati personali, sotto l'autorità del titolare del trattamento non possa trattare tali dati se non è istruito in tal senso dal lo stesso titolare del trattamento (salvo che lo richieda il diritto dell'Unione o degli Stati membri).

Al fine di garantire la conoscenza capillare delle disposizioni normative vigenti, ad ogni dipendente è data una specifica comunicazione, con apposita clausola (o allegato)al contratto di lavoro, contenente il richiamo ai principi ed alle norme di cui al presente Modello organizzativo, oltre che alle vigenti disposizioni nazionali e comunitarie e alle dettagliate istruzioni relative ai trattamenti che lo stesso dipendente sarà autorizzato ad effettuare.Tali istruzioni sono raggruppate per gruppi omogenei di dipendenti:

- assistenti amministrativi ATA e DSGA;
- personale docente ed educativo;

- collaboratori scolastici;
- personale tecnico ed animatori digitali.

Tutti i soggetti dipendenti, appartenenti ai sopra citati gruppi omogenei e che operano sotto la diretta autorità del titolare, sono autorizzati alle operazioni di trattamento dei dati effettuati presso l'istituto.

Il dirigente scolastico titolare del trattamento autorizza per iscritto gli addetti tramite atto individuale riferito al gruppo omogeneo di riferimento,specificando i trattamenti che sono autorizzati ad effettuare e le istruzioni da seguire affinchéle operazioni di trattamento siano in attuazione dei principi del Regolamento.L'atto di autorizzazione si intende decaduto in caso di cessazione del rapporto di lavoro con l'istituzione scolastica.

3.5. Il Contitolare del trattamento e i titolari autonomi

L'istituto effettua con regolarità un certo numero di attività in collaborazione con soggetti esterni, con i quali condivide o definisce congiuntamente le finalità e i mezzi del trattamento dei dati personali degli interessati. Tali attività includono, a mero titolo esemplificativo, tutti i progetti educativi portati avanti congiuntamente con enti locali, con cooperative sociali o con singoli professionisti.

In base alla previsione contenuta nell'articolo 26 del GDPR "*Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati*".

Il contitolare rappresenta dunque l'attore che si ritrova a condividere con l'istituto scolastico il ruolo di titolare del trattamentocosì come i relativi obblighi e responsabilità. La contitolarità implica in sostanza che tutte le parti coinvolte, ciascuna per la propria porzione digovernance convenzionalmente stabilita, siano in grado di determinare finalità e modalità del trattamento e che tali aspetti siano condivisi dalle altre parti.

l'istituto definirà con i diversi contitolari un accordo interno che definisce le rispettive responsabilità, non necessariamente ripartite in modo eguale.Il contratto rimane la forma di accordo più comune per definire la contitolarità ma questa può essere stabilita anche mediante memorandum d'intesa, a patto che quest'ultimo contenga tutti gli elementi previsti dalla normativa.

I contitolari determinano congiuntamente quali informazioni fornire e in che modo, fatti salvi i vincoli dell'articolo 26 comma tre del Regolamento (UE) 2016/679, per il quale indipendentemente dalle disposizioni dell'accordo fra contitolari l'interessato può esercitare i propri diritti nei confronti di ciascun titolare del trattamento.

Differenze tra contitolare, titolare autonomo e responsabile del trattamento

È utile sottolineare che, nel caso un attore perseguisse proprie finalità, non condivise con l'istituto, e fosse autonomo nel definire i mezzi del trattamento, esso non sarà un contitolare, bensì sarà da inquadrare quale "titolare autonomo".

Nei casi in cui, invece, fosse l'istituto a definire finalità e mezzi per conto dell'attore esterno, esso sarà da inquadrare come "responsabile del trattamento" (ci si riferisca al paragrafo dedicato al responsabile del trattamento).

3.6. Il Responsabile del trattamento

Il concetto di "Responsabile del trattamento" riveste un ruolo importante nel contesto della riservatezza e sicurezza dei trattamenti poiché serve ad individuare le responsabilità di coloro che si occupano più da vicino dell'elaborazione dei dati personali, sotto l'autorità diretta del Titolare del trattamento o per suo conto.

L'esistenza di un Responsabile del trattamento dipende da una decisione presa dal Titolare. Quest'ultimo può decidere di trattare i dati all'interno della propria organizzazione – ad esempio attraverso collaboratori autorizzati a trattare i dati sotto la sua diretta autorità - o di delegare tutte o una parte delle attività di trattamento a un'organizzazione esterna.

A norma dell'articolo 28, paragrafo 1 del GDPR "*Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato*".

Il paragrafo 3 dell'articolo 28 del GDPR prevede che "*I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento*"; il paragrafo 9, da ultimo, prevede che "*Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico*".

