MINISTERO DELL'ISTRUZIONE E DEL MERITO
ISTITUTO COMPRENSIVO
SCUOLA DELL'INFANZIA, PRIMARIA E SECONDARIA DI I° GRADO
"G. Philippone/Giovanni XXIII"
Via Sacramento, 106 – 92020 San Giovanni Gemini (Ag) - C.F./P.I. 93019650840
Cod. Mecc. AGIC818005 Tel.0922/903041 – e-mail: agic818005@istruzione.it
PEC: agic818005@pec.istruzione.it - sito web: www.ic-philippone.edu.it

SCHEMA ORGANIZZATIVO

IN MATERIA DI TUTELA DEI DATI PERSONALI AI SENSI DEL REGOLAMENTO UE 2016/679 (GDPR)

Storia del documento

1° stesura	01 Settembre 2024	Firma del Dirigente scolastico

INDICE DEL DOCUMENTO

1. PREMESSA

Il Regolamento UE 2016/679, denominato GDPR (in italiano RGPD, acronimo di "Regolamento Generale Protezione 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 nazionale attraverso 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 schema organizzativo del dirigente scolastico contiene disposizioni regolamentari minime la cui concreta attuazione è demandata all'organizzazione del personale operante all'interno della istituzione scolastica, nelle sue articolazioni gerarchiche. Unità omogenee di personale (11 atti autorizzativi/istruzioni)

2. PARTE I - NORME E PRINCIPI GENERALI

È bene ricordare le due definizioni dettate dal Regolamento europeo che costituiscono le basi fondanti l'intera struttura della privacy. Infatti, si intende per:

«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.

«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.

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'istituto per 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 da normative di settore.

Gli Uffici applicheranno la vigente normativa quando, durante tutto l'intero ciclo di vita di un documento, si verificasse la presenza di un trattamento di dati particolari. In questo caso si applicheranno tutte le misure di sicurezza al fine di garantire la più rigorosa tutela dei dati personali degli interessati.

In attuazione dei principi contenuti nella normativa nazionale e comunitaria vigenti, 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 Schema 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 (non obbligatori ma fortemente consigliati al personale in servizio), 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 a 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 [inteso come centro decisionale oppure come centro di imputazione giuridica] 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 a 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 controllo e incluso 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 organizzativa Il GDPR non prevede espressamente la figura degli "incaricati", bensì impone che chiunque agisca avendo accesso a dati personali sotto l'autorità del titolare del trattamento, non possa trattare tali dati se non è istruito in tal senso dallo 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 attraverso circolare interna contenente le dettagliate istruzioni relative ai trattamenti che lo stesso dipendente sarà autorizzato ad effettuare. Sono autorizzati al compimento delle operazioni di trattamento dei dati effettuati presso l'istituto, tutti i soggetti dipendenti e collaboratori a qualsiasi titolo, che operano sotto la diretta autorità del titolare. Il dirigente scolastico titolare del trattamento autorizza per iscritto gli addetti tramite atto individuale, specificando i trattamenti che gli stessi sono autorizzati ad effettuare e le istruzioni da seguire affinché le 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.

Referente privacy nei confronti del DPO

Tra i soggetti autorizzati al trattamento, qualora si ravvisi la necessità - nell'ottica di un adeguamento in qualità ai nuovi istituti previsti dal GDPR, alla luce del contesto, della natura e della complessità dei trattamenti effettuati – l'istituto potrà individuare con apposito atto di nomina uno o più dipendenti interni all'istituto a cui assegnare il compito di "Referente" del DPO.

Il Referente, se individuato, supporterà il Titolare nelle seguenti attività:

a) Mantenere i contatti con il DPO dell'istituto, recependo le sue indicazioni e attuando quanto da esso prescritto;

b) Informare il Titolare del trattamento, nonché i dipendenti che eseguono il trattamento, in merito agli obblighi derivanti dal GDPR. Tale attività comporta il supporto nella redazione di pareri, note, circolari, policy, newsletter con segnalazione delle novità normative e giurisprudenziali in materia di protezione dei dati personali e delle migliori best practice in materia di analisi e valutazione dei rischi;

c) Fornire supporto al DPO nella sorveglianza dell'osservanza del GDPR, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

Il Referente è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti e alle informazioni e dati di cui potrebbe venire a conoscenza nell'esercizio delle proprie funzioni. Egli è inoltre tenuto a segnalare al RPD ogni possibile situazione di conflitto di interesse, anche potenziale rispetto ai propri compiti, incarichi e funzioni. Ove i compiti assegnati al Referente vengano svolti in modo collettivo da parte di un team, dovrà essere designato un soggetto coordinatore.

Soggetti designati ex art. 2-quaterdecis

Il Codice Privacy, all'articolo 2-quaterdecies prevede che "*Il Titolare o il Responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. Il Titolare o il Responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta*".

Qualora si ravvisi la necessità - nell'ottica di un adeguamento in qualità ai nuovi istituti previsti dal GDPR, alla luce del contesto, della natura e della complessità dei trattamenti effettuati – il Titolare potrà delegare alcune proprie funzioni ad un soggetto designato, in possesso dei necessari requisiti di esperienza, capacità e professionalità (ad esempio: la tenuta del registro dei trattamenti, l'individuazione dei soggetti autorizzati al trattamento, l'individuazione dei soggetti "responsabili del trattamento" ai sensi dell'art. 28 del Regolamento, ecc.).

Soggetti autorizzati al trattamento dei dati

Il personale interno all'istituto (docenti, assistenti amministrativi, collaboratori scolastici, assistenti tecnici d'aula, assistenti comunali) sono raggruppati in "Unità Omogenee" in modo che ciascuna risponda alle stesse finalità di trattamento. Ciascun componente del gruppo, riceve una lettera di autorizzazione che firmerà quale atto recettizio, nella quale sono indicati quali categorie di dati possono essere trattate, le modalità di trattamento ed in generale, il comportamento da seguire al fine di preservare i diritti degli interessati.

Tutti i componenti delle suddette Unità ricevono periodicamente adeguate formazioni così da tenere aggiornati contenuti e comportamenti

3.5. Amministratore del sistema informatico

Al fine di ottemperare a quanto disposto dal Garante della Privacy con il provvedimento datato 27/11/2008 "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*" come modificato con successivo Provvedimento datato 25/06/2009, l'istituto si riserva la facoltà di nominare, se ritenuto necessario, un Amministratore del Sistema Informatico a garanzia che il proprio sistema informatico sia strutturato e gestito in modo da consentire l'attuazione delle misure tecniche e organizzative adeguate per la necessaria protezione dei dati personali trattati.

Amministratore del sistema informatico potrà essere designato un dipendente dell'istituto ovvero, nel caso di mancanza di un dipendente, nominato un soggetto esterno, sia esso una persona fisica o giuridica. In quest'ultimo caso la persona giuridica dovrà individuare al proprio interno un referente responsabile.

L'Amministratore, qualora nominato, dovrà essere in possesso di titolo di studio specifico in informatica almeno di scuola secondaria di secondo grado o laurea triennale e di comprovate conoscenze specialistiche tecniche e giuridiche in materia di sicurezza degli strumenti e dei programmi informatici per la protezione dei dati personali nonché della capacità di assolvere i compiti di competenza.

Nell'atto di designazione ovvero nel contratto di servizio all'Amministratore di Sistema dovranno essere riportati, altresì, tutti gli adempimenti – con tutto ciò che essi comportano sul piano delle procedure amministrative, dell'organizzazione, dell'adozione e verifica di ogni misura necessaria in materia di protezione dei dati personali – imposti dalle fonti di Diritto Europee e Nazionali, dal "Gruppo di Lavoro Europeo ex art. 29", dal Garante della Privacy, dalle disposizioni Regolamentari e dalle Direttive emanate dal Titolare del trattamento e dal Responsabile della protezione dei dati, nonché per conformarsi alla disciplina del Codice dell'Amministrazione Digitale di cui al Decreto Legislativo n. 82/2005 e ss.mm.ii., in particolare la cura dei seguenti adempimenti:

a) gestire l'hardware e i software dei server e delle postazioni di lavoro informatizzate;
b) impostare e gestire un sistema di autenticazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici;
c) registrare gli accessi logici (autenticazione informatica) ai sistemi di elaborazione ed agli archivi elettronici da parte degli amministratori di sistema; impostare e gestire un sistema di autorizzazione per i componenti degli organi di governo e di controllo interno, per il Responsabile per la protezione dei dati, per gli Incaricati dei trattamenti di dati personali effettuati con strumenti elettronici nonché di quanti siano autorizzati all'accesso ai dati personali contenuti nelle banche-dati informatizzate;
d) verificare costantemente che l'istituto abbia adottato le misure tecniche e organizzative adeguate per la sicurezza dei dati personali, provvedendo senza indugio agli adeguamenti eventualmente necessari, redigendo se necessario entro il 30 Settembre di ogni anno una apposita relazione da inviare al Dirigente e al Responsabile per la protezione dei dati in modo da attuare gli adempimenti amministrativi e contabili per la previsione nella successiva programmazione utile per la realizzazione delle ulteriori misure;

e) suggerire all'istituto l'adozione e l'aggiornamento delle misure di sicurezza adeguate per assicurare la sicurezza dei dati, atte a che i dati personali oggetto di trattamento siano custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Sin dalla definizione del presente Atto organizzativo, all'Amministratore del sistema informatico è:

f) fatto assoluto divieto di leggere, copiare, stampare o visualizzare i documenti o i dati degli utenti memorizzati sul sistema a meno che questo sia strettamente indispensabile per le operazioni attinenti ai ruoli allo stesso assegnati; tale divieto vale anche nei confronti di quanti non siano stati autorizzati dal Titolare o dai Responsabili del trattamento a conoscere i dati personali oggetto di trattamento;

g) fatto obbligo di dare tempestiva comunicazione al Titolare ed ai Responsabili del trattamento interessati nonché al Responsabile della protezione dei dati dei problemi di affidabilità sia dell'hardware che dei software eventualmente rilevati;

h) fatto obbligo di osservare scrupolosamente le informazioni e le disposizioni allo stesso impartite in merito alla protezione dei sistemi informatici, degli elaboratori e dei dati, sia da intrusioni che da eventi accidentali, il trattamento consentito, l'accesso e la trasmissione dei dati, in conformità ai fini della raccolta dei dati.

Il Responsabile della protezione dei dati procederà periodicamente ad impartire indicazioni puntuali per la corretta pianificazione delle attività svolte dall'Amministratore del sistema informatico, in modo da facilitarne la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

3.6. Amministratore di rete

L'istituto potrà nominare un Amministratore di rete attraverso la designazione di un proprio dipendente, ai sensi dall'art. 2-quaterdecis del Codice Privacy (D.Lgs. 196/2003 novellato dal D.Lgs. 101/2018), ovvero attraverso la nomina di un soggetto esterno, siano esso persona fisica o giuridica. In quest'ultimo caso la persona giuridica dovrà individuare al proprio interno un referente responsabile.

Nell'atto di designazione ovvero nel contratto di servizio all'Amministratore di rete dovranno essere riportati tutti gli adempimenti – con tutto ciò che essi comportano sul piano delle procedure amministrative, dell'organizzazione, dell'adozione e della verifica di ogni misura necessaria in materia di protezione dei dati personali – imposti dalle fonti di Diritto Europee e Nazionali, dal Garante per la protezione dei dati personali e dalle disposizioni emanate dal Titolare del trattamento o suggerite dal DPO dell'istituto, nonché per conformarsi alla disciplina del Codice dell'Amministrazione Digitale di cui al Decreto Legislativo n. 82/2005 e ss.mm.ii..

Gli ambiti di intervento dell'Amministratore di rete sono inerenti a:

a) aggiornamento delle politiche di sicurezza del Firewall e mantenimento della separazione delle reti di segreteria, aule/laboratori e WiFi, così come disposto dal Codice dell'Amministrazione digitale;

b) implementazione di meccanismi automatici o semi-automatici per il mantenimento dell'anagrafica dei PC autorizzati all'utilizzo della rete (misura minima come da indicazione AGID circolare 2/2017), anche in collaborazione con l'Amministratore di rete – ambito rete interna (LAN/WLAN);

c) mantenimento dei tracciati del DHCP server e della navigazione in rete (misura minima come da indicazione AGID circolare 2/2017);

d) applicazione di un meccanismo di accesso alle risorse Internet su base username e password personale da parte dei PC della rete (misura minima come da indicazione AGID circolare 2/2017), da gestire anche in collaborazione con eventuali referenti o incaricati tecnici interni all'istituto;

e) ottimizzazione della navigazione delle reti interne verso una o più linee esterne fornite da provider Internet e, ove necessario e possibile, proteggere la navigazione isolando la/le linea/linee internet eventualmente non funzionanti.

3.7. 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 trattamento così come i relativi obblighi e responsabilità. La contitolarità implica in sostanza che tutte le parti coinvolte, ciascuna per la propria porzione di governance 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 successivo paragrafo dedicato al responsabile del trattamento).

3.8. 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*".

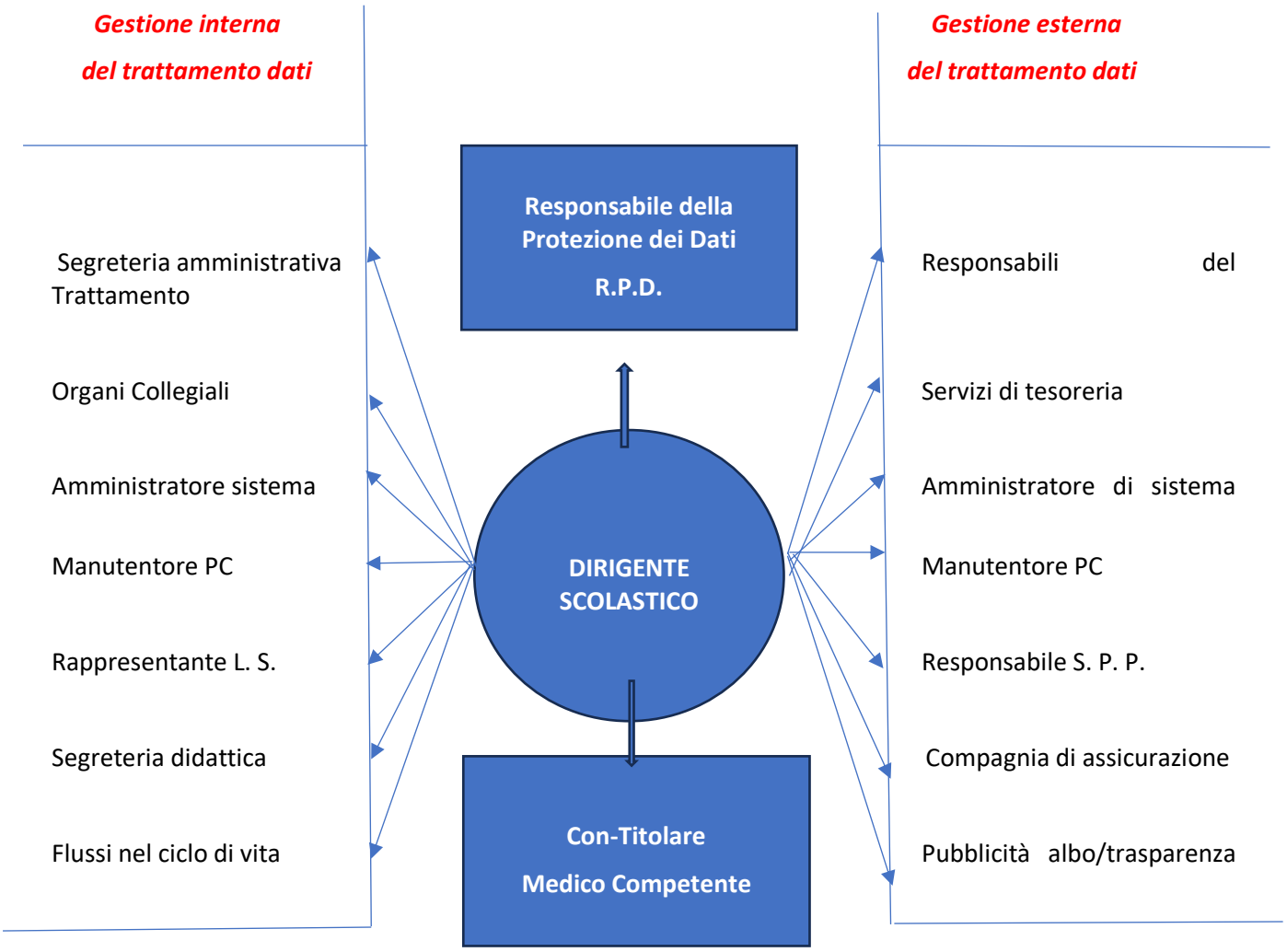
Per poter agire come Responsabile del trattamento occorrono quindi tre requisiti: essere una persona giuridica distinta dal Titolare e legata a quest'ultimo da un contratto, elaborare i dati personali per conto del Titolare ed essere assoggettato a quest'ultimo nella definizione delle finalità e dei 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.

Di seguito viene presentato il modello organizzativo adottato dalla Istituzione scolastica dal quale si evidenzia il concatenamento delle varie fasi del trattamento dei dati personali trattati dalla scuola in relazione alle due sezioni separate, una all'intero della scuola e l'altra dall'interno verso l'esterno della stessa.

ORGANIGRAMMA

GESTIONE DEL TRATTAMENTO DEI DATI PERSONALI IN TEMA DI PRIVACY



DIAGRAMMA

GESTIONE DEL TRATTAMENTO DEI DATI PERSONALI IN TEMA DI PRIVACY

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. Registro delle attività di trattamento

Ai sensi dell'articolo 30 del GDPR "Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità". La medesima norma individua il contenuto minimo di tale Registro, specificando poi che esso è tenuto in forma scritta, anche in formato elettronico e dev'essere messo a disposizione dell'autorità di controllo.

La tenuta di siffatto Registro si configura pertanto come base necessaria al fine di dimostrare la conformità dei trattamenti ai principi enucleati dal GDPR e non soltanto come strumento operativo di mappatura dei trattamenti effettuati. Un'altra grande differenza rispetto al D.lgs. 196/2003 è la modalità di mantenimento di tale documento. Non c'è più una scadenza di revisione annuale, ma viene richiesto che il documento sia sempre aggiornato.

È intenzione dell'istituto adottare un sistema informatico che meglio possa consentire l'aggiornamento e l'accesso alle informazioni. Il sistema informatico dovrà rispettare il contenuto prescritto dal GDPR e dovrà tener conto delle prescrizioni impartite dal Gruppo ex art. 29 (Ora Comitato europeo per la protezione dei dati) nonché dal Garante per la protezione dei dati personali.

Spetta al Titolare:

- effettuare la ricognizione integrale di tutti i trattamenti di dati personali svolti nell'istituto, al fine di consentire la compilazione del Registro;
- effettuare l'aggiornamento periodico, almeno annuale e, comunque, in occasione di modifiche normative, organizzative, gestionali che impattano sui trattamenti, della ricognizione dei trattamenti al fine di garantirne la costante rispondenza alle attività effettivamente svolte dalla struttura organizzativa;
- effettuare (ove necessario) l'analisi del rischio dei trattamenti e la determinazione preliminare dei trattamenti che possono presentare un rischio elevato per i diritti e le libertà degli Interessati, da sottoporre all'approvazione del Titolare;
- contribuire alla tenuta del Registro in relazione ai trattamenti della struttura organizzativa di competenza, fornendo le necessarie informazioni e valutazioni.

Una importante funzione di supervisione in ordine alla tenuta nonché aggiornamento del Registro delle attività di trattamento è demandata alla figura del DPO. Ai sensi dell'art. 39 del GDPR che disciplina infatti le prerogative del DPO si evince che tra le altre è tenuto a "sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo".

4.3. Valutazioni di impatto sulla protezione dei dati

Nel caso in cui una tipologia di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche (specie se eseguita su larga scala o se essa prevede l'uso di nuove tecnologie), il Titolare attuerà una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 RGDP, prima di effettuare il trattamento e considerati la natura, l'oggetto, il contesto e le finalità dello stesso.

La valutazione dell'impatto del trattamento (DPIA) è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi. Un processo di DPIA può riguardare una singola operazione di trattamento dei dati. Tuttavia, si potrebbe ricorrere a un singolo DPIA anche nel caso di trattamenti multipli simili tra loro in termini di natura, ambito di applicazione, contesto, finalità e rischi. Ciò potrebbe essere il caso in cui si utilizzi una tecnologia simile per raccogliere la stessa tipologia di dati per le medesime finalità.

La DPIA deve essere effettuata prima di procedere al trattamento, già dalla fase di progettazione del trattamento stesso anche se alcune delle operazioni di trattamento non sono ancora note, in coerenza con i principi di privacy by design e by default per determinare se il trattamento deve prevedere misure opportune in grado di mitigare i rischi. L'aggiornamento della valutazione d'impatto sulla protezione dei dati nel corso dell'intero ciclo di vita del progetto garantirà che la protezione dei dati e della vita privata sia presa in considerazione e favorisca la creazione di soluzioni che promuovono la conformità.

Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dall'Autorità di controllo ai sensi dell'art. 35, paragrafi 4-6, del GDPR. Fermo restando quanto indicato in tale articolo, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:

a) trattamenti valutativi o di scoring, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;

b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;

c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;

d) trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9 del GDPR;

e) trattamenti di dati su larga scala, tenendo conto: del numero di numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;

f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;

g) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;

h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;

i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Titolare, sentito il Responsabile della protezione dei dati (DPO) e gli Amministratori di del sistema informatico / rete / DAD (se esistente/i), ritenga motivatamente che non possa presentare un rischio elevato. Al contrario, il Titolare può, motivatamente, ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

La DPIA non è necessaria nei casi seguenti:

a) se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, paragrafo 1, del GDPR;

b) se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;

c) se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del 25 maggio 2018 in condizioni specifiche che non hanno subito modifiche;

d) se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.

Non è inoltre necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte dell'Autorità di controllo o dal DPO e che proseguano con le stesse modalità oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni dell'Autorità di controllo basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.

Una volta determinata la necessità di procedere ad una attività di DPIA si rende necessario procedere alla raccolta delle informazioni necessarie allo sviluppo successivo delle attività di analisi dei rischi e produzione del piano dei trattamenti. L'attività si scompone in ulteriori 4 sotto fasi:

a. raccolta delle informazioni per l'analisi dei rischi (informazioni presenti all'interno dei trattamenti, procedimenti coinvolti dal trattamento, finalità dei dati raccolti, flussi informativi, autorizzati all'accesso alle informazioni, asset model a sostegno dei trattamenti (applicativi, hardware, reti, ecc.). Le valutazioni che dovranno essere fatte durante la fase di analisi dei rischi devono tenere in considerazione due aspetti fondamentali: sia i rischi derivanti dai contenuti intrinseci del trattamento stesso comprendenti soprattutto modalità e finalità sia i rischi derivanti da possibili violazioni di sicurezza della protezione del dato).

b. valutazione dei rischi, di norma sviluppata nel classico concetto di valutazione degli impatti e probabilità afferenti ad una serie di minacce in grado di compromettere un asset (informativo) (alcuni esempi sono gli impatti derivanti da una violazione della sicurezza fisica; da una violazione dei dati di identificazione o attinenti l'identità personale; perdite finanziarie o al patrimonio, perdite dovute a frodi; turbamento per la diffusione di una notizia riservata, compromissione di uno stato di salute, evento lesivo dei diritti umani inviolabili o dell'integrità della persona; conseguenze di tipo discriminatorio, perdite di autonomia);

c. valorizzazione delle contromisure e rischio residuo. L'associazione di minacce e contromisure esistenti consente a questo punto di determinare il rischio effettivo che sarà confrontato con un valore di rischio accettabile;

d. piano di trattamento dei rischi.

Tutta la documentazione prodotta all'interno del processo di DPIA, partendo dal censimento e descrizione del trattamento, passando dalle valutazioni preliminari per arrivare, quando necessario, al calcolo di analisi dei rischi e relativo piano di trattamento, devono concorrere alla realizzazione di un documento finale in grado di dimostrare, oltre ovviamente ai risultati ottenuti, la corretta esecuzione formale del processo e la sua aderenza ai requisiti richiesti dal GDPR. Il documento deve inoltre esplicitare la frequenza di aggiornamento del DPIA, tanto maggiore quanto più si utilizzino tecnologie in evoluzione o si prevedono potenziali variazioni nei processi di trattamento.

L'istituto può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.

L'istituto deve consultare l'Autorità di controllo prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato (tale obbligo è previsto se si ritiene che il trattamento sottoposto a DPIA violi il GDPR, in particolare qualora l'istituto non abbia identificato o attenuato sufficientemente il rischio). Il Titolare consulta l'Autorità di controllo anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico.

Quando è stata richiesta una valutazione preventiva all'Autorità di Controllo il trattamento non può essere iniziato almeno fino a che in procedimento di consultazione preventiva si è concluso con successo.

Salvo diversa disposizione dell'Autorità di controllo è bene che la comunicazione di richiesta di consultazione avvenga con modalità che consentano di dimostrare la data certa della stessa comunicazione (es. PEC, Raccomandata, ecc.) visto che i tempi stabiliti per lo sviluppo del processo di consultazione preventiva decorreranno da tale data .L'attività include il recepimento dell'eventuale risposta e l'attuazione degli eventuali interventi necessari per aderire al parere fornito dall'Autorità.

Il DPO monitora lo svolgimento della DPIA. Può inoltre proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale. Eventuali

Responsabili del trattamento collaborano e assistono il Titolare oltre che il Responsabile della protezione dei dati nella conduzione della DPIA fornendo ogni informazione necessaria.

Gli amministratori del sistema informatico, di rete e della piattaforma DAD (se designati) forniscono il necessario supporto al Titolare per lo svolgimento della DPIA. Essi possono inoltre proporre di condurre una DPIA in relazione ad uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

Un esempio di un software applicativo per la gestione di un processo DPIA è "PIA", scaricabile gratuitamente dal sito di CNIL (Autorità francese per la protezione dei dati). Il software, al quale ha aderito anche il garante Italiano, non costituisce un modello al quale fare sempre riferimento (si ricorda che è stato concepito soprattutto per le PMI), ma può offrire un focus sugli elementi principali di cui si compone la procedura di DPIA. Può quindi costituire un utile supporto metodologico e di orientamento allo svolgimento di una DPIA, ma non va inteso come schema predefinito per ogni valutazione d'impatto che va integrata in ragione delle tipologie di trattamento esaminate. Può servire inoltre per comprendere meglio quali possono essere i requisiti di base di un applicativo DPIA adeguato alla propria realtà procedendo quindi ad una "*software selection*" più mirata e consapevole.

4.4. 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 svolgimento dell'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 al Titolare 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.

Il Titolare, 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 integrarla 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'istituto e 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 il Titolare 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

Tra gli adempimenti cogenti e fondamentali balzano in primo piano le c. d. Informative che il Regolamento europeo le presenta come ""*Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato".*

Lo stesso Regolamento europeo fornisce all'interessato due macro-famiglie di diritti:

1. quello della conoscenza, nella quale entrano a far parte il diritto di essere informato, il diritto di accesso, quello di avere notificato eventuali violazioni di dati personali, nonché le scelte propositive quali il diritto di rettifica, La modifica, l'estrazione, la raccolta, la conservazione e l'opposizione al trattamento.
2. e quello del controllo, nel quale entrano a far parte il diritto al consenso ed alla eventuale sua revoca, alla limitazione del trattamento, al trasferimento di dai dati e alla oblio/cancellazione parziale o totale dei dati, quali anche la comunicazione, alla diffusione.

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.

6. PARTE V – SULLE SANZIONI

Il Regolamento europeo rubrica nel suo art. 83 le "*Condizioni generali per infliggere sanzioni amministrative pecuniarie*". Infatti precisa che Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai sensi del presente articolo in relazione alle violazioni del presente regolamento siano in ogni singolo caso effettive, proporzionate e dissuasive, le quali sanzioni sono inflitte, in funzione delle circostanze di ogni singolo caso. Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto di altri parametri

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