Istituto di Istruzione Superiore
"Carlo Beretta"
Via G. Matteotti,299 – 25063 Gardone V.T. (BS)
Tel 030 8912336 (r.a.) Fax 030 8916121
E-mail: bsis00600c@istruzione.it
www.iiscberetta.edu.it

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

Sommario

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 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'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 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:

- 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);
- 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);
- 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);
- individuare i responsabili del trattamento, controllarne e garantirne l'operato (art. 28);
- agevolare l'esercizio dei diritti dell'interessato (art. 12) e fornire agli interessati le informazioni previste dal GDPR (art. 13);
- designare il Responsabile della protezione dei dati (art. 37) ponendolo in grado di svolgere adeguatamente l'attività (art. 38);
- istituire e tenere aggiornato un registro delle attività di trattamento svolte sotto la propria responsabilità (art. 30);
- nei casi ove ciò sia necessario e prima di procedere al trattamento, effettuare una valutazione dell'impatto sulla protezione dei dati personali (art. 35);
- comunicare all'autorità di controllo (art. 33) ed all'interessato (art. 34) eventuali violazioni dei dati;
- ricevere ed osservare provvedimenti, notifiche e ingiunzioni dell'autorità di controllo (art. 58);
- rispondere per il danno cagionato dal trattamento che violi il GDPR (art. 82);
- 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 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:

- 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);
- sorvegliare l'osservanza della normativa in materia di protezione dei dati personali, nonché delle politiche dell'istituto in materia di protezione dei dati personali;
- 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;
- fungere da punto di contatto per il garante per questioni connesse al trattamento;
- fungere da punto di contatto per gli interessati per questioni attinenti al trattamento dei propri dati personali e all'esercizio dei loro diritti;
- promuovere la formazione di tutto il personale dell'istituto in materia di protezione di dati personali e di sicurezza informatica;
- partecipare alla gestione degli incidenti di sicurezza nelle modalità previste da specifica policy dell'istituto;
- formulare gli indirizzi e monitorare la realizzazione del registro delle attività del trattamento di cui all'art. 30 del Regolamento
- 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 del 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 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, 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 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:

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

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;

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.).

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:

- gestire l'hardware e i software dei server e delle postazioni di lavoro informatizzate;
- impostare e gestire un sistema di autenticazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici;
- 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;
- 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 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;
- 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:

- 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;
- 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;
- 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 della piattaforma DAD

L'istituto potrà nominare un "Amministratore della piattaforma di Didattica a Distanza (DAD)", 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), oppure attraverso nomina di 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.
Nell'atto di designazione ovvero nel contratto di servizio all'Amministratore della piattaforma DAD 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 della Piattaforma DAD sono inerenti alla:

- impostazione dei permessi di utilizzo delle varie APP della suite, con particolare riferimento a quelle che permettono la fuoriuscita dal dominio scolastico (queste ultime vietate a meno di una esplicita autorizzazione da parte degli utenti interessati);
- impostazione dei criteri di sicurezza da assegnare ai dispositivi android da affidare in comodato d'uso (funzionalità "gestione dispositivi");
- creazione, modifica o cancellazione delle unità organizzative / gruppi di utenza;
- creazione, attivazione, disattivazione, modifica o cancellazione degli account utente;
- suddivisione degli utenti nei vari gruppi / unità organizzative, anche in relazione alle misure di sicurezza impostate;
- attivazione delle procedure di recupero password per gli utenti che ne facessero esplicita richiesta (con l'obbligo, in questi casi, di rendere necessario, per l'utente, il cambio della password al primo utilizzo);
- risoluzione di problematiche tecniche bloccanti;
- azzeramento dei dati a fine anno scolastico;

3.7. 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:

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

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;

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.

3.8. 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 paragrafo dedicato al responsabile del trattamento).

3.9. 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.

Il dirigente scolastico
Stefano Retali