Per poter agire come Responsabile del trattamento occorrono quindi tre requisiti: essere una persona giuridica distinta dal Titolare e legata a quest'ultimo da un contratto, elaborare i dati personali per conto del Titolare ed essere assoggettato a quest'ultimo nella definizione delle finalità e dei mezzi del trattamento.La liceità dell'attività di trattamento dei dati da parte del Responsabile è determinata dal mandato ricevuto dal Titolare del trattamento. Se va al di là del proprio mandato e se acquisisce un ruolo rilevante nella determinazione delle finalità o degli aspetti fondamentali dei mezzi del trattamento, il Responsabile diventa (con)Titolare se non addirittura titolare autonomo.

Spetta al Titolare identificare i responsabili della struttura organizzativa di competenza, e sottoscrivere i contratti/appendici contrattuali per il trattamento dei dati, avendo cura di tenere costantemente aggiornata la relativa documentazione. Il Titolare potrà effettuare delle verifiche periodiche volte ad assicurare il rispetto, da parte dei Responsabili, delle disposizioni impartite contrattualmente; la periodicità di tali verifiche, previste nel provvedimento o contratto di affidamento, è determinata in funzione della natura dei dati, della probabile gravità dei rischi, dei mezzi da utilizzare per il trattamento e della durata dell'affidamento.

4. PARTE III - ADEMPIMENTI E PROCEDURE

4.1. Misure per la sicurezza dei dati personali

I soggetti designati ai sensi dell'art.2-quaterdecis (tra i quali, l'Amministratore del sistema informatico, l'Amministratore della piattaforma DAD e l'Amministratore di rete) provvedono, per quanto di rispettiva competenza, all'adozione ed alla dimostrazione di aver adottato le misure tecniche ed organizzative adeguate per garantire un livello di sicurezza correlato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento includono:

- la minimizzazione dei dati (uso dei soli dati pertinenti e necessari alle finalità);
- la cifratura dei dati personali (uso di crittografia nei supporti di memorizzazione);
- la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi con cui sono trattati i dati personali (backup dei sistemi, anch'essi cifrati);
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico (ripristino dei sistemi a partire dai backup);
- una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

4.2. Violazione dei dati personali

Per violazione dei dati personali (in seguito "data breach") si intende la violazione di sicurezza che comporti, accidentalmente od in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dall'istituto (tale indicazione operativa pertanto si applica a tutti gli archivi/documenti cartacei ed a tutti i sistemi, anche informativi sui quali siano conservati i dati personali degli interessati, quali cittadini, dipendenti, fornitori, soggetti terzi, ecc.).

La segnalazione di un possibile Data Breach può provenire dall'esterno (cittadini, fornitori esterni, enti istituzionali ecc.) o dall'interno, da parte delle varie funzioni di settore durante il normale svolgimentodell'attività lavorativa (più frequentemente tali eventi vengono evidenziati da funzioni che svolgono attività di verifica e /o di controllo).

Colui il quale riceva la segnalazione dall'esterno o che rileva dall'interno l'evento anomalo di violazione di dati personali, deve darne immediata notizia alTitolare o al DPO, il quale conduce l'analisi volta ad individuare il grado di probabilità che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati. Tale analisi deve essere accompagnata dall'acquisizione di ogni documento ed informazioni utile allo scopo.

IlTitolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede ad informare immediatamente il DPO(direttamente ovvero attraverso la figura del Referente), nonché alla notifica della violazione all'Autorità di controllo.Diversamente, il Titolare motiva con atto scritto i motivi per cui non si ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.

Nel caso il Titolare decida di procedere con la notifica, essa dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.Qualora la notifica effettuata nelle 72 ore non sia completa, sarà sempre possibile in-

tegrarla in una o più fasi successive (ad es. nel caso di violazioni complesse per le quali occorrono indagini approfondite) corredandola con i motivi (analogamente come in caso di notifica in ritardo).

Nel caso in cui la scoperta della violazione non sia contestuale al verificarsi dell'evento che l'ha generata, devono essere indicate nella comunicazione le motivazioni che non hanno consentito l'immediata rilevazione dell'evento stesso e le misure adottate o che si intende adottare affinché ciò non si ripeta in futuro.

Il Responsabile del trattamento eventualmente coinvolto deve:

a) informare l'istituto tempestivamente ed in ogni caso entro e non oltre 24 ore dalla scoperta dell'evento, tramite PEC, di essere venuto a conoscenza di una violazione e fornire tutti i dettagli della violazione subita, in particolare una descrizione della natura della violazione dei dati personali, le categorie e il numero approssimativo di interessati coinvolti, nonché le categorie e il numero approssimativo di registrazioni dei dati in questione, l'impatto della violazione dei dati personali sull'istitutoe sugli Interessati coinvolti e le misure adottate per mitigare i rischi;

b) fornire assistenza all'istituto per far fronte alla violazione ed alle sue conseguenze soprattutto in capo agli Interessati coinvolti. Il Responsabile si attiverà per mitigare gli effetti delle violazioni, proponendo tempestive azioni correttive ed attuando tutte le azioni correttive approvate e/o richieste dall'istituto. Tali misure sono richieste al fine di garantire un livello di sicurezza adeguato al rischio correlato al trattamento eseguito.

Risulta opportuno e di particolare importanza che tutti gli atti di designazione a Responsabile del trattamento contengano una espressa previsione circa la necessità di informare l'istituto, senza ingiustificato ritardo, in caso di avvenuta conoscenza di una violazione di dati personali, anche solo probabile o possibile.

I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, sono i seguenti:

a) danni fisici, materiali o immateriali alle persone fisiche;

b) perdita del controllo dei dati personali;

c) limitazione dei diritti, discriminazione;

d) furto o usurpazione d'identità;

e) perdite finanziarie, danno economico o sociale.

f) decifratura non autorizzata della pseudonimizzazione;

g) pregiudizio alla reputazione;

h) perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

Ove ilTitolare ritenga che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata sia elevato, deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. Prima di procedere alla comunicazione della violazione ai soggetti interessati il testo della comunicazione, le modalità di notifica e le evidenze che attestano il reale livello di pregiudizio, dovranno essere concordate con il DPO. Nel caso in cui la comunicazione dovesse pregiudicare lo svolgimento delle verifiche sull'evento Data Breach, il Titolare può chiedere all'Autorità di controllo l'autorizzazione a ritardare la citata comunicazione per il tempo necessario all'espletamento di tali verifiche.

La probabilità e la gravità del rischio, per i diritti e le libertà dell'interessato, dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali;

- comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).

La notifica all'Autorità di controllo deve avere il contenuto minimo previsto dall'art. 33 del GDPR, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al su citato art. 33.

Ciascun addetto al trattamento deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio.È comunque opportuno che l'inventario delle violazioni tenga traccia anche delle varie fasi di gestione dell'evento, dalla rilevazione, all'analisi e alla sua risoluzione e conclusione.

Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dall'Autorità di controllo al fine di verificare il rispetto delle disposizioni del GDPR.

5. PARTE IV - DIRITTI DELL'INTERESSATO

5.1. Informativa e modalità per l'esercizio dei diritti dell'interessato

L'istituto adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 del GDPR nonché per gestire le comunicazioni in merito all'esercizio dei diritti riconosciuti dal GDPR in forma completa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.

Le informazioni di cui agli articoli 13 e 14 del GDPR sono fornite mediante predisposizione di idonea pagina web sul sito istituzionale e mediante pubblicazione o link nella sezione Amministrazione trasparente del portale. Per i trattamenti dei dati connessi alla gestione del rapporto di lavoro con il personale dipendente e con quello esterno è predisposta apposita informativa.

Una informativa breve è fornita, mediante idonei strumenti:

- attraverso appositi trafiletti nelle modulistiche consegnare agli interessati;
- in avvisi agevolmente visibili dal pubblico, posti nei locali di segreteria dell'istituto o diffusi nell'ambito di pubblicazioni istituzionali e mediante il sito internet del titolare;
- in apposita avvertenza inserita nei contratti ovvero nelle lettere di affidamento di incarichi del personale dipendente, dei soggetti con i quali vengono instaurati rapporti di collaborazione o libero-professionali, dei tirocinanti, dei volontari, degli stagisti ed altri soggetti che entrano in rapporto con l'istituto;
- in apposita avvertenza inserita nelle segnalazioni di disservizio e, in genere, in tutte le comunicazioni dirette all'Amministrazione;
- resa in sede di pubblicazione dei bandi, avvisi, lettere d'invito, ecc.

Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

L'istituto agevola l'esercizio dei diritti dell'interessato ai sensi degli articoli da 12 a 18 del GDPR. Nei casi di cui all'articolo 11, paragrafo 2, del GDPR l'istituto non può rifiutare di soddisfare la richiesta dell'interessato al fine di esercitare i suoi diritti ai sensi degli articoli da 12 a 18, salvo che dimostri che di non essere in grado di identificare l'interessato.

L'istituto fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta di esercizio dei diritti riconosciuti dal GDPR, senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. L'istituto informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta.

Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato.

Se non ottempera alla richiesta dell'interessato, l'istituto informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.

Le informazioni fornite ai sensi degli articoli 13 e 14 ed eventuali comunicazioni e azioni intraprese sulla base dei diritti riconosciuti dal GDPR sono gratuite. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, l'istituto può:

a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure

b) rifiutare di soddisfare la richiesta. Incombe al Titolare l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

Fatto salvo l'articolo 11 del GDPR, qualora l'istituto nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta di esercizio dei diritti riconosciuti dal GDPR, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato.

Il presente documento sarà aggiornato al più ogni 36 mesi o, comunque, a seguito di una modifica dell'assetto organizzativo dell'Istituto.

IL DIRIGENTE SCOLASTICO

Titolare del trattamento dati

firma autografa sostituita da indicazione a mezzo stampa,

ai sensi dell'art.3 D.Lgs. 39/1993