ISTITUTO COMPRENSIVO STATALE
"Giovanni XXII"
Largo dei Pini
92022 Cammarata
Codice Fiscale 93062680843

DISCIPLINARE INTERNO
IN MATERIA DI PROTEZIONE DI DATI PERSONALI

Redatto in conformità al:
- Regolamento (UE) 2016/679 del Parlamento e del Consiglio europeo
- Decreto legislativo n. 196 del giugno 2003
- Decreto ministeriale n. 305 del dicembre 2006

Storia delle modifiche

Vers.	Descrizione delle modifiche	Data emissione
1.0	Prima versione	Anno scolastico 2018-2019 - mese novembre

ISTITUTO COMPRENSIVO STATALE
"Giovanni XXIII"
Largo dei Pini
92022 Cammarata
Codice Fiscale 93062680843

Prot. N.

del

Indice del Disciplinare

Premesse introduttive . . . . . .

Capitolo 1 Presentazione dell'Istituzione scolastica . . . . . .
Par. 1 - Presentazione dell'istituzione scolastica
Par. 2 – Basi giuridiche

Capitolo 2 Principi di liceità . . . . . .
Par. 1 – Principi di liceità

Capitolo 3 Le definizioni . . . . . .
Par. 1 - Le Definizioni
Par. 2 - Il Trattamento di dati

Capitolo 4 Ripartizioni di ruoli . . . . . .
Par. 1 - Ripartizioni ruoli e compiti

Capitolo 5 La sicurezza informatica . . . . . .
Par. 1 – Descrizione dei modelli FNSC e ABSC
Par. 2 – Aspetto di privacy legati al Framework
Par. 3 – Contesto di riferimento all'analisi dei rischi
Par. 4 – Azioni da intraprendere per la prevenzione delle vulnerabilità e i risultati dei controlli

Capitolo 6 La Privacy e la sicurezza informatica della scuola . . . .
Par. 1 – La privacy e la sicurezza informatica
Par. 2 – L'Utilizzo dei servizi in cloud computing

Capitolo 7 L'interessato e i suoi diritti . . . . . .
Par. 1 - L'interessato e i suoi diritti
Par. 2 – L'Informativa e il consenso

Capitolo 8 Le sanzioni amministrativi e penali. . . . . .
Par. 1 – Le sanzioni

Capitolo 9 Altri temi . . . . . .
Par. 1 – Il Responsabile della protezione dei dati
Par. 2 – I Registri delle attività
Par. 3 – La Valutazione d'impatto

PREMESSE GENERALI

La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali.
Tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno. È opportuno che le persone fisiche abbiano il controllo dei dati personali che li riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche.

Al fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche, di rimuovere gli ostacoli alla circolazione dei dati personali e prevenire disparità che possono ostacolare la libera circolazione dei dati personali all'interno dell'Unione, è necessario l'esistenza di un regolamento che garantisca certezza del diritto e trasparenza agli operatori economici, comprese le micro, piccole e medie imprese, che offra alle persone fisiche in tutti gli Stati membri il medesimo livello di diritti azionabili e di obblighi e responsabilità dei titolari del trattamento e dei responsabili del trattamento, che assicuri un monitoraggio coerente del trattamento dei dati personali, sanzioni equivalenti in tutti gli Stati membri e una cooperazione efficace tra le autorità di controllo dei diversi Stati membri.
È opportuno assicurare un'applicazione coerente e omogenea delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione. Per quanto riguarda il trattamento dei dati personali per l'adempimento di un obbligo legale, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, gli Stati membri devono rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione delle norme del presente regolamento. In combinato disposto con la legislazione generale e orizzontale in materia di protezione dei dati che attua la direttiva 95/46/CE gli Stati membri dispongono di varie leggi settoriali in settori che richiedono disposizioni più specifiche. Il regolamento prevede anche un margine di manovra degli Stati membri per precisarne le norme, anche con riguardo al trattamento di categorie particolari di dati personali («dati sensibili»). In tal senso, il regolamento non esclude che il diritto degli Stati membri stabilisca le condizioni per specifiche situazioni di trattamento, anche determinando con maggiore precisione le condizioni alle quali il trattamento di dati personali è lecito.

Ancora, al fine di evitare l'insorgere di gravi rischi di elusione, la protezione delle persone fisiche deve essere neutrale sotto il profilo tecnologico e non deve dipendere dalle tecniche impiegate.

La protezione delle persone fisiche può applicarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali.
Il regolamento generale non si applica:
- a questioni di tutela dei diritti e delle libertà fondamentali o di libera circolazione dei dati personali riferite ad attività che non rientrano nell'ambito di applicazione del diritto dell'Unione, quali le attività riguardanti la sicurezza nazionale o quelle attività relative alla politica estera e di sicurezza comune dell'Unione;
- al trattamento di dati personali effettuato da una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico e quindi senza una connessione con un'attività commerciale o professionale. Le attività a carattere personale o domestico potrebbero comprendere la corrispondenza e gli indirizzari, o l'uso dei social network e attività online intraprese nel quadro di tali attività. Tuttavia, il regolamento europeo si applica ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell'ambito di tali attività a carattere personale o domestico;
- ai dati personali delle persone decedute. Gli Stati membri possono prevedere norme riguardanti il trattamento dei dati personali delle persone decedute.

I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare:
- se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo;
- se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano;
- se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di 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, al fine di creare o utilizzare profili personali;
- se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori;
- se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del regolamento. Al fine di poter dimostrare la conformità con il regolamento, il titolare del trattamento deve adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default. Tali misure potrebbero consistere, tra l'altro:
- nel ridurre al minimo il trattamento dei dati personali;

- pseudonimizzare i dati personali il più presto possibile;
- offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali;
- consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza.

Infine non è possibile disconoscere l'eventualità di bilanciamento tra il d. lgs. 196 del 2003, c.d. Codice della Privacy e il Regolamento Generale, il 675/2016.
E' doveroso precisare che quando una Nazione entra a far parte dell'Unione europea rinuncia ad una parte della propria sovranità lasciandola all'Unione Europea.

In base all'art. 99 (l'ultimo), il regolamento si dovrà applicare a partire dal 25 maggio 2018 e sarà obbligatorio nella sua interezza in tutti i paesi dell'Unione. Pertanto si deve intendere abrogata la Direttiva 95/46/CE mentre rimane in vigore la Direttiva 58/2002/CE.

Nonostante il Regolamento prevalga sulla legge nazionale interna, tuttavia la sola esistenza ed applicazione del Regolamento non comporta l'abrogazione automatica della legge statale regolante la materia medesima.

Pertanto formalmente sono ancora vigenti tutte quelle disposizioni della legge italiana non in contrasto con le nuove previsioni normative europee e quelle in contrasto dovranno essere in ogni caso disapplicate in favore della nuova disciplina.
Quindi il d. lgs. 196 non subisce alcuna abrogazione diretta e, al contrario, mantiene la sua forza normativa, subendo una sorta di **rilettura in chiave RGPD**; per cui:
- se non vi è compatibilità tra il d. lgs. 196 e il Regolamento 679/21016, il Codice privacy **non** si deve applicare più e ciò n favore del regolamento;
- mentre se vi è compatibilità tra le due norme, il d. lgs. 196 rimane applicabile continuando a dettare legge, anche in maniera più specifica rispetto al Regolamento Generale europeo.

Nei casi in cui non è possibile stabilire con certezza dove il diritto vada occorre che la scelta sia in linea con il **principio dell'accountability** su cui si basa l'intero Regolamento Generale.
Titolare e responsabile del trattamento devono responsabilizzarsi e mettere in atto misure di sicurezza adeguate alla loro realtà a seguito di un attento esame di bilanciamento su cui si basa la scelta.

Capitolo 1
Presentazione dell'istituzione scolastica. Basi giuridiche

Par. 1 - Presentazione dell'istituzione scolastica

Benvenuti nel nostro Istituto scolastico!

Il presente Disciplinare interno è stato realizzato non soltanto per conformarsi alla normativa europea nonché a quella italiana, in materia di protezione dei dati personali trattati dalla istituzione scolastica ma anche quella di informare tutti coloro che entrano in contatto con essa che saranno garantiti le libertà fondamentali sanciti dalla nostra Carta costituzionale nonché gli obblighi riguardanti la privacy e le libertà civili.

Infatti, Il regolamento europeo rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica.

Ed è ciò che questa scuola intende perseguire ogni volta che tratta i dati raccolti presso l'interessato, sia esso dipendente o alunno o fornitore, soprattutto nei momenti di auditing durante i quali la scuola vigilerà in maniera particolare.

I dati trattati ricadono in misure organizzative e tecniche, come nella tabella seguente.

ORGANIZZATIVE	TECNICHE
• Analisi dei rischi • Prescrizione di linee guida di sicurezza • Assegnazione di incarichi • Formazione del personale • Classificazione dei dati • Documentazione dei controlli periodici • Verifiche periodiche sui dati o trattamenti non corretti • Distruzione controllata dei supporti • Piano di disaster recover • Identificazione dell'incaricato • Controllo dell'aggiornamento antivirus • Controllo sull'operato degli addetti alla manutenzione e assimilabili • Controllo dei supporti consegnati in manutenzione • Controllo degli accessi a dati e programmi	• Vigilanza della sede • Ingresso controllato nei locali ove ha luogo il trattamento • Sistemi di allarme • Registrazione degli accessi • Custodia in classificatori o armadi non accessibili • Custodia in armadi blindati e/o ignifughi • Deposito in cassaforte • Dispositivi antincendio • Continuità dell'alimentazione elettrica • Verifica della leggibilità dei supporti • Autenticazione dell'incaricato

Descrizione dei locali ove sono organizzati gli uffici

L'edificio scolastico sorge su un'area urbana circondata da insediamenti residenziali.
Presenta lungo tutto il perimetro un muretto di cinta con sovrastanti inferriate e prospettanti con vie urbane a moderato traffico veicolare.
Presenta un solo access0, utile sia agli automezzi che ai pedoni. L'ingresso a scuola è costituito da un portone in alluminio anodizzato controllato dai collaboratori scolastici che svolgono la loro attività lavorativa nella bidelleria che si trova interno alla stessa.

L'Istituto Comprensivo si sviluppa in 7 Plessi: quello centrale nel quale si trovano gli uffici di segreteria dove vengono trattati i dati relativi a tutti i trattamenti come illustrato successivamente; ed nei rimanenti plessi il trattamento dei dati personali è relativo agli alunni il relativo luogo del trattamento è quello delle aule d'insegnamento.

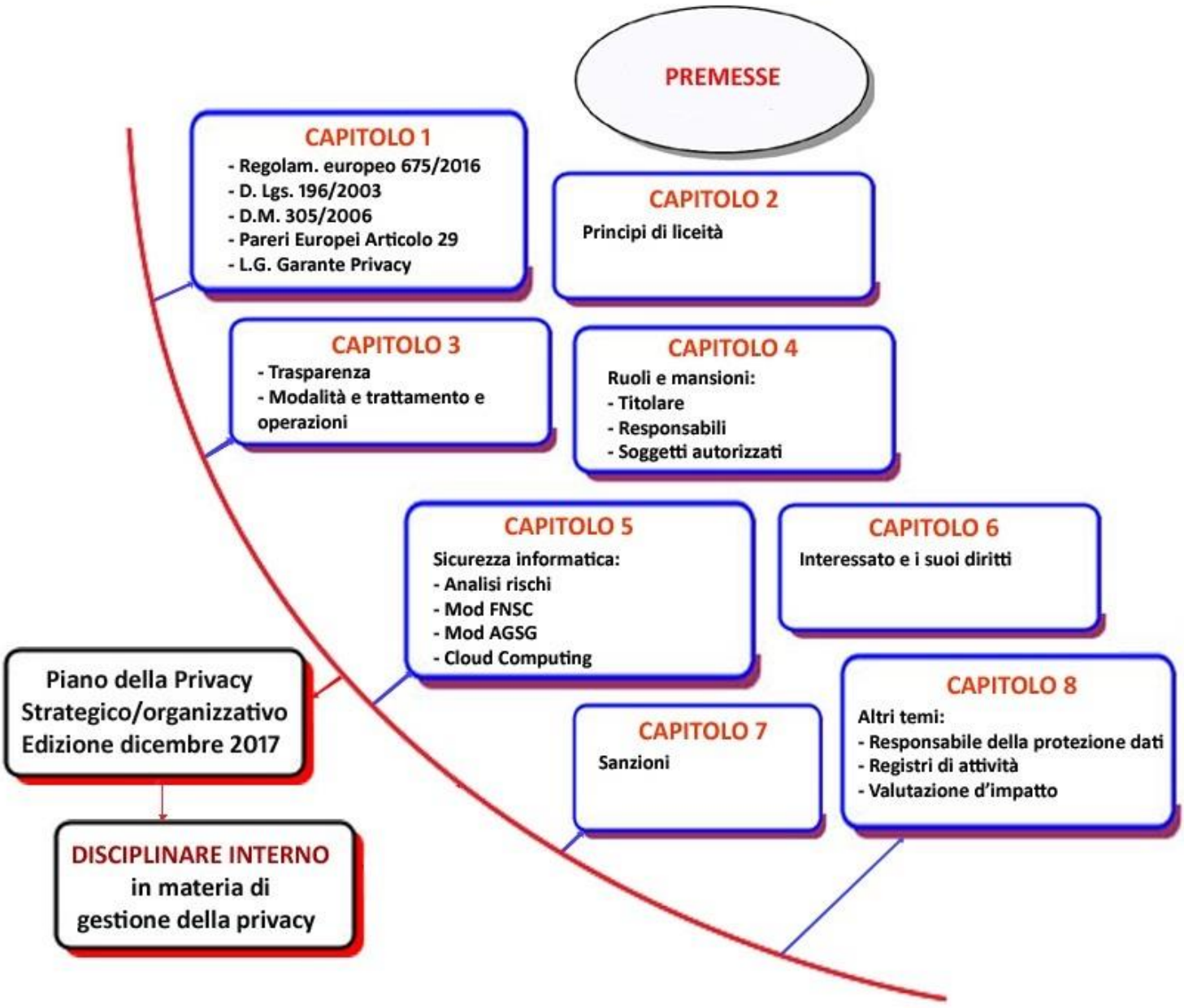
Plesso Centrale	Categorie di dati
Presidenza	**Tutte**
Ufficio del DSGA	**Tutte**
Segreteria Alunni	**Alunni**
Segreteria Personale	**Alunni Personale**
Aule di insegnamento	**Alunni**
Plesso "Giovanni XXIII" Primaria – Referente A. Manzella Plesso "Panepinto" Primaria – Referente Carmela Lupo Plesso "Santa Maria" Primaria – Referente M. C. Mulè	**Categorie di dati**
Aule d'insegnamento	**Alunni**
Plesso "Cacciapensieri" Infanzia – Referente A. Stornaiuolo Plesso "Terrrossa" Infanzia – Referente R. Scibetta Plesso "Gianguarna" Infanzia – Referente Rosa Scibetta	**Categorie di dati**
Aule d'insegnamento	**Alunni**
Plesso "Dante Alighieri" Scuola Media - Referente	**Categorie di dati**
Aule d'insegnamento	**Alunni**

Locali	Posizione e Descrizione	Uso
Locale_0	Si accede nell'area amministrativa direttamente dalla hall della scuola sita in Largo dei Pini. L'area amministrativa è costituita da n. 4 locali situati tutti sullo stesso piano, come descritti in planimetria. Si utilizzano cassetti, provvisti di adeguate serrature, per la conservazione immediata di pratiche e quanto altro prodotto durante l'attività lavorativa in attesa di essere trasferiti in archivi di transito prima della conservazione definitiva. Solo la segreteria didattica è dotata di grate in fero alle finestre. Gli accessi agli uffici sono metalliche. I condizionatori sono presenti negli uffici amministrativi. La scuola non possiede distruggi carta mentre gli estintori sono collocati lungo i corridoi in prossimità degli uffici. Infine, gli scanner sono negli uffici di segreteria e presidenza. I registri vengono conservati presso l'archivio al termine delle lezioni quotidiane	Area comune
Locale_1	Vengono trattati dati degli alunni e delle relative famiglie. Si utilizzano n. 2 computer dati in dotazione	Segreteria didattica
Locale_2	E' l'ufficio del direttore amministrativo. In questo ufficio sono trattati tutti i dati che affluiscono nella scuola utilizzando n. 1 computer dato in dotazione.	Ufficio del direttore amministrativo
Locale_3	E' l'ufficio di presidenza. In questo ufficio sono trattati tutti i dati che affluiscono nella scuola utilizzando n. 1 computer dato in dotazione	Ufficio di presidenza
Locale _4	E' la segreteria dove sono trattati tutti i dati del personale di ruolo e non, utilizzando n. 2 PC dati in dotazione.	Segreteria del personale

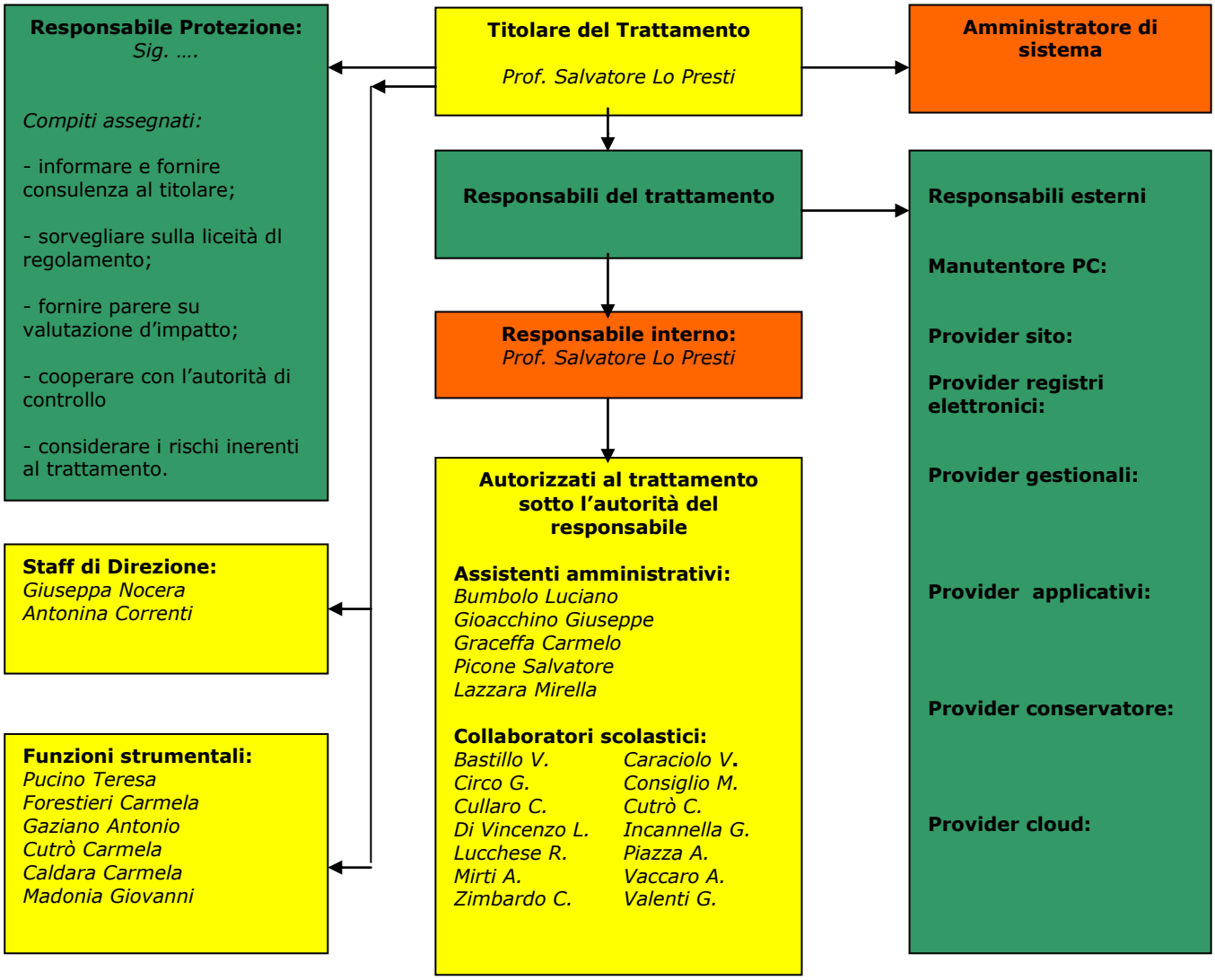
Dati identificativi del Soggetto Titolare

DIREZIONE E SEGRETERIA	Istituto Comprensivo Statale "Giovanni XXIII"
Indirizzo sede centrale	Largo dei Pini – 92022 Cammarata
Tipologie Scuola	Scuola dell'Infanzia – Scuola Primaria – Scuola Secondaria di I Grado
Anno scolastico	2018/2019
Codice meccanografico sede centrale	AGIC82700X
Codice IPA	istsc_agic82700x
Indirizzo e-mail	agic82700x@istruzione.it
Sito web	www.icgiovanni23esimo.gov.it
Posta Elettronica Certificata	agic82700x@pec.istruzione.it
Codice fiscale	93062680843
Alunni numero complessivo	655
Classi numero complessivo	39
Insegnanti numero complessivo	86
Personale ATA	18 di cui 4 Assistenti Amministrativi e 14 collaboratori scolastici.
Direttore dei Servizi generali ed Amministrativi	Sig.ra Lazzara Mirella
Dirigente Scolastico	Dott. Salvatore Lo Presti
Collaboratore Vicario	Prof.ssa Giuseppa Nocera
Responsabile del Servizio di Prevenzione e Protezione	Sig. Bennardo Giuseppe
Responsabile dei Lavoratori sulla Sicurezza	Sig. Antonino Mirti
Medico competente	Dott. Antonio Butera

PIANO STRATEGICO/ORGANIZZATIVO



Schema della Privacy della Istituzione Scolastica



Attività svolta

Il Piano di Offerta Formativa è uno strumento elaborato dal Collegio dei Docenti ed adottato dal Consiglio di Istituto, nel quale sono delineate l'insieme dei bisogni formativi e definisce i servizi generali che l'Istituto eroga, precisandone le scelte educative, curriculari, didattiche ed organizzative che intende esprimere e realizzare. Esprime le progettazioni curriculare, extracurriculare e quella educativa ed organizzativa.

Il P.T.O.F. o Piano Triennale dell'Offerta Formativa è un Documento contrattuale previsto dal Contratto Collettivo Nazionale e dal Regolamento sull'autonomia scolastica (DPR 275, 1999, art. 8). si costituisce come documento fondamentale della scuola italiana e illustra il Progetto specifico di ogni istituzione scolastica: il Piano riflette le esigenze del contesto culturale, sociale ed economico della realtà locale, tenendo conto della programmazione territoriale dell'Offerta Formativa.

Il Piano dell'Offerta Formativa è, allora, un documento incarnato nel tessuto del territorio in cui ogni singola istituzione scolastica è chiamata ad operare. Presenta l'offerta formativa della scuola, mette in evidenza il curricolo obbligatorio, comprensivo della quota nazionale e di quella assegnata alle istituzioni scolastiche, nonché le attività opzionali e migliorative del curricolo ordinario. Il PTOF costituisce la matrice del curricolo. Contiene i prospetti di riparto dei fondi finanziari ad esso attribuiti che consentono di comprendere le scelte di politica formativa della scuola.
Il Piano prevede i criteri e gli strumenti di valutazione e di autovalutazione delle dichiarazioni in esso contenute e presenta un impianto flessibile, trasparente, organizzato, integrato, orientato ad azioni di efficienza e di efficacia a tutti i livelli a garanzia e tutela degli alunni, delle famiglie, delle realtà istituzionali e non, con cui la scuola è chiamata ad interagire e collaborare.

E' elaborato dal Collegio dei Docenti sulla base degli indirizzi generali per le attività della scuola e delle scelte generali di gestione e di amministrazione definiti dal consiglio d'Istituto tenuto conto delle proposte e dei pareri formativi dagli organismi e dalle associazioni, ed è quindi il risultato di una sostanziale condivisione, di una autentica assunzione di responsabilità da parte di tutte le sue componenti.
Esso è adottato dal Consiglio d'Istituto.
Le proposte di integrazione, di modifiche, di aggiornamento, vengono predisposte dallo staff di Dirigenza anche su proposta di singoli gruppi di docenti.

Descrizione delle attività degli operatori scolastici

DOCENTI

L'attività del personale docente si esplica secondo la funzione prevista dalla normativa vigente, art. 395 del d. lgs. n. 297/94

- compresa l'attività di vigilanza sui minori in consegna;
- la progettazione didattica da attuarsi in incontri collegiali dei docenti di ciascun corso, da realizzarsi in momenti non coincidenti con l'orario di lezione;
- la realizzazione di iniziative educative in aule speciali o laboratori; in tali casi vengono utilizzate apparecchiature quali televisore, videoregistratore, telecamera, proiettore per film-diapositive-filmine fisse, episcopio, registratori, amplificatori, computer, macchine da scrivere meccaniche-elettriche-elettroniche, Lim e Tablet;
- l'assistenza educativa agli studenti;
- la partecipazione alle riunioni degli organi collegiali;
- i colloqui individuali con i genitori degli studenti;
- la partecipazione agli scrutini ed agli esami;
- i rapporti con gli specialisti operanti sul territorio.

COLLABORATORI SCOLASTICI

L'attività del personale non docente-ausiliario, si esplica secondo la funzione prevista per il personale ausiliario statale.

Competono al personale ausiliario (collaboratori scolastici):

- pulizia giornaliera degli ambienti scolastici utilizzati quotidianamente, compresi i servizi igienici, la palestra, i luoghi di passaggio abituale,
- pulizia periodica laboratori, vetrate, aule riunioni,
- bonifica periodica giardini e cortili,
- pulizia periodica locali deposito e seminterrati,
- trasporto arredi e materiale nelle/dalle aule,
- commissioni interne (circolari, messaggi),
- vigilanza continua all'ingresso,
- apertura/chiusura accessi,
- sorveglianza sugli studenti in caso di necessità,
- collaborazione con i docenti nell'assistenza a minori non autonomi,
- comando ed uso quadro elettrico generale e di piano,
- comando segnali acustici di avvertimento (campanella, sirena...),
- messa in funzione di macchine semplici (fotocopiatrice, proiettore, videoregistratore,...),
- affissioni nella scuola,
- riordino materiale con raccolta, trasporto sacchi rifiuti solidi,
- conservazione materiale di pulizia in luoghi non accessibili ai minori,

PERSONALE AMMINISTRATIVO

L'attività del personale amministrativo statale si esplica secondo la funzione prevista dalla normativa vigente e le definizioni poste dalle norme contrattuali.

Profilo: Direttore dei Servizi Generali ed Amministrativi

Svolge attività lavorativa complessa, che richiede conoscenza della normativa vigente nonché delle procedure amministrativo-contabili. Organizza i servizi amministrativi dell'unità scolastica o educativa ed è responsabile del funzionamento degli stessi. Ha autonomia operativa e responsabilità diretta nella definizione e nell'esecuzione degli atti a carattere amministrativo contabile di ragioneria e di economato, che assumono nei casi previsti rilevanza anche esterna. Sovrintende, nell'ambito delle direttive di massima impartite e degli obiettivi assegnati, ai servizi amministrativi e ai servizi generali dell'istituzione scolastica ed educativa e coordina il relativo personale. Provvede direttamente al rilascio di certificazioni, nonché di estratti e copie di documenti, che non comportino valutazioni discrezionali. Provvede, nel rispetto delle competenze degli organi di gestione dell'istituzione scolastica ed educativa, all'esecuzione delle delibere degli organi collegiali aventi carattere esclusivamente contabile e di quelle sottoposte a procedimento vincolato. Esprime pareri sugli atti riguardanti la gestione amministrativa e contabile del personale, elabora progetti e proposte inerenti il miglioramento organizzativo e la funzionalità dei servizi di competenza, anche in relazione all'uso di procedure informatiche. Cura l'attività istruttoria diretta alla stipulazione di accordi, contratti e convenzioni con soggetti esterni.

Può svolgere attività di formazione e aggiornamento ed attività tutorie nei confronti di personale neo assunto.

Profilo: Assistente amministrativo.

Esegue attività lavorativa richiedente specifica preparazione professionale e capacità di esecuzione delle procedure anche con l'utilizzazione di strumenti di tipo informatico. Ha autonomia operativa con margini valutativi nella predisposizione, istruzione e redazione degli atti amministrativo-contabili della istituzione scolastica ed educativa nell'ambito delle direttive e delle istruzioni ricevute. Svolge attività di diretta e immediata collaborazione con il responsabile amministrativo coadiuvandolo nelle attività e sostituendolo nei casi di assenza.

Ha competenza diretta della tenuta dell'archivio e del protocollo. Ha rapporti con l'utenza ed assolve i servizi esterni connessi con il proprio lavoro. Può essere addetto ai servizi di biblioteca e al controllo delle relative giacenze, nonché dello stato di conservazione del materiale librario. Nelle istituzioni scolastiche ed educative dotate di magazzino e addetto, con responsabilità diretta, alla custodia, alla verifica, alla registrazione delle entrate e delle uscite del materiale e delle derrate in giacenza.

Può svolgere attività di coordinamento di più addetti inseriti in settori o aree omogenee, attività di supporto amministrativo alla progettazione e realizzazione di iniziative didattiche, decise dagli organi collegiali.

In relazione alla introduzione di nuove tecnologie, anche di tipo informatico, partecipa alle iniziative specifiche di formazione e aggiornamento.

Par. 2 - Le basi giuridiche

La base giuridica utile alla comprensione e all'applicazione del Regolamento europeo è costituita dell'elenco di leggi e normative che sono alla base dello stesso regolamento.

1) Regolamento UE N. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile dl 2016 relativo "*alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)".*
2) Decreto legislativo N. 196 del 30 giugno 2003 in materia di "*Codice in materia di protezione di dati personali"*
3) Decreto del 7 dicembre 2006, N. 305 Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della pubblica istruzione, in attuazione degli articoli 20 e 21 del decreto legislativo 30 giugno 2003, n. 196, recante «*Codice in materia di protezione dei dati personali».*
4) Linee guida adottate dal Gruppo di lavoro europeo sulla tutela delle persone fisiche con riguardo al trattamento di dati personali, elemento identificativo: Documento 16/EN WP243 e le relative FAQ allegate
5) Parere adottato il 20 giugno 2007 dal Gruppo di lavoro Articolo 29 per la tutela delle persone fisiche con riguardo al trattamento di dati personali in materia di dato personale
6) Linee guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 adottate dal Gruppo di lavoro Articolo 29 il 4 aprile 2017 elemento identificativo: Documento 17/EN WP248
7) Linee guida sul diritto alla "portabilità dei dati" adottate dal Gruppo di lavoro Articolo 29 il 13 dicembre 2016 elemento identificativo: Documento 16/EN WP242 rev.0
8) Guida al Regolamento europeo in materia di protezione di dati personali redatto dal Garante italiano per la protezione dei dati.
9) Guida all'applicazione del Regolamento europeo redatto dal Garante italiano in materia di protezione dei dati personali
10) Linee guida redatte dal Garante italiano il 19 marzo 2015 n materia di trattamento di dati personali per profilazione on line [doc. web 3881513]
11) "Vademecum privacy" pubblicato dal Garante italiano per la protezione dei dati personali
12) "Cloud computing": proteggere i dati per non cadere dalle nuvole edito dal Garante italiano per la protezione dei dati personali;
13) "Raccomandazioni e proposte sull'utilizzo del cloud computing nella pubblica ammnistrazione" edito da DigitPA il 28 giugno 2012;
14) Modulo di implementazione delle misure minime di sicurezza per le pubbliche amministrazioni, pubblicato in Gazzetta Ufficiale della Repubblica Italiana il 4 aprile 2017;
15) Cyber Security National Lab. - Un framework Nazionale per la Cyber security
    Versione 1.0 del febbraio 2016

Capitolo 2
Principi di liceità

Par. 1 - Principi di liceità

Il trattamento dei dati personali deve essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica.

Il regolamento auspica applicabile i principi di protezione dei dati a tutte le informazioni relative a una persona fisica identificata o identificabile. I dati personali sottoposti a pseudonimizzazione, i quali devono essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, devono essere considerati informazioni su una persona fisica identificabile. Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici. I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca.

Il regolamento non si applica ai dati personali delle persone decedute. Gli Stati membri possono prevedere norme riguardanti il trattamento dei dati personali delle persone decedute.

L'applicazione della pseudonimizzazione ai dati personali può ridurre i rischi per gli interessati e aiutare i titolari del trattamento e i responsabili del trattamento a rispettare i loro obblighi di protezione dei dati. L'utilizzo dell'uso della «pseudonimizzazione» nel regolamento non è quindi intesa a precludere altre misure di protezione dei dati.

Al fine di creare incentivi per l'applicazione della pseudonimizzazione nel trattamento dei dati personali, dovrebbero essere possibili misure di pseudonimizzazione con possibilità di analisi generale all'interno dello stesso titolare del trattamento, qualora il titolare del trattamento abbia adottato le misure tecniche e organizzative necessarie ad assicurare, per il trattamento interessato, l'attuazione del regolamento, e che le informazioni aggiuntive per l'attribuzione dei dati personali a un interessato specifico siano conservate separatamente. Il titolare del trattamento che effettua il trattamento dei dati personali deve indicare le persone autorizzate all'interno dello stesso titolare del trattamento.

I minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali. Tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore. Il consenso del titolare della responsabilità genitoriale non deve essere necessario nel quadro dei servizi di prevenzione o di consulenza forniti direttamente a un minore.

Le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, a marcatori temporanei (cookies) o a identificativi di altro tipo, come i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle.

Qualsiasi trattamento di dati personali dovrebbe essere lecito e corretto. Dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano nonché la misura in cui i dati personali sono o saranno trattati. Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro. Tale principio riguarda, in particolare, l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento corretto e trasparente con riguardo alle persone fisiche interessate e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano. È opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento. In particolare, le finalità specifiche del trattamento dei dati personali dovrebbero essere esplicite e legittime e precisate al momento della raccolta di detti dati personali. I dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento. Da qui l'obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario. I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi. Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica. È opportuno adottare tutte le misure ragionevoli affinché i dati personali inesatti siano rettificati o cancellati. I dati personali dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche per impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento.

Perché sia lecito, il trattamento di dati personali dovrebbe fondarsi sul consenso dell'interessato o su altra base legittima prevista per legge dal regolamento o dal diritto dell'Unione o degli Stati membri, come indicato nel regolamento, tenuto conto della necessità di ottemperare all'obbligo legale al quale il titolare del trattamento è soggetto o della necessità di esecuzione di un contratto di cui l'interessato è parte o di esecuzione di misure precontrattuali adottate su richiesta dello stesso.

Il trattamento dovrebbe essere considerato lecito se è necessario nell'ambito di un contratto o ai fini della conclusione di un contratto.

Il trattamento di dati personali dovrebbe essere altresì considerato lecito quando è necessario per proteggere un interesse essenziale per la vita dell'interessato o di un'altra persona fisica. Il trattamento di dati personali fondato sull'interesse vitale di un'altra persona fisica dovrebbe avere luogo in principio unicamente quando il trattamento non può essere manifestamente fondato su un'altra base giuridica. Alcuni tipi di trattamento dei dati personali possono rispondere sia a rilevanti motivi di interesse pubblico sia agli interessi vitali dell'interessato, per esempio se il trattamento è necessario a fini umanitari, tra l'altro per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione o in casi di emergenze umanitarie, in particolare in casi di catastrofi di origine naturale e umana.

Il trattamento dei dati personali per finalità diverse da quelle per le quali i dati personali sono stati inizialmente raccolti dovrebbe essere consentito solo se compatibile con le finalità per le quali i dati personali sono stati inizialmente raccolti. In tal caso non è richiesta alcuna base giuridica separata oltre a quella che ha consentito la raccolta dei dati personali. Se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il titolare del trattamento, il diritto dell'Unione o degli Stati membri può stabilire e precisare le finalità e i compiti per i quali l'ulteriore trattamento è considerato lecito e compatibile. L'ulteriore trattamento a fini di archiviazione nel pubblico interesse, o di ricerca scientifica o storica o a fini statistici dovrebbe essere considerato un trattamento lecito e compatibile. La base giuridica fornita dal diritto dell'Unione o degli Stati membri per il trattamento dei dati personali può anche costituire una base giuridica per l'ulteriore trattamento. Per accertare se la finalità di un ulteriore trattamento sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento dovrebbe, dopo aver soddisfatto tutti i requisiti per la liceità del trattamento originario, tener conto tra l'altro di ogni nesso tra tali finalità e le finalità dell'ulteriore trattamento previsto, del contesto in cui i dati personali sono stati raccolti, in particolare le ragionevoli aspettative dell'interessato in base alla sua relazione con il titolare del trattamento con riguardo al loro ulteriore utilizzo; della natura dei dati personali; delle conseguenze dell'ulteriore trattamento previsto per gli interessati; e dell'esistenza di garanzie adeguate sia nel trattamento originario sia nell'ulteriore trattamento previsto.

Ove l'interessato abbia prestato il suo consenso o il trattamento si basi sul diritto dell'Unione o degli Stati membri che costituisce una misura necessaria e proporzionata in una società democratica per salvaguardare, in particolare, importanti obiettivi di interesse pubblico generale, il titolare del trattamento dovrebbe poter sottoporre i dati personali a ulteriore trattamento a prescindere dalla compatibilità delle finalità. In ogni caso, dovrebbe essere garantita l'applicazione dei principi stabiliti dal presente regolamento, in particolare l'obbligo di informare l'interessato di tali altre finalità e dei suoi diritti, compreso il diritto di opporsi. L'indicazione da parte del titolare del trattamento di possibili reati o minacce alla sicurezza pubblica e la trasmissione dei dati personali pertinenti a un'autorità competente in singoli casi o in più casi riguardanti lo stesso reato o la stessa minaccia alla sicurezza pubblica dovrebbero essere considerate nell'interesse legittimo perseguito dal titolare del trattamento. Tuttavia, tale trasmissione nell'interesse legittimo del titolare del trattamento o l'ulteriore trattamento dei dati personali dovrebbero essere vietati se il trattamento non è compatibile con un obbligo vincolante di segretezza, di natura giuridica, professionale o di altro genere.

Meritano una specifica protezione i dati personali che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali. Tra tali dati personali dovrebbero essere compresi anche i dati personali che rivelano l'origine razziale o etnica, essendo inteso che l'utilizzo dei termini «origine razziale» nel presente regolamento non implica l'accettazione da parte dell'Unione di teorie che tentano di dimostrare l'esistenza di razze umane distinte. Il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando saranno trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica. Tali dati personali non dovrebbero essere oggetto di trattamento, a meno che il trattamento non sia consentito nei casi specifici di cui al presente regolamento, tenendo conto del fatto che il diritto degli Stati membri può stabilire disposizioni specifiche sulla protezione dei dati per adeguare l'applicazione delle norme del presente regolamento ai fini della conformità a un obbligo legale o dell'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Oltre ai requisiti specifici per tale trattamento, dovrebbero applicarsi i principi generali e altre norme del presente regolamento, in particolare per quanto riguarda le condizioni per il trattamento lecito. È opportuno prevedere espressamente deroghe al divieto generale di trattare tali categorie particolari di dati personali, tra l'altro se l'interessato esprime un consenso esplicito o in relazione a esigenze specifiche, in particolare se il trattamento è eseguito nel corso di legittime attività di talune associazioni o fondazioni il cui scopo sia permettere l'esercizio delle libertà fondamentali.

I principi di trattamento corretto e trasparente implicano che l'interessato sia informato dell'esistenza del trattamento e delle sue finalità. Il titolare del trattamento dovrebbe fornire all'interessato eventuali ulteriori informazioni necessarie ad assicurare un trattamento corretto e trasparente, prendendo in considerazione le circostanze e del contesto specifici in cui i dati personali sono trattati. Inoltre l'interessato dovrebbe essere informato dell'esistenza di una profilazione e delle conseguenze della stessa. In caso di dati personali raccolti direttamente presso l'interessato, questi dovrebbe inoltre essere informato dell'eventuale obbligo di fornire i dati personali e delle conseguenze in cui incorre se si rifiuta di fornirli. Tali informazioni possono essere fornite in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone dovrebbero essere leggibili da dispositivo automatico.

Capitolo 3
Definizioni. Trattamento di dati. Cloud

Par. 1 - Definizioni

L'art. 4 del Regolamento europeo prescrive le seguenti definizioni:

1) «**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;
2) «**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;
3) «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
4) «**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
5) «**pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
6) «**archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
7) «**titolare del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
8) «**responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
9)«**destinatario**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati 4.5.2016 L. 119/33 Gazzetta ufficiale dell'Unione europea IT membri non

sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.

10) «**terzo**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

11) «**consenso dell'interessato**»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

12) «**violazione dei dati personali**»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

13) «**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

14) «**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

15) «**dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

16) «**stabilimento principale**»: a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale; b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

17) «**rappresentante**»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

18) «**impresa**»:la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) «**gruppo imprenditoriale**»:un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

20) «**norme vincolanti d'impresa**»:le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

21) «**autorità di controllo**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51; 4.5.2016 L 119/34 Gazzetta ufficiale dell'Unione europea IT
22) «**autorità di controllo interessata**»: un'autorità di controllo interessata dal trattamento di dati personali in quanto: a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure c) un reclamo è stato proposto a tale autorità di controllo;
23) «**trattamento transfrontaliero**»: a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;
24) «**obiezione pertinente e motivata**»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;
25) «**servizio della società dell'informazione**»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;
26) «**organizzazione internazionale**»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

Par. 2 - Descrizione del procedimento di trattamento dati

Il procedimento di trattamento dei dati personali è caratterizzato da tre attività:

1) **Input** – raccolta dati presso l'interessato o presso terzi o richiesta di comunicazione di dati personali a enti o persone giuridiche;
2) **Works** – ossia il complesso delle operazioni interne connesse al trattamento dei dati;
3) **Output** – fase della comunicazione o diffusione dei dati verso enti esterni.

La raccolta dei dati può essere effettuata o direttamente presso l'interessato o presso terzi, che conferiscono dati diversi dalla propria persona.
Secondo quanto previsto dall'art. 13 del Regolamento europeo [per i dati raccolti presso l'interessato] il trattamento può iniziare dopo l'ottenimento degli stessi da parte del titolare e il successivo art. 14 [per i dati non raccolti presso l'interessato], il trattamento può iniziare al momento della raccolta dei dati mentre l'interessato deve essere informato del trattamento entro 1 mese dall'ottenimento degli stessi.

La legge sulla *privacy* prevede due diversi regimi di legittimazione a seconda della natura del soggetto titolare del Trattamento:

a) se a procedere al Trattamento è un soggetto privato (cui sono equiparati gli enti pubblici economici), questo deve chiedere preliminarmente il consenso all'interessato, salvo i casi di esclusione espressamente previsti dall'art. 7 del Regolamento europeo.

b) se a procedere al Trattamento è un soggetto pubblico vige il principio di finalità istituzionale o **rilevante interesse pubblico** in forza del quale non necessita ottenere dal soggetto interessato un consenso preliminare al trattamento stesso. Il soggetto pubblico dovrà trattare i dati secondo i principi di necessità e pertinenza per l'assolvimento delle funzioni istituzionali.

Nella azione di **input** si dovrà verificare se la raccolta dei dati è pertinente, non eccedente e necessaria per lo svolgimento di funzioni istituzionali, nel rispetto dei limiti di legge o di regolamento.

1) Ogni documento cartaceo in ingresso ricevuto tramite posta tradizionale oppure ricevuto in busta chiusa consegnata a mano viene di norma consegnato chiuso al Dirigente Scolastico, che lo apre lo esamina e – nei casi di documenti con dati particolarmente riservati – lo protocolla personalmente nel registro di protocollo riservato e lo custodisce in apposito armadio ad accesso esclusivo normalmente chiuso a chiave. Per il trattamento della relativa pratica il Dirigente può portare a conoscenza altro soggetto da lui autorizzato che risponde ad un profilo di autorizzazioni in linea con la tipologia di dati oggetto di trattamento.

2) I documenti cartacei aperti direttamente presso i rispettivi Ufficio alunni o Ufficio personale vengono comunque consegnati al Dirigente scolastico. Fanno eccezione i documenti con dati neutri e documenti di routine), che vengono trattati direttamente dalle Segreterie.

3) I documenti ricevuti tramite posta elettronica sono scaricati da un soggetto autorizzato e smistati dalla piattaforma utilizzata per la dematerializzazione, all'ufficio di competenza.

In dottrina, con riferimento alle definizioni contenute nel Regolamento europeo, è ben evidenziato che nella definizione di trattamento è ricompressa una lunga serie di azioni potenzialmente lesivi, che possono essere suddivisi in quattro fasi:

f) fase *preliminare* di raccolta, di registrazione, di organizzazione e di strutturazione;

ff) fase di *elaborazione* che raggruppa la modificazione, l'adattamento, la selezione, l'estrazione, il raffronto o l'interconnessione, l'utilizzo, la limitazione e la pseudonomizzazione;

fff) fase di *circolazione e/o divulgazione* riguardante *la comunicazione* mediante trasmissione *e la diffusione* o qualsiasi altra forma di messa a disposizione*;*

ffff)fase *residuale* comprendente la conservazione, la cancellazione e la distruzione*.*

L'azione **works** è caratterizzata da due tipologie di operazioni che riguardano il trattamento interno;

- le operazioni statiche: registrazione, conservazione, organizzazione, cancellazione, la pseudonomizzazione e la distruzione;
- le operazioni dinamiche: elaborazione, modificazione, estrazione, selezione, uso, raffronto o interconnessione.

La differenza consiste nella progressiva trasformazione del dato.

Mentre le operazioni statiche non alterano il dato, quelle dinamiche, poiché presuppongono un intervento sulle informazioni originarie e quindi una trasformazione, danno vita ad informazioni via via di livello successivo (secondo livello, terzo livello ecc..) profondamente diverse da quelle originariamente raccolte.

I documenti contenenti dati sensibili vengono trattati dagli autorizzati in ambiente ad accesso selezionato.

L'azione di **output** prevede:

- **la comunicazione** che riguarda il far conoscere i dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
- **la diffusione** che riguarda il far conoscere i dati personali a soggetti indeterminati, diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

La differenza tra queste due operazioni è data dalla determinatezza o meno del soggetto destinatario delle informazioni. A tal fine la legge prevede:

a) l'interessato deve essere informato sulle categorie di soggetti ai quali i dati possono essere comunicati e sull'ambito di diffusione dei dati medesimi;
b) se i dati comuni sono trattati da un soggetto privato o da un ente pubblico economico per poter essere trasferiti da un soggetto terzo occorre il consenso dell'interessato, salvo i casi di esclusione previsti dalla legge;
c) se i dati comuni sono trattati da un soggetto pubblico per essere comunicati o diffusi a soggetti destinatari privati occorre una previsione specifica di legge o di regolamento;
d) se i dati sono di natura sensibile per poter essere trasferiti a terzi non previsti istituzionalmente occorre il consenso scritto dell'interessato quando il titolare sia un soggetto privato, una espressa autorizzazione di legge, nel caso di soggetti pubblici.

Tipologia e modalità del trattamento dei dati

A) – Tipologia del trattamento dei dati.

I dati personali verranno trattati da questa Istituzione Scolastica in modalità cartacea e automatizzata.
I dati personali **comuni** relativi a persone fisiche e giuridiche sono quelli che nella pratica attengono a riferimenti diretti od indiretti quali ad esempio il nome, il cognome, la data di nascita, la denominazione sociale, il codice fiscale, la partita iva, le immagini/fotografie, le pubblicazioni, le relazioni o report, le attestazioni, etc. Sono altresì considerati dati personali quelli relativi al traffico telefonico in generale, alle e-mail e ai c.d. *file di log,* cioè quelle informazioni computerizzate attraverso le quali è possibile sapere quando, con chi, e per quanto tempo ci si è collegati in rete.
I dati **sensibili** sono quelli che il Codice definisce come dati idonei a rilevare, anche indirettamente, l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale.
Nella tipologia di dati sensibili sono da considerarsi ricompresi anche le semplici indicazioni utilizzate spesso nell'ambito della gestione del personale, come ad esempio "iscritto al sindacato", "malato", "convalescenza", "aspettativa per malattia", fruizione di "permessi per visite mediche o per attività sindacali o politiche, "inidoneità" (psico-fisica, attitudinale,…)
I dati **giudiziari** sono le informazioni rinvenibili nei procedimenti emanati dal giudice penale per i quali è prevista la registrazione del casellario giudiziario, nonché i dati idonei a rilevare la qualità di imputato o di indagato e le sanzioni amministratiti dipendenti da reato. Si citano a titolo esemplificativo le sentenze di

condanna, i provvedimenti penali divenuti irrevocabili, i provvedimenti definitivi che riguardano misure di sorveglianza.
Tutti i dati personali trattati da questa Istituzione Scolastica sono necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi o richiesti ai fini fiscali, previdenziali o dati di natura bancaria.
I dati personali sono tutti relativi ad alunni, genitori, personale dipendente docente e non, A.T.A., collaboratori esterni, fornitori e sono prevalentemente raccolti presso gli interessati, ma anche presso terzi. I dati personali comuni, sensibili e giudiziari, trattati dai docenti riguardano esclusivamente gli alunni ed eventualmente anche quelli dei genitori. Quelli trattati dal personale di segreteria riguardano sia gli alunni che tutto il personale della scuola. Quelli trattati dal Dirigente scolastico riguardano tutti i dati che affluiscono nell'Istituto scolastico.

I dati sono quelli che ricadono nella banca dati **inerente ai trattamenti dell'area personale/alunni/contabilità,** di seguito specificate al fine di procedere al trattamento nel rispetto dei principi generali fissati dal regolamento europeo e delle procedure riportate nel Disciplinare interno, del quale la presente lettera è parte integrante, adottato da codesto Istituto comprensivo.

In allegato, posto alla fine del presente capitolo, si trovano elencate in tabella le Banche dati denominate "*Banche dati inerenti ai trattamenti dell'area personale/dell'area alunni/dell'area contabilità*" nella quale sono dettagliatamente descritte le autorizzazioni che ogni trattamento può effettuare, le categorie degli interessati, la categoria dei destinatari, la durata e gli archivi di conservazione, gli operatori autorizzati al trattamento, la categoria dei dati e di questi, per ultimo la loro natura, le modalità della raccolta e, infine, se la protezione del dato si origina fin dalla progettazione [art. 25 comma 2 del regolamento europeo] o avviene per impostazione predefinita [all'art. 25 com. 1 del regolamento europeo].

A] Banca dati inerente ai trattamenti dell'area personale

Autorizzazioni: Raccolta, registrazione, modifica, raffronto, organizzazione, conservazione, uso, conservazione; comunicazione; limitazione, interconnessione; consultazione.

B] Banca dati inerente ai trattamenti dell'area alunni

Autorizzazioni: Raccolta, registrazione, modifica, raffronto, organizzazione, conservazione, uso, conservazione; comunicazione; limitazione, interconnessione; consultazione.

C] Banca dati inerente ai trattamenti dell'area contabile

Autorizzazioni: Raccolta, registrazione, modifica, raffronto, organizzazione, conservazione, uso, conservazione; comunicazione; limitazione, interconnessione; consultazione.

Interessante è l'esame dello schema pubblicato dal Garante da cui si evince quale comportamento occorre assumere nella gestione del dato personale di natura sensibile. Tale schema è riportato, per comodità di spazio, alla pag. 28

B) - <u>Modalità del trattamento dei dati personali</u>

- *Dati personali trattati dal personale docente.* Questi dati trattati dai docenti, titolari e/o supplenti anche temporanei, sono contenuti in banche dati su supporto cartaceo ed anche elettronico che si possono classificare in:
    1. banche dati in cui hanno accesso più docenti. Queste sono:
        - il registro di classe;
        - il registro dei verbali del consiglio di classe di interclasse e intersezione;
        - la documentazione relativa alla programmazione didattica;
        - i documenti di valutazione;
        - i documenti dello stato di disabilità;
        - i certificati medici degli allievi e dei dipendenti;
        - la corrispondenza con le famiglie;
        - le giustificazione delle assenze degli alunni.
    2. banche dati in cui ha accesso il singolo docente. Queste sono:
        - il registro personale;
        - gli elaborati.

E' opportuno considerare i dati trattati dai docenti nel loro insieme come dati di natura sensibile. Il trattamento dei dati da parte dei docenti (tenuta dei registri, modalità di compilazione dei documenti di valutazione, verbalizzazioni, etc..) è definito puntualmente da norme di legge o da regolamenti.

- *Dati trattati dal personale di segreteria* – Le banche dati su supporto cartaceo e/o informatizzato, contenenti dati personali, cui ha accesso il personale di segreteria, raggruppati in insiemi omogenei, sono:
    - i fascicoli relativi al personale della scuola, docente non docente e collaboratori esterni;
    - i fascicoli degli alunni e degli ex alunni;
    - l'anagrafe dei fornitori;
    - i contratti;
    - la documentazione finanziaria e contabile;
    - la documentazione didattica trattata dai docenti per la conservazione;
    - i dati riguardanti gli infortuni degli alunni e dei dipendenti.

- *I dati trattati dal Dirigente Scolastico* – Le banche dati di stretta pertinenza del Dirigente sono:
    - i fascicoli del personale direttivo-docente, Amministrativo e dei Collaboratori scolastici;
    - i verbali delle assemblee degli Organi Collegiali;
    - il protocollo riservato;
    - i fascicoli del personale in prova.

Trattamento di categorie particolari di dati personali

Trattamento dei dati personali relativi a dati di natura sensibile

1. È vietato trattare dati personali [art. 9 del Regolamento] che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati

genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi:
a), b), c), e d) … *omissis*….
e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3;
i) …… *omissis* …….
j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.
3. I dati personali di cui al paragrafo 1 possono essere trattati per le finalità di cui al paragrafo 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti.
4. Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute.

Trattamento dei dati personali relativi a condanne penali e reati

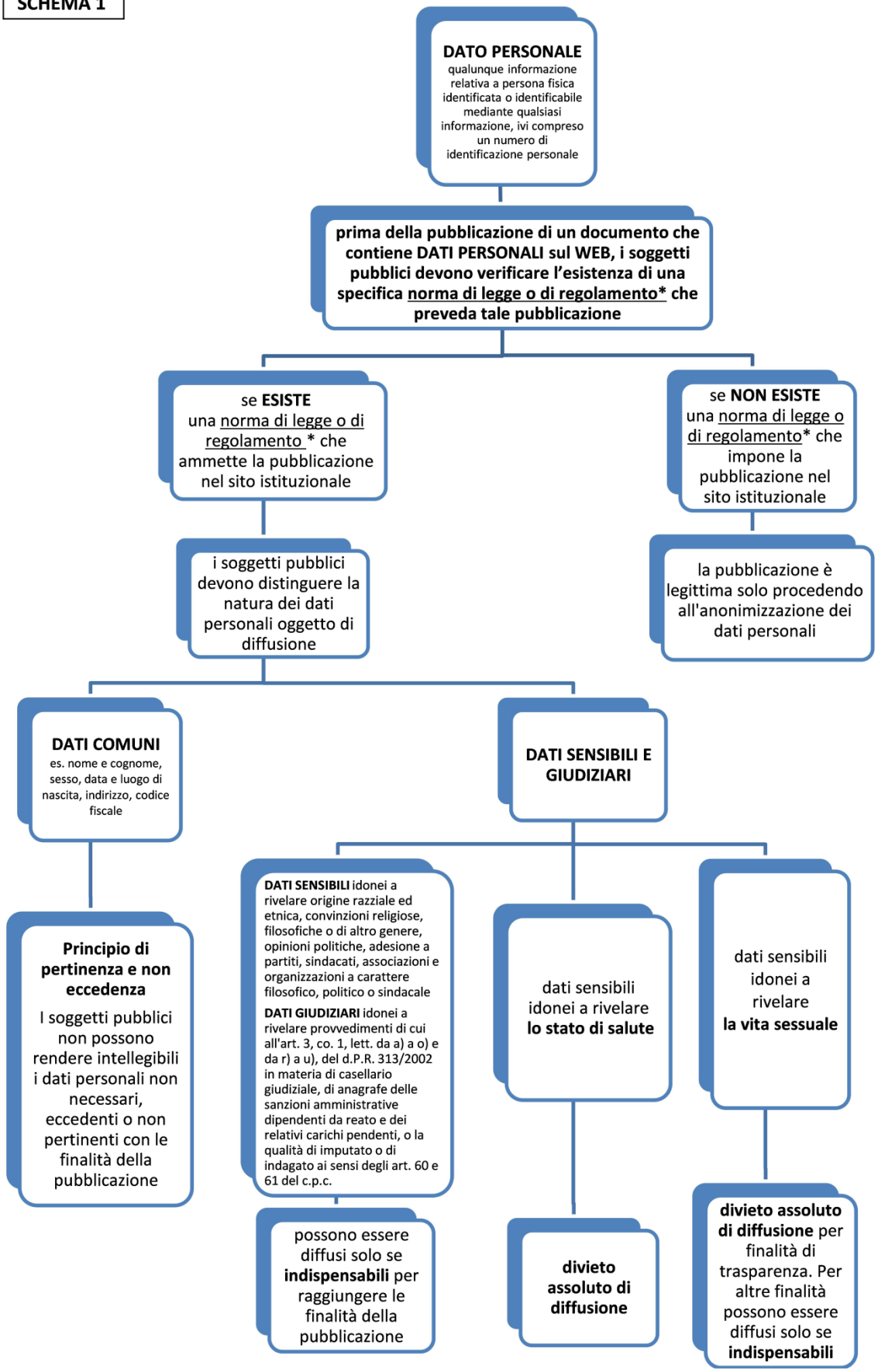
Il trattamento dei dati personali [art. 10 del Regolamento] relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

Trattamento che non richiede l'identificazione

Se le finalità per cui un titolare del trattamento tratta i dati personali non richiedono o non richiedono più l'identificazione dell'interessato, il titolare del trattamento non è obbligato a conservare, acquisire o trattare ulteriori informazioni per identificare l'interessato al solo fine di rispettare il regolamento europeo.

Qualora però il titolare del trattamento possa dimostrare di non essere in grado di identificare l'interessato, ne informa l'interessato, se possibile. In questi casi, gli articoli da 15 a 20 del Regolamento non si applicano tranne quando l'interessato, al fine di esercitare i diritti di cui ai suddetti articoli, fornisce ulteriori informazioni che ne consentano l'identificazione.

SCHEMA 1



* N.B. Si precisa che la diffusione di dati comuni è ammessa solo se prevista da una norma di legge o di regolamento, mentre la diffusione di dati sensibili o giudiziari è ammessa se prevista espressamente solo da una norma di legge.

Capitolo 4
Ripartizione ruoli e compiti ai soggetti che effettuano il trattamento dei dati personali

Par. 1 - Ripartizione ruoli e compiti ai soggetti che effettuano il trattamento dei dati personali

Il processo della sicurezza richiede che, prima ancora di pensare all'adozione delle concrete misure, vengano definite una serie di norme e procedure, miranti a regolamentare gli aspetti organizzativi e tecnici del processo medesimo, con riferimento:

- alla definizione dei ruoli, compiti e responsabilità per la gestione di tutte le fasi del trattamento dei dati personali;
- all'adozione di specifiche procedure, che vadano a completare e rafforzare le contromisure tecnologiche adottate.

La prima e la più generalizzata misura di sicurezza è prettamente di carattere organizzativo. Difatti, di seguito vengono riportate ruoli e mansioni dei soggetti che effettuano il trattamento dei dati personali.

a) Titolare del trattamento

L'Art. 4, comma 1. lettera f) del Regolamento definisce <<*titolare*>>,*"la persona fisica o giuridica, la autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione e degli Stati membri, il titolare del trattamento o i suoi criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri ".*

Al Titolare del trattamento, inteso **come centro decisionale** oppure **come centro di imputazione giuridica,** spetta l'onere di individuare e autorizzare uno o più Responsabili del Trattamento, qualora ciò fosse dettato da reali opportunità organizzative.

Tra i compiti non delegabili assegnati al Titolare è prevista la vigilanza sul rispetto da parte dei Responsabili degli autorizzati loro assegnati, nonché sulla diligente osservanza, cioè sulla dovuta diligenza, delle vigenti disposizioni in materia di trattamento, con particolare riguardo alle misure di sicurezza da adottare.

Il regolamento, pertanto:
- disciplina la **contitolarità del trattamento** *(art. 26)* e impone ai titolari di definire specificamente (con un atto giuridicamente valido ai sensi del diritto nazionale) il rispettivo ambito di responsabilità e i compiti **con particolare riguardo all'esercizio dei diritti degli interessati**, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari che operano congiuntamente.

- fissa più nei dettagli *(rispetto all'art. 29 del Codice)* le **caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento** attribuendogli specifici compiti: deve trattarsi, infatti, di un **contratto** (o altro atto giuridico conforme al diritto nazionale) e deve **disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell'art. 28** al fine di dimostrare che il responsabile fornisce "garanzie sufficienti" – quali, in particolare, la natura, durata e finalità del trattamento o dei trattamenti assegnati, le categorie di dati oggetto di trattamento, le misure tecniche e organizzative

adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel regolamento.

- prevede **obblighi specifici in capo ai responsabili del trattamento**, in quanto distinti da quelli pertinenti ai rispettivi titolari. Ciò riguarda, in particolare, la tenuta del **registro dei trattamenti** svolti *(ex art. 30, paragrafo 2)*; l'adozione di idonee **misure tecniche e organizzative per garantire la sicurezza** dei trattamenti *(ex art. 32 regolamento)*;

- **designa il Responsabile della protezione di dati (RPD)**, nei casi previsti dal regolamento o dal diritto nazionale *(si veda art. 37 del regolamento)*.

Responsabilità del titolare del trattamento. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento deve mettere in atto tutte le misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare [onere della prova], che il trattamento è effettuato conformemente al regolamento. Dette misure saranno riesaminate e aggiornate qualora necessario. Se ciò è proporzionato rispetto alle attività di trattamento, le misure adottate includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Il Titolare dell'Istituto Comprensivo è rappresentato dal Dirigente Scolastico pro-tempore nella persona del Prof. Salvatore Lo Presti
Il sua assenza è supplito, in tutte le sue funzioni, dalla prof.ssa Giuseppa Nocera, in qualità di collaboratore vicario

Nomina e mansioni degli operatori del trattamento:

b) Per le pubbliche amministrazioni la nomina del Responsabile della Protezione dei Dati è obbligatoria, ai sensi dell'art. 37 dl Regolamento. In base a tale articolo l'RPD "*è designato in funzione 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 cui all'articolo 39*".
E' previsto che il livello necessario di conoscenza specialistica dovrebbe essere determinato in

base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali oggetto di trattamento.
Il livello di conoscenza specialistica richiesto dal regolamento non trova una definizione definitiva precisa. Ne consegue la necessità di una attenzione nella scelta del RPD, e si deve tenere adeguatamente conto delle problematiche in materia di protezione dei dati con cui il titolare deve confrontarsi.

Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

Il titolare e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.

Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal regolamento.

Il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri.

Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.

I compiti del responsabile della protezione dei dati si possono sintetizzare in:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) sorvegliare l'osservanza del 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;

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
d) cooperare con l'autorità di controllo; e
e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Nell'eseguire i propri compiti il responsabile della protezione dei dati considera i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

c) Nomina dei Responsabili del trattamento

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.

In ottemperanza all'articolo 28 del regolamento, il titolare del trattamento può nominare uno o più responsabili, intesi come **centri organizzativi,** del trattamento con contratto o altro atto giuridico il quale deve procedere che il responsabile provveda a rispettare integralmente tutte le prescrizioni previste dal citato art. 28
Ai responsabili è conferita possibilità di nominare uno o più persone "autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare oppure del responsabile" e istruirli adeguatamente per renderle idonee a svolgere le mansioni assegnate.

d) Nomina degli Autorizzati al trattamento sotto l'autorità diretta del Responsabile.

Qualora la gestione delle banche dati richieda l'intervento operativo di altri soggetti, il titolare o il responsabile possono nominare uno o più autorizzati al trattamento con apposita comunicazione scritta. Sempre per iscritto devono essere specificati i compiti loro assegnati. La lettera di autorizzazione deve essere sottoscritta dal soggetto interessato, come atto recettizio. Loro compito è quello di svolgere gli incarichi assegnati, dettagliatamente specificati nella lettera di incarico, sempre nel pieno rispetto del regolamento. In caso di incidenti o di conoscenza di circostanze che possano far venir meno i requisiti minimi di sicurezza, gli autorizzati dovranno comunicare tempestivamente tale circostanza al responsabile del trattamento o, in mancanza, al titolare.
Se non diversamente previsto nella lettera di incarico, gli incaricati del trattamento vengono nominati a tempo indeterminato e decadono per dimissioni o per revoca.
La distribuzione delle autorizzazioni, in relazione **all'area amministrativa** è quella strettamente connessa all'ordine di servizio definito ad inizio di anno scolastico con nota comunicata a tutti gli interessati.
Il **collaboratore scolastico** qualora tratti anche saltuariamente dati personali, dovrà essere autorizzato con specifico atto in relazione alla tipologia dei dati trattati.
Il responsabile del trattamento dei dati ha nominato le seguenti persone le cui lettere d'incarico, in allegato**,** fanno parte integrante del presente Disciplinare Interno:

N°	NOMINATIVO
1	Bastillo Vita
2	Bumbolo Luciano
3	Caracciolo Vincenzo
4	Circo Giuseppe
5	Consiglio M.Carmela
6	Cullaro Angelo
7	Ciucio Stefano
8	Cutrò Carmela
9	Giacchino Giuseppe
10	Graceffa Carmelo
11	Incannella Gianni
12	Lazzara Mirella
13	Lucchese Raimondo
14	Mirti Antonino
15	Piazza Antonino
16	Picone Salvatore
17	Valenti Giovanna
18	Zimbardo Carmelo

Per quanto concerne i **docenti** sono da considerare, per la propria sfera di competenza, autorizzati al trattamento e come tale devono essere nominati mediante specifico atto scritto che elenchi puntualmente le categorie dei dati cui può avere accesso, la tipologie degli stessi dati e vincoli specifici applicabili alle varie tipologie di dati e le istruzioni in merito ai soggetti cui i dati possono essere comunicati o diffusi.
Chi incarica i docenti al trattamento dei dati è direttamente il Dirigente scolastico, Prof. Salvatore Lo Presti, le cui lettere di autorizzazione, in allegato, fanno parte integrante del presente Disciplinare.
I docenti e i componenti degli Organismi collegiali autorizzati sono quelli che si evidenziano dall'organico della scuola o da decreti emessi dal Dirigente scolastico
Infine, si precisa che si effettuano le relative autorizzazioni anche per il personale **supplente temporaneo, docente e ATA** in relazione al proprio profilo professionale di appartenenza.

e) Nomina dell'Amministratore di sistema

Il Responsabile del trattamento o il Titolare conferiscono a uno o più autorizzati le mansioni di gestione delle soluzioni informatiche sia hardware che software adottate per la gestione e la tenuta in sicurezza delle banche dati. L'autorizzazione avviene per iscritto e verranno dettagliati i compiti assegnati, compreso quello di approntare i mezzi necessari per effettuare le copie di sicurezza dei dati e il loro ripristino in caso di accidentale distruzione. L'Amministratore di sistema ha anche l'onere di valutare periodicamente lo stato di efficienza delle soluzioni informatiche adottate e provvedere alla loro modifica o integrazione in base all'esperienza acquisita e al progresso tecnologico.
Qualora non fosse già stato autorizzato un altro soggetto, l'Amministratore di sistema può essere nominato come custode delle credenziali di autenticazione (codici identificativi, User ID, Password, ecc.)

assegnate ad ogni soggetto autorizzato. L'amministratore, nello svolgere questo incarico, si atterrà a quanto previsto nel presente Disciplinare per il custode delle credenziali di autenticazione.
Il profilo dell'Amministratore di sistema ed assimilabili è obbligatorio per l'Istituto scolastico e la nomina dovrà rispondere ai requisiti evidenziati nel provvedimento del Garante del 27.11.2008
Il titolare dell'Istituto non ha designato come amministratore di sistema alcun profilo

f) Nomina del custode delle credenziali di autenticazione

Il Responsabile, di concerto con il titolare, può nominare uno o più custodi delle credenziali di autenticazione per l'accesso ai sistemi di elaborazione dati. L'autorizzazione deve avvenire per iscritto e il relativo contratto deve essere conservato in un luogo sicuro da parte del soggetto che conferisce l'autorizzazione.
Il *Custode delle credenziali* prende visione di tutte le credenziali di accesso da custodire. Le credenziali non dovranno essere divulgate e dovranno essere custodite in luogo sicuro. Spetta al custode definire le modalità di utilizzo delle credenziali di autenticazione in caso di impedimenti o prolungata assenza dell'incaricato alle quali sono state assegnate.
In mancanza di un custode delle credenziali di autenticazione, le mansioni sopra riportate saranno svolte dall'Amministratore del sistema o, in mancanza ancora, dal soggetto che può conferire l'incarico (Responsabile o Titolare del trattamento).
Il Titolare dell'Istituto Comprensivo non ha nominato alcun profilo come custode delle credenziali di autenticazione per cui tale incarico ricade direttamente sul Titolare dei dati.

g) Nomina del custode dell'archivio storico ad accesso controllato.

Il responsabile, di concerto con il titolare, designa un custode dell'archivio ad accesso controllato a cui sono consegnate le chiavi dell'archivio (la scuola possiede locali adibiti ad archivio dove vengono conservati i documenti storici contenenti anche dati sensibili e giudiziari). L'autorizzazione è assegnata per iscritto e la lettera controfirmata dall'interessato, per presa visione, è conservata in luogo sicuro da parte del soggetto che conferisce l'incarico.
Sono nominati custodi dell'archivio ad accesso controllato gli Assistenti Amministrativi
E' compito del custode dell'archivio ad accesso controllato tenere sempre chiuso a chiave tale locale e consegnare la stessa alle persone autorizzate ad accedervi.
Occorre annotare nell'apposito registro degli accessi all'archivio tutti coloro che vi accedono al di fuori dell'orario di servizio.
La lettera di autorizzazione deve riportare le caratteristiche della nomina quali il periodo di tempo della nomina e le condizioni di decadenza della stessa.

h) Gestione dell'impianto di videoregistrazione.

Al momento della stesura del presente Disciplinare l'Istituto comprnsivo non dispone di alcun sistema di videoregistrazione.
In ipotesi in cui l'Istituzione scolastica, ricorrendo i presupposti di legge per l'attivazione dei relativi impianti, sarà tenuta alle osservanza scrupolosa dell'Art. 134 del Codice e del Provvedimento Generale emanato dal Garante il 29/04/2004 recante norme sulla videosorveglianza
Saranno rispettati i seguenti principi generali così come prescritte dalla normativa:

1. **di necessità.** Poiché l'installazione di un sistema di videosorveglianza comporta l'introduzione di un vincolo, di una limitazione o di un condizionamento per il cittadino, va applicato il principio di necessità e quindi va escluso ogni uso superfluo ed evitati eccessi e ridondanze;
2. **di liceità**. E' previsto dal Codice che i dati personali devono essere trattati con liceità e secondo correttezza, intendendo quest'ultima come "buona fede". Condizione essenziale per la liceità è che vengano rispettate tutte le disposizioni inerenti la protezione dei dati compresi non solo nel Codice della Privacy, ma anche in tutte le disposizioni di legge.
   Appare infine evidente il rispetto del codice penale che vieta le intercettazioni di comunicazioni e conversazioni;
3. **di finalità**. Gli scopi perseguiti devono essere determinati, espliciti e legittimi. Ciò comporta che il titolare possa perseguire solo finalità di sua pertinenza. Una finalità legittima è che il sistema di videosorveglianza servono come misura complementare volta a migliorare la sicurezza all'interno o all'esterno dove si svolgono attività, anche, di servizi.
   In ogni caso possono essere perseguite solo finalità determinate e rese trasparenti e conoscibili attraverso adeguate comunicazioni e/o cartelli di avvertimento al pubblico. Le finalità così individuate devono essere correttamente riportate nell'informativa;
4. **di proporzionalità**. La videosorveglianza è lecita solo se è rispettato il principio di proporzionalità, sia nella scelta se e quali apparecchiature di ripresa installare, sia nelle varie fasi del trattamento. Occorre, pertanto, limitare rigorosamente la durata comunque temporanea dell'eventuale conservazione, l'eventuale duplicazione delle immagini registrate, la creazione di una banca dati delle immagini registrate;
5. **di pertinenza e non eccedenza**. Occorre raccogliere solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo di visuale delle riprese, evitando immagini dettagliate, ingrandite o dettagli non rilevanti e stabilendo in modo conseguente la localizzazione delle telecamere e le modalità di ripresa.

Tra gli **adempienti** da seguire si fornirà agli interessati idonea informativa ai sensi dell'art. 13 del Regolamento attraverso un cartello di contenuto anche semplificato di informativa "adeguata" con segnaletiche visibili, sintetiche e di immediata interpretazione, posizionate opportunamente. In luoghi diversi dalle aree esterne il cartello si integrerà con almeno un avviso circostanziato che riporti gli elementi base.

Capitolo 5
Sicurezza informatica

Par. 1 – Descrizione dei modelli FNSC e ABSC

Nel recente passato si è assistito ad una rapida evoluzione della minaccia cibernetica ed in particolare per quella incombente sulla pubblica amministrazione, che è divenuta un bersaglio specifico per alcune tipologie di attaccanti particolarmente pericolosi.
Se da un lato la pubblica amministrazione continua ad essere oggetto di attacchi dimostrativi, provenienti da soggetti spinti da motivazioni politiche ed ideologiche, sono divenuti importanti e pericolose le attività condotte da gruppi organizzati, non solo di stampo propriamente criminale.

I pericoli legati a questo genere di minaccia sono particolarmente gravi per due ordini di motivi.
Il primo è la quantità di risorse che gli attaccanti possono mettere in campo, che si riflette sulla sofisticazione delle strategie e degli strumenti utilizzati. Il secondo è che il primo obiettivo perseguito è il mascheramento dell'attività, in modo tale che questa possa procedere senza destare sospetti. La combinazione di questi due fattori fa sì che le *Misure Minime di Sicurezza ICT per le pubbliche amministrazioni* emesse in attuazione della Direttiva del Presidente del Consiglio dei Ministri nel 2015, pur tenendo nella massima considerazione le difese tradizionali, quali gli antivirus e la difesa perimetrale, pongono l'accento sulle misure rivolte ad assicurare che le attività degli utenti rimangano sempre all'interno dei limiti previsti. Infatti elemento comune e caratteristico degli attacchi più pericolosi è l'assunzione del controllo remoto della macchina attraverso una scalata ai privilegi.

Nei fatti le misure preventive, destinate ad impedire il successo dell'attacco, devono essere affiancate da efficaci strumenti di rilevazione, in grado di abbreviare i tempi, oggi pericolosamente lunghi, che intercorrono dal momento in cui l'attacco primario è avvenuto e quello in cui le conseguenze vengono scoperte. Oltre tutto una lunga latenza della compromissione rende estremamente complessa, per la mancanza di log, modifiche di configurazione e anche avvicendamenti del personale, l'individuazione dell'attacco primario, impedendo l'attivazione di strumenti efficaci di prevenzione che possano sicuramente impedire il ripetersi degli eventi.

In questo quadro diviene fondamentale la rilevazione delle anomalie operative e ciò rende conto dell'importanza data agli inventari, che costituiscono classi di misure imprescindibili, nonché la protezione della configurazione, altrettanto importante che segue la classe operativa delle misure.

Non è possibile trascurare attività di rilevante importanza quali:

- la priorità alla duplice rilevanza dell'analisi delle vulnerabilità. In primo luogo le vulnerabilità sono l'elemento essenziale per la scalata ai privilegi che è condizione determinante per il successo dell'attacco; pertanto la loro eliminazione è la misura di prevenzione più efficace. Secondariamente si deve considerare che l'analisi dei sistemi è il momento in cui è più facile rilevare le alterazioni eventualmente intervenute e rilevare un attacco in corso;
- la gestione degli utenti, in particolare gli amministratori. La sua rilevanza è dimostrata dalla sensibilizzazione sempre maggiore che la pubblica amministrazione ha sentito in questo ultimo periodo;

- alcuni attacchi complessi prevedono in qualche fase l'installazione di codice malevolo e la sua individuazione può impedirne il successo o rilevarne la presenza;
- Le copie di sicurezza sono, alla fine dei conti, l'unico strumento che garantisce il ripristino dopo un incidente;
- E per ultima classe, ma non meno importante, la protezione dei dati personali che costituendo il motivo principale del presente documento deve la sua presenza alla considerazione che l'obiettivo principale degli attacchi più gravi è la sottrazione di informazioni.

Questa istituzione scolastica ha analizzato i due modelli ABSC e Framework le cui caratteristiche fondamentali sono presentate analiticamente di seguito.

A) Il modello ABSC: *AgID Basic Security Control*

La Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015, in considerazione *dell'esigenza di consolidare un sistema di reazione efficiente, che raccordi le capacità di risposta delle singole Amministrazioni, con l'obiettivo di assicurare la resilienza dell'infrastruttura informatica nazionale, a fronte di eventi quali incidenti o azioni ostili che possono compromettere il funzionamento dei sistemi e degli assetti fisici controllati dagli stessi*, visto anche l'inasprirsi del quadro generale con un preoccupante aumento degli eventi cibernetici a carico della Pubblica Amministrazione, sollecita *tutte le Amministrazioni e gli Organi chiamati ad intervenire nell'ambito degli assetti nazionali di reazione ad eventi cibernetici* a *dotarsi, secondo una tempistica definita e comunque nel più breve tempo possibile, di standard minimi di prevenzione e reazione ad eventi cibernetici*. A fine di agevolare tale processo l'Agenzia per l'Italia Digitale è stata impegnata a *rendere prontamente disponibili indicatori degli standard di riferimento, in linea con quelli posseduti dai maggiori partner del nostro Paese e dalle organizzazioni internazionali di cui l'Italia è parte*.

Il documento che contiene le Misure minime di sicurezza ICT per le Pubbliche Amministrazioni e che costituiscono parte integrante del più ampio disegno delle regole tecniche per la sicurezza informatica della pubblica amministrazione vengono emanate in forma autonoma, in attuazione della Direttiva già citata, come anticipazione urgente della regolamentazione in corso di emanazione, al fine di fornire sia un riferimento utile a stabilire se il livello di protezione offerto da un'infrastruttura risponde alle esigenze operative, individuando anche gli interventi idonei per il suo adeguamento, che un riferimento normativo e tempestivo alle pubbliche amministrazioni e consentire, così, di intraprendere un percorso di verifica ed adeguamento.
Il modello ammette l'esistenza di 8 classi le quali pongono l'accento sopra gli aspetti di prevenzione piuttosto che su quelli di risposta e ripristino (come propone il modello FNSC).

1- Inventario dei dispositivi autorizzati e non autorizzati.
2- Inventario dei software autorizzati e non autorizzati.
3- Proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server.
4- Valutazione e correzione continua della vulnerabilità.
5- Uso appropriato dei privilegi dell'amministratore.
6- Difese contro i malware.
7- Copie di sicurezza.
8- Protezione dei dati personali.

Tale modello propone tre livelli di sicurezza. Il primo **"Minimo"** specifica il livello sotto il quale nessuna amministrazione può scendere; i controlli in essa indicati debbono riguardarsi come obbligatori. Il secondo, lo **"Standard"** può essere assunto come base di riferimento nella maggior parte dei casi, mentre il terzo l'**"Alto"** può riguardarsi come un obiettivo a cui tendere.
Questa istituzione scolastica ha deciso di conformarsi al livello **Minimo** del modello ABSC avendo cura di pervenire al successivo secondo livello allorquando avrà verificato che la buona prassi avrà condotto la sicurezza informatica della scuola ad un ragionevole apprezzamento.

B) Il modello FNSC [Framework Nazionale di Sicurezza Cibernetica presentato dal CIS Sapienza nel febbraio 2016].

Il sistema economico e sociale dei paesi avanzati è diventato fortemente dipendente dal cyberspace, quello insieme di reti e sistemi informativi con i quali vengono erogati servizi indispensabili a cittadini, da parte degli enti governativi, delle infrastrutture critiche, delle imprese e della pubblica amministrazione.

I sistemi informativi sono divenuti elementi chiave nella gestione di infrastrutture fisiche come reti elettriche, sistemi industriali, sistemi di trasporto, ecc. Tuttavia il cyberspace e le sue componenti essenziali sono esposti a numerosi rischi. In primis, trattandosi di sistemi complessi e in rapida evoluzione, vi è una costante presenza di vulnerabilità. Nonostante gli sforzi, siccome non vi è oggi possibilità di disporre di sistemi non vulnerabili, anche a causa della moltitudine di attacchi di diverso tipo, disponibili nel mercato nero, occorre tenere sempre in considerazione eventuali minacce.

Una o più di queste vulnerabilità possono essere sfruttate da un attaccante per entrare illecitamente nei sistemi informativi di una organizzazione permettendo quindi all'attaccante di leggere, trafugare o cancellare informazioni critiche fino a prendere il controllo dell'asset informatico o degli asset fisici. Queste vulnerabilità, insieme al fatto che la consapevolezza di questa situazione non è ancora molto elevata a tutti i livelli della società, fanno si che il rischio cyber diventi molto rilevante per una organizzazione, al pari di quello finanziario e reputazionale.

Gli attacchi informatici, cresciuti negli ultimi anni in modo esponenziale per complessità e risorse utilizzate, non possono essere fermati dalle singole organizzazioni, ma hanno bisogno di una risposta dal sistema paese, poiché tendono a diminuirne la prosperità economica e l'indipendenza.
Il rischio cyber non può essere annullato ma è importante che una nazione sviluppata si doti di una serie di strumenti e metodologie per migliorare la consapevolezza, affrontare in modo strutturato la risposta e supportare le organizzazioni, gli enti e le organizzazioni pubbliche e private, residenti sul proprio territorio, per la riduzione del rischio e la mitigazione degli effetti di eventuali, possibili incidenti di sicurezza.

In questo ambito emerge il tema della responsabilità che può incombere sulle organizzazioni, pubbliche o private, e sugli individui dotati di poteri rappresentativi e direzionali, per la violazione di dovere di diligenza, prudenza e perizia nella tutela delle posizioni di garanzia che l'ordinamento attribuisce ai singoli e alle persone giuridiche. L'adesione al Framework, rappresentativo delle pratiche generalmente riconosciute e internazionalmente validate, permette una più agevole dimostrazione della applicazione della dovuta diligenza, riferendosi a razionali, oggettivi e misurabili, in applicazione del principio di dovere di diligenza.

Si è adottato un Framework Nazionale di cyber security il cui scopo è quello di offrire alla scuola un approccio volontario e omogeneo per affrontare la cyber security al fine di ridurre il rischio legato alla minaccia cyber. L'approccio di questo Framework è intimamente legato a una analisi del rischio e non a standard tecnologici.

Il Framework, presentato dal CIS Sapienza nel febbraio 2017, di cyber security del NIST (*National Institute of Standards and Tecnology*), orientato alle infrastrutture critiche per cercare una armonizzazione internazionale, è specializzato sulla realtà produttiva Italiana, fatta in particolare di piccole-medie imprese e pubbliche amministrazioni.

La cyber security è quella pratica che consente a una entità (organizzazione, cittadino, ente, nazione ecc.) la protezione dei propri asset fisici e la confindezialità, integrità e disponibilità delle proprie informazioni dalle minacce che arrivano dal cyber space.
A sua volta, il cyber space viene definito come il complesso ecosistema risultante dall'interazione di persone, software e servizi su Internet per mezzo di tecnologie, dispositivi e reti ad esso connesse

Il modello **FNSC** (*Framework Nazionale di Sicurezza Cibernetica*) del NIST propone un quadro d'insieme altamente flessibile diretto principalmente alle infrastrutture critiche; si è evoluto nella direzione delle caratteristiche del sistema socio-economico del nostro Paese ottenendo un Framework settoriale che può essere contestualizzato su settori produttivi specifici o su tipologie di aziende o enti pubblici con determinate caratteristiche.

Nel Framework Nazionale sono presenti tre concetti importanti:

I livelli di priorità. I livelli di priorità definiscono qual è la priorità con cui si deve affrontare ogni singola Subcategory del Framework. Da notare che ogni ente è libero di contestualizzare i propri livelli di priorità in base al tipo di attività, alla dimensione, al suo profilo di rischio.
I livelli di maturità. I livelli di maturità definiscono le diverse modalità con cui si può implementare ogni singola Subcategory del Framework. Il livello di maturità deve esser valutato attentamente dal singolo ente in base alla propria attività e alla sua dimensione nonché al suo profilo di rischio. Tipicamente livelli di maturità maggiori richiedono sforzi maggiore, sia dal punto di vista economico che di gestione. Per alcune Subcategory non è possibile definire livelli di maturità.
Contestualizzazione del Framework. Creare una contestualizzazione del Framework (per un settore produttivo, per società di servizi o per enti pubblici), significa selezionare le Function, le Category e Subcategory del Framework pertinenti, specificandone livelli di priorità e di maturità adatti al contesto di applicazione. Questa istituzione scolastica ha contestualizzato il Framework nazionale nel rispetto della protezione dei dati personali (Regolamento europeo e Codice privacy).

Negli ultimi tempi l'opinione pubblica è stata esposta a numerosi casi eclatanti di attacchi cyber, alcuni anche con effetti importanti. In alcuni casi si è trattato di attacchi da parte di attori collegabili a governi come, ad esempio, quello a danno di Sony Pictures; in altri casi si è trattato dell'utilizzo della dimensione cyber per attività e attacchi misti (terrorismo, operazioni di spionaggio, operazioni militari). Anche le piccole e medie imprese cominciano a comprendere che esiste un problema che potrebbe coinvolgerle, non sempre però comprendendo che le conseguenze potrebbero essere disastrose.

Il livello di consapevolezza è aumentato di conseguenza e ci si inizia a domandare quale sia il proprio livello di preparazione. Questo processo di aumento della consapevolezza, ancora estremamente acerbo nel nostro Paese, deve essere necessariamente accompagnato da strumenti metodologici a supporto. Tali strumenti devono essere semplici, adatti a qualunque tipologia di utente, in grado di fornire una tabella di marcia per raggiungere un livello minimo di preparazione nella protezione delle informazioni e/o della reputazione propria e della propria azienda. Il Framework Nazionale nasce proprio in quest'ottica.

Infine è fondamentale rimarcare che la minaccia cyber richiede una risposta coordinata pubblico privato, in primo luogo di tipo nazionale. Nessuno dei due attori può rispondere singolarmente a questa minaccia, poiché il privato non può controllare minacce che possono arrivare da qualunque parte del mondo e il pubblico ha bisogno del privato poiché molti servizi essenziali sono ormai gestiti e/o forniti da questi ultimi e un attacco potrebbe portare a conseguenze dirette per i cittadini.

Il Framework Nazionale di cyber security rappresenta uno degli elementi essenziali per un aumento di resilienza domestica dei sistemi e delle reti rispetto a tale minaccia. *L'adozione di un Framework è quindi un passo fondamentale anche nell'ottica di migliorare la propria reputazione, e favorire investimenti internazionali nel nostro Paese.*

Indipendentemente dal settore e dalla tipologia di rischi, c'è una certa convergenza sul definire il rischio come la materializzazione di un evento negativo che possa inficiare gli obiettivi aziendali.
Esso può essere visto come il risultato di tre fattori: la minaccia, la vulnerabilità e l'impatto. L'analisi delle tre componenti fondamentali può consentire a una organizzazione di ridurre il rischio attraverso una serie di tecniche, che vanno dalla riduzione delle vulnerabilità alla riduzione del possibile danno; in alcuni casi si può anche contemplare la riduzione della minaccia, ove sia possibile. Ogni organizzazione deve valutare i propri rischi e, in base al proprio livello di tolleranza, decidere quali contromisure adottare. In generale, essendo un concetto altamente legato all'aleatorietà delle variabili che lo determinano, non si considera possibile poter ridurre un rischio a zero, esiste di conseguenza sempre un livello di rischio residuo da considerare. Le organizzazioni devono valutare l'equilibrio tra riduzione del rischio, rischio residuo e la propria "tolleranza" al rischio. Il rischio residuo può essere quindi accettato, oppure trasferito nelle sue conseguenze economiche all'esterno, per esempio attraverso l'uso di prodotti assicurativi

Il compito fondamentale della cyber security è la protezione e la tutela della missione delle organizzazioni/aziende dai rischi derivanti dal cyberspace e dai sistemi informativi. Tutte le organizzazioni sono esposte a una moltitudine di rischi di varia natura. Sebbene vi siano molte definizioni, il senso comune ci insegna che il rischio non è altro che la possibilità di perdere qualcosa di valore: questo valore può essere un oggetto fisico, del denaro, il proprio stato di salute, un valore sociale, un livello di benessere emotivo. Il rischio è quindi legato all'incertezza di eventi prevedibili o improvvisi, diretti o indiretti, misurabili o non misurabili. L'incertezza è legata sia agli eventi sia alle loro cause e ai loro effetti, non sempre facilmente identificabili e definibili.
Proprio per questa caratteristica di incertezza, uno stesso rischio può essere percepito in modo molto diverso, a seconda del soggetto che ne valuta le caratteristiche..

Si riporta di seguito una breve descrizione delle 5 Function che caratterizza un Framework e che sono state implementate nella contestualizzazione dello stesso per le scuole, come è evidenziato di seguito:

Identify – La Function Identify è legata alla comprensione del contesto aziendale, degli asset che supportano i processi critici della attività e dei relativi rischi associati. Tale comprensione permette infatti a un ente di definire risorse e investimenti in linea con la strategia di gestione del rischio e con gli obiettivi scolastici.
Le Category all'interno di questa Function sono: Asset Management; Governance; Strategia di gestione del rischio.

Protect - La Function Protect è associata all'implementazione di quelle misure volte alla protezione dei processi di attività e degli asset scolastici, indipendentemente dalla loro natura informatica.
Le Category all'interno di questa Function sono: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; Protective Technology.

Detect – La Function Detect è associata alla definizione e attuazione di attività appropriate per identificare tempestivamente incidenti di sicurezza informatica.
Le Category all'interno di questa Function sono: Security Continuous Monitoring; Detection Processes

Respond – La Function Respond è legata alla definizione e attuazione delle opportune attività per intervenire quando un incidente di sicurezza informatica sia stato rilevato. L'obiettivo è contenere l'impatto determinato da un potenziale incidente di sicurezza informatica.
Le Category all'interno di questa Function sono: Communications; Mitigation.

Recover – La Function Recover è associata alla definizione e attuazione delle attività per la gestione dei piani e delle attività per il ripristino dei processi e dei servizi impattati da un incidente. L'obiettivo è garantire la resilienza dei sistemi e delle infrastrutture e, in caso di incidente, supportare il recupero tempestivo delle operazioni delle attività.
Le Category all'interno di questa Function sono: Improvements; Communications.

L'adozione del Framework da parte della scuola è stata contestualizzata all'ambiente scolastico. Questa prevede, in prima istanza, che siano verificate e attuate tutte quelle Subcategory del Framework classificate come a priorità alta. Difatti rappresentano le azioni essenziali da completare per contrastare le principali e più comuni minacce cyber e proteggere i sistemi della scuola comunemente esposti. E' stata strutturata in 5 aree di indirizzo, a loro volta organizzate in complessive in 15 sotto-aree come di seguito riportate.

A1. Analisi dei rischi sulle aree e sui locali

A2. Identificazione degli asset e governo della sicurezza

- A2.1 Identificazione degli asset
- A2.2 Assegnazione Responsabilità
- A2.3 Uso appropriato dei privilegi di amministratore
- A2.4 Conformità a Leggi e Regolamenti

A3. Identificazione delle minacce

- A3.1 Protezione da Virus
- A3.2 Valutazione e correzione continua della vulnerabilità

A4. Protezione dei sistemi e delle infrastrutture

A4.1 Protezione perimetrale

A4.2 Controllo Accessi

A4.3 Configurazione Sicura Sistemi

A4.4 Aggiornamento Sistemi

A4.5 Formazione di Base del Personale

A4.6 Backup e Restore

A5. Gestione degli incidenti di sicurezza

A5.1 Risposta agli Incidenti di Sicurezza

A5.2 Protezione dei dati personali

Aspetti di privacy legati al Framework
Sono evidenziate le funzioni, le rispettive Category e le corrispondenti Subcategory

Funzione	Category	Subcategory
IDENTIFIDY (ID) Identificazione	***Asset Management (ID.AM)*** I dati, il personale, i dispositivi e i sistemi e le facilities necessari alla scuola sono identificati e gestiti in coerenza con gli obiettivi di business e con la strategia di rischio della scuola.	**ID.AM-1** **ID.AM-2** **ID.AM-3** **ID.AM-6**
	Governance (ID.GV) Le politiche, le procedure e i processi per gestire e monitorare i requisiti della scuola (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di cyber security.	**ID.GV-1** **ID.GV-2** **ID.GV-3**
	Risk Assessment (ID.RA) La scuola comprende il rischio di cyber security inerente l'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui	**ID.RA-1** **ID.RA-4** **ID.RA-5**
PROTECT (PR) Protezione	***Access Control (PR.AC)*** L'accesso agli asset ed alle relative risorse è limitato al personale, ai processi, ai dispositivi, alle attività e alle transazioni effettivamente autorizzate	**PR.AC-1** **PR.AC-2** **PR.AC-3** **PR.AC-4**
	Awareness and Training (PR.AT) Il personale e le terze parti sono sensibilizzate e formate in materia di cyber security e ricevono adeguata preparazione, coerente con le politiche, le procedure e gli accordi esistenti, per svolgere correttamente i compiti e le responsabilità legate alla sicurezza delle informazioni	**PR.AT-1** **PR.AT-2** **PR.AT-4**
	Data Security (PR.DS) I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio della scuola, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-1** **PR.DS-6**
	Information Protection Processes and Procedures (PR.IP) Sono attuate e adeguate nel tempo politiche di sicurezza (che indirizzano scopo, ambito, ruoli e responsabilità, impegno da parte del management e coordinamento tra le diverse entità organizzative), processi e procedure per gestire la protezione dei sistemi informativi e degli assets.	**PR.IP-1** **PR.AT-2** **PR.AT-4** **PR.IP-5** **PR.IP-12**
	Maintenance (PR.MA) La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti	**PR.MA-1** **PR.MA-2**
	Protective Technology (PR.PT) Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-2** **PR.PT-3** **PR.PT-4**
DETECT (DE) Accertamento	***Security Continuous monitoring (DE.CM)*** I sistemi informativi e gli asset sono monitorati periodicamente per identificare eventi di cyber security e per verificare l'efficacia delle misure di protezione	**DE.CM-1** **DE.CM-3** **DE.CM-4** **DE.CM-8**

	Detection Processes (DE.DP) Sono adottati, mantenuti e verificati nel tempo i processi e le procedure di monitoraggio per assicurare una tempestiva e adeguata comprensione degli eventi di sicurezza	**DE.DP-4**
RESPOND (RS) Risposta	***Communications (RS.CO)*** Le attività di risposta sono coordinate con le parti interne ed esterne, per includere eventuale supporto da parte degli organi di legge o dalle forze dell'ordine	**RS.CO-2** **RS.CO-3** **RS.CO-4** **RS.CO-5**
	Mitigation (RS.MI) Vengono eseguite azioni per prevenire l'espansione di un evento di sicurezza, per mitigare i sui effetti e per rimuovere l'incidente.	**RS.MI-1** **RS.MI-2** **RS.MI-3**
RECOVER (RC) Ripristino	***Improvements (RC.IM)*** I piani di ripristino ed i relativi processi sono migliorati tenendo conto delle "lesson learned" per le attività future.	**RC.IM-1**
	Communications (RC.CO) Le attività di ripristino a seguito di un incidente sono coordinate con le parti interne ed esterne, come ad esempio, le vittime, gli ISP, i proprietari dei sistemi attaccati, i vendor, i CERT/C SIRT	**RC.CO-2**

Legenda dei codici delle subcategory
secondo il modello Framework Nazionale di Sicurezza Cibernetica

[*Legenda della colonna "Rischio"*:

- I numeri progressivi identificano il rischio.
- I codici dei rischi contrassegnati con il simbolo * in rosso sono quelli previsti dalle normative di riferimento per il raggiungimento dei livelli minimi di sicurezza ICT per le pubbliche amministrazioni.
- Il simbolo "●" identifica il rischio interno alla scuola, mentre il simbolo "▲" quello esterno.

Consulta il grafico di pag. 56]

Acronimo			**Descrizione**
FNSC			**Framework Nazionale di Sicurezza Cibernetica**
ABSC			**Agid Basic Security Control(s)**
Codici della Funzione Identify e relative subcategorie			**Descrizione delle subcategory**
Rischio			
1	ID.AM-1*	●	Sono censiti i sistemi e gli apparati fisici in uso nella scuola
2	ID.AM-2*	●	Sono censiti le piattaforme e le applicazioni software in uso nella scuola
3	ID.AM-3*	●	I flussi di dati e comunicazioni inerenti la scuola sono identificati.
4	ID.AM-5*	▲	Le risorse (es: hardware, dispositivi, dati e software) sono prioritizzati in base alla loro classificazione (e.g. confidenzialità, integrità, disponibilità), criticità e valore per il business dell'organizzazione
5	ID.AM-6*	●	Sono definiti e resi noti ruoli e responsabilità inerenti la cyber security per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner, ..)

6	ID.GV-1	●	E' identificata e resa nota una policy di sicurezza delle informazioni
7	ID.GV-2	●	Ruoli e responsabilità inerenti la sicurezza delle informazioni sono coordinati ed allineati con i ruoli interni ed i partner esterni.
8	ID.GV-3	●	I requisiti legali in materia di cyber security, con l'inclusione degli obblighi riguardanti la privacy e le libertà civili, sono compresi e gestiti
9	ID.RA-1*	●	Le vulnerabilità delle risorse (es. sistemi, locali,dispositivi) della scuola sono identificate e documentate.
10	ID.RA-4*	●	Sono identificati i potenziali impatti sul business e le relative probabilità di accadimento.
11	ID.RA-5*	▲	Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio.
Codici della Funzione Protect e relative subcategorie			**Descrizione delle Subcategory**
Rischio			
12	PR.AC-1*	●	Le identità digitali e le credenziali di accesso per gli utenti e per i dispositivi autorizzati sono amministrate.
13	PR.AC-2*	●	L'accesso fisico alle risorse è protetto e amministrato.
14	PR.AC-3*	▲	L'accesso remoto alle risorse è amministrato.
15	PR.AC-4*	●	Gli accessi alle risorse sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni.
16	PR.AT-1*	●	Tutti gli utenti sono informati e addestrati
17	PR.AT-2*	●	Gli utenti privilegiati (ad es. gli amministratori di sistema) comprendono ruoli e responsabilità.
18	PR.AT-4	●	I dirigenti e i vertici comprendono ruoli e responsabilità
19	PR.DS-1	▲	I dati e le informazioni memorizzate sono protette
20	PR.DS-5*	▲	Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak)
21	PR.DS-6*	▲	Vengono implementate tecniche di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni
22	PR.IP-1*	▲	Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale
23	PR.IP-2*	▲	Eventuali sistemi in esercizio che vengono compromessi devono essere ripristinati utilizzando la configurazione standard.
24	PR.IP-4*	●	I backup delle informazioni sono eseguiti, amministrati e verificati periodicamente.
25	PR.IP-5*	●	Sono rispettate le policy ed i regolamenti relativi agli ambienti fisici in cui operano le risorse dell'organizzazione

26	PR.IP-9*	▲	Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente e/o disastro
27	PR.IP-12*	▲	Viene sviluppato e implementato un piano di gestione delle vulnerabilità.
28	PR.MA-1*	●	La manutenzione e la riparazione delle risorse e dei sistemi è svolta e registrata in modo tempestivo e portata a termine attraverso l'utilizzo di strumenti controllati ed autorizzati.
29	PR.MA-2*	●	La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati.
30	PR.PT-2*	●	I supporti di memorizzazione removibili sono protetti ed il loro uso è ristretto in accordo con la policy.
31	PR.PT-3*	●	L'accesso alle risorse e ai sistemi è limitato secondo il principio di minima funzionalità.
32	PR.PT-4	▲	Le reti di comunicazione e controllo sono protette.
Codici della Funzione Detect e relative subcategorie			**Descrizione delle Subcategory**
Rischio			
33	DE.CM-1*	▲	Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cyber security.
34	DE.CM-3*	●	Viene svolto il monitoraggio del personale per rilevare potenziali eventi di cyber security.
35	DE.CM-4*	●	Il codice malevolo viene rilevato.
36	DE.CM-7*	●	Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati .
37	DE.CM-8*	●	Vengono svolte scansioni per l'identificazione di vulnerabilità.
38	DE.DP-5	●	Il codice non autorizzato su dispositivi mobili viene rilevato
Codici della Funzione Respond e relative subcategorie			**Descrizione delle Subcategory**
Rischio			
39	RS.CO-2*	▲	Sono stabiliti dei criteri per documentare gli incidenti/eventi.
40	RS.MI-1*	▲	In caso di incidente vengono messe in atto procedure atte a contenerne l'impatto.
41	RS.MI-2*	▲	In caso di incidente vengono messe in atto procedure atte a mitigarne gli effetti.
42	RS.MI-3	▲	Le nuove vulnerabilità sono mitigate o documentate come rischio accettato.
Codici della Funzione Recover e relative subcategorie			**Descrizione delle Subcategory**
Rischio			
43	RC.CO-2*	●	A seguito di un incidente vengono gestite le pubbliche relazioni
44	RC.RP-1	●	Esiste un piano di risposta (response plan) e viene eseguito durante o dopo un evento

Questa istituzione scolastica ha, pertanto, contestualizzato gli obiettivi di sicurezza conformandoli ai principi generali del **FNSC** e coniugandoli con quelli delle **Misure Minime** del modello ABSC fissando allo stesso tempo, obiettivi di prevenzione da un lato con quelli di risposta e ripristino dall'altro.

Contesto di riferimento all'analisi dei rischi.

L'attività d'impresa, riferibile anche a quella della scuola, è caratterizzata da un indissolubile legame con il rischio, il quale è una caratteristica intrinseca dell'attività stessa e le capacità di identificazione, valutazione e gestione dei rischi sono alla base del successo della sicurezza informatica. L'interesse per la gestione del rischio ha assunto rilievo a partire dagli anni '90 e si è gradualmente accresciutosi nell'ultimo decennio esplodendo negli anni più recenti.

Il tradizionale approccio al concetto di rischio viene abbandonato a favore di un processo di gestione integrato basato su soluzioni organizzative riconosciute e condivise dall'intera organizzazione,tanto che le ultime crisi a partire dall'attuale millennio hanno contribuito a diffondere nelle imprese la consapevolezza di come anche rischi apparentemente insignificanti possano causare gravi danni, qualora non vengano gestiti adeguatamente, circostanza ancor più probabile nel caso le diverse tipologie di eventi rischiosi interagiscano tra loro. Ne deriva che un buon modello di gestione del rischio deve permettere la comprensione dei potenziali aspetti positivi e negativi di tutti i fattori che possono influenzare l'organizzazione, incrementando la probabilità di successo della strategia e riducendo l'incertezza sul raggiungimento degli obiettivi generali dell'azienda. Il rischio, dunque, diviene un ulteriore fattore produttivo in ambito aziendale da gestire secondo i principi di imprenditorialità e managerialità comuni. L'evoluzione del contesto economico così come la mutata considerazione del rischio hanno portato alla creazione di innovativi modelli di gestione dello stesso nell'ambito aziendale.

L'evoluzione subita dal concetto di rischio ha portato alla creazione di innovativi modelli di gestione dello stesso in ambito aziendale.

L'istituzione scolastica ha scelto, anche in questo caso, un Framework, patrocinato dall'Università "la Sapienza" progettato per l'identificazione e la gestione di eventi che potrebbero avere un impatto, sia positivo che negativo, sulla scuola, focalizzato nel mantenere il livello di rischio all'interno della soglia accettabile di rischio accettabile (propensione al rischio) e concepito per dare una ragionevole garanzia in relazione al raggiungimento dei propri obiettivi

In questo modello, la gestione dei rischi si affianca alla regolare attività operativa e diventa parte integrante dell'intera struttura organizzativa, risultando essenziale alla rilevazione delle eventuali interconnessioni presenti tra le diverse tipologie di rischio.

Di fatto, solo considerando la scuola come un'unica entità nella quale si articolano diverse aree e attività interconnesse tra loro è possibile sfruttare appieno le potenzialità della gestione del rischio.

Dunque, il modello scelto promuove una gestione organica e integrata di tutte le tipologie di rischio così da valutare meglio la rischiosità assunta dalla scuola sia nel dettaglio che a livello d'insieme. Una valutazione del profilo di rischio globale consente da una parte di verificare e analizzare la coerenza delle scelte effettuate, e dall'altra di allineare il livello di rischiosità con il livello di rischio accettabile. Una completa e dettagliata valutazione del rischio è fondamentale ed essenziale per una corretta valutazione e selezione delle strategie e dei relativi obiettivi. Dunque, la gestione integrata dei rischi assume una natura strategica, tattica e competitiva capace di influenzare positivamente l'intero processo di creazione di valore per la scuola.

L'analisi del rischio

Nel processo di analisi del rischio, primaria rilevanza ha la definizione dell'ambiente interno e degli obiettivi strategici dell'azienda. L'ambiente interno costituisce l'identità essenziale di un'organizzazione, determina i modi in cui il rischio è considerato e affrontato dalle persone che operano in azienda, i valori etici e l'ambiente di lavoro in generale. In questo ambito risulta fondamentale la definizione la conoscenza della gestione del rischio. Questa rappresenta le attitudini comuni che caratterizzano l'approccio al rischio, come viene considerato in tutte le attività, come viene individuato e gestito. Ne deriva l'identificazione del Rischio accettabile, ovvero la propensione al rischio, che riflette il modo in cui vengono percepiti e identificati gli eventi, quali tipi di rischi vengono accettati o meno e come verranno gestiti.

Il rischio accettabile individuato deve essere il risultato di un confronto tra i vertici e gli operatori, in quanto influirà sia sulle scelte strategiche, sia su quelle operative di pertinenza dei vari uffici.

La soglia di rischio tollerabile deve essere stabilita sulla base dell'attività svolta, dell'organizzazione che l'adotta e di altre variabili. Tale soglia determina i livelli di scostamento accettabili rispetto al raggiungimento dell'obiettivo, viene definita tolleranza al rischio ed è misurabile con la stessa unità di misura scelta per gli obiettivi.
Il grafico che segue segna un chiaro esempio sulla gestione dl rischio nel quale viene rappresentata la zona individuata in rosso come rischio dannoso contribuendo alla designazione dei tre livelli di rischi Basso, Medio ed Alto.

Il processo di analisi del rischio inizia con l'identificazione degli eventi di rischio che potrebbero inficiare il raggiungimento degli obiettivi aziendali. Ognuno dei rischi identificati diviene oggetto di due valutazioni: prima e dopo le azioni di mitigazione messe in essere dai vertici. Dalla prima valutazione si determina il rischio intrinseco, ovvero il massimo livello di rischio possibile senza alcuna azione di mitigazione applicata. La seconda valutazione determina invece il rischio residuo, ovvero la porzione di rischio che rimane in capo alla scuola dopo aver messo in atto le attività di controllo esistenti sul rischio inerente. Per azioni di mitigazioni si intendono tutte quelle attività poste in essere per ridurre la probabilità del manifestarsi del rischio e/o l'impatto collegato. La valutazione del rischio avviene su due dimensioni:

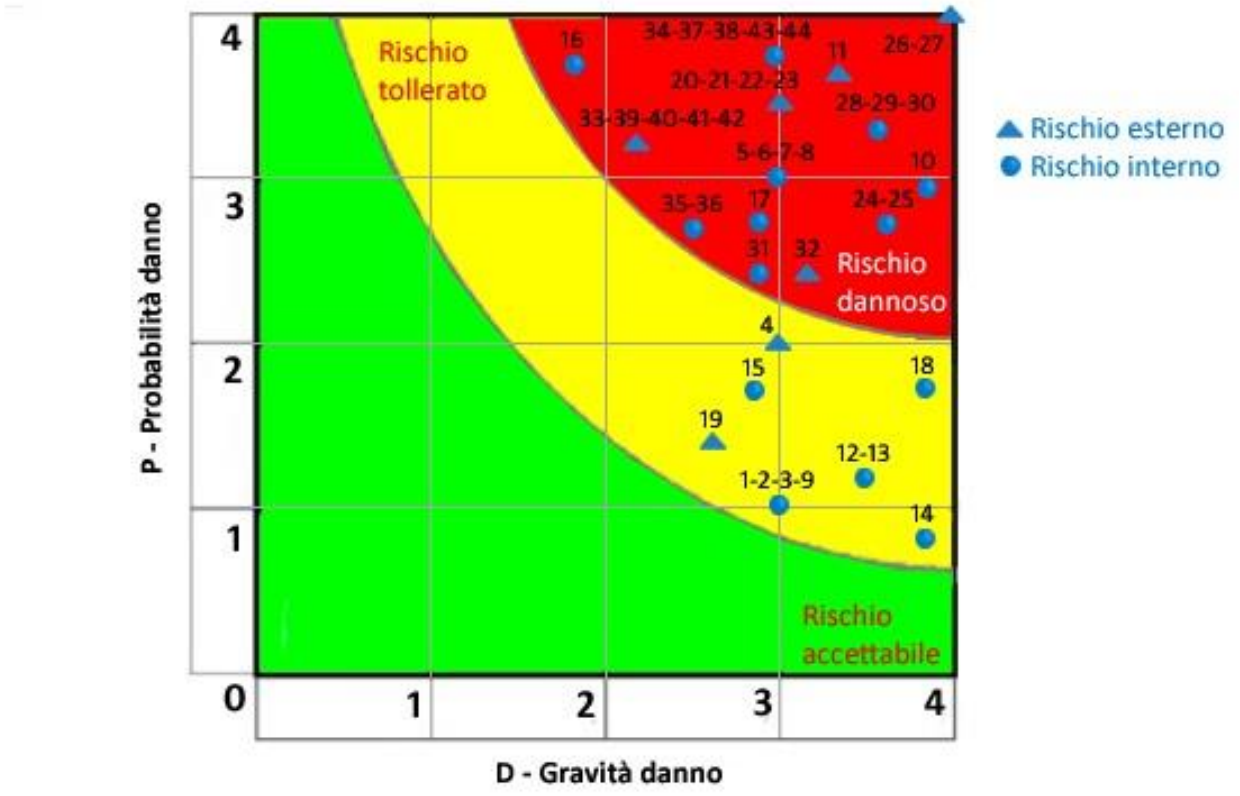
1) la probabilità dell'accadimento;
2) la gravità del danno a seguito dell'accadimento.

La probabilità dell'accadimento di un rischio è la possibilità che l'evento/rischio identificato si manifesti in un dato orizzonte temporale. Questo aspetto rimane uno dei più complessi e controversi del processo di analisi del rischio. In assenza di informazioni quantitative precise, che possono provenire dall'analisi dello storico di esperienze simili pregresse o da studi e analisi specifiche dei fenomeni d'interesse, è possibile stabilire la probabilità di accadimento sulla base della sensibilità ed esperienza del personale riguardo a funzioni di loro competenza. Sarà poi possibile determinare e costruire una matrice dei rischi, simile a quella mostrata in Figura che segue, ovvero una rappresentazione sintetica del posizionamento relativo dei singoli rischi rispetto al rischio accettabile e al rischio tollerato, consentendo ai vertici di identificare le priorità di azione e le possibili strategie di risposta al rischio.
La valutazione del rischio, data dal prodotto di probabilità di accadimento e gravità del danni, genera tre livelli di rischio:

Rischio Basso – Non rilevante: il rischio rientra all'interno del rischio accettabile e di conseguenza non sono necessarie misure di controllo o strategie di mitigazione ulteriori;

Rischio Medio – Monitorare: il rischio supera il primo livello ma rientra nel rischio tollerato. Questa tipologia di rischio solitamente viene sottoposta a costante monitoraggio/gestione da parte dei vertici;

Rischio Alto – Evitare/Ridurre: Il rischio supera i livelli precedenti. Necessita un'elevata attenzione da parte della direzione che deve quali strategie di trattamento applicare: riduzione/mitigazione del rischio, trasferimento del rischio o eliminazione della fonte di rischio.



I vertici della scuola dopo avere preso visione dei rischi residui, determina come allinearli con i livello di rischio accettabile attraverso un piano di trattamento dei rischi.

L'inadeguatezza delle tradizionali forme di gestione del rischio è stata compresa anche dalle autorità regolamentari che, negli ultimi tempi, come già verificato, hanno gradualmente implementato vincoli sempre più stringenti in materia di gestione e consapevolezza del rischio. La stessa concezione del rischio ha subito una significativa modifica: dapprima fenomeno unicamente ricondotto a situazioni negative, viene oggi considerato un artefice del successo dell'azienda, qualora questa riesca ad estrarne il valore intrinseco. Il rischio non è, dunque, unicamente un onere da sopportare, bensì, se ben gestito, può diventare un fattore critico di successo e dare un vantaggio competitivo ed economico in grado di garantire lo sviluppo e la protezione della stessa attività.

A1. – Analisi dei rischi sulle aree e sui locali

A1. – Analisi dei rischi sulle aree e sui locali

Descrizione secondo il modello ABSC	I locali devono essere provvisti di estintori per sopprimere eventuali focolai di incendio. L'accesso ai locali è sempre controllato durante il normale svolgimento dell'attività lavorativa. L'ingresso agli stessi à consentito solo alle persone autorizzate. Controllare periodicamente interruzione di corrente elettrica, di acqua e di aria condizionata, funzionamento dei gruppi di continuità, radiazione elettromagnetica e scariche elettrostatiche.	
Subcategory	ID.AM-6 PR.AT-4	**Livello rischio stimato: Lieve** del tipo R= PxG R=1*3
Controlli applicabili durante le fasi dell'audit	Il dirigente scolastico e il responsabile del trattamento dei dati devono essere consapevoli e comprendere le responsabilità associate a rischi di carattere fisico. Questo deve essere evidente durante tutto il trattamento dei dati. Devono essere stabiliti e formalizzati le responsabilità legati alla sicurezza dei locali, come ad esempio tutti gli ingressi che accedono alla scuola, gli ingressi ai locali che ospitano le segreterie. All'interno della scuola deve essere identificata una figura che rappresenti il punto di riferimento per vigilare e controllare tutti gli accessi Tutte le assegnazioni di responsabilità devono essere opportunamente formalizzate.	

A2. - Identificazione degli asset e governo della sicurezza

Tab. A2.1 - Identificazione degli asset

Descrizione secondo i modelli ABSC e Framework	L'applicazione di contromisure di sicurezza finalizzate a ridurre il rischio cyber deve avvenire su tutti i sistemi e i computer della scuola e in particolare su quelli valutati come critici per la attività della stessa. È indispensabile pertanto disporre di un inventario di tutti gli asset rappresentati dalle informazioni, applicazioni, sistemi e apparati informatici presenti all'interno dell''istituzione scolastica. Registrare attributi importanti, come ad esempio la posizione fisica, il proprietario, la funzione di riferimento, le dipendenze, ecc. risulta funzionale alle attività di governo e gestione della cyber security. Ad esempio, un inventario delle risorse è in grado di abilitare l'identificazione dei sistemi che necessitano dell'applicazione di uno specifico aggiornamento software. Pertanto sono da realizzare due azioni: **- un inventario dei dispositivi autorizzati e non autorizzati:** gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati e non gestiti siano individuati e sia loro impedito l'accesso. **- in inventario dei software autorizzati e non autorizzati:** gestire attivamente (inventariare, e tracciare e correggere) tutti i software sulla rete in modo che sia installato solo software autorizzato, mentre il software non autorizzato sia individuato e ne venga impedita l'installazione o l'esecuzione.	
Subcategory	a) ID.AM-1 b) ID.AM-2	**Livello rischio stimato: Lieve** del tipo R= PxG R=1*3
Controlli applicabili durante le fasi dell'audit	a) Deve essere predisposto un inventario delle informazioni, applicazioni, sistemi e apparati presenti nella scuola a livello IT. b) L'inventario deve rispondere ai seguenti criteri: - Sono riportate per gli asset censiti come minimo le tipologie di informazioni trattate, la posizione, la funzione di riferimento, il responsabile, i referenti coinvolti a diverso titolo nelle attività di gestione e manutenzione, dipendenze e ulteriori dettagli utili per l'attuazione dei controlli menzionati nelle successive sotto-aree (ad es. tipologia hardware, versioni software, informazioni trattate, contratti di servizio ecc.) - Sono identificati i sistemi con maggiore rilevanza in termini di conseguimento degli obiettivi della scuola e quelli coinvolti a diverso titolo nel rispetto di vincoli normativi cogenti, - Sono registrati tutti i cambiamenti di stato legati agli asset, come acquisizione, installazione, operatività e ritiro. c) Implementare un inventario delle risorse attive. Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete. Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP. e) Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi serve, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco. Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	

Tab. A2.2 - Assegnazione Responsabilità

Descrizione secondo il modello Framework	L'assegnazione dei ruoli e delle responsabilità è un elemento indispensabile per assicurare un corretto governo dei rischi e permettere un'efficace operatività, intesa come attuazione dei controlli di prevenzione e/o contrasto delle minacce di cyber security a cui la scuola è esposta. E' fondamentale che tutto il personale sia consapevole dei ruoli e delle responsabilità di sicurezza, correlate allo svolgimento della attività lavorative. Ai vertici scolastici, nelle figura della dirigenza e più in generale alla "proprietà", è assegnato il ruolo chiave di definizione delle priorità e di assegnazione delle risorse associate alle iniziative di cyber security. Questi difatti sono i responsabili ultimi per i rischi cyber all'interno della scuola.	
Subcategory	ID.AM-6 PR.AT-4	**Livello rischio stimato: Lieve** del tipo R= PxG R=1*3
Controlli applicabili durante le fasi dell'audit	Il dirigente scolastico e l'amministratore del sistema devono essere consapevoli e comprendere le responsabilità associate a rischi di cyber security. Questo deve essere evidente durante tutto il trattamento dei dati. Devono essere stabiliti e formalizzati i ruoli e le responsabilità legati alla cyber security, come ad esempio quelli previsti per la protezione dei sistemi e delle infrastrutture o quelli legati all'uso corretto degli strumenti informatici, per tutto il personale e le terzi parti interessate (ad es. i fornitori, i clienti, i partner). All'interno della scuola deve essere identificata una figura che rappresenti il punto di riferimento per la cyber security (cioè il responsabile per la cyber security), con il compito di coordinare le diverse iniziative di cyber security e contattare le autorità e il CERT Nazionale in caso di eventi di ampia portata. Tutte le assegnazioni di responsabilità devono essere opportunamente formalizzate.	

Tab. 2.3 - Uso appropriato dei privilegi dell'amministratore

Descrizione Secondo il modello ABSC	Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.	
Subcategory	a) PR.AC-4 PR.PT-3 b) ID.AM-6 PR.AT-2 DE.CM-3 c) PR.IP-1 d) PR.AC-1 PR.AT-2 e) ID.AM-6 f) ID.AM-6 PR.AT-2 g) PR.AC-1 PR.AT-2	**Livello rischio stimato: Lieve** del tipo R= PxG R=1*3
Controlli applicabili durante le fasi dell'audit	a) Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi. Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedono i privilegi, registrando ogni accesso effettuato. b) Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata. c) Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dello amministratore predefinito con valori coerenti con quelle delle utenze amministrative in uso. d) Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza, impedendo che le stesse possano essere riutilizzate a breve distanza di tempo. e) Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse. Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona. f) Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso. g) Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza. Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	

Tab. A2.4 - Conformità a leggi e regolamenti

Descrizione secondo il modello Framework	La crescita esponenziale delle tecnologie dell'informazione e del processo di digitalizzazione in atto ha comportato e comporterà anche in futuro, la necessità per tutte le aziende, compreso le scuola, di adeguarsi costantemente a leggi e regolamenti specifici, volti a tutelare utenti e organizzazioni nello spazio cyber. Pertanto, la scuola ha l'obbligo di conoscere e ottemperare alle leggi e ai regolamenti applicabili al proprio contesto, soprattutto in relazione ai mercati in cui essa opera e alla tipologia di servizi informatici fruiti e/o erogati.	
Subcategory	ID.GV-1 ID.GV-3	**Livello rischio stimato: Lieve** del tipo R= PxG R=1*3
Controlli applicabili durante le fasi dell'audit	Individuare le leggi e i regolamenti che hanno un impatto diretto o indiretto sulla cyber security (es. Computer Crime, Data Breach Notification, proprietà intellettuale), aggiornando periodicamente il censimento Identificare, attraverso un'attività di monitoraggio periodico, ogni potenziale non conformità rispetto a quanto richiesto da leggi e regolamenti e preparare un piano specifico di adeguamento in cui indirizzare tali non conformità, condividendo gli impatti e le implicazioni specifiche con il vertice istituzionale. Applicare le misure definite nel piano di adeguamento, approvato dai vertici. Verificare nel tempo l'effettiva applicazione delle misure necessarie a garantire la conformità con leggi e regolamenti, condividendo con i referenti scolastici preposti, i gap e/o le criticità che possono comportare non conformità e ripercussioni legali di carattere civile e/o penale	

A.3 - Identificazione delle minacce

Tab. A3.1 - Protezione da Virus

Descrizione secondo i modelli Framework e ABSC	I sistemi informativi sono comunemente esposti a software malevoli, denominati malware, soprattutto se connessi a internet. La compromissione attraverso malware può avvenire mediante diverse modalità, quali l'apertura di una e-mail infetta, la navigazione su siti compromessi, l'apertura di file su dispositivi locali o contenuti su memorie di massa esterne (come Storage USB). Soluzioni di protezione specifiche devono essere adottate per monitorare, individuare e rimuovere il software malevolo.	
Controlli applicabili durante le fasi dell'audit	Soluzioni di protezione da malware (es. software antivirus e/o soluzioni per protezione endpoint) devono essere adottate su tutti i sistemi aziendali come computer, server e dispositivi mobili aziendali, inclusi quelli afferenti ai sistemi di controllo industriale (es. sistemi SCADA) La protezione malware deve essere efficace nel contrasto a tutte le forme di malware: Virus, Worm, Trojan, Spyware, Rootkit, Botnet, Keystroke Loggers, Adware. La protezione da malware deve essere mantenuta costantemente aggiornata nel tempo, ricorrendo il più possibile a meccanismi automatici di aggiornamento che prevedano controlli come minimo giornalieri; La soluzione di protezione da malware deve essere sempre attiva e non disattivabile dagli utenti. Deve essere inoltre configurata per: 1 - Rimuovere o isolare (porre in quarantena) i file infetti da malware 2 - Eseguire scansioni a intervalli regolari di tutti i file 3 - Fornire notifiche nel caso di identificazione di sospetto malfare La soluzione deve assicurare la protezione nei seguenti casi: 1 - Accesso a file e dati memorizzati localmente, su dispositivi esterni o su server centralizzati (es. file server) 2 - Accesso a e-mail e relativi allegati 3 - Accesso a pagine web durante navigazione internet, prevenendo la connessione a siti malevoli 4 - Accesso Instant Messanger e qualsiasi altra forma di comunicazione che consenta lo scambio di file o di informazioni.	
Subcategory	a) DE.CM-4 DE.CM-5 b) DE.CM-1 c) PR.PT-3 DE.CM-7 d) PR.PT-2 e) PR.AT-1 DE.CM-4 f) PR.AT-2 DE.CM-4 g) DE.CM-1 DE.CM-4	**Livello rischio stimato: Lieve** del tipo R= PxG R=1*3
Controlli applicabili durante le fasi dell'audit	a) Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico. b) Installare s tutti i dispositivi firewall ed IPS personali. c) Limitare l'uso di dispositivi esterni a quelli necessari per l'attività aziendali. d) Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili. e) Disattivare l'esecuzione automatica dei contenuti dinamici (ad es. macro) presenti nei file. f) Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione. g) Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (ad es. cab)	

Tab. A3.2 - Valutazione e correzione continua della vulnerabilità.

Descrizione secondo il modello ABSC	Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.	
Subcategory	a) ID.RA-1 DE.CM-3 b) DE.CM-8 c) PR.MA-1 d) PR.IP-12 RS.MI-3 e) ID.RA-4 ID.RA-5 PR.IP-12 f) PR.IP-12	**Livello rischio stimato: Lieve** del tipo R= PxG R=1*3
Controlli applicabili durante le fasi dell'audit	a) Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazione delle vulnerabilità più critiche. b)Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza. c)Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.. Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando le misure adeguate al loro livello di maturità d) Verificare che le vulnerabilità emesse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio. e) Definire un paino di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e delle tipologie degli apparati (per es. server esposti, server interni, PdL, portatili, ….) g)Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	

Tab. A4.1 - Protezione perimetrale

Descrizione secondo l modello Framework	Le reti di computer della scuola, collegate a Internet o interconnesse con altre reti, devono essere protette da attaccanti volti ad avere accesso ai sistemi, computer e alle informazioni ivi contenute. Un dispositivo di sicurezza di rete come il firewall, posizionato sul perimetro della rete, è in grado di proteggere la stessa contro le minacce cyber basilari - attacchi che richiedono capacità e tecniche limitate, e che conseguentemente risultano largamente diffusi - limitando il traffico di rete in entrata e in uscita alle sole connessioni autorizzate. Tali restrizioni si ottengono applicando delle impostazioni di configurazione note come regole (o policy) del firewall. Questa soluzione deve essere opportunamente installata, configurata e gestita nel tempo, al fine di non vanificare il conseguimento delle specifiche finalità.	
Subcategory	PR.PT-4	**Livello rischio stimato: Lieve** del tipo R= PxG R=1*3
Controlli applicabili durante le fasi dell'audit	Uno o più firewall (o dispositivi di protezione equivalenti) devono essere installati sul perimetro di rete più esterno dell'organizzazione (ed esempio tra la rete Internet e la rete interna) Ogni regola che consenta il passaggio di traffico attraverso il firewall, legato a comunicazioni informatiche, deve essere soggetta ad approvazione da parte di un referente aziendale Servizi non approvati o servizi tipicamente vulnerabili devono essere disattivati o bloccati, attraverso specifiche regole del firewall Le regole firewall che non sono più necessarie (ad esempio perché il servizio non è più necessario) devono essere rimosse o disabilitate in modo tempestivo Le password associate alle credenziali di amministrazione dei firewall devono essere modificate, in alternativa a quelle fornite di base dal produttore e attribuite ad account uninominali L'interfaccia amministrativa utilizzata per gestire il sistema deve essere protetta da accesi non autorizzati, attraverso tecniche di Strong Authentication (es. basata su due fattori indipendenti di autenticazione) o password forti se acceduta solamente dalla rete interna. Le utenze devono essere bloccate dopo un numero massimo di tentativi di accesso non andati a buon fine	

Tab. A4.2 - Controllo Accessi

Descrizione secondo l modello Framework	Modalità di controllo accessi devono essere stabilite per limitare l'accesso alle informazioni, applicazioni, sistemi, reti e in generale dispositivi informatici aziendali da parte di tutti le tipologie di utenti. L'obiettivo è garantire che solo gli utenti effettivamente autorizzati possano accedere a tali sistemi o dati, assicurando il livello di privilegio minimo necessario a esercitare le proprie funzioni.	
Subcategory	PR.AC-1 PR.AC-3 PR.AC-4 PR.AT-2 PR.MA-2	**Livello rischio stimato: Lieve** del tipo R= PxG R=1*3
Controlli applicabili durante le fasi dell'audit	Le misure di controllo degli accessi devono interessare: (a) Tutte le tipologie di individui (dipendenti, fornitori, partner, ecc.) (b) Tutti i tipi di informazione, servizi o sistemi con cui gli individui devono interagire Tutto il personale (interno ed esterno) deve essere univocamente identificato e autenticato per accedere a servizi, sistemi e informazioni aziendali attraverso l'impiego di identificativi nominali (account) Nel caso di impiego di strumenti di autenticazione come username e password, questi devono rispondere ai seguenti criteri: (a) Impiego di password robuste (almeno 8 caratteri alfanumerici e utilizzo di caratteri speciali, es. $, #, !,?,"), possibilmente attuato attraverso meccanismi di impostazione e controllo automatici (b) Aggiornamento periodico delle password con cadenza non superiore ai 60 giorni L'assegnazione delle credenziali di accesso e dei relativi privilegi devono essere soggetti a un processo di approvazione e deve avvenire nel rispetto dei seguenti principi: (a) Minimo privilegio, ovvero con assegnazione dei privilegi minimi necessari a esercitare le proprie mansioni (i.e. Least Privilegi) (b) Accesso alle sole informazioni strettamente necessarie allo svolgimento delle proprie mansioni (i.e., Need-to-Know) (c) Segregazione dei ruoli, al fine di separare attività incompatibili tra soggetti diversi Le credenziali impiegate per attività specifiche, come quelle di amministrazione dei sistemi e delle applicazioni informatiche, devono essere gestite nel rispetto dei seguenti criteri: (a) Limitate a un numero ristretto di individui, preventivamente autorizzati e gestite in conformità con la normativa vigente (b) Differenziate da quelli impiegate per altri scopi Gli account e i privilegi di accesso devono essere disabilitati quando non più necessari (es. cambiamento di struttura, abbandono dell'organizzazione) o dopo un periodo di inattività	

Tab. A4.3 - Configurazione sicura dei sistemi

Descrizione secondo l modello Framework	I computer e i dispositivi di rete non possono essere considerati sicuri quando configurati con le impostazioni standard fornite in origine dai produttori. Spesso infatti le credenziali amministrative, o in generale le configurazioni impostate dal produttore, sono pubbliche o insicure e potrebbero essere usate per ottenere l'accesso non autorizzato ai sistemi di un'azienda e alle informazioni in questi contenute. Applicando alcuni semplici accorgimenti di sicurezza durante la configurazione di nuovi computer o sistemi informatici è possibile ridurre considerevolmente i rischi e le probabilità che un attacco informatico vada a buon fine.	
Subcategory	PR.IP-1	**Livello rischio stimato: Lieve** del tipo R= PxG R=1*3
Controlli applicabili durante le fasi dell'audit	Disabilitare le utenze non strettamente necessarie, soprattutto quelle caratterizzate da privilegi elevati (es. utenze amministrative e di sistema e di sistema) Cambiare immediatamente le utenze non nominali e qualsiasi password standard pre-impostata dai produttori, adottando utenze uninominali e password robuste Rimuovere o disabilitare il software e i servizi non necessari (incluse applicazioni e strumenti di amministrazione) Disabilitare le funzioni di "auto avvio" al fine di prevenire ad esempio la possibilità che un software venga automaticamente eseguito quando un dispositivo esterno (es. Storage USB) è connesso a un computer Adottare un personal firewall (o equivalente) su PC, laptop e altri dispositivi informatici di produttività personale o aziendale, bloccando le connessioni di rete non autorizzate Utilizzare protocolli di rete cifrati per la gestione remota dei server e dei dispositivi di rete (es. SSH, SSL) Impostare le utenze tecniche (application to application o machine to machine) in maniera tale che non ne sia possibile l'utilizzo interattivo da parte di utenti Attivare le funzionalità logging sui sistemi. In caso di trattamento di dati personali, occorre conformarsi a quanto previsto dalla normativa in materia. Configurare i sistemi in maniera tale che l'utente finale non possa modificare in autonomia le configurazioni impostate	

Tab. A4.4 - Aggiornamento dei sistemi

Descrizione secondo l modello Framework	I software presenti su tutti i computer e più in generale sui sistemi informatici possono contenere difetti ed errori, genericamente conosciuti come "vulnerabilità". Queste rappresentano degli elementi di debolezza intrinseci, sfruttabili da individui o gruppi di attaccanti, come anche da malware o altri programmi malevoli. Le vulnerabilità, dal momento della loro scoperta, fino al momento in cui sono eventualmente sfruttate, devono essere individuate e gestite attraverso opportune contromisure, come ad esempio l'installazione degli aggiornamenti rilasciati dai produttori software, proprio per risolvere una o più vulnerabilità. I produttori di software sono difatti responsabili per la fornitura di correzioni per le vulnerabilità identificate, nel più breve tempo possibile, in forma di aggiornamenti software, conosciuti anche come "Patch di sicurezza" e rilasciati ai clienti nell'ambito dei contratti di licenza. Per ridurre i rischi di compromissione di informazioni e sistemi informatici attraverso lo sfruttamento delle vulnerabilità del software, le aziende e organizzazioni devono gestire efficacemente tali processi di aggiornamento del software.	
Subcategory	RS.MI-3	**Livello rischio stimato: Lieve** del tipo R= PxG R=1*3
Controlli applicabili durante le fasi dell'audit	I software installati sui sistemi aziendali come computer, server, apparati di rete, dispositivi mobili, ecc. devono disporre della licenza del fornitore in modo da garantire la disponibilità di aggiornamenti di sicurezza o di aggiornamenti che comunque possano avere un impatto su di essa Le aziende devono individuare e ottenere Patch (inclusi aggiornamenti critici, service pack), quando resi disponibili per porre rimedio alle vulnerabilità scoperte, interagendo con i produttori di software o completando il recupero delle stesse dai siti web ufficiali o autorizzati da questi ultimi Gli aggiornamenti devono essere installati in modo tempestivo e,ove possibile, previa valutazione degli impatti, attraverso meccanismi che prevedano l'aggiornamento automatico degli stessi Il software non più supportato (cioè Out-of-Date) deve essere rimosso dai sistemi aziendali o sostituito con versioni più recenti (e per le quali il produttore rilascia gli aggiornamenti)	

Tab. A4.5 - Formazione di base del personale

Descrizione secondo l modello Framework	Gli utenti della scuola che interagiscono con i sistemi informatici rappresentano la principale fonte di rischio cyber. I comportamenti non consoni o errati possono vanificare le più sofisticate misure di sicurezza adottate dalla scuola. Per migliorare la consapevolezza degli utenti nell'utilizzo consono degli strumenti informatici e delle informazioni, la scuola deve prevedere specifici programmi di sensibilizzazione e formazione, volti a migliore la percezione dei rischi cyber e a promuovere l'utilizzo di comportamenti appropriati. Specifici programmi di sensibilizzazione e formazione devono essere rivolti a tutto il personale interno o esterno che accede, direttamente o indirettamente, ai sistemi informatici e alle informazioni dell'organizzazione. Tali programmi devono essere orientati a creare una cultura della sicurezza cyber, tale da prevenire comportamenti non consoni e ridurre di conseguenza l'esposizione ai rischi.	
Subcategory	PR.AT-1	**Livello rischio stimato: Lieve** del tipo R= PxG R=1*3
Controlli applicabili durante le fasi dell'audit	Pieno coinvolgimento e approvazione dei piani di formazione e sensibilizzazione del personale da parte dei vertici aziendali che ne comunicano l'importanza e ne monitorano il completamento Svolgimento di sessioni con cadenza almeno annuale mediante formazione in aula e/o ricorrendo all'utilizzo di piattaforme di e-learning Richiami alla cyber security integrati nelle attività quotidiane, mediante il ricorso a diverse tecniche e modalità di comunicazione (es. poster esplicativi negli uffici, e-mail di sensibilizzazione sui rischi e i comportamenti corretti, distribuzione di opuscoli specifici, sezioni dedicate su siti e portali interni). I temi trattati devono includere come minimo: (a) Principi di sicurezza (b) Utilizzo appropriato degli strumenti aziendali (PC, dispositivi mobili, ecc.) e rischi correlati al loro utilizzo improprio o non corretto (c) Comportamenti da tenere in caso di eventi sospetti (es. ricezione di mail sospette, comportamenti non usuali degli strumenti aziendali) o nel caso di incidenti di sicurezza (es. compromissioni di sistemi o supporti esterni) (d) Ruoli e responsabilità specifiche in tema di cyber security (e) Leggi o regolamenti applicabili e conseguenze in caso di violazione Formazione dedicata e specialistica per gli utenti dotati di privilegi di accesso elevati (es. Amministratori di sistemi informatici), volti ad accrescere e mantenere nel tempo aggiornate le competenze specifiche sui rischi cyber e sulle relative tecniche di protezione	

Tab. A4.6 - Backup & Restore

Descrizione secondo i modelli Framework e ABSC	La disponibilità delle informazioni e dei sistemi è essenziale per garantire l'operatività stessa di un'azienda nel mercato. Il controllo primario da attuare è rappresentato dal salvataggio delle informazioni di business e delle configurazioni dei sistemi, su supporti dedicati, da impiegare in caso di disastri, guasti o errori umani, favorendo il ripristino della normale operatività. Adottare procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità.	
Controlli applicabili durante le fasi dell'audit	Devono essere adottati adeguati meccanismi e strumenti finalizzati al salvataggio e ripristino di informazioni e dati Deve essere definita la tipologia (parziale o totale) e la frequenza di completamento dei salvataggi. Questa deve essere stabilita in base alle esigenze di business dell'organizzazione, i requisiti di sicurezza delle informazioni, gli obblighi di legge e la criticità delle informazioni, trattate rispetto al mantenimento delle attività operative Deve essere verificato periodicamente (es. attraverso attività di test) il buon esito delle attività di salvataggio e di ripristino di informazioni e dati I backup devono essere conservati in una sede remota, a una distanza sufficiente dalla sede principale, o avvalendosi di servizi cloud aventi analoga finalità, per evitare compromissioni in caso di eventi di disastro. Questi devono essere protetti con analoghe misure di carattere fisico e logico, rispetto a quelle adottate nelle sedi principali.	
Subcategory	a) PR.IP-4 b) PR.DS-1 PR.DS-6 c) PR.AC-2 PR.IP-4 PR.IP-5 PR.IP-9	**Livello rischio stimato: Lieve** del tipo R= PxG R=1*3
Controlli applicabili durante le fasi dell'audit	a) Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema. b) Assicurare la riservatezza delle informazioni contenute nelle copie di riserva mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud. c) Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	

A5. Gestione degli incidenti di sicurezza

Tab. A5.1- Risposta agli incidenti di sicurezza

Descrizione secondo l modello Framework	Nei casi in cui le misure di sicurezza non siano in grado o risultino limitatamente efficaci nella prevenzione di eventi avversi di sicurezza (es. compromissione di un sistema, accesso non autorizzato alle informazioni), l'organizzazione deve avere la capacità di rispondere rapidamente ed efficacemente a un potenziale incidente di sicurezza, riducendo gli impatti e limitando la possibilità di occorrenze future.	
Subcategory	RS.MI-1 RS.CO-2 RS.MI-2	**Livello rischio stimato: Lieve** del tipo R= PxG R=1*3
Controlli applicabili durante le fasi dell'audit	Descrivere e rendere note a tutto il personale interessato le prassi da adottare in caso di sospetta violazione o incidente di sicurezza (p. es., processo di gestione degli incidenti) Il processo di gestione degli incidenti deve definire come minimo: (a) Criteri generali da adottare per riconoscere e documentare un incidente (b) Tipologie di incidenti con relativa scala della severità, necessarie a effettuare una prima classificazione (c) Elenco dei referenti interni (es. responsabile Sistemi Informativi, responsabile Comunicazione, Responsabile legale, Direzione Aziendale) ed esterni (es. organi di Polizia Giudiziaria, fornitori esterni) da contattare in caso di incidente (d) Criteri di notifica degli incidenti ai diversi referenti e criteri di risposta, relativi ruoli e responsabilità, finalizzati a contenere gli impatti e/o mitigarne gli effetti in funzione di ciascuna tipologia e severità (e) Criteri, ruoli e responsabilità, procedure per il ripristino della situazione precedente al verificarsi dell'incidente	

Protezione dei dati personali

Descrizione secondo il modello ABSC	Processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti.	
Subcategory:	a) ID.RA-1 DE.CM-3 b) DE.CM-8 c) PR.MA-1 d) PR.IP-12 RS.MI-3 e) ID.RA-4 ID.RA-5 PR.IP-12 f) PR.IP-12	**Livello rischio stimato: Lieve** del tipo R= PxG R=1*3
Controlli applicabili durante le fasi dell'audit	a) Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazione delle vulnerabilità più critiche. b)Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza. c)Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.. Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli isolati, adottando le misure adeguate al loro livello di maturità d) Verificare che le vulnerabilità emesse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio. e) Definire un paino di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e delle tipologie degli apparati (per es. server esposti, server interni, PdL, portatili, ….) f)Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	

Capitolo 6
La privacy e la sicurezza informatica della scuola

Par. 1 – La privacy e la sicurezza informatica della scuola

Il Regolamento europeo è entrato in vigore nella primavera del 2016 e impone la piena conformità di tutte le organizzazioni privati e pubblici entro il prossimo 25 maggio del 2018.

Il Regolamento europeo prevale sulla legge nazionale e ciò non comporta l'automatica abrogazione della legge statale interna che regola la medesima materia.

Sebbene formalmente ancora vigente il d. lgs 196/2013, tutte quelle disposizioni della legge interna in contrasto con le nuove previsioni normative europee dovranno essere in ogni caso disapplicate, in favore della nuova disciplina.

Il considerando 10 del Regolamento generale sancisce che *"per quanto riguarda il trattamento dei dati personali per l'adempimento di un obbligo legale, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione delle norme del presente regolamento". E ancora "…il presente regolamento prevede anche un margine di manovra degli Stati membri per precisarne le norme, anche con riguardo al trattamento di categorie particolari di dati personali".*

Il d. lgs. 196/2003 non subisce dunque alcuna abrogazione diretta e, al contrario, mantiene la sua forza normativa e subisce tuttavia una **"rilettura in chiave Regolamento europeo".**
In base a ciò è opportuno eseguire il seguente bilanciamento:

a) Dove non vi è compatibilità tra quanto disposto dal Codice della Privacy e quanto previsto dal Regolamento europeo, il Codice lascia il passo alle nuove disposizioni europee: la legge statale deve essere disapplicata in favore del regolamento europeo;

b) Laddove vi sia compatibilità tra le due norme, il Codice rimane applicabile continuando a dettare legge, anche in maniera più specifica rispetto al Regolamento europeo.

Laddove il Codice della Privacy disciplini in maniera più dettagliata aspetti e ambiti che il Regolamento non approfondisce, occorre verificare se l'esistente normativa interna è in linea con gli scopi del nuovo Regolamento.

Il caso ora espresso trova applicazione nelle misure di sicurezza. Queste sono disciplinate in maniera molto approfondita dal Codice, al punto che l'allegato B del codice prevede un elenco di misure minime di sicurezza.

Il Regolamento europeo non parla di misure minime, ma si esprime solamente in termini di adeguatezza: l'art. 32 del Regolamento europeo recita infatti che *"Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, 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, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento".

Nonostante sia presente un elenco esemplificativo e non esaustivo di misure tecniche e organizzative di sicurezza, il Regolamento non effettua una tipizzazione puntuale come quella dell'allegato B del Codice: tale scelta è in linea con il **principio di responsabilizzazione** su cui si basa l'intero Regolamento. Titolare e responsabile del trattamento devono responsabilizzarsi e mettere in atto misure di sicurezza adeguate alla realtà dell'istituzione scolastica.

Il Framework Nazionale è implementato in maniera conforme al panorama normativo italiano e, in particolar modo, alle disposizioni del Codice. In tal senso, la Subcategory "ID.GV-3: I requisiti legali in materia di cyber security, con l'inclusione degli obblighi riguardanti la privacy e le libertà civili, sono compresi e gestiti" prevede che tutta la normativa in vigore in termini di cyber security e protezione dei dati personali sia identificata e analizzata in accordo al tipo di attività svolto dall'organizzazione e al tipo di dati trattati. In linea generale, il Codice individua quali titolari del trattamento: "la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e obblighi:
- di sicurezza (artt. 31-34);
- e di comunicazione (artt. 19-22, 25-27, 32, 32-bis e 39).

Di seguito saranno descritti tali obblighi e la relazione con le Subcategory del Framework che questi implicano per i soggetti individuati.

- Obblighi di sicurezza

Gli obblighi di sicurezza, relativi ai dati personali oggetto del trattamento, sono declinati all'articolo 31 del Codice, il quale impone che questi siano "custoditi e controllati [...] 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". Alcuni di questi obblighi sono esplicitati nell'articolo 34 e nell'allegato tecnico di riferimento B sotto forma di misure minime di sicurezza (intese come "il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta").
Tali misure comprendono:

a) autenticazione informatica;

b) adozione di procedure di gestione delle credenziali di autenticazione;

c) utilizzazione di un sistema di autorizzazione;

d) aggiornamento periodico (almeno annuale) dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;

e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici (strumenti elettronici da aggiornare almeno ogni 6 mesi; gli aggiornamenti dei programmi volti a prevenire la vulnerabilità dei sistemi elettronici almeno annualmente);

f) adozione di procedure per la custodia di copie di sicurezza (salvataggio dei dati almeno settimanale), il ripristino della disponibilità dei dati e dei sistemi (entro 7 giorni);

g) adozione di procedure per la gestione e l'uso di supporti rimovibili;

h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Tali disposizioni fanno si che cinque Subcategory del Framework proposto siano da considerarsi obbligatorie per quelle organizzazioni che trattano dati personali mediante strumenti elettronici.
Tali Subcategory sono:

- PR.DS-1: I dati e le informazioni memorizzate sono protette;
- PR.IP-9: Sono attivi e amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro;
- PR.PT-2: I supporti di memorizzazione removibili sono protetti e il loro uso è ristretto in accordo alle policy;
- PR.PT-3: L'accesso alle risorse e ai sistemi è limitato secondo il principio di minima funzionalità
- PR.AC-2: L'accesso fisico alle risorse è protetto e amministrato.

L'esplicitazione delle misure minime di cui sopra non riduce, a ogni modo, l'importanza degli obblighi più generali di sicurezza a cui devono attenersi i titolari del trattamento di dati personali, ai sensi dell'articolo 31 del Codice. Questi ultimi sono, infatti, responsabili in sede giudiziaria (a norma dell'articolo 2050 del Codice Civile, in materia di responsabilità per l'esercizio di attività pericolose) di eventuali danni causati da violazioni del predetto articolo 31 e per sottrarsi alla pena del risarcimento, sono tenuti a dimostrare il rispetto degli obblighi di sicurezza, in virtù del principio dell'inversione dell'onere della prova.

- Gli obblighi di comunicazione

Gli obblighi di comunicazione variano a seconda del titolare del trattamento e della tipologia del dato personale oggetto del trattamento stesso.
Nello specifico:

- per soggetti pubblici (esclusi gli enti pubblici economici) e per dati non sensibili e giudiziari (artt. 19 e 39):

– la comunicazione da parte di un soggetto pubblico ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento. In mancanza di tale norma la comunicazione è ammessa in qualunque forma quando è comunque necessaria per lo svolgimento di funzioni istituzionali, previa comunicazione al Garante. Il conseguente trattamento dei dati può iniziare se è decorso il termine

di 45 giorni dall'invio della comunicazione al Garante (salvo sua diversa determinazione anche successiva);

– la comunicazione da parte di un soggetto pubblico a privati o a enti pubblici economici e la diffusione da parte di un soggetto pubblico sono ammesse unicamente quando sono previste da una norma di legge o di regolamento.

- per soggetti pubblici (esclusi gli enti pubblici economici) e per dati sensibili e giudiziari (artt. 20-22):

– il trattamento dei dati sensibili e giudiziari da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge o provvedimento del Garante;

– i dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità;

– i dati idonei a rivelare lo stato di salute non possono essere diffusi. In ogni caso, la diffusione dei dati sensibili e giudiziari è ammessa solo se prevista da espressa disposizione di legge.

- per privati ed enti pubblici economici (artt. 25-27):

– è fatta salva la comunicazione o diffusione di dati richieste, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici, per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati;

– i dati sensibili possono essere oggetto di trattamento con o senza il consenso scritto dell'interessato e previa autorizzazione del Garante. I dati idonei a rivelare lo stato di salute non possono essere diffusi;

- il trattamento di dati giudiziari da parte di privati o di enti pubblici economici è consentito soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili.

Ciò implica che nel Framework proposto, le Subcategory relative alla comunicazione siano da considerarsi ad alta priorità per le categorie di soggetti e le tipologie di dati trattati di cui sopra, indipendentemente da quanto indicato nella contestualizzazione che tali soggetti hanno preso come riferimento. Le pratiche in oggetto sono:

- DE.DP-4: L'informazione relativa agli eventi rilevati è comunicata a tutte le parti interessate;
- RC.CO-1: A seguito di un incidente vengono gestite le pubbliche relazioni;
- RS.CO-2: Sono stabiliti dei criteri per documentare gli incidenti/eventi;
- RS.CO-3: Le informazioni sono condivise in maniera coerente con il piano di risposta;
- RS.CO-4: Il coordinamento con le parti interessate dell'organizzazione avviene in coerenza con i piani di risposta;
- RS.CO-5: È attuata una condivisione spontanea delle informazioni con le parti interessate esterne all'organizzazione (information sharing) per ottenere una maggior consapevolezza della situazione (c.d. situational awareness).

- Il monitoraggio dell'attività del personale

Prima della riforma introdotta dal "Jobs Act", l'articolo 4, comma 1 dello Statuto dei lavoratori sanciva il divieto di utilizzo di "impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori". Il decreto legislativo di riforma n. 151/2015 ha modificato tale disposizione, in linea con le pronunce del Garante in merito, sancendo che "gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali". Tali disposizioni vanno tenute in debito conto nell'implementazione della Subcategory

- DE.CM-3: Viene svolto il monitoraggio del personale per rilevare potenziali eventi di cyber security.

- Informazioni classificate e segreto di Stato

Il Decreto del Presidente del Consiglio dei Ministri 6 novembre 2015, comprendente la "Disciplina della firma digitale dei documenti classificati" (Decreto n. 4/2015) e le "Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva" (Decreto n. 5/2015), introduce nuovi elementi per la tutela di tali documenti, alla luce dei rischi cibernetici e in relazione alle necessità di protezione dei dati personali. Ne consegue che le disposizioni contenute in questi atti vadano tenute in debito conto, da parte di tutti i soggetti pubblici e privati che gestiscono in via informatizzata questioni coperte da segreto di Stato e informazioni classificate, nell'implementazione delle seguenti Subcategory:

ID.GV-1: È identificata e resa nota una policy di sicurezza delle informazioni;
ID.GV-3: I requisiti legali in materia di cyber security, con l'inclusione degli obblighi riguardanti la privacy e le libertà civili, sono compresi e gestiti;
PR.AC-1: Le identità digitali e le credenziali di accesso per gli utenti e per i dispositivi autorizzati sono amministrate;
PR.AC-3: L'accesso remoto alle risorse è amministrato;
PR.DS-1: I dati e le informazioni memorizzate sono protette.

Par. 2 – Utilizzo dei servizi in cloud computing

Con il termine cloud computer, o semplicemente cloud, ci si riferisce ad un insieme di tecnologie e di modalità di fruizione di servizi informatici che favoriscono l'utilizzo e l'erogazione di software, la possibilità di conservare e di elaborare grandi quantità di informazioni via Internet.

Il cloud offre, a seconda dei casi, il trasferimento della conservazione o dell'elaborazione dei dati dai computer degli utenti ai sistemi del fornitore.

Il cloud consente, inoltre, di usufruire di servizi complessi senza doversi necessariamente dotare né di computer e altri hardware avanzati, né di personale in grado di programmare o gestire il sistema.

Tutto può essere demandato all'esterno, in *outsourcing*, e a un costo potenzialmente limitato, in quanto le risorse informatiche necessarie per i servizi richiesti possono essere condivise con altri soggetti che hanno le stesse esigenze.

Le soluzioni offerte dal cloud generalmente possono essere più flessibili, efficienti, adattabili ed economiche più di quelle sviluppate *in-house*. Ma possono comportare il rischio di una potenziale perdita di controllo sui propri dati.

Spesso utilizziamo tecnologie cloud senza neppure saperlo. Alcuni dei più diffusi servizi di posta elettronica o di elaborazione testi sono in cloud cioè "sulle nuvole". Anche molte delle funzioni offerte dai cellulari di nuova generazione (i cosiddetti smartphone) sono basate sul cloud: ad esempio quelle che sfruttano la geolocalizzazione consigliandoci i locali o gli esercizi commerciali più vicini, che consentono di ascoltare musica o di accedere a giochi on line, nonché tante altre funzioni e "*app*"(applicazioni).

I cloud sono di diversi tipi:

1. **Private Cloud -** La "nuvola privata" è una infrastruttura informatica (rete di computer collegati per offrire servizi) per lo più dedicata alle esigenze di una singola organizzazione, ubicata nei suoi locali o anche affidata in gestione ad un terzo (nella tradizionale forma dell'hosting dei server), nei confronti del quale il titolare dei dati può esercitare un controllo puntuale. Le "nuvole private" possono essere paragonate ai tradizionali "data center" nei quali, però, sono usati degli accorgimenti tecnologici che permettono di ottimizzare l'utilizzo delle risorse disponibili e di potenziarle agevolmente in caso di necessità.
2. **Public Cloud -** Nel caso della "nuvola pubblica", l'infrastruttura è di proprietà di un fornitore specializzato nell'erogazione di servizi che mette a disposizione di utenti, aziende o amministrazioni i propri sistemi attraverso la condivisione e l'erogazione via Internet di applicazioni informatiche, di capacità elaborativa e di "stoccaggio" dati. La fruizione di tali servizi avviene tramite la rete Internet e implica il trasferimento dei soli dati o anche dell'attività di elaborazione presso i sistemi del fornitore del servizio, il quale assume un ruolo importante in ordine all'efficacia delle misure adottate per garantire la protezione delle informazioni che gli sono state affidate. Con il cloud pubblico l'utente insieme ai dati, infatti, cede una parte importante del controllo esercitabile su di essi.
3. **Altre "nuvole".** Esistono altri tipi di cloud con caratteristiche miste, - quali i cloud ibridi (*hybrid cloud*) - caratterizzati da soluzioni che prevedono l'utilizzo di servizi erogati da infrastrutture private accanto a servizi acquisiti da cloud pubblici - e i cloud di gruppo (*community cloud*), in cui l'infrastruttura è condivisa da diverse organizzazioni a beneficio di una specifica comunità di utenti.

I tre modelli di servizi cloud più presenti sono:

1) Cloud Infrastructure as a Service – IaaS (Infrastruttura cloud resa disponibile come servizio).
Il fornitore del servizio cloud offre, secondo un modello detto "a consumo", gli strumenti hardware e software di base (spazi di memoria, sistemi operativi, programmi di virtualizzazione…), cioè server virtuali remoti che l'utente finale può utilizzare in sostituzione o in affiancamento ai sistemi già presenti nei locali dell'azienda o dell'amministrazione. Tali fornitori sono in genere operatori di mercato specializzati, che dispongono di un'infrastruttura tecnologica, complessa e spesso distribuita in aree geografiche diverse.
Il presente modello prevede che il servizio offerto consista in una infrastruttura con capacità computazionale, di memorizzazione, e di rete, sulla quale l'utente possa installare ed eseguire il software a lui necessario, dal sistema operativo alle applicazioni. L'utente può richiedere al fornitore di servizi un insieme di macchine virtuali sulle quali può, direttamente o tramite lo stesso fornitore, installare i sistemi operativi ed i software necessari alle sue necessità.

2) Cloud Software as a Service – SaaS (Software erogato come servizio del cloud).
Il fornitore eroga via Internet una serie di servizi applicativi ponendoli a disposizione degli utenti finali. Si pensi, ad esempio, ad applicazioni comunemente usate negli uffici erogate in modalità web quali l'elaborazione di fogli di calcolo o di testi, la gestione del protocollo e delle regole per l'accesso informatico ai documenti, la rubrica dei contatti e i calendari condivisi, ma anche ai più avanzati servizi di posta elettronica.

3) Cloud Platform as a Service – PaaS (Piattaforme software fornite via Internet come servizio).
Il fornitore offre soluzioni evolute di sviluppo software che rispondono alle specifiche esigenze del cliente.
In genere questo tipo di servizi è rivolto a operatori di mercato che li utilizzano per sviluppare e ospitare soluzioni applicative proprie (ad esempio applicativi per la gestione finanziaria, della contabilità o della logistica), allo scopo di assolvere a esigenze interne, oppure per fornire a loro volta servizi a terzi. Anche nel caso dei PaaS, il servizio erogato dal fornitore limita la necessità per il fruitore di doversi dotare internamente di strumenti hardware o software specifici o aggiuntivi.

Da quanto precede, pertanto, si evince che è opportuno scegliere bene il tipo di cloud e il modello di servizio più adatto alle proprie esigenze. In particolare se si decide di adottare il public cloud, dove quasi tutto il processo viene esternalizzato e i "nostri" dati più preziosi sono dislocati "lontano" dal nostro controllo diretto. Il concetto di cloud può apparire evanescente, "virtuale".
In realtà, con le sue tecnologie si possono gestire servizi estremamente concreti, quali la distribuzione dei prodotti di un'azienda, i servizi dell'anagrafe di un Comune, le prenotazioni e le analisi mediche, il conto bancario on line e tanto altro. Nessuno lascerebbe in deposito il proprio portafoglio con i documenti e lo stipendio alla prima persona incontrata al mercato. Né affiderebbe il proprio libro mastro o i contratti stipulati con clienti e fornitori a un commercialista sconosciuto che gli promette di risparmiare, senza prima essersi accertato su come saranno conservati o utilizzati documenti così preziosi. La voce "risparmio" non deve quindi essere l'unico fattore di scelta.
I grandi fornitori globali di cloud computing si contano sulle dita di una mano. Quasi tutte le altre società che offrono servizi e infrastrutture tra le "nuvole" si avvalgono infatti delle aziende leader mondiali. Questa situazione riduce di molto la capacità negoziale di una singola impresa o di una piccola

amministrazione pubblica, rendendo difficile trasformare la flessibilità tecnologica in flessibilità contrattuale. In questi casi la scelta di consorziarsi con altri soggetti pubblici o imprese che hanno le medesime esigenze (ad es. tramite le associazioni di categoria) potrebbe garantire una capacità contrattuale maggiore. Prima di optare per un certo tipo di "nuvola", è comunque opportuno che l'utente verifichi la quantità e la tipologia di dati che intende esternalizzare (ad esempio dati personali, in particolare quelli sensibili, oppure dati critici per la propria attività, come progetti riservati o coperti da brevetto o segreto industriale), valutando gli eventuali rischi e le possibili conseguenze derivanti da tale scelta. È vero che il cliente spesso non ha capacità di negoziare una riformulazione dei termini in uso proposti da chi offre i servizi: può però scegliere tra differenti provider. Anche i fornitori cloud, comunque, potrebbero trarre nuove opportunità dalla definizione di clausole "pro-privacy" o da una eventuale preventiva certificazione indipendente sul rispetto della normativa europea sulla protezione dei dati personali per i servizi da loro offerti. La risposta ad alcune domande può aiutare a sviluppare una corretta analisi dell'impatto economico e organizzativo di queste tecnologie all'interno di un'impresa o di una pubblica amministrazione.

Obblighi del Cloud provider alla custodia dei dati

La possibilità di conservare i dati in luoghi geografici differenti, pone problemi attinenti sia sulla normativa applicabile in caso di contenzioso fra utente e fornitore, sia in relazione alle disposizioni nazionali che disciplinano il trattamento, l'archiviazione e la sicurezza dei dati.

Qualora il Cloud provider abbia avuto la titolarità dei dati ricevuti dalla scuola ed abbia stabilimento in Italia, sarà tenuto anche al rispetto delle misure di sicurezza di cui al d. lgs. 196/2003.

Il rapporto diviene più complesso qualora il Cloud provider e l'utilizzatore si trovano in luoghi e nazioni diverse. In primo luogo si deve vedere se c'è l'autorizzazione dell'utente a spostare e frammentare i dati anche al di fuori dell'ordinamento originario. In secondo luogo se, pur avendo l'autorizzazione, i dati possono essere effettivamente trasferiti.

L'adozione da parte del fornitore del servizio di tecnologie proprie può, in taluni casi, rendere complessa per l'utente la transizione di dati e documenti da un sistema Cloud all'altro o lo scambio di informazioni con soggetti che utilizzino servizi Cloud di fornitori differenti, ponendone quindi a rischio la portabilità e l'interoperabilità dei dati. Il servizio virtuale potrebbe, inoltre, in assenza di adeguate garanzie in merito alla qualità della connettività di rete, risultare degradato in presenza di elevati picchi di traffico o addirittura indisponibile laddove si verifichino eventi anomali quali, ad esempio, guasti, impedendo l'accessibilità temporanea ai dati in esso conservati.

Inoltre gli obblighi di conservazione non riguardano tutti i dati conferiti per la memorizzazione, ma esclusivamente i dati classificati come "dati personali". A tal fine, i dati che possono essere gestiti tramite *Privacy policy* e consenso al trattamento sono dei dati che consentono di identificare il rispettivo titolare o altri individui.

Il sistema di autorizzazioni e consensi, seppur necessario per legge, non è sufficiente ad autorizzare il Cloud provider alla complessiva e completa gestione di una universalità di dati depositati in Cloud in assenza di ulteriori previsioni contrattuali.

Obblighi del Cloud provider alla sicurezza dei dati

Il fornitore del servizio di Cloud assume, pertanto, la responsabilità di preservare

- la riservatezza,
- l'integrità,
- la disponibilità dei dati,
- assicurare la portabilità e l'interoperbilità tra cloud diversi

Tali obblighi sono, però, commisurati al tipo di servizio offerto ed al regime contrattuale adottato.

In particolare il garante Privacy ha stabilito che: "*i trattamenti di dati personali richiedono, infatti, una ponderazione dei rischi legati alla sicurezza ed alla fruibilità delle informazioni. Pertanto, vanno tenute in debito conto le particolari caratteristiche delle nuove tecnologie, allo scopo di governare i potenziali pericoli che possono derivare da utilizzi scarsamente consapevoli e da modelli innovativi adottati con metodi, prassi e processi non ancora sufficientemente consolidati e in grado di mitigare le eventuali criticità. È quindi opportuno, anche nei casi di Cloud computing, razionalizzarne le peculiarità al fine di individuare i potenziali rischi insiti in tali servizi e quindi poter adottare efficaci e specifiche misure di prevenzione. Nel caso del Cloud computing, il trasferimento dei dati dai computer locali, nella fisica disponibilità e nel diretto controllo esercitabile dal titolare, verso sistemi remoti di proprietà di un terzo fornitore del servizio, presenta, accanto a potenziali utilità, anche i seguenti aspetti che necessitano di specifica attenzione […]*"

Il Garante, tra gli aspetti critici legati alla sicurezza dei dati personali, individua quelli che necessitano di specifica attenzione. In particolare, l'utente affida i dati ai sistemi di un fornitore remoto, perdendone il controllo diretto ed esclusivo, affidando la riservatezza e la disponibilità delle informazioni allocate sulla nuvola ai meccanismi di sicurezza adottati dal service provider. I dati personali potrebbero, inoltre, passare per una catena di trasformazione dei servizi acquisiti presso altri service provider, diversi dal fornitore con cui l'utente ha stipulato il contratto, col rischio di non sapere quale dei gestori intermedi possa accedere ai dati.

In particolare, il Codice Privacy prevede espressamente che "*i dati personali oggetto di trattamento sono 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*".

L'utilizzo delle misure idonee è obbligatorio nel Cloud poiché il trattamento dei dati personali avviene con sistema telematico. Per questo motivo, il Codice Privacy, individua alcune misure idonee la cui adozione è obbligatoria e presidiata da apposite sanzioni:

- autenticazione informatica;
- adozione di procedure di gestione delle credenziali di autenticazione;
- utilizzazione di un sistema di autorizzazione;

- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli autorizzati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Sono, inoltre, previsti una serie di obblighi in capo al Cloud provider per quanto riguarda il materiale allocato sulla nuvola e per tutti gli utilizzi del servizio quanto alla responsabilità civile e penale per eventuali danni o illeciti e ciò sulla base sia delle ordinarie norme civilistiche che delle norme del d. lgs. 70/2003 di attuazione della Direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione.

Infine è bene ricordare che la migliore sicurezza deriva dallo stesso fruitore del sistema. Sarebbe buona prassi, infatti, pretendere da coloro che accedono ai dati tramite il Cloud, di utilizzare password più robuste di quelle minime previste dal Codice secondo le quali "*le password devono essere composte da almeno 8 caratteri alfanumerici con l'utilizzo di alcuni caratteri speciali* ".

Tali requisiti minimi, non appaiono al passo coi tempi, poiché i calcolatori attuali sarebbero in grado di forzare in poco tempo una password con tali caratteristiche, vista la loro potente capacità di calcolo.

CAPITOLO 7
Interessato e i suoi diritti

Par. 1 – L'Interessato e i suoi diritti

Definendo "l'interessato" come la persona fisica cui si riferiscono i dati personali", ragioniamo attorno ai diritti dell'interessato.

La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. La Carta dei diritti fondamentali dell'Unione europea e il trattato sul funzionamento dell'Unione europea stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

I principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali devono rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza. Il regolamento è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche.

Se, nel corso di attività elettorali, il funzionamento del sistema democratico presuppone, in uno Stato membro, che i partiti politici raccolgano dati personali sulle opinioni politiche delle persone, può esserne consentito il trattamento di tali dati per motivi di interesse pubblico, purché siano predisposte garanzie adeguate.

Il titolare del trattamento, se i dati personali che tratta non gli consentono di identificare una persona fisica, non deve essere obbligato ad acquisire ulteriori informazioni per identificare l'interessato al solo fine di rispettare una disposizione del regolamento. Tuttavia, il titolare del trattamento non deve rifiutare le ulteriori informazioni fornite dall'interessato al fine di sostenere l'esercizio dei suoi diritti. L'identificazione include l'identificazione digitale di un interessato, ad esempio mediante un meccanismo di autenticazione quali le stesse credenziali, utilizzate dall'interessato per l'accesso (login) al servizio on line offerto dal titolare del trattamento.

Il principio della trasparenza impone che le informazioni destinate al pubblico o all'interessato siano concise, facilmente accessibili e di facile comprensione e che sia usato un linguaggio semplice e chiaro.
Tali informazioni potrebbero essere fornite in formato elettronico, ad esempio, se destinate al pubblico, attraverso un sito web. Ciò è particolarmente utile in situazioni in cui la molteplicità degli operatori coinvolti e la complessità tecnologica dell'operazione fanno sì che sia difficile per l'interessato comprendere se, da chi e per quali finalità sono raccolti dati personali che lo riguardano, quali la pubblicità online.
Dato che i minori meritano una protezione specifica, quando il trattamento dati li riguarda, qualsiasi informazione e comunicazione deve utilizzare un linguaggio semplice e chiaro che un minore possa capire facilmente.

È opportuno prevedere modalità volte ad agevolare l'esercizio, da parte dell'interessato, dei diritti di cui al regolamento, compresi i meccanismi per richiedere e, se del caso, ottenere gratuitamente, in particolare

l'accesso ai dati, la loro rettifica e cancellazione e per esercitare il diritto di opposizione. Il titolare del trattamento deve predisporre anche i mezzi per inoltrare le richieste per via elettronica, in particolare qualora i dati personali siano trattati con mezzi elettronici. Il titolare del trattamento è tenuto a rispondere alle richieste dell'interessato senza ingiustificato ritardo e al più tardi entro 1 mese estendibile fino a 3 mesi in casi di particolare complessità. Il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso negativo, motivando il suo eventuale diniego. La risposta fornita all'interessato deve essere intelligibile, concisa, trasparente e facilmente accessibile, oltre ad utilizzare un linguaggio semplice e chiaro.

Spetta al titolare valutare la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato, ma soltanto se si tratta di richieste manifestamente infondate o eccessive (anche ripetitive). Il diritto di accesso prevede, in ogni caso, il diritto di ricevere una copia dei dati personali oggetto di richiesta. Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; può essere dato oralmente solo se così richiede l'interessato.

Un interessato deve avere il diritto di accedere ai dati personali raccolti che lo riguardano e di esercitare tale diritto facilmente e a intervalli ragionevoli, per essere consapevole del trattamento e verificarne la liceità. Ciò include il diritto di accedere ai dati relativi alla salute, ad esempio le cartelle mediche contenenti informazioni quali diagnosi, risultati di esami, pareri di medici curanti o eventuali terapie o interventi praticati. Ogni interessato deve pertanto avere il diritto di conoscere e ottenere comunicazioni in relazione alla finalità per cui i dati personali sono trattati, ove possibile al periodo in cui i dati personali sono trattati, ai destinatari dei dati personali, alla logica cui risponde qualsiasi trattamento automatizzato dei dati e, almeno quando è basato sulla profilazione, alle possibili conseguenze di tale trattamento.
Ove possibile, il titolare del trattamento deve poter fornire l'accesso remoto a un sistema sicuro che consenta all'interessato di consultare direttamente i propri dati personali. Tuttavia, tali considerazioni non dovrebbero condurre a un diniego a fornire all'interessato tutte le informazioni. Se il titolare del trattamento tratta una notevole quantità d'informazioni riguardanti l'interessato, il titolare in questione deve poter richiedere che l'interessato precisi, prima che siano fornite le informazioni, l'informazione o le attività di trattamento cui la richiesta si riferisce.

Il titolare del trattamento deve adottare tutte le misure ragionevoli per verificare l'identità di un interessato che chieda l'accesso, in particolare, nel contesto di servizi online e di identificativi online. Il titolare del trattamento non deve conservare dati personali al solo scopo di poter rispondere a potenziali richieste.

Un interessato deve conoscere di esercitare il diritto di ottenere la rettifica dei dati personali che lo riguardano e il «diritto all'oblio» se la conservazione di tali dati violi il regolamento o il diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento. In particolare, l'interessato deve esercitare il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati, quando abbia ritirato il proprio consenso o si sia opposto al trattamento dei dati personali che lo riguardano o quando il trattamento dei suoi dati personali non sia altrimenti conforme al regolamento.
Tale diritto è in particolare rilevante se l'interessato ha prestato il proprio consenso quando era minore, e quindi non pienamente consapevole dei rischi derivanti dal trattamento, e vuole successivamente eliminare tale tipo di dati personali, in particolare da internet.

L'interessato deve poter esercitare tale diritto indipendentemente dal fatto che non sia più un minore. Tuttavia, deve essere lecita l'ulteriore conservazione dei dati personali qualora sia necessaria per esercitare il diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale, per eseguire un compito di interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, per motivi di interesse pubblico nel settore della sanità pubblica, a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, ovvero per accertare, esercitare o difendere un diritto in sede giudiziaria.

Per rafforzare il «diritto all'oblio» nell'ambiente online, è opportuno che il diritto di cancellazione sia esteso in modo tale da obbligare il titolare del trattamento che ha pubblicato dati personali a informare i titolari del trattamento che trattano tali dati personali di cancellare qualsiasi link verso tali dati personali o copia o riproduzione di detti dati personali. Nel fare ciò, è opportuno che il titolare del trattamento adotti misure ragionevoli tenendo conto della tecnologia disponibile e dei mezzi a disposizione del titolare del trattamento, comprese misure tecniche, per informare della richiesta dell'interessato i titolari del trattamento che trattano i dati personali.

Le modalità per limitare il trattamento dei dati personali potrebbero consistere, tra l'altro, nel trasferire temporaneamente i dati selezionati verso un altro sistema di trattamento, nel rendere i dati personali selezionati inaccessibili agli utenti o nel rimuovere temporaneamente i dati pubblicati da un sito web. Negli archivi automatizzati, la limitazione del trattamento dei dati personali dovrebbe in linea di massima essere assicurata mediante dispositivi tecnici in modo tale che i dati personali non siano sottoposti a ulteriori trattamenti e non possano più essere modificati. Il sistema dovrebbe indicare chiaramente che il trattamento dei dati personali è stato limitato.

Per rafforzare ulteriormente il controllo sui propri dati è opportuno anche che l'interessato abbia il diritto, qualora i dati personali siano trattati con mezzi automatizzati, di ricevere in un formato strutturato, di uso comune, leggibile da dispositivo automatico e interoperabile i dati personali che lo riguardano che abbia fornito a un titolare del trattamento e di trasmetterli a un altro titolare del trattamento. È opportuno incoraggiare i titolari del trattamento a sviluppare formati interoperabili che consentano la portabilità dei dati. Tale diritto dovrebbe applicarsi qualora l'interessato abbia fornito i dati personali sulla base del proprio consenso o se il trattamento è necessario per l'esecuzione di un contratto. Non dovrebbe applicarsi qualora il trattamento si basi su un fondamento giuridico diverso dal consenso o contratto. Per sua stessa natura, tale diritto non dovrebbe essere esercitato nei confronti dei titolari del trattamento che trattano dati personali nell'esercizio delle loro funzioni pubbliche. Non dovrebbe pertanto applicarsi quando il trattamento dei dati personali è necessario per l'adempimento di un obbligo legale cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Il diritto dell'interessato di trasmettere o ricevere dati personali che lo riguardano non dovrebbe comportare l'obbligo per i titolari del trattamento di adottare o mantenere sistemi di trattamento tecnicamente compatibili. Qualora un certo insieme di dati personali riguardi più di un interessato, il diritto di ricevere i dati personali non deve pregiudicare i diritti e le libertà degli altri interessati in ottemperanza del presente regolamento. Inoltre tale diritto non dovrebbe pregiudicare il diritto dell'interessato di ottenere la cancellazione dei dati personali e le limitazioni di tale diritto di cui al presente regolamento e non dovrebbe segnatamente implicare la cancellazione dei dati personali riguardanti l'interessato forniti da quest'ultimo per l'esecuzione di un contratto, nella misura in cui e fintantoché i dati personali siano necessari

all'esecuzione di tale contratto. Ove tecnicamente fattibile, l'interessato dovrebbe avere il diritto di ottenere che i dati personali siano trasmessi direttamente da un titolare del trattamento a un altro.

Qualora i dati personali possano essere lecitamente trattati, essendo il trattamento necessario per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, ovvero per i legittimi interessi di un titolare del trattamento o di terzi, l'interessato deve comunque avere il diritto di opporsi al trattamento dei dati personali che riguardano la sua situazione particolare. È opportuno sapere che incombe al titolare del trattamento dimostrare che i suoi interessi legittimi obbligatori prevalgono sugli interessi o sui diritti e sulle libertà fondamentali dell'interessato.

Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato dovrebbe avere il diritto, in qualsiasi momento e gratuitamente, di opporsi a tale trattamento, sia con riguardo a quello iniziale o ulteriore, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto. Tale diritto deve essere esplicitamente portato all'attenzione dell'interessato e presentato chiaramente e separatamente da qualsiasi altra informazione.

L'interessato deve avere il diritto di non essere sottoposto a una decisione, che possa includere una misura, che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona, quali il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani. Tale trattamento comprende la «profilazione», che consiste in una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere 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, ove ciò produca effetti giuridici che la riguardano o incida in modo analogo significativamente sulla sua persona.
Tuttavia, è opportuno che sia consentito adottare decisioni sulla base di tale trattamento, compresa la profilazione, se ciò è espressamente previsto dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento, anche a fini di monitoraggio e prevenzione delle frodi e dell'evasione fiscale secondo i regolamenti, le norme e le raccomandazioni delle istituzioni dell'Unione o degli organismi nazionali di vigilanza e a garanzia della sicurezza e dell'affidabilità di un servizio fornito dal titolare del trattamento, o se è necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento, o se l'interessato ha espresso il proprio consenso esplicito. In ogni caso, tale trattamento dovrebbe essere subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione. Tale misura non dovrebbe riguardare un minore.

Al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli

interessi e i diritti dell'interessato e che impedisca tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero che comportano misure aventi tali effetti. Il processo decisionale automatizzato e la profilazione basati su categorie particolari di dati personali dovrebbero essere consentiti solo a determinate condizioni.

Par. 2 – L'Informativa e il consenso

Abbiamo voluto riservare per ultimo il diritto fondante dei diritti dell'interessato, la

INFORMATIVA

I contenuti dell'informativa intesa come il diritto principale sono elencati **in modo tassativo** negli articoli 13 e 14 del regolamento.

In particolare, il titolare **DEVE SEMPRE** consegnare e specificare nell'informativa:

- I dati di contatto del Responsabile della protezione dei dati (RPD);
- Il nominativo di almeno un responsabile del trattamento dei dati;
- Le finalità del trattamento;
- La categoria degli interessati;
- I destinatari dei dati;
- Il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione;
- La base giuridica del trattamento, qual è il suo interesse legittimo se quest'ultimo costituisce la base giuridica del trattamento, nonché se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo; sono state inserite specifiche clausole contrattuali modello, ecc.).;
- Le modalità di presentazione un reclamo all'autorità di controllo;
- I comportamenti di processi decisionali automatizzati (anche la **profilazione**), specificando anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

Tempi e modelli dell'informativa

Nel caso di dati personali non raccolti direttamente presso l'interessato, l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure al momento della comunicazione **(**NON della registrazione) dei dati a terzi o all'interessato**.**

L'informativa deve avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile; occorre utilizzare un linguaggio chiaro e semplice, e per i minori occorre prevedere informative idonee. L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico se destinate al pubblico, attraverso un sito web, anche se sono ammessi "altri canali". Può essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui all'art. 12, paragrafo 1 del regolamento.

Il regolamento ammette, soprattutto, l'utilizzo di icone per presentare i contenuti dell'informativa in forma sintetica, ma solo "in combinazione" con l'informativa estesa (art. 12, paragrafo 7 del regolamento). Queste icone dovranno essere identiche in tutta l'Unione europea.

Informativa in forma sintetica

(ai sensi dell'art. 7, paragrafo 7)

	La **raccolta** di dati personali è limitata al **minimo** necessario per ogni specifica finalità del trattamento	
	La **memorizzazione** di dati personali è limitata al **minimo** necessario per ogni specifica finalità del trattamento	
	Il **trattamento** di dati personali è limitato alle finalità per le quali sono stati raccolti	
	Non sono forniti dati personali a terze parti commerciali	
	Non sono effettuati la vendita e l'affitto di dati personali	
	La comunicazione di dati personali avviene nel rispetto delle normative vigenti	
	I dati personali non sono memorizzati in forma **non cifrata**	
	Sono **minimizzati** i tempi di conservazione delle immagini	

Sono inoltre parzialmente diversi (rispetto quanto precisato nel Codice) i requisiti che il regolamento fissa per l'esonero dall'informativa, anche se occorre sottolineare che spetta al titolare, in caso di dati personali raccolti da fonti diverse dall'interessato, valutare se la prestazione dell'informativa agli interessati comporti uno sforzo sproporzionato del Codice.

Consenso

Perché sia lecito, il trattamento di dati personali dovrebbe fondarsi sul consenso dell'interessato o su altra base legittima prevista per legge dal regolamento o dal diritto dell'Unione o degli Stati membri, come indicato nello stesso regolamento.

Pertanto i soggetti pubblici, in ambito scolastico, non devono richiedere il consenso all'interessato ai sensi dell'art. 18 c. 4 del Codice in ordine al trattamento di dati comuni.

Il trattamento di dati sensibili e giudiziari, invece, è consentito anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente, fermo restando che il trattamento sia necessario per lo svolgimento delle funzioni istituzionali.

La tipologia dei dati sensibili e giudiziari, le operazioni eseguibili e le finalità di rilevante interesse pubblico, sempre in ambito scolastico, sono state regolamentate dal D.M. 305 del 6/12/2006, ancora vigente.

E' importante rilevare quanto dispone il regolamento in merito ai fornitori di servizi Internet e i social media, i quali dovranno richiedere il consenso ai genitori o a chi esercita la potestà genitoriale per trattare i dati personali dei minori di 16 anni.

Il consenso potrà essere revocato in ogni momento. I trattamenti effettuati fino a quel momento dal titolare sulla base del consenso rimarranno comunque legittimi.

CAPITOLO 8
Le sanzioni

Par. 1 – Le sanzioni

Tra le caratteristiche salienti del Regolamento europeo sulla privacy, la parte sanzionatoria occupa, per l'interesse dei Titolari, dei Responsabili e degli autorizzati un posto sicuramente di rilievo.

Per una completa comprensione dell'argomento si è preferito riportare gli articoli del Regolamento che afferiscono al tema che stiamo presentando.

Capo VIII- Mezzi di ricorso, responsabilità e sanzioni

Art. 77 – Diritto di proporre reclamo all'autorità di controllo

1. Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi il presente regolamento ha il diritto di proporre reclamo a un'autorità di controllo, segnatamente nello Stato membro in cui risiede abitualmente, lavora oppure del luogo ove si è verificata la presunta violazione.
2. L'autorità di controllo a cui è stato proposto il reclamo informa il reclamante dello stato o dell'esito del reclamo, compresa la possibilità di un ricorso giurisdizionale ai sensi dell'articolo 78.

Art. 78 – Diritto a un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo

1. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale, ogni persona fisica o giuridica ha il diritto di proporre un ricorso giurisdizionale effettivo avverso una decisione giuridicamente vincolante dell'autorità di controllo che la riguarda.
2. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale, ciascun interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora l'autorità di controllo che sia competente ai sensi degli articoli 55 e 56 non tratti un reclamo o non lo informi entro tre mesi dello stato o dell'esito del reclamo proposto ai sensi dell'articolo 77.
3. Le azioni nei confronti dell'autorità di controllo sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'autorità di controllo è stabilita.
4. Qualora siano promosse azioni avverso una decisione di un'autorità di controllo che era stata preceduta da un parere o da una decisione del comitato nell'ambito del meccanismo di coerenza, l'autorità di controllo trasmette tale parere o decisione all'autorità giurisdizionale.

Art. 79 – Diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento o del responsabile del trattamento

1. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale disponibile, compreso il diritto di proporre reclamo a un'autorità di controllo ai sensi dell'articolo 77, ogni interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora ritenga che i diritti di cui gode a norma del presente regolamento siano stati violati a seguito di un trattamento.
2. Le azioni nei confronti del titolare del trattamento o del responsabile del trattamento sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha uno stabilimento. In alternativa, tali azioni possono essere promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'interessato risiede abitualmente, salvo che il titolare

del trattamento o il responsabile del trattamento sia un'autorità pubblica di uno Stato membro nell'esercizio dei pubblici poteri.

Art. 80 – Rappresentanza degli interessati

Art. 81 – Sospensione delle azioni

Art. 82 – Diritto al risarcimento e responsabilità

1. Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.

2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.

3.Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

4. Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.

5. Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2.

6. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2.

Art. 83 – Condizioni generali per infliggere sanzioni amministrative pecuniarie

1. Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai sensi del presente articolo in relazione alle violazioni del presente regolamento di cui ai paragrafi 4, 5 e 6 siano in ogni singolo caso effettive, proporzionate e dissuasive.

2. Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta alle misure di cui all'articolo 58, paragrafo 2, lettere da a) a h) e j), o in luogo di tali misure. 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 dei seguenti elementi:

a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;

b) il carattere doloso o colposo della violazione;

c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;

d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;

e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;

f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

g) le categorie di dati personali interessate dalla violazione;

h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;

i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;

j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; e

k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

3. Se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento o un responsabile del trattamento viola, con dolo o colpa, varie disposizioni del presente regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave.

4. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10.000.000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43;

b) gli obblighi dell'organismo di certificazione a norma degli articoli 42 e 43;

c) gli obblighi dell'organismo di controllo a norma dell'articolo 41, paragrafo 4;

5. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 20.000.000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

a) i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9;

b) i diritti degli interessati a norma degli articoli da 12 a 22;

c) i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49;

d) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX;

e) l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1.

6. In conformità del paragrafo 2 del presente articolo, l'inosservanza di un ordine da parte dell'autorità di controllo di cui all'articolo 58, paragrafo 2, è soggetta a sanzioni amministrative pecuniarie fino a 20.000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

7. Fatti salvi i poteri correttivi delle autorità di controllo a norma dell'articolo 58, paragrafo 2, ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro.

8. L'esercizio da parte dell'autorità di controllo dei poteri attribuitile dal presente articolo è soggetto a garanzie procedurali adeguate in conformità del diritto dell'Unione e degli Stati membri, inclusi il ricorso giurisdizionale effettivo e il giusto processo.

9. Se l'ordinamento giuridico dello Stato membro non prevede sanzioni amministrative pecuniarie, il presente articolo può essere applicato in maniera tale che l'azione sanzionatoria sia avviata dall'autorità di controllo competente e la sanzione pecuniaria sia irrogata dalle competenti autorità giurisdizionali nazionali, garantendo nel contempo che i mezzi di ricorso siano effettivi e abbiano effetto equivalente alle sanzioni amministrative pecuniarie irrogate dalle autorità di controllo. In ogni caso, le sanzioni pecuniarie irrogate sono effettive, proporzionate e dissuasive. Tali Stati membri notificano alla Commissione le disposizioni di legge adottate a norma del presente paragrafo al più tardi entro 25 maggio 2018 e comunicano senza ritardo ogni successiva modifica.

Art. 84 – Sanzioni

1. Gli Stati membri stabiliscono le norme relative alle altre sanzioni per le violazioni del presente regolamento in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 83, e adottano tutti i provvedimenti necessari per assicurarne l'applicazione. Tali sanzioni devono essere effettive, proporzionate e dissuasive.

2. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del paragrafo 1 al più tardi entro 25 maggio 2018, e comunica senza ritardo ogni successiva modifica.

In conformità dell'art. 83 paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10.000.000 di euro, o per imprese fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

Descrizione articolo	Articoli
Gli obblighi del titolare e del responsabile del trattamento a norma degli articoli descritti nella colonna a fianco	8, 11- da 25 a 39- 42 e 43
Gli obblighi dell'organismo di certificazione a norma degli articoli segnati a fianco	42 e 43
Gli obblighi dell'organismo di controllo a norma dell'articolo segnato a fianco	41 par. 4

In conformità dell'art. 83 paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 20.000.000 di euro, o per imprese fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

Descrizione articolo	Articoli
I principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli segnati a fianco	5, 6, 7 e 9
I diritti dell'interessato, a norma degli articoli segnati a fianco	da 12 a 22
I trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale, a norma degli articoli segnati a fianco	da 44 a 49
Qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del Capo IX – "*Disposizioni relative a specifiche situazioni di trattamento*"	da art. 85 a 91: Trattamenti e libertà di espressione e di informazione; trattamento e accesso del pubblico a documenti ufficiali; trattamento del numero di identificazione nazionale; trattamento di dati nell'ambito dei rapporti di lavoro; trattamento ai fini di archiviazione, di ricerca scientifica o storica; obblighi di segretezza; protezione di dati presso chiese e religiosità
L'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi: - dell'art. 58, paragrafo 2, - o il negato accesso in violazione dell'art. 58, paragrafo 1.	Art. 58.2 Ogni autorità di controllo ha tutti i poteri correttivi seguenti: avvertite, ammonire, ingiungere, imporre, revocare, ordinare al titolare e/o al responsabile esistenze violazioni o altro su vari illeciti segnalati. Art. 58.1 Ogni autorità di controllo ha tutti i poteri di indagine su diversi temi.

In conformità dell'art. 83 paragrafo 2 del presente articolo, l'inosservanza di un ordine da parte dell'autorità di controllo di cui all'articolo 58, paragrafo 2, è soggetta a sanzioni amministrative pecuniarie fino a 20.000.000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

E' bene precisare, infine, che mentre le nuove sanzioni amministrative sono disciplinate dagli articoli sopra riportati, **le sanzioni penali**, invece, non trovando alcuna traccia nel regolamento, rimangono di competenza di ogni singolo Stato membro, quindi saranno irrogate sanzioni nel rispetto del Codice Privacy.

Pertanto, abbiamo riportato di seguito la tabella che racchiude e sintetizza i reati ancora vigenti.

Art. 167 – Trattamento illecito di dati	*"Co. 1- Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per se o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli artt. 18, 19, 23, 123 e 126, ovvero in applicazione dell'art. 129, è punito, se dal fatto deriva nocumento, con la reclusione d 6 a 18 mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da 6 a 24 mesi".* Art. 18: Principi applicabili a tutti i trattamenti effettuati da soggetti pubblici Art. 19: Principi applicabili al trattamento di dati diversi da quelli sensibili e giudiziari Art. 23: Consenso Art. 123: Dati relativi al traffico riguardanti abbonati e utenti Art. 126: Dati relativi all'ubicazione Art. 129: Comunicazioni indesiderate *"Co. 2 - Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri o di recare ad altri un danno procede al trattamento di dati personali in violazione di quanto disposto dagli artt. 11, 17, 20, 21, 22 co. 8, 11, 25, 26, 27, e 45 è punito, se dal fato deva nocumento, con la reclusione da 1 a 3 anni".,* Art. 11: Modalità del trattamento e requisiti dei dati Art. 17: Trattamento che presenta rischi specifici Art. 20: Principi applicabili al trattamento di dati sensibili Art. 21: Principi applicabili al trattamento di dati giudiziari Art. 22: Principi applicabili al trattamento di dati sensibili e Giudiziari; co. 8: i dati idonei rilevare lo stato di salute non possono essere diffusi Art. 25: Divieti di comunicazione e diffusione Art. 27: Garanzie per i dati giudiziari Art. 45: Trasferimenti vietati
Art. 168 - Falsità nelle dichiarazioni rese al Garante	*"Chiunque, nella notificazione di cui all'art. 37, o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti e documenti falsi, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da 6 mesi a tre anni"*

CAPITOLO 9
Altri temi

Par. 1 – Designazione del Responsabile della Protezione dei dati

Art. 37 - Designazione del Responsabile della Protezione dei dati

1. Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure

c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10*.*

2. Un gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati, a condizione che un responsabile della protezione dei dati sia facilmente raggiungibile da ciascuno stabilimento.

3. Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.

4. Nei casi diversi da quelli di cui al paragrafo 1, il titolare e del trattamento, il responsabile del trattamento o le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento possono o, se previsto dal diritto dell'Unione o degli Stati membri, devono designare un responsabile della protezione dei dati. Il responsabile della protezione dei dati può agire per dette associazioni e altri organismi rappresentanti i titolari del trattamento o i responsabili del trattamento.

5. Il responsabile della protezione dei dati è designato in funzione 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 cui all'articolo 39.

6. Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.

7. Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.

Articolo 38 Posizione del responsabile della protezione dei dati

1. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

2. Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

3. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il

responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.

4. Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.

5. Il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri.

6. Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.

Articolo 39 Compiti del responsabile della protezione dei dati

1. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) 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;

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;

d) cooperare con l'autorità di controllo; e

e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Articolo 30 - Registri delle attività di trattamento

1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:
a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

2. Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:
a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

3. I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.

4. Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.

5. Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

Par. 3 – Valutazione d'impatto

Articolo 35 ***Valutazione d'impatto sulla protezione dei dati***

1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.

3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

4. L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.

5. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato. 6.Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.

7. La valutazione contiene almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e

d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.

9. Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.

10. Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica,

tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.

11. Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

Articolo 36 - Consultazione preventiva

1. Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.

2. Se ritiene che il trattamento previsto di cui al paragrafo 1 violi il presente regolamento, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'autorità di controllo fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento e può avvalersi dei poteri di cui all'articolo 58. Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. L'autorità di controllo informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione.

3. Al momento di consultare l'autorità di controllo ai sensi del paragrafo 1, il titolare del trattamento comunica all'autorità di controllo:

a) ove applicabile, le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale;

b) le finalità e i mezzi del trattamento previsto;

c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente regolamento;

d) ove applicabile, i dati di contatto del titolare della protezione dei dati;

e) la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35;

f) ogni altra informazione richiesta dall'autorità di controllo.

4. Gli Stati membri consultano l'autorità di controllo durante l'elaborazione di una proposta di atto legislativo che deve essere adottato dai parlamenti nazionali o di misura regolamentare basata su detto atto legislativo relativamente al trattamento.

5. Nonostante il paragrafo 1, il diritto degli Stati membri può prescrivere che i titolari del trattamento consultino l'autorità di controllo, e ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica.