ISTITUTO D'ISTRUZIONE SUPERIORE
"G. Salerno"
Via R. Chinnici
90024 Gangi
Codice fiscale 95005290820

INDICE GENERALE
del Disciplinare Interno

PREMESSE GENERALI
Perché un Regolamento Europeo

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.

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.

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:

a) 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;
b) 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;
c) 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;
d) se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori;
e) 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:

1. nel ridurre al minimo il trattamento dei dati personali;
2. l'uso della pseudonimizzazione dei dati personali prima possibile;

3. offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali;
4. consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza.

SEZIONE I
Inquadramento normativo fondamentale

Le norme giuridiche fondamentali, in ambito scolastico, fondamentalmente sono:

1. Il Regolamento dell'Unione europea 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 in materia di Regolamento generale sulla protezione dei dati, di seguito individuato come Regolamento europeo.
2. Il Decreto legislativo n. 196 del 30 giugno 2003 "Codice in materia di protezione dei dati personali recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento europeo.
3. Il Decreto ministeriale 7 dicembre 2006, n. 305, "Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della pubblica istruzione".

Occorre tenere in attenta considerazione anche le seguenti Linee Guida emesse dal Garante:

1. Linee guida in materia di trattamento di dati personali per profilazione on line [doc. web 3881513].
2. Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri soggetti obbligati [doc. web 3134436].
3. Le nuone linee guida in materia di trasparenza e privacy [doc. web 3152130].
4. La scuola a prova di Privacy: La nuova guida del Garante per la protezione dei dati personali per "insegnare la Privacy e rispettarla a scuola" [doc. web 5601934].

Il Garante per la protezione dei dati ha proceduto alla revisione delle Autorizzazioni generali al trattamento esistenti, alla luce del Decreto legislativo n. 101 del settembre 2018 e in base all'analisi effettuata ne sono state individuate soltanto cinque e di queste soltanto due sono di interesse in ambito scolastico:

1. Autorizzazione Generale N. 1 - Autorizzazione al trattamento di dati sensibili nei rapporti di lavoro.
2. Autorizzazione Generale N. 8 - Autorizzazione al trattamento di dati genetici

Infine le Linee guida di pertinenza del Gruppo europeo dei Garanti risultano essere:

1. Sul concetto di dati personali emesso da Gruppo di Lavoro Articolo 29: WP 136
2. Sul *coud computing* emesso da Gruppo di Lavoro Articolo 29: WP 196
3. Linee guida sul diritto alla portabilità emesso da Gruppo di Lavoro Articolo 29: WP 242 rev. 0
4. Linee Guida su RPD emesso da Gruppo di Lavoro Articolo 29: WP 243 rev. 01

SEZIONE II
Le principali definizioni

L'art. 4 è dedicato alle definizioni utilizzate dal regolamento europeo. Vengono riportate i punti che si rilevano di maggiore interesse per gli scopi del presente Disciplinare.

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 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. «Autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51.

SEZIONE III
Le novità del Regolamento

Le novità del Regolamento sono veramente tante e tutte importanti.

Proviamo a presentare le più significative.

1. Designazione del Responsabile (*interno*) del trattamento dei dati.

Le istituzioni scolastiche, da una attenta lettura dell'art. 28, non possono designare nessun responsabile (*interno*) del trattamento dei dati. E' naturalmente possibile individuare il profilo all'esterno della scuola.

L'argomento è trattato con minuzia di particolari nella SEZIONE VI alla pag. 21

2. Designazione del profilo del Contitolare del trattamento.

Anche questo argomento è trattato nella SEZIONE VI alla pag. 22

3. Nomina del Responsabile della protezione dei dati.

L'argomento è trattato con minuzia di particolari nella SEZIONE VI alla pag. 24

4. Le informative.

I contenuti dell'informativa sono contenuti in modo tassativo negli articoli 13 e 14 del regolamento. In particolare il titolare deve sempre specificare i dati di contatto del RPD e del Titolare, la base giuridica del trattamento, quale è il suo legittimo interesse se quest'ultimo costituisce la base giuridica del trattamento, nonché se trasferisce i dati personali raccolti verso Paesi esteri e, in caso affermativo, con quali strumenti. Ed ancora ulteriori informazioni dovranno essere specificati sil periodo di conservazione e il diritto di proporre reclamo all'autorità di controllo. Ed infine, se il trattamento comportA processi automatizzati (anche la profilazione), l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

Nel caso in cui i dati non sono raccolti 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 del dato.

L'informativa deve avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile, utilizzando un linguaggio chiaro e semplice.

In linea di principio sarà fornita per iscritto e preferibilmente in formato elettronico. E' prevista la possibilità di utilizzare le icone per presentare i contenuti dell'informativa in forma sintetica, ma solo in combinazione con l'informativa estesa.

5. Registro dei trattamenti.

Tutti i titolari i responsabili devono tenere un registro delle operazioni di trattamenti i cui contenuti sono indicati nell'art. 30 del regolamento. Il MIUR ha fornito un modello in excel (dalla scuola scaricato e compilato rendendolo così perfettamente rispondente alle indicazioni del succitato art. 30).

Il registro dei trattamenti è uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione dell'Unità di controllo, ma anche allo scopo di disporre di un quadro aggiornato (e da aggiornare continuamente, se necessario) di trattamenti in essere all'interno della scuola indispensabile per ogni valutazione e analisi del rischio. Tale registro deve avere forma scritta, anche elettronica e deve essere esibito su richiesta del Garante.

La tenuta del registro dei trattamenti **non** costituisce un adempimento formale bensì è **parte integrante di un sistema di corretta gestione dei dati personali.**

6. Violazione dei dati.

L'art. 4 del regolamento definisce violazione dei dati personali cole la "*violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la modifica, la divulgazione non autorizzata o l'accesso ai dato personali trasmessi, conservati o comunque trattati".*

Quindi, una violazione di dati non è solo un evento doloso come un attacco informatico, ma può essere anche un evento accidentale come un accesso abusivo, un incidente (un incendio o una calamità naturale), la semplice perdita di una chiavetta USB o la sottrazione di documenti con dati personali (furto o smarrimento di un notebook di un dipendente).

Tutti i titolari dovranno notificare all'Autorità di controllo le violazioni di dati personali di cui vengono a conoscenza entro 72 ore e comunque senza ingiustificato ritardo, ma soltanto se ritengono probabile che tale violazione derivino rischi per i diritti e le libertà degli interessati.

Pertanto, la notifica all'Autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta al titolare.

Se la propobilità di tale rischio è elevata si dovrà informare delle violazioni anche gli interessati e sempre senza ingiustificato ritardo. I contenuti della notifica all'Autorità e della eventuale comunicazione agli interessati sono indicati, in via esclusiva agli art. 33 e 34 del regolamento.

7. Valutazione d'impatto (DPIA).

La valutazione d'impatto è una procedura prevista dall'art. 35 del regolamento che mira a descrivere un trattamento di dati per valutarne la necessità e la proporzionalità nonché i relativi rischi, allo scopo di approntare misure idonee ad affrontarli.

Una DPIA può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi.

La DPIA è uno strumento importante in termini di responsabilizzazione, in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del regolamento, ma anche ad attestare di avere adottato misure idonee a garantire il rispetto di tali prescrizioni.

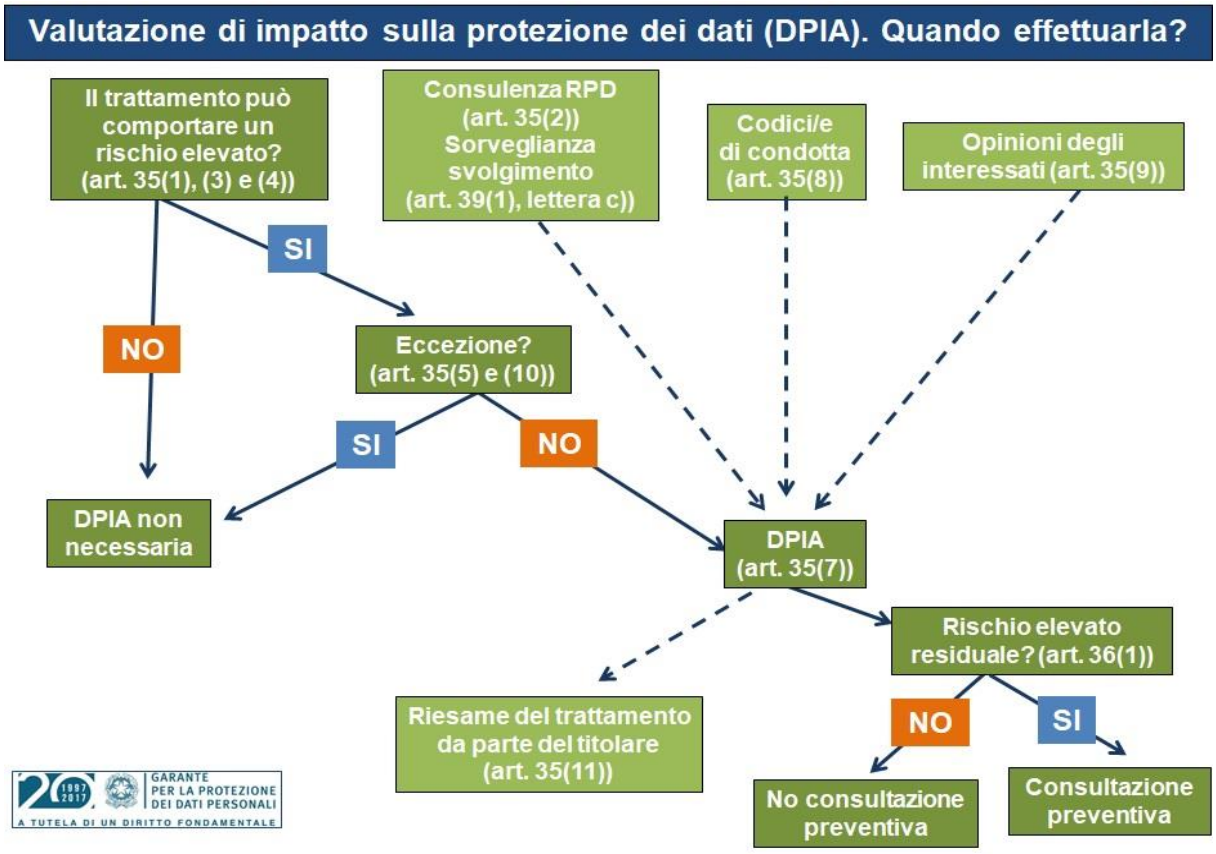
In altri termini, la DPIA è una procedura che permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali. Viene suggerito dal Gruppo dei Garanti di valutarne l'impiego per tutti i trattamenti e non solo nei casi in cui il regolamento lo prescrive come obbligatoria.

La DPIA deve essere condotta prima di procedere al trattamento. Dovrebbe essere previsto un riesame continuo della DPIA, ripetendo la valutazione a intervalli regolari.

La DPIA è obbligatoria effettuarla in tutti i casi in cui un rischio può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

La DPIA, di contro, non è necessaria per i trattamenti che non presentano rischio elevato per i diritti e libertà delle persone fisiche oppure quanto i trattamenti sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA.

Ecco la DPIA suggerita dal Garante Privacy:



SEZIONE IV
Attività svolta dagli operatori dei trattamenti

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.

<u>Descrizione delle attività degli operatori scolastici</u>

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 programmazione 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,;
- 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.

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.

I 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,

SEZIONE V
Il Sistema organizzativo della scuola

Presentazione dell'istituzione scolastica

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 da tabella che segue.

ORGANIZZATIVE	TECNICHE
Vigilanza della sede	Autenticazione degli autorizzati. Modificazione
Sistema di allarme	Registrazione degli accessi
Consegna delle chiavi della scuola al personale	Prescrizione di linee guida di sicurezza
L'accesso consentito è registrato	Analisi dei rischi
Ingresso controllato nei locali ove ha luogo il trattamento	Dispositivi antincendio
Assegnazione di incarichi: autorizzati, …..	Continuità dell'alimentazione elettrica -UPS
Identificazione dell'incaricato	Controllo dell'aggiornamento antivirus
Custodia in classificatori o armadi non accessibili	Controllo dei supporti consegnati in manutenzione
Custodia in armadi blindati e/o ignifughi	Verifica della leggibilità dei supporti: custodia e cancellazione
Deposito in cassaforte	
Formazione del personale	Distruzione controllata dei supporti
Controllo degli accessi a dati e programmi	Piano di disaster recover
Verifiche periodiche sui dati e trattamenti	Controllo sull'operato degli addetti ai PC
Documentazione dei controlli periodici	
Custodia di dati particolari	
Cartellini identificativi	
Informative	

Descrizione dei locali ove sono organizzati gli uffici

L'edificio scolastico sorge su un'area sub-urbana non 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 accesso, 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 d'Istruzione Secondaria si sviluppa in Plessi: quello centrale nel quale si trovano gli uffici di segreteria dove vengono trattati i dati relativi a tutti i trattamenti e nel restante plesso dove 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
Ufficio Collaboratori del Dirigente scolastico	Alunni - Personale
Segreteria Alunni e Protocollo	Tutte
Segreteria amministrativa	Personale
Aule di insegnamento	Alunni
Plesso "Liceo" Via F.sco Giunta – Referente	Categorie di dati
Aule d'insegnamento e Sala docenti	Alunni

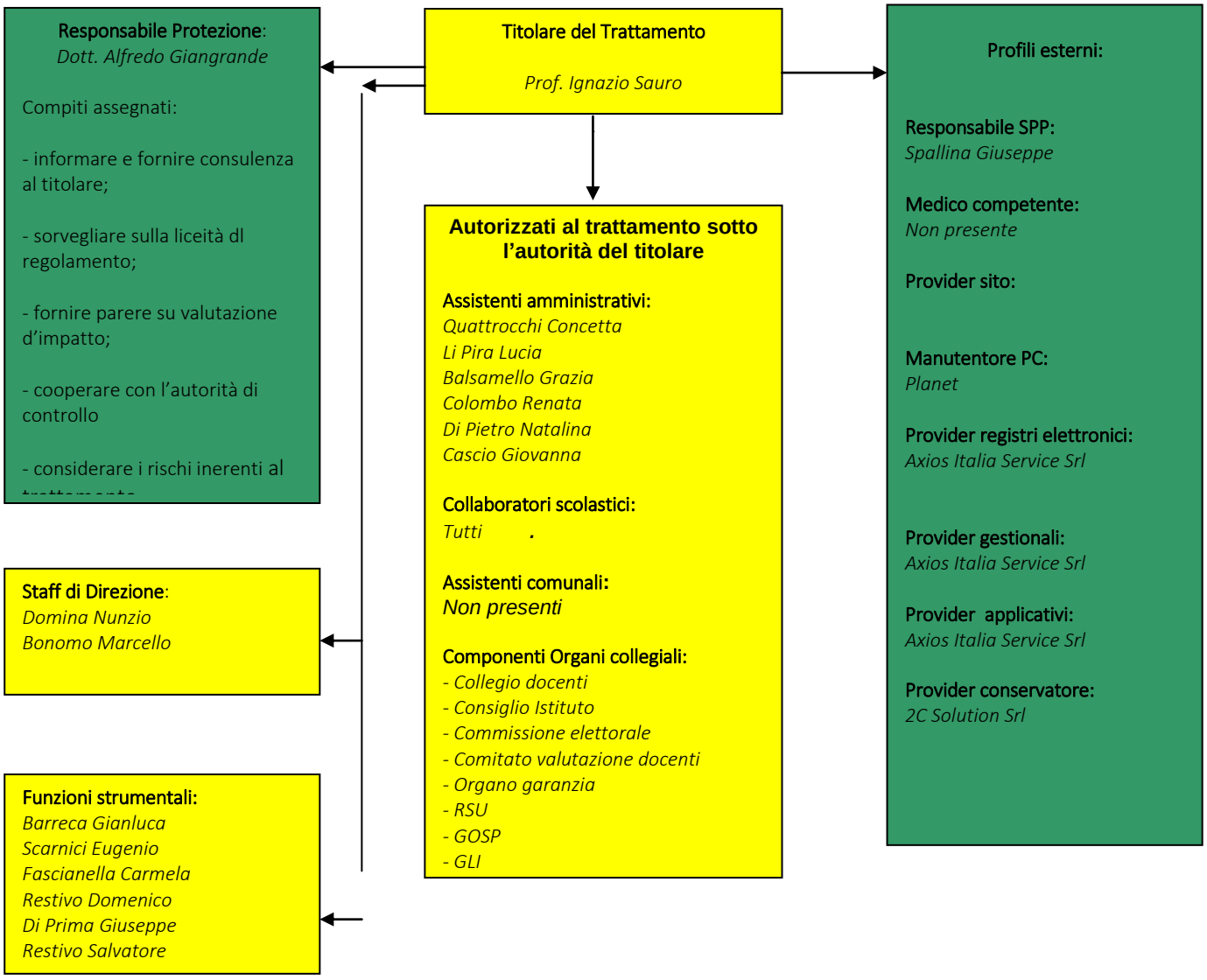
Descrizione dei locali ove si effettua il trattamento dei dati

Locali	Posizione e Descrizione	Uso
Locale_0	Si accede nell'area amministrativa direttamente dalla hall della scuola sita nella via R. Chinnici posta a piano terra. L'area amministrativa è costituita da n. 4 locali situati tutti sullo stesso piano, come descritti di seguito. 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. Gli uffici di segreteria non presentano grate protettive alle finestre e in essi sono presenti i condizionatori d'aria. Le porte di accesso sono in legno muniti di normale serratura. Gli estintori sono stati collocati in ambienti interni e all'esterno così	Area comune
Locale_1	In questa segreteria vengono trattati i dati personali degli alunni e quelli del protocollo. Si utilizzano 3 computer dati in dotazione	Segreteria Didattica. Ufficio del protocollo
Locale_2	E' l'ufficio del direttore amministrativo. In questo ufficio sono trattati tutti i dati che affluiscono nella scuola utilizzando il computer dato in dotazione.	Ufficio del Direttore amministrativo
Locale_3	E' la segreteria del personale. Sono trattati i dati relativi al personale di ruolo e non, utilizzando 2 computer dati in dotazione.	Segreteria del personale
Locale _4	E' la direzione dove sono trattati tutti i dati personali che affluiscono nella scuola, utilizzando il PC dato in dotazione.	Ufficio del DS
Locale_5	E' l'ufficio dei collaboratori del dirigente. Sono trattati i dati relativi agli alunni e al personale utilizzando PC dati in dotazione.	Ufficio collaboratori Dirigente

Dati identificativi del Soggetto Titolare

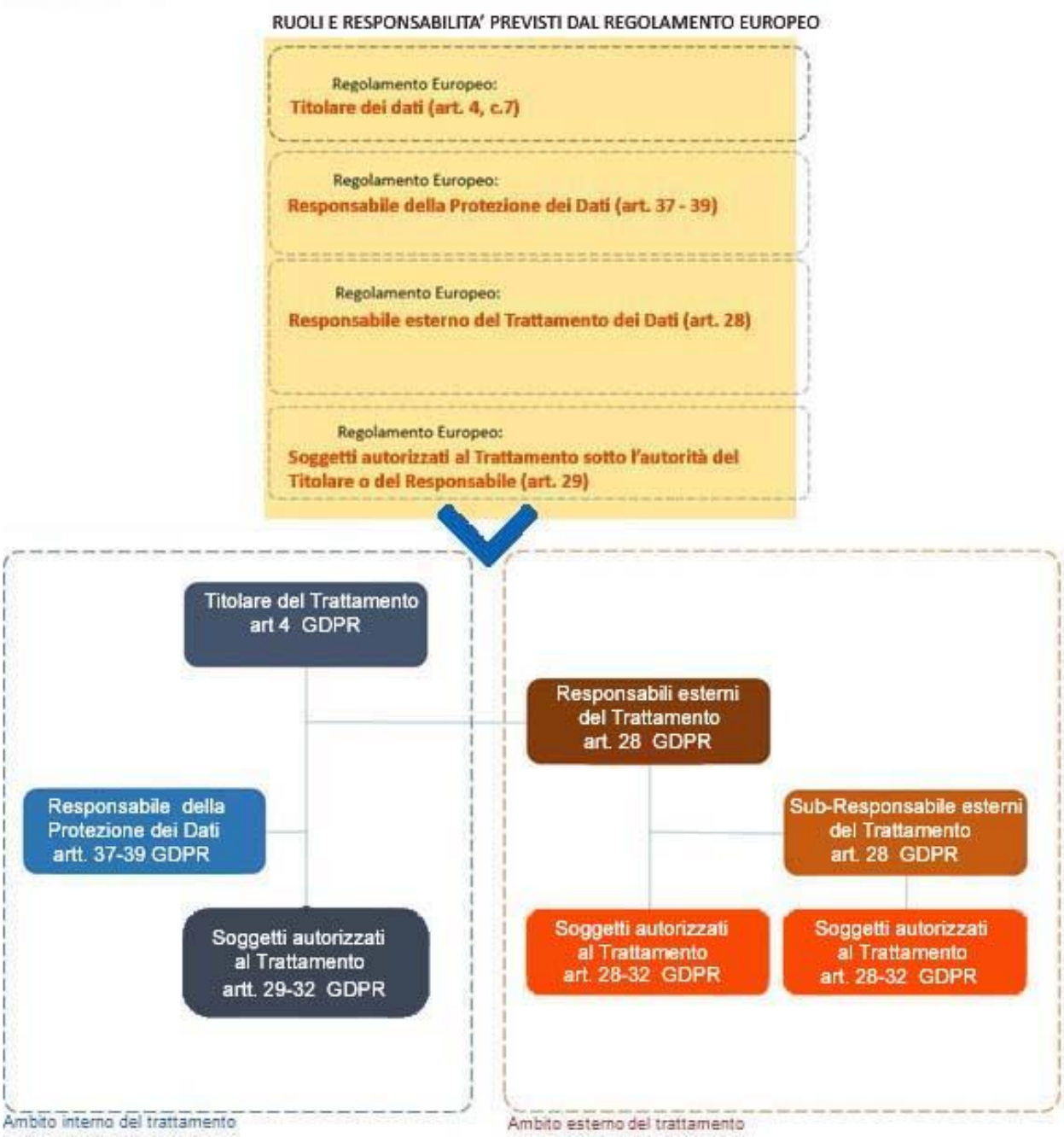
DIREZIONE E SEGRETERIA	Istituto d'Istruzione Superiore "G. Salerno"
Indirizzo sede centrale	Via R. Chinnici, 1 – 90024 Gangi
Tipologie Scuola	Istituto tecnico Economico – Liceo Classico – Liceo Scientifico
Anno scolastico	20192020
Codice meccanografico sede centrale	PAIS01700B
Codice IPA	istsc_pais01700b
Indirizzo e-mail	paics01700b@istruzione.it
Sito web	www.icfloriosanlorenzo.gov.it
Posta Elettronica Certificata	paics01700b@pec.istruzione.it
Codice fiscale	95005290820
Alunni numero complessivo	480
Classi numero complessivo	24
Insegnanti numero complessivo	72
Personale ATA	21 di cui 1 DSGA, 5 Assistenti Amministrativi, 3 Assistenti Tecnici e 12 collaboratori scolastici.
Direttore dei Servizi generali ed Amministrativi	Rag. Concetta Quattrocchi
Dirigente Scolastico	Prof. Ignazio Sauro
Collaboratore Vicario	Prof. Domina Nunzio
Responsabile del Servizio di Prevenzione e Protezione	Ing. Giuseppe Spallina
Responsabile dei Lavoratori sulla Sicurezza	Prof. Nasello Sebastiano
Medico competente	=======

Schema della Privacy della Istituzione Scolastica



SEZIONE VI
I Profili soggettivi: CHI tratta i dati personali

Scopo della presente Sezione è definire la distribuzione dei compiti e delle responsabilità nell'ambito del soggetti preposti al trattamento dei dati



A] – Il titolare dei dati personali

Al Titolare del trattamento, inteso **come centro decisionale** oppure **come centro di imputazione giuridica,** spetta l'onere di individuare e autorizzare Responsabili del trattamento, qualora ciò fosse dettato da reali opportunità organizzative i quali effettuano il trattamento dei dati per conto del titolare.

L'art. 4, c. 7 del Regolamento precisa che «Titolare del trattamento» è 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.

L'art. 24 statuiscono le Responsabilità secondo il comma 1.: «1. *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 mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.»*

2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione

Obblighi generali del titolare del trattamento

L'art. 24, oltre al comma 1. del riquadro precedente, recita:

2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.»

IDENTIFICAZIONE:
L'entità' giuridica della scuola è rappresentata dal Dirigente scolastico Prof. Ignazio Sauro

Il suddetto principio generale viene declinato in 3 fasi di compliance, secondo il seguente schema logico:

B] – Responsabile del trattamento dei dati

L'art. 4, c. 8 dispone: *«responsabile del trattamento» è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.*

L'art. 28 stabilisce **le responsabilità** del profilo in esame:

1. 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.

2. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

IDENTIFICAZIONE:
La scuola NON è rappresentata da alcuna entità giuridica in qualità di Responsabile del trattamento dei dati

La norma fissa più nei dettagli le caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento dei dati attribuendogli specifici compiti: costui deve trattare i dati per conto del titolare del trattamento tramite 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, – per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento effettuato soddisfi il regolamento e garantisca le tutela dell'interessato.

La norma 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)*.

Il ruolo del Responsabile del trattamento è chiaramente **riservato** ad un **soggetto esterno** all'Ente, con riferimento ai fornitori di servizi. Tratta i dati attenendosi alle istruzioni del titolare, assume responsabilità proprie e ne risponde alle Autorità di controllo e alla Magistratura.

Il titolare del trattamento, a sua discrezione, può distribuire incarichi interni, ma la responsabilità rimane sua e dell'eventuale responsabile (esterno) se nominato.

In ambito scolastico il decreto legislativo 196 del 2003 novellato dal decreto legislativo 101/2018 viene in aiuto al titolare nell'art. 2-quaterdecies rubricato "*Attribuzione di funzioni e compiti a soggetti designati*" che così recita testualmente:

« *1. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.*

2. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.>

C] - Responsabile della protezione dei dati (RPD)

L'art. 37, nei commi che interessano la scuola, **stabilisce**:

« 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.

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.

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.

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.»

IDENTIFICAZIONE:
La scuola ha designato come Responsabile della Protezione dei dati il Dott. Alfredo Giangrande

La designazione del RPD riflette il nuovo approccio del regolamento europeo (art. 39), maggiormente responsabilizzante, essendo finalizzata a facilitare l'attuazione del regolamento da parte del titolare e del responsabile. Il ruolo di RPD è di tutelare i dati personali, non gli interessi del titolare del trattamento. E ciò appare ovvio soprattutto nell'ambito degli enti pubblici e delle aziende che effettuano un monitoraggio su larga scala degli individui. Il RPD deve, infatti, possedere un'adeguata conoscenza delle normative e delle prassi di gestione dei dati personali, e deve adempiere alle proprie funzioni in piena autonomia ed indipendenza, e in assenza di conflitti di interesse. In tal senso non può ricoprire tale incarico un soggetto che si trova ai vertici aziendali, quindi in grado di influenzare le scelte adottate in materia di trattamento dei dati.

Ovviamente, titolare e responsabile del trattamento devono mettere a disposizione del RPD le risorse umane e finanziarie per poter svolgere il suo compito.

L'articolo 38 del Regolamento europeo stabilisce che il titolare del trattamento e il responsabile del trattamento si assicurano che il RPD non riceva alcuna istruzione per quanto riguarda l'esecuzione dei suoi compiti. Inoltre, il RPD non può essere rimosso o penalizzato dal titolare o dal responsabile del trattamento per l'adempimento dei propri compiti. Questo proprio a tutela della sua autonomia. In tal senso appare difficile ritenere che tale autonomia sia giustificabile nell'ambito di un rapporto di lavoro dipendente, per cui sarebbe preferibile che il RPD sia un soggetto esterno.

Il RPD è designato (art. 37) dal titolare o dal responsabile del trattamento, in base ad un contratto. La designazione dovrà essere comunicata all'Autorità di controllo nazionale; per l'Italia l'Ufficio del Garante per la privacy.
Tale designazione è obbligatoria solo in tre casi, ed uno di essi è che il titolare è un'amministrazione pubblica o un ente pubblico.

Vi sono numerosi obblighi che il titolare (o il responsabile del trattamento) hanno verso il responsabile per la protezione dei dati, ove presente:

1. supportare il RPD nell'esecuzione dei suoi compiti;
2. fornire le risorse necessarie per l'esecuzione dei suoi compiti;
3. consentire l'accesso ai dati e alle operazioni di trattamento;
4. assicurare l'accesso del RPD ai massimi livelli manageriali dell'azienda;
5. assicurarsi che gli altri compiti del RPD non interferiscano con la sua responsabilità primaria quale RPD;
6. non fornire alcuna istruzione al RPD sui suoi compiti;
7. non penalizzare o licenziare il RPD per l'esecuzione dei suoi compiti.

Il RPD ha un ruolo consultivo, e svolge i seguenti compiti:

1. informare e consigliare il titolare o il responsabile del trattamento, nonché i dipendenti, sugli obblighi previsti dalle norme in materia;
2. verificare l'attuazione e l'applicazione delle norme;
3. se richiesto, fornire pareri ed assistere il titolare in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare i relativi adempimenti;
4. cooperare con le autorità di controllo;
5. fungere da punto di contatto, non solo per l'autorità di controllo ma anche per gli interessati al trattamento, in merito a qualunque problematica connessa ai loro dati o all'esercizio dei loro diritti;
6. consultare l'autorità di controllo anche di propria iniziativa.

Il RPD non è, però, personalmente responsabile dell'inosservanza degli obblighi in materia di protezione dei dati personali, infatti è compito del titolare (art. 24) mettere in atto le misure tecniche ed organizzative adeguate. Il RPD risponde solo per lo svolgimento dei suoi obblighi di consulenza ed assistenza nei confronti del titolare, che è (eventualmente in solido col responsabile) l'unico soggetto responsabile del rispetto della normativa. Il titolare, quindi, potrà solo avanzare pretese risarcitorie basate sulla responsabilità contrattuale, nei confronti del RPD.

D] - Contitolari del trattamento

L'art. 26 del Regolamento **statuisce** quanto segue:

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

2. L'accordo di cui sopra deve riflettere adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

3. Indipendentemente dalle disposizioni dell'accordo di cui sopra, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento.»

IDENTIFICAZIONE:
La scuola non è rappresentata da alcuna entità giuridica come contitolare

La contitolarità si verifica quando esiste una condizione per la quale due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento stesso. Non è semplice individuare situazioni di contitolarità. Pertanto è bene rivedere i rapporti contrattuali esistenti, in cui vi è un trattamento di dati personali, per verificare se sussistono i presupposti della contitolarità e quindi per comprendere se il rapporto tra le parti è paritario in merito al trattamento dati, oppure se vi è un rapporto gregario, in cui una delle parti è titolare e l'altra ricopre il ruolo di responsabile del trattamento.

Il regolamento obbliga i contitolari a disciplinare il rapporto attraverso un rapporto interno, in cui, in maniera chiara, è necessario regolamentare:

1. le rispettive responsabilità in merito all'osservanza degli obblighi derivanti da Regolamento;
2. i rispettivi obblighi in merito all'esercizio dei diritti dell'interessato;
3. le rispettive funzioni relativamente alla comunicazione dell'informativa;
4. indicare un punto di contatto utile agli interessati.

Su entrambi i contitolari gravano le medesime responsabilità relativamente agli obblighi derivanti dalle nuove norme e dunque entrambi sono passibili delle sanzioni previste per i Titolari del trattamento.

Nella situazione di contitolarità l'interessato può esercitare i propri diritti, ai sensi del Regolamento, nei confronti di e contro ciascun titolare del trattamento, avendo il diritto di ricorrere indistintamente a uno dei due soggetti.

Il contatto del contitolare deve essere annotato nella opportuna scheda del Registro dei trattamenti.

E] - Trattamento sotto l'autorità del titolare o del responsabile del trattamento. Istruzione obbligatoria

L'art. 29 del Regolamento **recita**:
« *Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento*.»

L'art. 32 c. 4, ancora, **recita**:
«*Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri*.»

La formazione costituisce, pertanto, un prerequisito per potere operare all'interno della scuola. Essa deve, alla luce della normativa di riferimento,, con sessioni sia giuridiche sia sui profili organizzativi della scuola, e pragmatico (come si evince dal termine utilizzato, "istruito") e riguardare tutti i soggetti autorizzati.

La formazione non deve essere considerata un mero adempimento burocratico, ma come un'opportunità per rendere consapevoli gli operatori dei rischi connessi al trattamento dei dati, delle misure di sicurezza, per migliorare i processi organizzativi e i servizi erogati, evitare danni reputazionali, ridurre i rischi di sanzioni amministrative e rendere più competitiva la scuola.

L'obbligo formativo non può essere sottovalutato da parte della scuola, in quanto la mancata erogazione della formazione scatta, come previsto dall'art. 83 del Regolamento una sanzione amministrativa pecuniaria fino a 10 milioni di euro (come precisato nella PARTE XIII dedicata alle sanzioni.

F] – Autorizzazioni al trattamento dei dati dell'area amministrativa

Qualora la gestione dei trattamenti dei dati richieda l'intervento operativo di soggetti, il titolare può designare 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 ed ha valore di 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 titolare.
Se non diversamente previsto nella lettera di incarico, gli autorizzati al trattamento vengono nominati a tempo indeterminato e decadono per trasferimento 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.

Le lettere di autorizzazione al trattamento dei dati personali sono emesse ai sensi dell'art. 29, per cui gli autorizzati agiscono sotto la diretta autorità del titolare anche in materia di istruzione obbligatoria che il titolare vorrà loro organizzare.

Gli autorizzati risultano essere:

- gli assistenti amministrativi,
- i collaboratori scolastici addetti a servizi particolari (servizi esterni, portineria, servizi di fotoriproduzione);
- assistenti comunali per l'accoglienza e per l'assistenza alla persona;
- il Responsabile del Sistema di Prevenzione e Protezione [RSPP];
- il Responsabile del lavoratori sulla sicurezza [RLS];
- il manutentore del sistema informatico;
- l'amministratore di sistema;
- il medico competente;
- la banca tesoriere.

Le lettere autorizzative sono consultabili in Appendice.

i nominativi degli soggetti autorizzati al trattamento dei dati personali hanno l'obbligo di frequentare i cicli d'istruzione, ai sensi degli artt. 29 e 32 c. 4 del Regolamento che il titolare organizzerà nel tempo e in qualunque modalità. Gli operatori che hanno l'obbligo di partecipare ai corsi di istruzione organizzati dal Dirigente scolastico sono sinteticamente enucleati nella figura di pag. 18

G] – Autorizzazioni al trattamento dei dati dell'area didattica

Nell'area didattica sono autorizzati al trattamento dei dati personali, ai sensi dello stesso art. 29, e sotto l'autorità diretta del Dirigente scolastico i componenti degli Organi Collegiali che seguono. Le relative lettere autorizzative sono consultabili in Appendice.

- Componenti del Collegio dei Docenti
- Collaboratori diretti del Dirigente scolastico
- Componenti del Consiglio d'Istituto
- La Rappresentanza Unitaria Sindacali
- Componenti del Comitato Elettorale
- Componenti del Comitato di Valutazione dei docenti
- Componenti dell'Organo di Garanzia
- Componenti del Gruppo Operativo di Supporto Psicopedagogico
- Componenti di altri eventuali Gruppi operativi della scuola

H] – Manutentore (interno o esterno)dell'impianto informatico delle segreterie

Il manutentore del sistema informatico della scuola, contrariamente a quanto disponeva il Codice Privacy, non solo non è soggetto a trattamento dei dati personali, ma gli è vietato trattarli.

In ogni caso queste figure non "trattano" dati personali, li possono solo "vedere" (cioè raccogliere") ovvero ne hanno accesso casualmente, nel corso delle normali operazioni di aggiornamento, assistenza e manutenzione dei sistemi.

Lo svolgimento delle normali mansioni di tecnico comporta, però, di regola la concreta capacità, per atto intenzionale, ma anche per caso fortuito, di accedere in modo privilegiato a risorse del sistema informativo e a dati personali *cui non è legittimato ad accedere rispetto ai profili di autorizzazione attribuiti.*

Pertanto, la scuola nel dovere tutelare i dati personali degli interessati provvederà a fare sottoscrivere una lettera di incarico ai tecnici nella quale saranno descritte le regole da seguire perché siano rispettati il riserbo in ordine alle informazioni delle quali si sia venuti a conoscenza nel corso dell'intervento tecnico.

Le normative che saranno rispettate sono: [art. 326 del codice penale (rivelazione e utilizzazione di segreti d'ufficio) e, art. 28 della legge 241/90 e s.m.i.**]**

I] – 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 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 alcun profilo come amministratore di sistema.

L] - Nomina del custode dell'archivio storico ad accesso controllato

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 come tale incarico viene assunto direttamente dal Titolare dei dati.

M] – Gestione dell'impianto di videoregistrazione

Questa Istituzione scolastica, avendo riscontrato esistenti i presupposti di legge per l'attivazione di un impianto di videosorvaglianza, ne ha installato uno le cui modalità osservano il Provvedimento generale emanato dal Garante il 29/04/2004 recante norme sulla videosorveglianza, con registrazione delle immagini.

Saranno rispettati i seguenti principi generali così come prescritte dalla normativa succitata:

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** obbligatori da seguire si trovano le seguenti attività:

1. il progetto che deve perseguire l'ottenimento degli obiettivi da raggiungere;
2. il parere favorevole della installazione dell'impianto espresso dalla RSU e dal Collegio dei Docenti;
3. la relazione tecnica del sistema redatta dal fornitore nella quale di devono evidenziare:
    a. la tipologie delle telecamere:
    b. il numero delle telecamere e l loro posizionamento;
    c. la loro posizione deve essere segnata in adeguate planimetrie;
    d. l'intervallo di tempo nel quale l'impianto è disattivato;
    e. le modalità di cancellazione delle immagini;
    f. l'intervallo di tempo in cui sono visibili le immagini;
4. il nome del Responsabile del trattamento delle immagini;
5. il luogo di conservazione del videoregistratore;
6. l'istallazione della informativa sintetica provvista degli elementi base che deve rimandare alla informativa estesa e dove questa è consultabile;
7. le informative sintetiche devono essere collocate in prossimità di ogni telecamera e leggibili anche con limitata luminosità.

SEZIONE VII
I Profili soggettivi: COSA trattare

Viene , di seguito, riportata la definizione di trattamento di dati così da comprendere meglio ciò che si dirà.

Per Trattamento si deve intendere *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.*

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 l'adattamento o la modificazione, l'estrazione, il raffronto o l'interconnessione, l'utilizzo, la limitazione;

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.

Le categorie dei trattamenti sono affrontati di seguito.

1. Trattamento di dati comuni.

I dati personali c. d. comuni relativi a persone fisiche 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, l'indirizzo di posta elettronica, 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,* ed anche ai codici IP statici e non cioè quelle informazioni computerizzate attraverso le quali è possibile sapere quando, con chi, e per quanto tempo ci si è collegati in rete; questi dati sono liberamente trattabili.

2. 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.

3. 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.

2. 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.

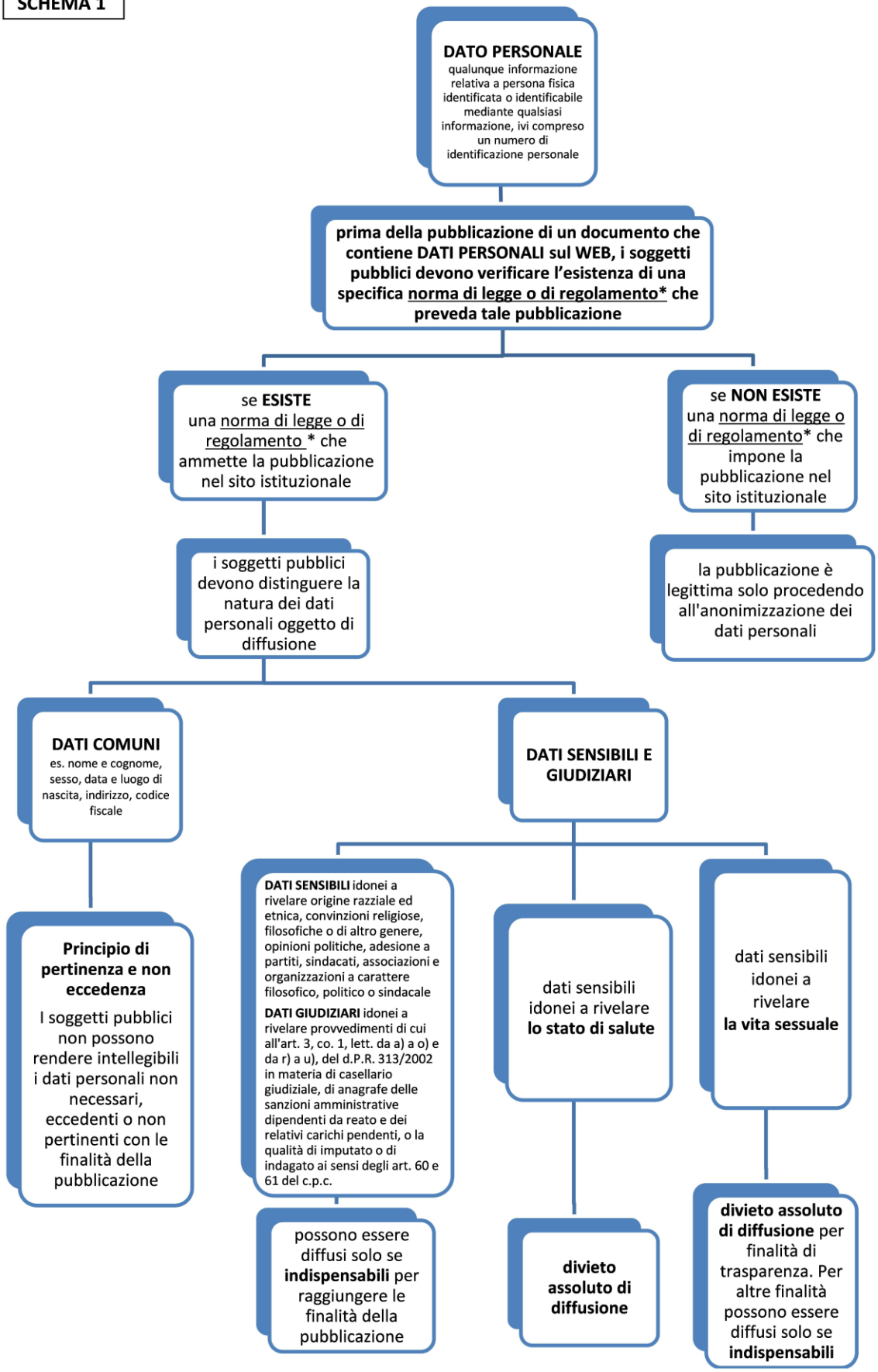
5. I dati personali devono essere sottoposti a cautele applicando quanto prescritto dall'art. 25 del Regolamento che prevede che la loro protezione si origina fin dalla progettazione [art. 25 comma 2] o avviene per impostazione predefinita [all'art. 25 com. 1].

I permessi concessi sono le operazioni che la definizione del trattamento propone: la loro identificazione dipende dalle mansioni che l'autorizzato è chiamato a svolgere

.

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 nella pagina successiva per motivi di spazio..

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.

SEZIONE VIII
I Profili soggettivi: COME trattare dati personali

Per rispondere sulle modalità di trattamento dei dati personali interviene sapientemente l'art. 5 del Regolamento rubricato: *Principi applicabili al trattamento di dati personali* che offre con grande chiarezza le modalità che devono essere seguite obbligatoriamente da tutti gli autorizzati al trattamento.

Di seguito una sintesi dei principi introdotti dal Regolamento

	Imprese ed enti avranno più responsabilità (accountability), ma potranno beneficiare di semplificazioni. In caso di inosservanza delle regole sono previste sanzioni, anche elevate. Il Regolamento è direttamente applicabile e vincolante in tutti gli Stati membri dell'Unione europea e non richiede una legge di recepimento nazionale. Inoltre, si applica integralmente alle imprese situate fuori dall'Unione europea che offrono servizi o prodotti a persone che si trovano nel territorio dell'Unione Europea.
	Tutte le aziende, ovunque stabilite, dovranno quindi rispettare le regole fissate nell'Ue. Fra le principali novità del Regolamento c'è il cosiddetto «sportello unico» (one stop shop), che semplificherà la gestione dei trattamenti e garantirà un approccio uniforme. Salvo casi specifici, le imprese stabilite in più Stati o che offrono prodotti e servizi in vari Paesi dell'Ue, per risolvere possibili problematiche sull'applicazione e il rispetto del Regolamento potranno rivolgersi ad un solo interlocutore: cioè all'Autorità di protezione dei dati del Paese dove si trova il loro stabilimento principale.
	Il Regolamento promuove la responsabilizzazione (accountability) dei titolari del trattamento e l'adozione di approcci e politiche che tengano conto costantemente del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati. Il principio-chiave è garantire la protezione dei dati fin dalla fase di ideazione e progettazione di un trattamento o di un sistema, e adottare comportamenti che consentano di prevenire possibili problematiche. Ad esempio, è previsto l'obbligo di effettuare valutazioni di impatto prima di procedere ad un trattamento di dati che presenti rischi elevati per i diritti delle persone, consultando l'Autorità di protezione dei dati in caso di dubbi. Viene inoltre introdotta la figura del «Responsabile della protezione dei dati» (RPD), incaricato di assicurare una gestione corretta dei dati personali nelle imprese.
	Il Regolamento introduce regole più chiare in materia di informativa e consenso, definisce i limiti al trattamento automatizzato dei dati personali, pone le basi per l'esercizio di nuovi diritti, stabilisce criteri rigorosi per il trasferimento dei dati al di fuori dell'Ue e per i casi di violazione dei dati personali.
	L'informativa diventa sempre di più uno strumento di trasparenza riguardo al trattamento dei dati personali e all'esercizio dei diritti. Per facilitare la comprensione dei contenuti, nell'informativa si potrà fare ricorso anche a icone, identiche in tutta l'Unione europea. Gli interessati dovranno sapere se i loro dati sono trasmessi al di fuori dell'Ue e con quali garanzie; cosi come dovranno sapere che hanno il diritto di revocare il consenso a determinati trattamenti, come quelli a fini di marketing diretto.

	Resta vietato il trasferimento di dati personali verso Paesi situati al di fuori dell'Unione europea o organizzazioni internazionali che non rispondono agli standard di adeguatezza in materia di tutela dei dati, rispetto ai quali il Regolamento introduce criteri di valutazione più stringenti. Come avviene già oggi, in mancanza di un riconoscimento di adeguatezza da parte della Commissione europea, i titolari potranno utilizzare per il trasferimento specifiche garanzie contrattuali, per le quali il Regolamento prevede norme dettagliate e vincolanti. In assenza di garanzie contrattuali o riconoscimenti di adeguatezza, i dati potranno essere trasferiti solo con il consenso esplicito dell'interessato, oppure qualora ricorrano particolari condizioni (ad esempio, quando il trasferimento è indispensabile per rispettare specifici obblighi contrattuali, per importanti motivi di interesse pubblico, per esercitare o difendere un diritto in sede giudiziaria, ecc.).
	Il titolare del trattamento dovrà comunicare eventuali violazioni dei dati personali all'Autorità nazionale di protezione dei dati. Se la violazione dei dati rappresenta una minaccia per i diritti e le libertà delle persone, il titolare dovrà informare in modo chiaro, semplice e immediato anche tutti gli interessati e offrire indicazioni su come intende limitare le possibili conseguenze negative. L'Autorità di protezione dei dati potrà comunque imporre al titolare del trattamento di informare gli interessati sulla base di una propria autonoma valutazione del rischio associato alla violazione.
	Grazie all'introduzione del cosiddetto «diritto all'oblio», gli interessati potranno ottenere la cancellazione dei propri dati personali anche on line da parte del titolare del trattamento qualora ricorrano alcune condizioni previste dal Regolamento: se i dati sono trattati solo sulla base del consenso; se i dati non sono più necessari per gli scopi rispetto ai quali sono stati raccolti; se i dati sono trattati illecitamente; oppure se l'interessato si oppone legittimamente al loro trattamento.

L'art. 5 del Regolamento testualmente statuisce che:

< I dati personali, pertanto, sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ***(«liceità, correttezza e trasparenza»);***

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali ***(«limitazione della finalità»);***

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

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

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o

a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato ***(«limitazione della conservazione»);***

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

2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).

Pertanto, il Titolare del trattamento, garantisce l'applicazione dei principi fondamentali della privacy, sanciti dal Regolamento europeo nel suo art. 5 ed identificati sinteticamente nella seguente tabella:

Principio generale con riferimento alla legge	Descrizione
Liceità, correttezza e trasparenza art. 5, c. 1, lett. A	Ogni trattamento di dati è legittimato da specifici requisiti, quali un consenso espresso dell'interessato, un obbligo di legge, un contratto. I dati sono trattati in modo corretto e trasparente nei confronti dell'interessato
Finalità ***art. 5, c. 1, lett. B***	I dati personali sono raccolti e trattati solo per finalità predeterminate, esplicite e legittime.
Necessità, non Eccedenza Essenzialità art. 5, c. 1, lett. C	L'utilizzo dei dati personali è sempre ridotto al minimo necessario, essenziale per il raggiungimento delle finalità dichiarate; sono raccolti e trattati solo se funzionali al raggiungimento delle finalità dichiarate e sono trattati con modalità e strumenti proporzionali alle finalità da raggiungere.
Esattezza, Completezza, Aggiornamento art. 5, c.1, lett. d	I dati personali sono puntualmente verificati in modo che sia garantita la loro esattezza, completezza ed aggiornamento.
Conservazione art. 5, c1, lett. e	I dati personali sono conservati per un periodo di tempo limitato al raggiungimento delle finalità dichiarate.
Sicurezza art. 5, c. 1, lett. f	I dati personali sono sempre raccolti e trattati previa adozione di idonee misure di sicurezza.
Riservatezza art. 5, c. 1, lett. f	I dati sono trattati da soggetti adeguatamente identificati, autorizzati ed istruiti.

Competenza **(riservato al solo titolare)** art. 5, c. 2	Il titolare è competente per il rispetto dei principi generali in materia di privacy ed in grado di comprovarlo.

SEZIONE IX
La sicurezza cibernetica

Capitolo 5
Sicurezza cibernetica

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 descritte 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.

L'Agenzia per l'Italia digitale ha imposto con la Circolare n. 2 del 18 aprile 2017 a tutte le pubbliche amministrazioni la compilazione della tabella scaricabile secondo il modello ABSC, con l'obiettivo di raggiungere il "Livello Minimo" indispensabile per il raggiungimento del successivo livello Standard.

La succitata tabella, divisa in 8 classi, permette a tutte le pubbliche amministrazioni di controllare se tali misure minime di sicurezza ICT sono presenti ed eventualmente di intervenire nel caso in cui tale obiettivo non fosse stato raggiunto.

Le otto classi dispongono:

ABSC1 (CSC1): Inventario dei dispositivi autorizzati e non autorizzati.

Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo a dispositivi autorizzati, mentre i dispostivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso).

ABSC2 (CSC2): Inventario dei software autorizzati e non autorizzati.

Gestire attivamente (inventariare, tacciare e correggere) tutti i software della rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venda impedita l'installazione o l'esecuzione.

ABSC3 (CSC3): Proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server.

Istituire, implementare e gestire attivamente (tracciare, segnalare e correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni.

ABSC4 (CSC4): Valutazione e correzione continua della vulnerabilità.

Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare le finestra di opportunità per gli attacchi informatici.

ABSC5 (CSC5): Uso appropriato dei privilegi dell'amministratore.

Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.

ABSC8 (CSC8): Difese contro i malware.

Contro l'installazione, la diffusione e l'esecuzione di codice maligno in diversi puti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive.

ABSC10 (CSC10): Copie di sicurezza.

Procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentire il ripristino in caso di necessità.

ABSC13 (CSC13): Protezione dei dati personali.

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.

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, alla cui realizzazione hanno collaborato l'Agenzia per l'Italia Digitale, il Garante per la protezione dei dati personali, il Ministero dello sviluppo economico].

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 secondo il Regolamento europeo e il Codice privacy 196/203 così come modificato d. lgs. 101 del 2018

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. 54]

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, già presentato all'inizio del presente Capitolo e pienamente condiviso dal Garante per la protezione dei dati che ha suggerito l'effettuazione della contestualizzazione ottenuta estrapolando dallo schema generale presente del documento originale tutte le subcategorie collegate al Codice per la protezione dei dati personali ottenendo così le tabelle che precedono.

Il Framework utilizzato è stato 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.

L'identificazione del livello di rischio è stata effettuata elaborando i risultati prodotti dalle alcune fasi propedeutiche e gli indici di rischio sono stati fissati mediante una scala, articolata a tre valori, come di seguito riportata nel presente capitolo.

L'analisi dei rischi permette di associare ad ogni danno, corrispondente ad un pericolo, una valutazione circa la gravità del danno stesso e la probabilità che si verifichi.

La mappatura dei rischi avviene attraverso la matrice di rischio, che permette di combinare le probabilità (che si verifichi l'evento considerato) e la gravità (delle prevedibili conseguenze) in modo indicizzato (indice di criticità), secondo una funzione matematica del tipo:

$$R = f(D,P)$$

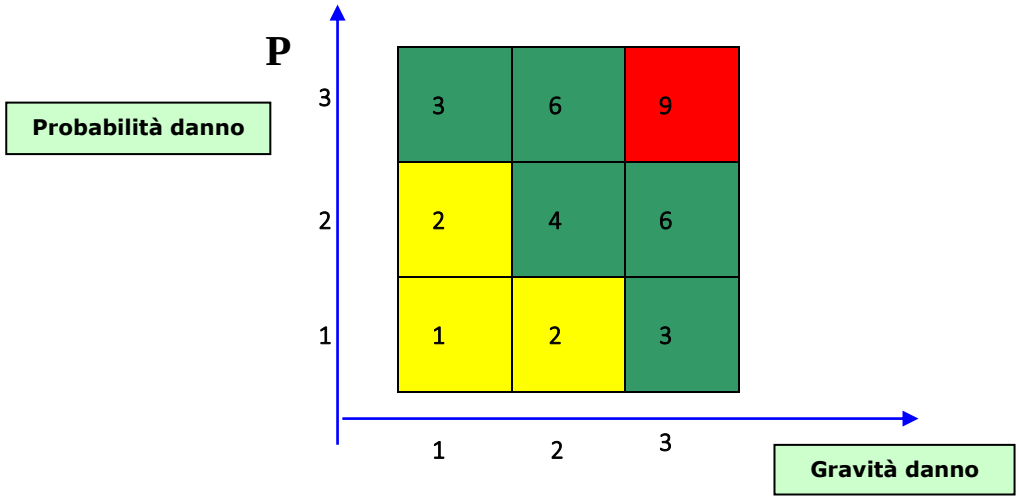
dove è:

R = intensità del rischio

D = intensità delle conseguenze (dimensione del danno)

P = probabilità del verificarsi di un evento che genera una danno

La matrice proposta per la valutazione dei rischi (R = P x D) è del tipo 3 x 3 e si può raffigurare in una rappresentazione avente in ascisse la gravità del danno ed in ordinata la probabilità del suo verificarsi.



La scala della probabilità e della dimensione del danno vengono riportate appresso.

La definizione della scala di probabilità fa riferimento principalmente all'esistenza di una correlazione più o meno diretta tra la carenza riscontrata e la probabilità che si verifichi l'evento indesiderato, tenuto conto della frequenza e della durata delle operazioni/lavorazioni che comportano rischi per la sicurezza dei dati personali

E' possibile procedere alla classificazione dei rischi in termini relativi, distinguendo il rischio in fasce di livello, facilitando quindi il processo decisionale.

Per ognuno dei parametri suddetti è possibile individuare una scala di valori secondo i seguenti criteri:

PROBABILITA' o FREQUENZA

Livello	Evento	Definizioni/criteri
3	Alta probabilità	Frequenza alta. Sono stati registrati alcuni episodi già accaduti. L'evento può verificarsi per la carenza o l'assenza di pochi elementi.
2	Probabile	Frequenza medio bassa. Sono noti sporadici episodi, lontani nel tempo. L'evento si potrebbe verificare con la concomitanza di situazioni particolarmente sfavorevoli.
1	Estremamente improbabile	Frequenza bassa. Non sono stati registrati episodi. L'evento potrebbe verificarsi con la coincidenza di altri episodi singolarmente improbabili.

PRIORITA' DEGLI INTERVENTI

Una tale rappresentazione è un importante punto di partenza per la definizione delle priorità e la programmazione temporale degli interventi di prevenzione e protezione da adottare. La valutazione numerica e cromatica del livello di rischio permette di identificare la priorità degli interventi da effettuare, ad esempio:

Livello rischio		Azioni	Priorità intervento	
R > 6	ALTO	Azioni correttive IMMEDIATE	3	immediato
4 ≤ R ≤ 6	MODERATO	Azioni correttive/migliorative da programmare nel BREVE-MEDIO TEMPO	2	entro 6 mesi
1 ≤ R ≤ 2	LIEVE	Interventi e azioni correttive non sono indispensabili. TENERE IL RISCHIO SOTTO CONTROLLO	1	

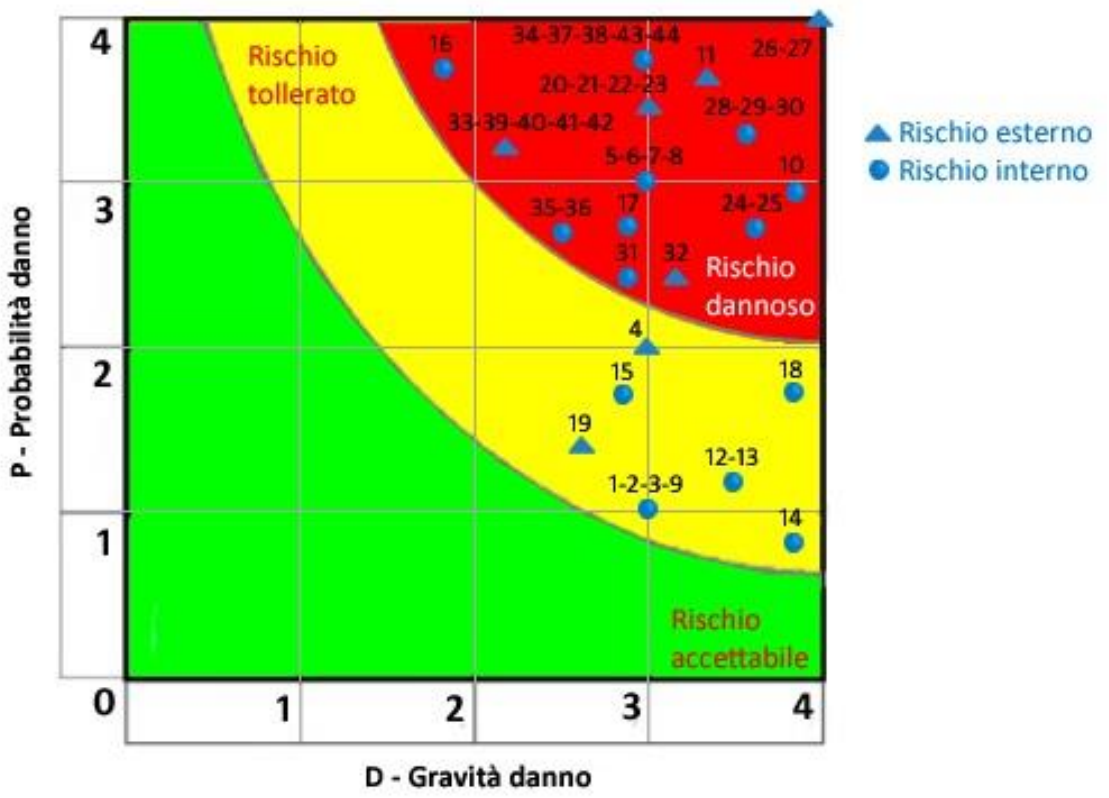
E' stato poi possibile determinare e costruire una matrice dei rischi, simile a quella mostrata in Figura che segue, ovvero una rappresentazione sintetica del posizionamento relativo dei singoli rischi rispetto al rischio accettabile e al rischio tollerato, consentendo ai vertici di identificare le priorità di azione e le possibili strategie di risposta al rischio.

La valutazione del rischio, data dal prodotto di probabilità di accadimento e gravità del danno, genera tre livelli di rischio riportati nel grafico che segue nel quale sono riportate solo tre aree diversamente colorate: la rossa, il alto a destra individuata come area di "**rischio dannoso**" dalla quale bisogna uscire programmando perché ciò accada in tempi ragionevoli, quella centrale di colore giallo che individua l'area di "**rischio tollerato**", ed infine la terza, la verde individuata come area di "**rischio accettabile**".

Rischio Lieve o accettabile– 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 Moderato o tollerato – 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 o dannoso – Evitare/Ridurre: Il rischio supera i livelli precedenti. Necessita un'elevata attenzione da parte della direzione che deve organizzare 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.

SEZIONE X
Metodologia di gestione della compliance

Il sistema documentale

Operativamente il modello di conformità viene declinato attraverso l'implementazione del **Sistema Documentale** di seguito descritto:

Principio generale con riferimento alla legge	Descrizione
Disciplinare interno art. 5, c. 2	Il presente manuale è finalizzato a fornire evidenza del rispetto dei requisiti del Regolamento europeo
Autorizzazione e istruzioni Art. 29	Fascicolo con cui si autorizzano ed istruiscono gli autorizzati ad un corretto e lecito trattamento dei dati acquisiti dalla scuola.
Nomina autorizzati esterni Art. 28	Modulo da utilizzarsi per richiedere garanzie di tutela a tutti i soggetti esterni che trattano dati per conto della scuola.
Accordo di Contitolarità Art. 26	Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento.
Trattamento nuovo art. 25	Format per le valutazioni preliminari da effettuarsi prima dell'inizio di nuove attività di trattamento. .
Registro dei trattamenti	E' opportuno che tale registro sia aggiornato e revisionato periodicamente.
Registro violazioni art. 33	Format per la registrazione degli eventi che possono compromettere la sicurezza dei dati personali.
Comunicazione violazioni art. 34	Format per la comunicazione dei data breach all'Autorità garante ed agli interessati.
Informative agli interessati art. 13 e 14	Informazioni fornite a tutto il personale interessato in merito al trattamento dei loro dati personali da parte della scuola.
Informativa web art. 13	Ulteriori informazioni in merito alle privacy policy adottate dall'organizzazione
Diciture semplificate art. 13	Eventuali modalità semplificate di informativa (es: inserimento in disclaimer email, informative sintetiche, ….
Diritti interessati artt. 15 - 21	Format per una corretta gestione delle richieste di esercizio dei diritti da parte degli interessati.

Aggiornamento, distribuzione, validazione, divulgazione, validità

Il suddetto sistema documentale è gestito come segue.

Aggiornamento

- Il presente disciplinare interno sarà oggetto di verifica ed aggiornamento su base semestrale.
- Su base annuale sarà inoltre effettuato un audit di conformità complessivo, con verifica dei rating di rischio assegnati e validità del piano di sicurezza implementato.
- Gli allegati saranno oggetto di aggiornamento immediato in caso di variazioni significative dei contenuti.

Repository

- Tutti i documenti sono conservati in Originale presso la sede della scuola.
- Una copia conforme digitale è conservata presso sede della società incaricata alla Protezione dei dati personali (RPD)

Validazione

La validazione del presente disciplinare interno è effettuato dal Titolare in calce allo stesso ed è da ritenersi estesa a tutti gli allegati.

Divulgazione

Il Disciplinare e i relativi allegati sono divulgabili individualmente solo a soggetti direttamente coinvolti nel sistema, oppure a soggetti preposti a verifiche di legge (es: autorità ispettive, ……). Su specifica e motivata richiesta potranno essere portate a conoscenza di ulteriori soggetti interessati (eventualmente in forma semplificata e priva di dati personali in chiaro).

Validità

Ai sensi delle significative novità introdotte dal Regolamento europeo il Titolare ha deciso di effettuare una revisione complessiva della compliance privacy, pertanto il presente disciplinare e relativi allegati annullano e sostituiscono la documentazione precedentemente adottata (ci si riserva la facoltà di effettuare semplici integrazioni in merito alla documentazione già sottoscritta con gli autorizzati / interessati, per esempio moduli di nomina ed informative).

Perimetro di applicazione

Il presente disciplinare si applica a tutti i trattamenti effettuati dalla scuola in qualità di Titolare. In particolare si applica ai trattamenti effettuati:

- presso la sede centrale e plessi;
- da personale autorizzato;
- attraverso strumenti elettronici forniti dalla scuola.

Altri possibili ruoli privacy

E' importante ricordare che il D. legislativo 101 del 2018 prevede nel suo art. 2-quaterdecies la possibilità di nominare in Comitato ristretto di operatori della scuola con l'incarico di coordinare temi privacy definibili in seno allo stesso Comitato, senza assumere responsabilità verso l'esterno.

Scopo della presente SEZIONE è quello di fornire ai dirigenti scolastici uno strumento di controllo continuo per vigilare sulla conformità di tutte le procedure alle disposizioni del Regolamento europeo così da creare il c. d. "onere della prova", indispensabile per dimostrare l'adozione di tutte le misure idonee ad evitare il verificarsi di danni, cioè di avere impiegato ogni cura ed attenzione atta ad impedire il verificarsi dell'evento dannoso.

Pertanto, il titolare e il responsabile del trattamento mettono in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

E' bene precisare che qualunque intervento di semplice controllo o anche con effetti migliorativi devono essere sempre accompagnati da processi di verbalizzazione i cui contenuti di linguaggio semplice, chiaro ed esaustivo, riporteranno il nome del verbalizzante, la data dell'intervento, la sua natura, l'obiettivo da raggiungere o quello raggiunto.

In caso di interventi migliorativi da realizzare dovranno essere indicati anche la data di completamento e il nominativo dell'operatore.

E' consigliabile utilizzare un unico registro denominato "*registro dei verbali*" ove verbalizzare, a cura del Dirigente scolastico, tutti gli interventi eseguiti in modo strettante cronologico, da gestire come se fosse il diario di bordo della nave.

Tale registro può essere mantenuto in modalità informatica; in questo caso occorre che mensilmente vengano "chiusi" a cura del Dirigente scolastico gli interventi eseguiti nel mese apponendo al termine la propria firma digitale.

La presente PARTE, quindi, è suddivisa in due sezioni, una dedicata agli adempimenti di misure di natura organizzativa e l'altra di natura tecnica.

1^ Sezione dedicata all'adozione di misure organizzative.

Misura organizzativa n. 1	Descrizione dell'intervento
Consegna delle chiavi della scuola CONTROLLARE E VERBALIZZARE LA MISURA SEMESTRALMENTE	Occorre effettuare precisa e dettagliata ricognizione di tutti gli accessi alla scuola. Stabilire quali aperture devono restare attive e in corrispondenza di queste predisporre due copie in originale, conservate separatamente, una a cura del Dirigente scolastico e l'altra del Direttore amministrativo . Si consegneranno copie di chiavi ai collaboratori scolastici che avranno assegnati determinati accessi, verbalizzando le avvenute consegne. In ordine all'ingresso principale i collaboratori scolastici addetti a tale servizio, si impegnano a non lasciare mai incustodito l'accesso. Devono verbalizzare in apposito registro gli accessi utilizzando quello predisposto dalla scuola. Per tale servizio devono essere autorizzati al trattamento, con relativa lettera autorizzativa, chi è designato a ciò.

Misura organizzativa n. 2	Descrizione dell'intervento
Sistema di allarme CONTROLLARE E VERBALIZZARE LA MISURA ANNUALMENTE	Occorre che di questo strumento, utile alla tutela fisica dei dati, si mantenga efficiente il sistema verificando periodicamente il buon funzionamento della batteria di cui è dotato il sistema. Pertanto, di dovrà identificare una persona esperta che sappia effettuare il controllo e informare il dirigente che verbalizzerà il risultato nell'apposito registro dei verbali.

Misura organizzativa n. 3	Descrizione dell'intervento
Sistema antincendio	L'impianto antincendio è l'insieme degli elementi tecnici che hanno la funzione di prevenire, eliminare, limitare o segnalare incendi. Le scuole hanno profili interni che hanno il compito di effettuare controlli nel mantenere efficienti gli estintori, ed altro, che devono essere posizionati in modo idoneo per rispondere ai rischi potenziali del verificarsi di un incendio.

Misura organizzativa n. 4	Descrizione dell'intervento
Controllo periodicamente del buon funzionamento dei gruppi di continuità (UPS) CONTROLLARE E VERBALIZZARE LA MISURA TRIMESTRALMENTE	Un grippo statico di continuità è una apparecchiatura utilizzata per mantenere costantemente alimentati in corrente alternata apparecchi elettrici. Basti pensare la fine che possono fare i dati personali già elaborati se sono sottoposti alla immediata interruzione di corrente elettrica. L'uso dei gruppi di continuità garantisce per un breve periodo di tempo l'erogazione della corrente così da poter "salvare" i lavori in essere. Per controllare la funzionalità dei gruppi basta accendere tutti i computer della LAN, staccare l'interruttore centrale e verificare che gli UPS rimangono in funzione. Se la risposta dovesse risultare negativa, chiamare urgentemente un tecnico per intervenire con consapevolezza. Questa operazione deve essere verbalizzata e controllare successivamente l'esito dell'intervento del tecnico. **La verbalizzazione va effettuata anche se la funzionalità degli UPS risultasse positiva.** Si suggerisce di provvedere a sostituire gradualmente gli attuali UPS con gli ultimi ritrovati che garantiscono autonomamente il salvataggio dell'attività in corso per un periodo di tempo limitato, ma bastevole e questo dispositivo lo esegue in autonomia utilizzando gli ultimi minuti a disposizione prima che la batteria si scarica completamente.

Misura organizzativa n. 5	Descrizione dell'intervento
Interventi tecnici sui personal computer CONTROLLARE E VERBALIZZARE LA MISURA AL MOMENTO	Ogni volta che un tecnico interviene tecnicamente su un computer che richiede il trasferimento dello stesso in manutenzione, si dovrà creare un verbale di consegna descrivendo in esso la presunta tipologia di intervento da effettuare. La successiva fattura emessa dal tecnico riporterà pedissequamente la descrizione che deve trovare riscontro con la ricevuta che accompagna il computer. Di questa operazione si lascerà debita traccia nel registro dei verbali. Analogamente se un computer dovesse essere trasferito da un ufficio ad un altro **occorre verbalizzare** anche questa operazione.

Misura organizzativa n. 6	Descrizione dell'intervento
Modificazione delle credenziali di accesso al proprio computer CONTROLLARE E VERBALIZZARE LA MISURA ALMENO TRIMESTRALMENTE ED AVENTALMENTE AL MOMENTO	Le parole chiave **personali** vanno direttamente gestite dagli utenti dei calcolatori attraverso modalità alcune delle quali qui vengono richiamate: - La eventuale chiave di accensione e di accesso agli applicativi software su elaboratori connessi in rete e dello screen saver, sono conosciute **soltanto** dall'autorizzato. Egli stesso provvederà ad elaborarla, mantenendola segreta e modificandola periodicamente, con cadenza almeno trimestrale se il computer contiene dati sensibili. Alla prima elaborazione, ed ad ogni modifica delle credenziali, ogni autorizzato dovrà trascriverla su un foglio, da riporre in busta chiusa intestando la stessa con il proprio cognome, nome e data. Sarà cura di ogni autorizzato consegnare detta busta al custode delle credenziali, ritirando la precedente ed annotando l'operazione in apposito registro dedicato. Il custode delle credenziali lascerà traccia della modificazione nel registro dei verbali. - I requisiti minimi che gli autorizzati devono utilizzare nell'elaboratore e modificare le password sono i seguenti: * la password deve essere composta da almeno **otto caratteri oppure,** nel caso in cui lo strumento elettronico non permetta una tale lunghezza, da un numero di caratteri al massimo consentito; * almeno ¼ dei caratteri che compongono la password deve essere di natura numerica, gli altri alfabetici con l'inclusione di qualche carattere speciale; * la password non deve contenere riferimenti agevolmente riconducibili all'interessato (non solo nomi, cognomi, soprannomi, ma neppure date di nascita propria, dei figli o di persone vicine); * la password non deve contenere nomi di persone; * la password deve essere diversa dal nome di utente *(Username);* * la password di accensione deve essere diversa dalle altre password. Quando il titolare della password si assente, il supplente designato dalla scuola, riceverà la busta contenente le credenziali dell'assente che saranno utilizzate dal supplente per l'attività lavorativa a cui è chiamato. Sostituirà la password dell'assente. Al ritorno dell'operatore eseguirà tutti passaggi descritti precedentemente e sostituirà ancora una volta le credenziali. Tutte queste operazioni dovranno essere annotare pedissequamente nel registro di verbali.

Misura organizzativa n. 7	Descrizione dell'intervento
Custodia e cancellazione dei dati in supporti ottici CONTROLLARE E VERBALIZZARE LA MISURA AL MOMENTO	Il problema della cancellazione delle informazioni riguarda chiunque mantenga memorizzati su dispositivi elettronici dati relativi a terzi: è infatti compito di chi detiene stabilmente dati di assicurare che questi non possano andare dispersi se acquisiti anche in modo incontrollato da estranei. La semplice cancellazione dei file o la formattazione dell'hard disk, infatti, non sempre realizzano una vera cancellazione delle informazioni registrate, che rimangono spesso fisicamente presenti e tecnicamente recuperabili. E' severamente proibito l'uso di "chiavette" per conservare dati e/o per l'utilizzo degli stessi fuori l'ambiente scolastico. Per prevenire l'acquisizione indebita di dati è necessario operare in diversi modi e tempi a seconda delle circostanze: ⇒ *preventivamente, con tecniche di memorizzazione sicura.* La memorizzazione sicure dei file si può realizzare sui più diffusi sistemi operativi con l'attivazione di funzionalità crittografiche proprie del sistema. Basta, pertanto fare riferimento alla casa che ha fornito il sistema operativo. Laddove la casa produttrice non avesse disponibile tali funzionalità si può ottenere il risultato desiderato con l'installazione di adeguati prodotti aggiuntivi. ⇒ *immediatamente prima della cessione o dismissione dell'apparato*

	elettronico, con strumenti software di cancellazione sicura (a condizione che l'elaboratore sia funzionante). Le principali produttrici (commerciali e non) illustrano nel dettaglio in sezioni del loro sito web, le modalità per affrontare il problema della cancellazione sicura con procedimenti che variano a seconda della casa produttrice. Più in particolare, se se il sistema operativo adottato è WS Windows, l'utente può fare riferimento alle pagine informative pubblicate nel sito che illustrano nel dettaglio le modalità per affrontare il problema della cancellazione di interi volumi di dati qualora non sia stata preventivamente adottata la soluzione della memorizzazione sicura. Analogo comportamento è praticabile allorquando il sistema operativo adottato è Apple MacOS X, che incorpora una funzione "svuotamento del cestino in modalità sicura", potranno trovare informazioni dettagliate sul sito del produttore. Infine, gli utenti che adottano un sistema operativo del tipo open source o comunque con licenze d'uso non commerciabili sono disponibili per i sistemi Unix o Linux alcuni sistemi e da questi si distingue per affidabilità ed efficacia il DBAN utilizzabile con efficacia. Nel caso in cui il dispositivo elettronico da sottoporre a smaltimento non sia più funzionante, e non siano applicabili le misure software, allo scopo di garantire l'impossibilità di recupero dei dati da parte di terzi estranei occorre procedere con modalità hardware, basate sull'uso di dispositivi di demagnetizzazione o con la distruzione fisica. I dispositivi di demagnetizzazione permettono "l'azzeramento" delle aree magnetiche delle superfici o di altre memorie a stato solido, agendo anche sui circuiti elettronici che fanno parte del dispositivo a causandone l'inutilizzabilità successiva. In determinati casi è necessario ricorrere alla distruzione fisica dei dispositivi di memoria danneggiando irreparabilmente tali dispositivi. Infine, è opportuno che al termine delle operazioni di cancellazione dei dati da supporti di memorizzazione, si deve effettuare un verbale di constatazione delle operazioni eseguite nel registro dei verbali
Misura organizzativa n. 8	Descrizione dell'intervento
Antivirus I LIVELLI DI PROTEZIONE CHIESTI ALL'ANTIVIRUS DIPENDONO DA MOLTE VARIABILI. OCCORRE DEFINIRE QUALE CONFIGURAZIONE DEBBA AVERE LA LAN.	Un antivirus da solo, per quanto affidabile ed efficiente, non è da considerare una protezione totale contro la totalità dei virus informatici esistenti al mondo. Inoltre, un antivirus si basa su determinate regole ed algoritmi scritti da esseri umani, e pertanto queste possono portare a errori positivi, ossia file riconosciuti come infetti quanto non lo sono, e falsi negativi, il caso opposto, oppure a decisioni sbagliate. Dal punto di vista tecnico ci sono svariati metodi che si possono utilizzare per prevenire e individuare malware. Un'ulteriore limitazione è dovuta al fatto che un virus potrebbe essere ancora non abbastanza diffuso, r quindi non essere ancora stato studiato da tutti i produttori di antivirus. Pertanto è indispensabile installare **esclusivamente antivirus licenziato** nel server della LAN della scuola in modo che, essendo autoaggiornante, automaticamente aggiornerà tutti i client della rete.

Misura organizzativa n. 9	Descrizione dell'intervento
Cartellini idenficativi CONTROLLARE E VERBALIZZARE LA MISURA ANNUALMENTE	Quanto segue è tratto dalle Linee guida *in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico* (al punto 6.4), emesse dal Garante per la privacy. L'esibizione di cartellini identificativi costituisce un esempio di diffusione di dati personali. Nell'ambito del lavoro alle dipendenze delle pubbliche amministrazioni i cartellini identificativi possono rappresentare un valido strumento per garantire trasparenza ed efficacia dell'azione amministrativa, nonché per migliorare il rapporto tra operatori ed utenti. Nel selezionare i dati personali destinati ad essere diffusi attraverso i cartellini identificativi, le amministrazioni sono tenute a rispettare i principi di pertinenza e non eccedenza dei dati in rapporto alle finalità perseguite. Pertanto, può risultare ingiustificato riportare nei suddetti cartellini ulteriori elementi rispetto alla qualifica, al ruolo professionale, alla fotografia ed un codice identificativo, quale può essere il nome per esteso e il cognome riportando solo l'iniziale seguito da un punto. La fonte normativa che obbliga l'uso dei cartellini identificativi è il d. lgs. 27 ottobre 2009, n. 150, che dispone, appunto, all'art. 73, comma 2, l'obbligo di esporre cartellini o targhe identificativi.

Misura organizzativa n. 10	Descrizione dell'intervento
Accesso agli archivi storici CONTROLLARE E VERBALIZZARE LA MISURA AL MOMENTO	Molte scuole hanno distribuito l'archivio storico cartaceo in diverse sedi, Basti pensare all'effetto della verticalizzazioni subito da molte scuole. Occorre pertanto che siano designati ed autorizzati, per ciascun plesso sede di archivio, addetti al prelevamento di documenti e al deposito degli stessi. Tutte le operazioni di prelievo e deposito o di variazione di addetti, saranno verbalizzati nel registro dei verbali. Utile sarebbe l'uso di un registro.

Misura organizzativa n. 11	Descrizione dell'intervento
Custodia e gestione di dati particolari CONTROLLARE E VERBALIZZARE LA MISURA TRIMESTRALMENTE	Le apparecchiature informatiche e gli archivi cartacei, chiusi in armadi, contenenti dati particolari sono situati in carpette separate da quelle contenenti dati generali in locali ad accesso controllato. Per quanto riguarda il trattamento di dati di natura sensibile idonei a rilevare lo stato di disabilità degli alunni censiti in Anagrafe Nazionale degli Studenti nella partizione separata basta applicare quanto prescritto nel decreto ministeriale n. 162 del luglio 216.

Misura organizzativa n. 12	Descrizione dell'intervento
Informative CONTROLLARE E VERBALIZZARE LA MISURA SEMESTRALMENTE	Le informative costituiscono l'elemento fondamentale ed obbligatorio, per dare una dimostrazione della trasparenza amministrativa della scuola. Esse devono essere rintracciate facilmente dall'interessato e poste in apposita sezione del sito web dedicata alla privacy nella scuola. Le informative devono riguardare: gli alunni, il personale, i fornitori, gli alunni

	censiti in ANS, le immagini registrate in videosorveglianza, i cookies del sito.

Misura organizzativa n. 13	Descrizione dell'intervento
Lettere di autorizzazione al trattamento dei dati CONTROLLARE E VERBALIZZARE LE VARIAZIONI DELLA MISURA ANNUALMENTE	Le lettere autorizzative sono rilasciate, come atto recettizio, ai sensi dell'art. 28 del Regolamento europeo. Da responsabile del trattamento, se presente, o dal titolare del trattamento. Importante è titolare che il successivo art. 29 prescrive che chiunque abbia accesso a dati personali non può trattare tali dati se non è istruito, sotto l'autorità del responsabile o dal titolare, che si assumono la responsabilità di tale istruzione. Occorre, pertanto, controllare periodicamente il contenuto di tali lettere che devono essere rilasciate a: - gli assistenti amministrativi; - ai collaboratori scolastici che svolgono attività speciali di tipo fotoriproduzione per gli uffici amministrativi, servizi esterni, portineria, servizi a disabili; - RLS; - docenti; - collaboratori del dirigente scolastico; - autorizzati esterni, il tipo tecnico della manutenzione dei PC, RSPP, …. - supplenti, per periodi brevi e non, di docenti ed ATA. Su questo punto il collaboratore scolastico che predispone il relativo contratto utilizzerà il modello della relativa lettera di autorizzazione al trattamento che si troverà sul suo desktop, inserirà i dati anagrafici, lo stesso protocollo del contratto (se possibile). Una copia (unitamente al contratto e all'informativa) va consegnata al supplente mentre l'altra, sottoscritta dal supplente, va conservata nel fascicolo digitale dell'interessato.

SEZIONE XI
I diritti dell'interessato

Articolo 15 - **Diritto di accesso dell'interessato ai propri dati.**

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;

b) le categorie di dati personali in questione;

c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;

f) il diritto di proporre reclamo a un'autorità di controllo;

g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.

3. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

4. Il diritto di ottenere una copia di cui al paragrafo 3. non deve ledere i diritti e le libertà altrui.

Articolo 16 - **Diritto di rettifica**

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Articolo 17 - **Diritto alla cancellazione («diritto all'oblio»)**

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali.

Articolo 18 - **Diritto di limitazione di trattamento**

L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre almeno una delle ipotesi previste dall'articolo.

Articolo 19 - **Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento.**

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Articolo 20 - **Diritto alla portabilità dei dati.**

"l'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti".

Articolo 21- **Diritto di opposizione.**

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano compresa la profilazione. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Articolo 22 - **Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione.**

L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

SEZIONE XII
L'Ufficio del Garante: unità di controllo

Per una completa comprensione dell'argomento si è preferito riportare gli articoli del Regolamento che afferiscono al tema che stiamo presentando nella presente **SEZIONE** congiuntamente ai corrispondenti articoli del decreto legislativo 101/2018 che hanno integrato in maniera considerevole il Regolamento stesso.

L'art. 2-bis del decreto legislativo n. 101 del 2018, rubricato come: **Autorità di controllo** nel suo art. 1 statuisce che *L'Autorità' di controllo di cui all'articolo 51 del Regolamento e' individuata nel Garante per la protezione dei dati personali, di seguito «Garante», di cui all'articolo 153.*

Art. 154/101. – Compiti del Garante

1. Oltre a quanto previsto da specifiche disposizioni e dalla Sezione II del Capo VI del Regolamento, il Garante, ai sensi dell'articolo 57, paragrafo 1, lettera v), del Regolamento medesimo, anche di propria iniziativa e avvalendosi dell'Ufficio, in conformità alla disciplina vigente e nei confronti di uno o più titolari del trattamento, ha il compito di:

a) controllare se i trattamenti sono effettuati nel rispetto della disciplina applicabile, anche in caso di loro cessazione e con riferimento alla conservazione dei dati di traffico;

b) trattare i reclami presentati ai sensi del regolamento, e delle disposizioni del presente codice, anche individuando con proprio regolamento modalità specifiche per la trattazione, nonché fissando annualmente le priorità delle questioni emergenti dai reclami che potranno essere istruite nel corso dell'anno di riferimento;

c) promuovere l'adozione di regole deontologiche, nei casi di cui all'articolo 2-quater;

d) denunciare i fatti configurabili come reati perseguibili d'ufficio, dei quali viene a conoscenza nell'esercizio o a causa delle funzioni;

e) trasmettere la relazione, predisposta annualmente ai sensi dell'articolo 59 del Regolamento, al Parlamento e al Governo entro il 31 maggio dell'anno successivo a quello cui si riferisce;

f) assicurare la tutela dei diritti e delle libertà fondamentali degli individui dando idonea attuazione al Regolamento e al presente codice;

g) provvedere altresì all'espletamento dei compiti ad esso attribuiti dal diritto dell'Unione europea o dello Stato e svolgere le ulteriori funzioni previste dall'ordinamento.

2. Il Garante svolge altresì, ai sensi del comma 1, la funzione di controllo o assistenza in materia di trattamento dei dati personali prevista da leggi di ratifica di accordi o convenzioni internazionali o da atti comunitari o dell'Unione europea.

Art. 154-bis/101. Poteri del Garante

1. Oltre a quanto previsto da specifiche disposizioni, dalla Sezione II del Capo VI del Regolamento e dal presente codice, ai sensi dell'articolo 58, paragrafo 6, del Regolamento medesimo, il Garante ha il potere di:

a) adottare linee guida di indirizzo riguardanti le misure organizzative e tecniche di attuazione dei principi del Regolamento, anche per singoli settori e in applicazione dei principi di cui all'articolo 25 del Regolamento;

b) approvare le regole deontologiche di cui all'articolo 2-quater.

2. Il Garante può invitare rappresentanti di un'altra autorità amministrativa indipendente nazionale a partecipare alle proprie riunioni, o essere invitato alle riunioni di altra autorità amministrativa indipendente nazionale, prendendo parte alla discussione di argomenti di comune interesse; può richiedere, altresì, la collaborazione di personale specializzato addetto ad altra autorità amministrativa indipendente nazionale.

3. Il Garante pubblica i propri provvedimenti sulla base di quanto previsto con atto di natura generale che disciplina anche la durata di tale pubblicazione, la pubblicità nella Gazzetta Ufficiale della Repubblica italiana e sul proprio sito internet istituzionale nonché i casi di oscuramento.

4. In considerazione delle esigenze di semplificazione delle micro, piccole e medie imprese, come definite dalla raccomandazione 2003/361/CE, il Garante per la protezione dei dati personali, nel rispetto delle disposizioni del Regolamento e del presente Codice, promuove, nelle linee guida adottate a norma del comma 1, lettera a), modalità semplificate di adempimento degli obblighi del titolare del trattamento.

Art. 154-ter/101. Potere di agire e rappresentanza in giudizio

1. Il Garante e' legittimato ad agire in giudizio nei confronti del titolare o del responsabile del trattamento in caso di violazione delle disposizioni in materia di protezione dei dati personali.
2. Il Garante e' rappresentato in giudizio dall'Avvocatura dello Stato, ai sensi dell'articolo 1 del regio decreto 30 ottobre 1933, n. 1611.
3. Nei casi di conflitto di interesse, il Garante, sentito l'Avvocato generale dello Stato, può stare in giudizio tramite propri funzionari iscritti nell'elenco speciale degli avvocati dipendenti di enti pubblici ovvero avvocati del libero foro.

Art. 157/101. - Richiesta di informazioni e di esibizione di documenti

1. Nell'ambito dei poteri di cui all'articolo 58 del Regolamento, e per l'espletamento dei propri compiti, il Garante può richiedere al titolare, al responsabile, al rappresentante del titolare o del responsabile, all'interessato o anche a terzi di fornire informazioni e di esibire documenti anche con riferimento al contenuto di banche di dati.

Art. 158/101. Accertamenti

1. Il Garante può disporre accessi a banche di dati, archivi o altre ispezioni e verifiche nei luoghi ove si svolge il trattamento o nei quali occorre effettuare rilevazioni comunque utili al controllo del rispetto della disciplina in materia di trattamento dei dati personali.
2. I controlli di cui al comma 1, nonché quelli effettuati ai sensi dell'articolo 62 del Regolamento, sono eseguiti da personale dell'Ufficio, con la partecipazione, se del caso, di componenti o personale di autorità di controllo di altri Stati membri dell'Unione europea.
3. Il Garante si avvale anche, ove necessario, della collaborazione di altri organi dello Stato per lo svolgimento dei suoi compiti istituzionali.
4. Gli accertamenti di cui ai commi 1 e 2, se svolti in un'abitazione o in un altro luogo di privata dimora o nelle relative appartenenze, sono effettuati con l'assenso informato del titolare o del responsabile, oppure previa autorizzazione del

presidente del tribunale competente per territorio in relazione al luogo dell'accertamento, il quale provvede con decreto motivato senza ritardo, al più tardi entro tre giorni dal ricevimento della richiesta del Garante quando è documentata l'indifferibilità dell'accertamento.

5. Con le garanzie di cui al comma 4, gli accertamenti svolti nei luoghi di cui al medesimo comma possono altresì riguardare reti di comunicazione accessibili al pubblico, potendosi procedere all'acquisizione di dati e informazioni on-line. A tal fine, viene redatto apposito verbale in contraddittorio con le parti ove l'accertamento venga effettuato presso il titolare del trattamento.

Art. 159/101. Modalità

1. Il personale operante, munito di documento di riconoscimento, può essere assistito ove necessario da consulenti tenuti al segreto su ciò di cui sono venuti a conoscenza, nell'esercizio delle proprie funzioni, in ordine a notizie che devono rimanere segrete. Nel procedere a rilievi e ad operazioni tecniche può altresì estrarre copia di ogni atto, dato e documento, anche a campione e su supporto informatico o per via telematica. Degli accertamenti e' redatto sommario verbale nel quale sono annotate anche le eventuali dichiarazioni dei presenti.

2. Ai soggetti presso i quali sono eseguiti gli accertamenti e' consegnata copia dell'autorizzazione del presidente del tribunale, ove rilasciata. I medesimi soggetti sono tenuti a farli eseguire e a prestare la collaborazione a tal fine necessaria. In caso di rifiuto gli accertamenti sono comunque eseguiti e le spese in tal caso occorrenti sono poste a carico del titolare con il provvedimento che definisce il procedimento, che per questa parte costituisce titolo esecutivo ai sensi degli articoli 474 e 475 del codice di procedura civile.

3. Gli accertamenti, se effettuati presso il titolare o il responsabile o il rappresentante del titolare o del responsabile, sono eseguiti dandone informazione a quest'ultimo o, se questo è assente o non è designato, alle persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile ai sensi dell'articolo 2-quaterdecies. Agli accertamenti possono assistere persone indicate dal titolare o dal responsabile.

4. Se non e' disposto diversamente nel decreto di autorizzazione del presidente del tribunale, l'accertamento non può essere iniziato prima delle ore sette e dopo le ore venti, e può essere eseguito anche con preavviso quando ciò può facilitarne l'esecuzione.

5. Le informative, le richieste e i provvedimenti di cui al presente articolo e agli articoli 157 e 158 possono essere trasmessi anche mediante posta elettronica ((...)).

6. Quando emergono indizi di reato si osserva la disposizione di cui all'articolo 220 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, approvate con decreto legislativo 28 luglio 1989, n. 271.

Art. 160/101. Particolari accertamenti

1. Per i trattamenti di dati personali di cui all'articolo 58, gli accertamenti sono effettuati per il tramite di un componente designato dal Garante.

2. Se il trattamento non risulta conforme alle norme del Regolamento ovvero alle disposizioni di legge o di Regolamento, il Garante indica al titolare o al responsabile le necessarie modificazioni ed integrazioni e ne verifica l'attuazione. Se l'accertamento e' stato richiesto dall'interessato, a quest'ultimo e' fornito in ogni caso un riscontro circa il relativo esito, se cio' non pregiudica azioni od operazioni a tutela dell'ordine e della sicurezza pubblica o di prevenzione e repressione di reati o ricorrono motivi di difesa o di sicurezza dello Stato.

3. Gli accertamenti non sono delegabili. Quando risulta necessario in ragione della specificità della verifica, il componente designato può farsi assistere da personale specializzato tenuto al segreto su ciò di cui sono venuti a conoscenza in ordine a notizie che devono rimanere segrete. Gli atti e i documenti acquisiti sono custoditi secondo modalità tali da assicurarne la segretezza e sono conoscibili dal presidente e dai componenti del Garante e, se necessario per lo svolgimento delle funzioni dell'organo, da un numero delimitato di addetti all'Ufficio individuati dal Garante sulla base di criteri definiti dal Regolamento di cui all'articolo 156, comma 3, lettera a).

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. 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.

SEZIONE XIII
Le Sanzioni

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	da 44 a 49

segnati a fianco	
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.

Si riportano gli articoli pertinenti alle violazioni amministrative e non, dettate dalle seguenti norme del decreto legislativo 101 del 2018.

Art. 166/101.

Criteri di applicazione delle sanzioni amministrative pecuniarie e procedimento per l'adozione dei provvedimenti correttivi e sanzionatori

1. Sono soggette alla sanzione amministrativa di cui all'articolo 83, paragrafo 4, del Regolamento le violazioni delle disposizioni di cui agli articoli 2-quinquies, comma 2, 2-quinquiesdecies, 92, comma 1, 93, comma 1, 123, comma 4, 128, 129, comma 2, e 132-ter. Alla medesima sanzione amministrativa e' soggetto colui che non effettua la valutazione di impatto di cui all'articolo 110, comma 1, primo periodo, ovvero non sottopone il programma di ricerca a consultazione preventiva del Garante a norma del terzo periodo del predetto comma.

2. Sono soggette alla sanzione amministrativa di cui all'articolo 83, paragrafo 5, del Regolamento le violazioni delle disposizioni di cui agli articoli 2-ter, 2-quinquies, comma 1, 2-sexies, 2-septies, comma 7, 2-octies, 2-terdecies, commi 1, 2, 3 e 4, 52, commi 4 e 5, 75, 78, 79, 80, 82, 92, comma 2, 93, commi 2 e 3, 96, 99, 100, commi 1, 2 e 4, 101, 105 commi 1, 2 e 4, 110-bis, commi 2 e 3, 111, 111-bis, 116, comma 1, 120, comma 2, 122, 123, commi 1, 2, 3 e 5, 124, 125, 126, 130, commi da 1 a 5, 131, 132, 132-bis, comma 2, 132-quater, 157, nonché delle misure di garanzia, delle regole deontologiche di cui rispettivamente agli articoli 2-septies e 2-quater.

3. Il Garante è l'organo competente ad adottare i provvedimenti correttivi di cui all'articolo 58, paragrafo 2, del Regolamento, nonché ad irrogare le sanzioni di cui all'articolo 83 del medesimo Regolamento e di cui ai commi 1 e 2.

4. Il procedimento per l'adozione dei provvedimenti e delle sanzioni indicati al comma 3 può essere avviato, nei confronti sia di soggetti privati, sia di autorità pubbliche ed organismi pubblici, a seguito di reclamo ai sensi dell'articolo 77 del Regolamento o di attività istruttoria d'iniziativa del Garante, nell'ambito dell'esercizio dei poteri d'indagine di cui all'articolo 58, paragrafo 1, del Regolamento, nonché in relazione ad accessi, ispezioni e verifiche svolte in base a poteri di accertamento autonomi, ovvero delegati dal Garante.

5. L'Ufficio del Garante, quando ritiene che gli elementi acquisiti nel corso delle attivita' di cui al comma 4 configurino una o più violazioni indicate nel presente titolo e nell'articolo 83, paragrafi 4, 5 e 6, del Regolamento, avvia il procedimento per l'adozione dei provvedimenti e delle sanzioni di cui al comma 3 notificando al titolare o al responsabile del trattamento le presunte violazioni, nel rispetto delle garanzie previste dal Regolamento di cui al comma 9, salvo che la previa notifica della contestazione non risulti incompatibile con la natura e le finalità del provvedimento da adottare.

6. Entro trenta giorni dal ricevimento della comunicazione di cui al comma 5, il contravventore può inviare al Garante scritti difensivi o documenti e può chiedere di essere sentito dalla medesima autorità.

7. Nell'adozione dei provvedimenti sanzionatori nei casi di cui al comma 4 si osservano, in quanto applicabili, gli articoli da 1 a 9, da 18 a 22 e da 24 a 28 della legge 24 novembre 1981, n. 689; nei medesimi casi può essere applicata la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, sul sito internet del Garante. I proventi delle sanzioni, nella misura del cinquanta per cento del totale annuo, sono riassegnati al fondo di cui all'articolo 156, comma 8, per essere destinati alle specifiche attività di sensibilizzazione e di ispezione nonché di attuazione del Regolamento svolte dal Garante.

8. Entro il termine di cui all'articolo 10, comma 3, del decreto legislativo n. 150 del 2011 previsto per la proposizione del ricorso, il trasgressore e gli obbligati in solido possono definire la controversia adeguandosi alle prescrizioni del Garante, ove impartite, e mediante il pagamento di un importo pari alla metà della sanzione irrogata.

9. Nel rispetto dell'articolo 58, paragrafo 4, del Regolamento, con proprio regolamento pubblicato nella Gazzetta Ufficiale della Repubblica italiana, il Garante definisce le modalità del procedimento per l'adozione dei provvedimenti e delle sanzioni di cui al comma 3 ed i relativi termini, in conformità ai principi della piena conoscenza degli atti istruttori, del contraddittorio, della verbalizzazione, nonché della distinzione tra funzioni istruttorie e funzioni decisorie rispetto all'irrogazione della sanzione.

10. Le disposizioni relative a sanzioni amministrative previste dal presente codice e dall'articolo 83 del Regolamento non si applicano in relazione ai trattamenti svolti in ambito giudiziario.

Art. 167/101. Trattamento illecito di dati

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, e' punito con la reclusione da sei mesi a un anno e sei mesi.

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sè o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2-sexies e 2-octies, o delle misure di garanzia di cui all'articolo 2-septies ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2-quinquiesdecies arreca nocumento all'interessato, e' punito con la reclusione da uno a tre anni.

3. Salvo che il fatto costituisca più grave reato, la pena di cui al comma 2 si applica altresì a chiunque, al fine di trarre per sè o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento, arreca nocumento all'interessato.

4. Il Pubblico ministero, quando ha notizia dei reati di cui ai commi 1, 2 e 3, ne informa senza ritardo il Garante.

5. Il Garante trasmette al pubblico ministero, con una relazione motivata, la documentazione raccolta nello svolgimento dell'attività' di accertamento nel caso in cui emergano elementi che facciano presumere la esistenza di un reato. La trasmissione degli atti al pubblico ministero avviene al più tardi al termine dell'attività' di accertamento delle violazioni delle disposizioni di cui al presente decreto.

6. Quando per lo stesso fatto e' stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa e' stata riscossa, la pena e' diminuita.

Art. 167-bis/101. Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala.

1. Salvo che il fatto costituisca più grave reato, chiunque comunica o diffonde al fine di trarre profitto per sé o altri ovvero al fine di arrecare danno, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, in violazione degli articoli 2-ter, 2-sexies e 2-octies, è punito con la reclusione da uno a sei anni.

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, comunica o diffonde, senza consenso, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, e' punito con la reclusione da uno a sei anni, quando il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione.

3. Per i reati di cui ai commi 1 e 2, si applicano i commi 4, 5 e 6 dell'articolo 167.

Art. 167-ter/101 - Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sè o altri ovvero di arrecare danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala e' punito con la reclusione da uno a quattro anni.

2. Per il reato di cui al comma 1 si applicano i commi 4, 5 e 6 dell'articolo 167.

Art. 168/101. Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante

1. Salvo che il fatto costituisca più grave reato, chiunque, in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, e' punito con la reclusione da sei mesi a tre anni.

2. Fuori dei casi di cui al comma 1, e' punito con la reclusione sino ad un anno chiunque intenzionalmente cagiona un'interruzione o turba la regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti.