ISTITUTO COMPRENSIVO - *CENTRO STORICO ALBA*
Scuola Secondaria di I Grado, Scuola Primaria, Scuola dell'Infanzia
Via Balbo n.8 - 12051 (CN) - TEL. 0173 441732
C.F. 90051370048 - Codice meccanografico: CNIC85600V
e-mail cnic85600v@istruzione.it - https://centrostoricoalba.edu.it

Politica generale per il trattamento dei dati personali

Allegato 09 al Regolamento di Istituto approvato con delibera n. 6 del 07/11/2025

Istruzione operativa per l'attuazione dei principi del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali all'interno dell'Istituto scolastico

Documento	**DPMS 01-001**	**Politica generale per il trattamento e la protezione dei dati personali**
		Revisione 0 del 7/11/2025

Premessa

L'Istituto scolastico tratta numerose informazioni personali, per tali intendendosi ai sensi di legge tutti i dati riferibili "*a persone fisiche identificate o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale*" (es. nome, cognome, indirizzi di residenza, e-mail, foto, immagini, etc.); tali dati vengono trattati in qualità di titolare del trattamento o condivisi con il MIUR (nei casi previsti dalla legge o dai regolamenti).

Sotto il profilo qualitativo, oltre a dati personali identificativi c.d. "comuni", si possono rinvenire informazioni di carattere "sensibile", ovvero le **categorie particolari di personali** come quelli idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché genetici, biometrici e i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Inoltre, per il trattamento dei dati personali, si utilizzano sia strumenti informatici (elaboratori o software complessi) sia supporti cartacei o altri supporti di memorizzazione.

Oggetto

Il presente documento ha per oggetto misure procedimentali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, di seguito indicato con "RGPD", Regolamento Generale Protezione Dati), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, nell'Istituto scolastico.

Inoltre, il presente documento descrive i ruoli, le responsabilità, le modalità di governo e di gestione operativa in materia di trattamento di dati personali adottati dall'**Istituto Comprensivo Centro storico di Alba**, in qualità di Titolare del trattamento (nel seguito anche "**Scuola**") in ottemperanza al **Regolamento (UE) 2016/679 (RGPD).**

Campo di applicazione

L'ambito di applicazione del presente documento riguarda la SCUOLA che tratta dati personali in proprio e su delega del Ministero, sul territorio dello Stato italiano, anche in caso di trasferimento di dati personali da e verso l'estero (Paesi UE ed extra UE).

Destinatari e perimetro

Destinatari della presente Politica sono tutto il personale amministrativo (ATA), i collaboratori scolastici e i docenti, con riguardo alla gestione interna ed esterna dei dati personali. Tutti i soggetti impiegati a vario titolo sono, pertanto, tenuti a seguire i requisiti per il trattamento dei dati personali espressi nella presente politica.

Regole generali per il trattamento e la protezione dei dati personali

1. Principali definizioni

Nell'allegato A "**Glossario e definizioni**" sono riportate le principali definizioni richiamate nel presente documento.

2. Principi generali

La SCUOLA si impegna a far rispettare il Regolamento Europeo 2016/679 e in particolare i seguenti principi da esso tratti a tutto il personale e, in alcuni casi, ai fornitori o esperti esterni coinvolti nella gestione dei dati personale del cui trattamento è Titolare.

I dati personali devono essere sempre trattati in modo lecito e secondo correttezza sempre nel rispetto delle disposizioni di cui al D. Lgs. 30 giugno 2003 n. 196 (e s.m.i.) e del Regolamento UE 2016/679.

L'articolo 5 del Regolamento UE 2016/679 richiede che i dati personali siano:

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;

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, adottando 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;

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").

Tutti i dipendenti e i collaboratori della SCUOLA, pertanto, sono tenuti a riconoscere se stanno raccogliendo, elaborando, condividendo o utilizzando dati personali. Devono essere consapevoli dei principi generali del Regolamento UE 2016/679 e dei principi che governano la gestione dei dati

personali nella SCUOLA. Devono inoltre avere chiare le modalità per riferire i problemi relativi al trattamento dei dati personali al Responsabile della Protezione dei Dati nominato.

Tutto il personale che svolge detta attività (di seguito indicato come "**il Personale**") è tenuto ad attivarsi per far sì che i dati personali trattati siano sempre esatti e aggiornati.
I trattamenti non devono mai eccedere le finalità per le quali sono stati concepiti.

2.1 Raccolta e utilizzo dei dati

I dati personali devono essere raccolti ed elaborati in modo lecito, corretto e trasparente, e nel rispetto dei principi del Regolamento UE 2016/679.

La SCUOLA deve pertanto assicurare che:
- i dati personali vengano raccolti ed utilizzati solo per un giustificato motivo;
- prima della raccolta sia comunicata all'interessato una informativa con le indicazioni su come i suoi dati saranno utilizzati;
- i dati personali vengano utilizzati solo per lo scopo specifico descritto nell'informativa o nel modulo per il consenso (nei soli casi previsti);
- sia mantenuto un registro con tutte le informazioni relative alle attività di trattamento svolte.

2.2 Trattare i dati personali in modo lecito, legittimo e trasparente nei confronti dell'interessato

I dati personali devono essere trattati in modo lecito e legittimo rispetto alle finalità specifiche indicate nell'informativa presentata all'interessato (o nel modulo per il consenso, se previsto).

Il trattamento dei dati personali non deve violare gli obblighi di legge, il diritto comune, le finalità istituzionali o i termini contrattuali sottoscritti con l'interessato.

Non devono essere trattati dati personali per ulteriori finalità incompatibili con quella iniziale specificata nell'informativa. In caso di utilizzo dei dati personali per una finalità aggiuntiva o diversa da quella originariamente indicata, l'interessato deve essere informato del nuovo trattamento ed eventualmente fornire il suo consenso (se necessario quale base giuridica ulteriore).

Ogni comunicazione con l'interessato deve essere presentata in un modo chiaro e facilmente comprensibile.

La SCUOLA deve garantire che i dati personali raccolti siano adeguati per le finalità previste dell'organizzazione scolastica. A tal fine:
- i processi che comportano il trattamento di dati personali e i nuovi sistemi IT che supportano tale trattamento devono essere analizzati prima del trattamento, in modo da assicurare che le informazioni trattate siano pertinenti e non eccessive;
- devono essere previsti controlli periodici relativamente ai processi e ai sistemi IT che trattano dati personali per garantire che il trattamento non ecceda le finalità iniziali previste.

Laddove non è rilevante o necessario elaborare dati personali per gli scopi dell'organizzazione, la SCUOLA deve garantire che tali dati personali non vengano trattati.

3. Struttura organizzativa

Le norme sulla protezione dei dati personali individuano alcune figure organizzative obbligatorie:

3.1 Titolare del trattamento

La **SCUOLA** rappresentata ai fini previsti dal RGPD dal Dirigente Scolastico, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "**Titolare**").

La SCUOLA garantisce il rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 RGPD: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.

La SCUOLA mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al RGPD. Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.

Il Titolare adotta misure appropriate per fornire all'interessato (es. alunni o genitori):

a) le informazioni indicate dall'art. 13 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;

b) le informazioni indicate dall'art. 14 RGPD, qualora i dati personali non stati ottenuti presso lo stesso interessato.

La SCUOLA provvede a:

a) nominare eventuali Responsabili esterni del trattamento (es. fornitori di applicativi o del Registro elettronico) o designati/referenti interni (es. il DSGA), che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza.

b) nominare il Responsabile della Protezione dei Dati (RPD);

c) nominare quale Responsabile del trattamento i soggetti pubblici o privati affidatari di attività e servizi per conto della SCUOLA, relativamente alle banche dati gestite da soggetti esterni alla SCUOLA in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali;

d) decidere, in piena autonomia, in ordine alle finalità e alle modalità dei trattamenti dei dati personali, nonché agli strumenti utilizzati e al profilo della sicurezza;

e) autorizzare e istruire il personale che effettua operazioni di trattamento all'interno della SCUOLA.

La SCUOLA favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del GDPR e per dimostrarne il concreto rispetto da parte del Titolare.

3.2 Designati al trattamento (delegati)

L'art. 2-quaterdecies ("Attribuzione di funzioni e compiti a soggetti designati") del D.Lgs. 196/2003 (come novellato dal D.Lgs. n. 101/2018) dispone che "*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".

Pertanto, il DSGA, in funzione del ruolo ricoperto e delle attività espletate, viene individuato quali "**designato/delegato al trattamento dei dati**" relativamente ai servizi e all'ufficio di competenza, con compiti di supporto al Dirigente Scolastico, supervisione e controllo delle attività di trattamento e della conformità dei trattamenti alla normativa italiana ed europea in materia di protezione dei dati.

Ciò avviene con apposito atto formale, accompagnato da puntuali indicazioni operative per il corretto assolvimento dei compiti in materia di protezione dei dati, da notificarsi per iscritto al Designato.

Il Designato al trattamento dei dati personali risponde al Titolare di ogni violazione o mancata attivazione di quanto previsto dalla normativa in materia di riservatezza, sicurezza, protezione dei dati; riferisce periodicamente al Titolare in ordine alle modalità di svolgimento dei compiti assegnati; verifica che la documentazione cartacea e digitale e le relative procedure informatizzate che supportano l'attività di trattamento dei dati di propria competenza, rispondano ai principi di necessità, minimizzazione, pertinenza e non eccedenza, segnalando al Titolare eventuali situazioni di potenziale rischio.

Deve rispettare e uniformare la propria attività alle seguenti specifiche prescrizioni indicate nell'atto di designazione a "DESIGNATO AL TRATTAMENTO DEI DATI PERSONALI".

Il Designato al trattamento dei dati è tenuto ad adottare ogni misura necessaria per il rispetto della riservatezza nell'erogazione della sua attività lavorativa.

3.3 Responsabile del trattamento

Nomina dei responsabili esterni

Nei casi in cui un soggetto terzo effettua trattamenti di dati personali per conto della SCUOLA e non può essere considerato come autonomo Titolare, questi è nominato come **Responsabile trattamento dati esterno** ai sensi dell'art. 28 del Regolamento UE 2016/679.

Relativamente alla formalizzazione della nomina conseguente a tutte le tipologie di accordi/contratti, ogni soggetto interno preposto alle attività di instaurazione del rapporto ha la responsabilità di garantire che tutti i contratti aventi per oggetto in via diretta o indiretta un trattamento dei dati in nome e per conto della SCUOLA contemplino delle specifiche clausole, definite in accordo con il Responsabile della Protezione dei Dati, in cui si prevede la nomina della controparte a Responsabile esterno del trattamento oggetto del contratto. In alternativa il contratto dovrà essere integrato con la lettera di designazione a Responsabile Trattamento dei dati esterno.

3.4 Soggetto autorizzato del trattamento (ex Incaricato)

La SCUOLA designa come "Soggetto autorizzato del trattamento" tutto il proprio personale ATA, docente e collaboratori scolastici; contestualmente all'assunzione, il Titolare fornisce l'informativa e il Decreto Dirigenziale di nomina a "Soggetto autorizzato del trattamento".

La SCUOLA può designare come soggetti autorizzati (ex Incaricati) anche persone fisiche (esterne alla SCUOLA) che, per esigenze legate alle attività contrattualizzate, partecipano ai trattamenti di dati personali di cui la **SCUOLA** è Titolare.

Ogni soggetto autorizzato deve attenersi alle istruzioni ricevute dal Titolare, dal Designato interno (o Designato al trattamento) o dal Responsabile della Protezione dei Dati.

3.5 Amministratori di sistema

La SCUOLA adotta le misure di sicurezza necessarie ad adempiere alle prescrizioni definite dal Garante nel Provvedimento[1] dedicato alla figura dell'Amministratore di Sistema.

La SCUOLA ha definito specifiche procedure operative per disciplinare i seguenti aspetti:

- selezione e nomina degli Amministratori di Sistema (sia per il personale interno che per i consulenti esterni), attribuzione privilegi, aggiornamento dell'elenco degli amministratori di sistema e relativa formazione obbligatoria
- modifica e revoca delle nomine degli Amministratori di Sistema e dei relativi privilegi prevedendo il successivo aggiornamento del suddetto elenco
- verifica dell'attività degli Amministratori di Sistema
- gestione dei contratti di outsourcing e introduzione in questi ultimi delle opportune clausole per gli adempimenti Privacy in materia di Amministratori di Sistema
- gestione delle richieste da parte degli interessati di consultazione dell'elenco degli Amministratori di Sistema.

3.6 Responsabile della protezione dati (Data Protection Officer)

Il Titolare del trattamento ha designato il **Responsabile della protezione dei dati / Data Protection Officer** (in seguito indicato con "RPD" o "DPO") un soggetto giuridico esterno qualificato, in possesso di esperienza ultra decennale sui temi della Data Protection; oltre ad essere un obbligo di legge, l'RPD si configura quale figura essenziale per il rispetto delle nuove norme in materia di protezione dei dati e punto di riferimento per quanti all'interno della SCUOLA compiono operazioni di trattamento in qualità di Designati e/o autorizzati.
Il RPD diventa figura di garanzia e, pertanto, supporta la SCUOLA nel miglioramento delle attuali prassi e procedure, al fine di adeguarlo alle normative europee sul GDPR e alle ulteriori norme nazionali.

Il Responsabile Protezione Dati - RPD è incaricato dei seguenti compiti:

a) informare e fornire consulenza al Titolare nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD e dalle altre normative relative alla protezione dei dati. In tal senso il RPD può indicare al Titolare e/o al Responsabile del trattamento i settori funzionali ai quali riservare un *audit* interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;
b) sorvegliare l'osservanza del RGPD e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e del Responsabile del trattamento. Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare;

[1] Provvedimento Garante del 27 novembre 2008 - Gazzetta Ufficiale n. 300 del 24 dicembre 2008 (modificato in base al provvedimento del 25 giugno 2009), "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema".

c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare;
d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il RPD in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD;
e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD è comunicato dal Titolare al Garante;
f) altri compiti e funzioni a condizione che il Titolare del trattamento si assicuri che tali compiti e funzioni non diano adito a un conflitto di interessi. L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del RPD.

Il Titolare del trattamento assicura che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:

- il RPD è invitato a partecipare alle riunioni di coordinamento, consigli d'istituto o di classe, che abbiano per oggetto questioni inerenti la protezione dei dati personali;
- il RPD deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;
- il parere del RPD sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal RPD, è necessario motivare specificamente tale decisione;
- il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

4. Riservatezza dei dati

Il Personale deve sempre usare la massima discrezione sui dati personali di cui sia a conoscenza, curando attentamente la loro protezione.

Per assicurare tale discrezione è importante che gli spazi operativi destinati al ricevimento degli alunni o dei genitori, alla raccolta dei documenti ed alla loro conservazione siano opportunamente delimitati, per evitare il fortuito accesso da parte di terzi o di personale non interessato. Anche le comunicazioni tra colleghi di dati personali deve limitarsi a quanto necessario per l'espletamento dell'attività lavorativa, evitando di condivide informazioni con soggetti non autorizzati (es. occorre fare attenzione a chi ha accesso ai nominativi degli allievi con disturbi specifici dell'apprendimento, limitandone la conoscenza ai soli soggetti legittimati previsti dalla normativa, ad esempio i professori che devono predisporre il piano didattico personalizzato).

E' vietata ogni comunicazione di dati all'esterno della SCUOLA, salvo il caso in cui ciò sia necessario per lo svolgimento degli incarichi affidati o se deve essere effettuata per adempiere a un obbligo di legge o di regolamento.

Ogni informazione, sia che si tratti di attività attuali sia che si tratti di attività future, ed ogni altro materiale utilizzato o prodotto dai prestatori d'opera (dipendenti, consulenti o incaricati di ditte esterne) in relazione al proprio impiego/attività, è di proprietà della SCUOLA.

E' vietato copiare, diffondere, pubblicare, inviare notizie e/o informazioni tecniche che in qualche modo possano ridurre la sicurezza di funzionamento d'impianti o reti o che in qualche modo possano permettere di arrecare danni, anche di immagine, alla SCUOLA.

E' fatto divieto ad ogni dipendente o collaboratore della SCUOLA, salvo espressa autorizzazione, rilasciare comunicazioni o interviste a nome e per conto della stessa.

5. Trattamenti dei dati personali

Tutte i settori e uffici della SCUOLA sono responsabili di verificare, prima dell'effettivo trattamento, la necessità di operare su dati personali; nel caso si presenti tale fattispecie e se si tratta di categorie particolari di dati o dati giudiziari, le stesse funzioni coinvolgono il Responsabile Protezione dei Dati per concordare con questo le modalità più adeguate di trattamento.

In particolare, i casi che richiedono specifici presidi sono quelli relativi a:

- trattamenti di dati biometrici o genetici;
- trattamenti di categorie particolari di dati e dati giudiziari;
- trattamenti di dati di minori;
- trattamenti di dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;
- dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo ("profilazione");
- trasferimento di dati personali verso Paesi extra Ue.

In dettaglio, tutte le funzioni che nella SCUOLA raccolgono, utilizzano e conservano i dati personali devono:

- mantenere i dati personali in modo accurato e aggiornato per tutto il ciclo di vita degli stessi (dalla raccolta alla distruzione);
- garantire la sicurezza dei dati personali, nel rispetto delle Policy e delle Procedure della SCUOLA in materia di sicurezza delle informazioni;
- impedire l'utilizzo improprio dei dati personali per uno scopo che non è compatibile con lo scopo originale per il quale i dati sono stati raccolti;
- conservare i dati personali solo per la durata necessaria allo scopo indicato nell'informativa o per il tempo previsto dalla legge.

5.1 Archiviazione

La SCUOLA deve garantire che i dati personali siano archiviati e trattati in modo sicuro, con misure appropriate alla loro riservatezza e sensibilità. Deve essere prestata particolare attenzione alla memorizzazione dei dati personali su supporti rimovibili, dispositivi portatili (es. pen drive) o sistemi di storage di terze parti (ad es. cloud storage).

5.2 Trasferimento

Se i dati personali sono trasferiti elettronicamente o manualmente all'interno della SCUOLA o verso soggetti esterni, deve essere garantita la riservatezza delle informazioni trattate (ad esempio, per i trasferimenti elettronici, utilizzando la crittografia).

5.3 Controllo accessi

La SCUOLA deve garantire che, laddove sia consentito l'accesso ai dati personali da parte dei propri dipendenti e collaboratori, tale accesso deve essere autorizzato e limitato al solo personale per il quale è previsto il trattamento nell'ambito dello svolgimento delle proprie mansioni lavorative.

La SCUOLA deve informare il personale che l'accesso ai dati personali è valido solo a scopo lavorativo e per scopi legittimi.

Se vengono trattati dati personali ad alto rischio, la SCUOLA deve garantire che i meccanismi di controllo accessi implementati siano adeguati a proteggere la sensibilità di queste informazioni.

La SCUOLA deve monitorare gli accessi ai dati personali e tenere conto di eventuali violazioni nell'ambito della valutazione del rischio per la sicurezza delle informazioni.

6. Sicurezza del trattamento[2]

Il Titolare del trattamento mette in atto, con l'ausilio degli Amministratori del sistema informatico interni o esterni a cui viene delegata l'attuazione, misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Costituiscono misure tecniche ed organizzative che possono essere adottate:

- sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro), back up e procedure di disaster recovery/business continuity, pseudonimizzazione e cifratura;
- misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

[2] NdR: l'adozione di adeguate misure di sicurezza è lo strumento fondamentale per garantire la tutela dei diritti e delle libertà delle persone fisiche. Il livello di sicurezza è valutato tenuto conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. L'efficace protezione dei dati personali è perseguita sia al momento di determinare i mezzi del trattamento (fase progettuale) sia all'atto del trattamento.

La conformità del trattamento dei dati al RGDP in materia di protezione dei dati personali è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.

Il Titolare e ciascun Responsabile del trattamento eventualmente coinvolto si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

6.1 Minimizzare il trattamento dei dati personali rispetto alle finalità individuate

La SCUOLA deve mettere in atto misure tecniche e organizzative per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento, sia per quanto riguarda la quantità dei dati personali raccolti che per il periodo di conservazione.

Tali misure devono garantire che, per impostazione predefinita, i dati personali trattati non siano resi accessibili a un numero indefinito di persone senza l'autorizzazione dell'interessato.

In fase di definizione di un nuovo processo, o di progettazione di un nuovo sistema informativo utilizzato per il trattamento dei dati personali, deve essere garantito che:

- il trattamento sia ridotto al minimo per impostazione predefinita;
- vengano utilizzati, ove possibile, dati non riconducibili direttamente alle persone fisiche;
- le funzionalità implementate siano trasparenti rispetto al trattamento dei dati personali.
- venga conservata adeguata documentazione sulle attività di "privacy by design" implementate e sui risultati ottenuti.

Per ciascun trattamento, deve essere definito il periodo di conservazione dei dati personali, individuando alternativamente:

- l'eventuale periodo minimo di conservazione richiesto dai termini di legge, oppure il periodo minimo di conservazione stabilito da policy interne della SCUOLA;
- una giustificazione documentata dei criteri che determinano il periodo di conservazione.

Al termine del periodo di conservazione stabilito, tutte le copie dei dati personali non più richiesti per le attività operative della SCUOLA devono essere rimossi, facendo riferimento alle procedure di cancellazione (o anonimizzazione) definite dalla SCUOLA in base al "Piano di conservazione e scarto per gli archivi delle Istituzione scolastiche (massimario)".

Qualora i dati personali debbano essere trasferiti per la conservazione a lungo termine (ad esempio per dati che hanno un valore ai fini dell'archiviazione nell'interesse pubblico), devono essere sottoposti a misure tecniche e organizzative appropriate in modo da salvaguardare i diritti e le libertà dell'interessato.

7. Registro delle attività di trattamento

Il Registro è tenuto dal Titolare, nella persona del Dirigente Scolastico, presso la sede della SCUOLA in forma telematica e/o cartacea.

Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni:

a) il nome e i dati di contatto della SCUOLA, degli eventuali Contitolari del trattamento e del RPD;
b) le finalità del trattamento;
c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

Ogni Autorizzato (o Designato) può verificare, per la parte (settore) di propria competenza, la correttezza e completezza delle informazioni inserite e ad aggiornare il Registro laddove necessario.

8. Valutazioni d'impatto sulla protezione dei dati (DPIA)

Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una **valutazione dell'impatto** del medesimo trattamento (**DPIA**) ai sensi dell'art. 35 RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, p. 3, RGDP, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:

a) trattamenti valutativi o di *scoring*, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;
b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;
c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;
d) trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9 e 10 del RGDP;
e) trattamenti di dati su larga scala, tenendo conto: del numero di numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;
f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;
g) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti della SCUOLA, soggetti con patologie psichiatriche, pazienti, anziani e minori;
h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;

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

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Titolare ritenga motivatamente che non può presentare un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

Il Titolare deve consultarsi con il RPD anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il RPD monitora lo svolgimento della DPIA.

9. Violazione dei dati personali (Data Breach)

Per violazione dei dati personali (in seguito "*data breach*") si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dalla SCUOLA.

Possiamo considerare realizzata una violazione di dati nei seguenti casi:

- Lettura (presumibilmente i dati non sono stati copiati);
- Copia (i dati sono ancora presenti sui sistemi del titolare);
- Alterazione (i dati sono presenti sui sistemi ma sono stati alterati);
- Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione);
- Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione).

Di seguito alcuni possibili esempi:

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

Il personale addetto al trattamento qualora venga a conoscenza, nell'espletamento delle attività di competenza o indirettamente nello svolgimento delle stesse, del verificarsi di eventuali violazioni dei dati personali o di incidenti di sicurezza che possano esporre a rischio di violazione dei dati (data breach) deve tempestivamente informare il Dirigente Scolastico, anche attraverso il DSGA, e il Responsabile della Protezione dei Dati.

Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy. *La notifica dovrà*

avvenire entro 72 ore e comunque senza ingiustificato ritardo, utilizzando la procedura operativa predisposta (Gestione Data Breach).

Anche l'eventuale Responsabile esterno del trattamento nominato è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione entro 24 ore. E' opportuno, pertanto, che ciascun contratto di servizi con i fornitori esterni nominati quali "Responsabili ex art. 28 del RGPD" preveda clausole specifiche al riguardo.

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

- danni fisici, materiali o immateriali alle persone fisiche;
- perdita del controllo dei dati personali;
- limitazione dei diritti, discriminazione;
- furto o usurpazione d'identità;
- perdite finanziarie, danno economico o sociale.
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari,
- giudiziari).

Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi.

10. Riscontro delle richieste di accesso ai dati personali

Il Dirigente Scolastico e il DSGA, in collaborazione del Responsabile Protezione Dati, ha la responsabilità di gestire le richieste da parte degli interessati pervenute alla SCUOLA relativamente alle casistiche identificate dagli artt. 15-22 e seguenti del Regolamento UE 2016/679, utilizzando la procedura operativa predisposta.

Il Dirigente Scolastico e il DSGA, in collaborazione con il Responsabile della Protezione dei Dati, deve assicurare che l'interessato riceva riscontro alla sua richiesta entro 30 giorni. A tal fine Il Dirigente Scolastico e il DSGA sono supportati:

- dal personale ATA e dai Docenti che effettuano il trattamento in questione;
- dagli esperti legali per definire il testo della risposta;
- dagli outsourcee per raccogliere i dati personali, eventualmente trattati dai sistemi informatici, necessari a fornire il riscontro richiesto.

11. Comunicazione e diffusione dei dati

Una specifica attenzione va dedicata alle ipotesi di comunicazione o diffusione dei dati. In altri termini, ogni qual volta si prospetti l'eventualità di divulgare (in qualsiasi forma o modo) dati personali, è necessario procedere alle seguenti verifiche, specie se a riguardo di dati sensibili:

- verifica della legittimità della divulgazione alla luce della informativa fornita all'interessato;
- verifica di eventuali normative e regolamenti che consentano/rendano obbligatoria la divulgazione.

11.2 Condividere e comunicare i dati personali

I dati personali possono essere condivisi con altre Scuole, autorità pubbliche, agenzie governative o soggetti terzi (pubblici e/o privati) nel rispetto delle leggi vigenti e del Regolamento UE 2016/679.

In caso di condivisione con soggetti terzi di dati personali di cui la SCUOLA è titolare, si deve ottenere la garanzia che il soggetto terzo abbia la capacità e l'intenzione di proteggere tali dati in conformità agli standard e ai principi espressi dalla presente Policy.

Un contratto per il trattamento dei dati è richiesto ogniqualvolta a un soggetto terzo abbia accesso ai dati personali di cui la SCUOLA è titolare per elaborarli per conto della stessa SCUOLA. Tutti i contratti devono comprendere i principi generali e le condizioni per il trattamento dei dati personali.

11.3 Condividere i dati personali con soggetti terzi

La SCUOLA deve assicurare che, in caso di condivisione di dati personali con un altro soggetto, le responsabilità di entrambe le parti riguardo la protezione delle informazioni siano formalmente documentate in un accordo o contratto scritto.

Tale contratto deve garantire che, laddove il soggetto terzo utilizzi i dati personali per le proprie finalità:

- siano esplicitamente riportate le finalità per le quali le informazioni possono essere utilizzate dalla terza parte, con eventuali limitazioni o restrizioni sull'ulteriore utilizzo per altri scopi;
- il soggetto terzo fornisca una prova del proprio impegno nei confronti della SCUOLA per garantire il trattamento dei dati personali in modo da non contravvenire alla legislazione vigente.

Ogni nuovo trattamento che comporta la condivisione di dati personali con terze parti deve essere conforme con quanto indicato nell'informativa fornita all'interessato.

La SCUOLA deve assicurarsi inoltre di avere:

- una base legale per la condivisione dei dati;
- di aver fornito un'adeguata comunicazione all'interessato della condivisione dei dati;
- di aver tenuto in considerazione il principio di limitazione delle finalità del trattamento;
- di aver ottenuto il consenso dell'interessato, dove previsto.

12. Trasferire i dati personali all'estero (extra UE)

In alcuni casi dati personali possono essere condivisi con soggetti terzi che operano all'estero nel rispetto delle prescrizioni previste dal Regolamento UE 2016/679.

12.1 Trasferire i dati personali al di fuori dell'Unione Europea solo con adeguate garanzie

Qualora si renda necessario il trasferimento dei dati personali al di fuori dell'Unione Europea, la SCUOLA deve garantire la protezione dei diritti e delle libertà degli interessati:

- includendo nei contratti con le terze parti condizioni specifiche per assicurare la protezione dei dati personali;
- verificando la conformità rispetto ad un codice di condotta o ad un meccanismo di certificazione del soggetto terzo;

- mettendo in atto regole vincolanti interne nel caso in cui il trasferimento avvenga verso un'altra entità che si trova al di fuori dell'Unione Europea.

13. Misure di sicurezza per il trattamento di dati personali effettuato senza strumenti elettronici

In particolare, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento effettuate senza l'ausilio di strumenti elettronici, chiunque tratti dati all'interno della SCUOLA deve conservare gli atti, i documenti e ogni altro supporto contenente dati personali in ambienti controllati (ad esempio, locali, armadi o cassetti muniti di serratura), prelevandoli per il solo tempo necessario al loro utilizzo e restituendoli a chi ne ha la responsabilità e l'autorizzazione alla conservazione, al termine delle operazioni affidate. Nel dettaglio:

a) il materiale cartaceo contenente dati personali deve essere controllato e custodito con diligenza in modo da impedire che durante le quotidiane operazioni di lavoro terzi non autorizzati possano prenderne visione e, se il materiale contiene dati sensibili o giudiziari, esso dovrà essere conservato, sino alla restituzione, in contenitori muniti di serratura. Al termine del lavoro tutto il materiale dovrà essere riposto in armadi, cassetti o altri contenitori muniti di serratura, in maniera che ad essi non accedano persone prive di autorizzazione;

b) l'accesso agli archivi contenenti dati sensibili o giudiziari deve essere controllato;

c) gli atti ed i documenti contenenti dati personali sensibili o giudiziari sono affidati al personale esclusivamente per lo svolgimento dei relativi compiti assegnati in forma scritta: i medesimi atti e documenti sono controllati e custoditi dai predetti soggetti fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate

d) il personale ammesso, a qualunque titolo, agli archivi contenenti dati sensibili o giudiziari, dopo l'orario di chiusura, sono identificati e registrati: quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate;

e) è obbligatorio distruggere o rendere inutilizzabili i documenti cartacei e i supporti rimovibili, magnetici o ottici dismessi in modo da garantire che i dati ivi contenuti non possano più essere ricostruiti e/o utilizzati (anche parzialmente) da parte di terzi non autorizzati al trattamento: anche il materiale destinato al macero ed i supporti magnetici o ottici da eliminare devono essere trattati in modo che risulti tecnicamente impossibile recuperare, anche parzialmente, i dati contenuti negli stessi. Pertanto occorre prevederne la distruzione (se disponibili, con le apposite macchine "distruggi documenti/supporti" o con tecnologie similari) in modo da garantire che i dati in essi contenuti non possano essere ricostruiti, anche parzialmente, o utilizzati;

f) tutte le stampe effettuate, contenenti dati personali, dovranno essere trattate in modo da evitare che terzi non autorizzati possano prenderne visione oppure accedervi e/o produrne copie.

Il Dirigente Scolastico e il DSGA verificano la corretta applicazione da parte degli incaricati/autorizzati di tutte le procedure previste in materia di trattamenti effettuati.

Il Dirigente Scolastico e il DSGA verificano in particolare che l'accesso agli archivi cartacei sia consentito al solo personale autorizzato e che la distruzione dei supporti cartacei che contengono dati personali venga effettuato in conformità alla normativa vigente.

14. Misure di sicurezza per il trattamento di dati personali effettuato con strumenti elettronici (Regole per l'utilizzo di strumenti informatici)

Il Titolare e il Personale autorizzato al trattamento dei dati, qualora durante lo svolgimento della loro attività lavorativa utilizzino strumenti informatici devono rispettare quanto previsto dal "**Regolamento per l'utilizzo degli strumenti informatici, posta elettronica e Internet" della SCUOLA**.

15. Smaltimento o riuso di apparecchiature elettriche ed elettroniche

Il Dirigente Scolastico e il DSGA sono responsabili dell'adozione di opportune misure di sicurezza, anche con l'ausilio o conferendo incarico a terzi tecnicamente qualificati, per garantire l'inesistenza o la non intelligibilità di dati personali sui supporti di memorizzazione destinati al reimpiego, al riciclaggio o allo smaltimento.

16. Verifiche periodiche

Oltre alla normale verifica delle attività operative in capo al Dirigente Scolastico e al DSGA ovvero al Responsabile della Protezione dei Dati, sono previste verifiche periodiche in accordo con la normativa vigente, al fine di **verificare il rispetto della presente Politica generale per il trattamento dei dati personali.**

La SCUOLA si riserva comunque le facoltà previste dalla normativa vigente di effettuare specifici controlli ad hoc nel caso di segnalazioni di attività che hanno causato danno, che ledono diritti di terzi o che, comunque, risultino illegittime.

All'interno del Modello Organizzativo per la Protezione Dati previsto dalla SCUOLA (Data Protection Management System, c.d. DPMS), le attività di valutazione delle misure organizzative, procedurali e tecniche sono in carico del Responsabile della Protezione dei Dati o altri professionisti.

Riguardo a tali controlli il presente Regolamento costituisce preventiva e completa informativa nei confronti dei dipendenti e collaboratori.

ATTUAZIONE

Formazione e Consapevolezza

La SCUOLA deve garantire che tutti i dipendenti e i collaboratori siano informati sui principi espressi dalla presente Politica e che comprendano le responsabilità derivanti dal trattamento dei dati personali.

La SCUOLA deve assicurare che tutto il personale che tratta dati personali prenda parte alla formazione fornita periodicamente in base al proprio ruolo istituzionale.

La documentazione relativa alla partecipazione del personale alla formazione deve essere conservata come evidenza delle competenze acquisite.

Riferire potenziali inadempienze

Qualsiasi dipendente che venga a conoscenza di una possibile violazione della presente Politica e/o del Regolamento UE 2016/679 è tenuto a riferire immediatamente al Responsabile della Protezione

dei Dati personali (DPO).

I dipendenti che riferiscono potenziali inadempienze, che forniscono informazioni o che partecipano in altro modo a qualsiasi inchiesta o indagine interna su possibili inadempienze saranno protetti contro le ritorsioni secondo le normative vigenti.

Responsabilità e Implementazione

Il Dirigente Scolastico, il DSGA e il Personale che partecipa ai trattamenti ha il compito di rispettare la presente Politica nella propria attività e area di responsabilità.

Tutti i dipendenti sono responsabili del rispetto dei principi e delle regole definite nella presente Policy.

SANZIONI

È fatto obbligo a tutti i Dipendenti e collaboratori della SCUOLA di osservare le disposizioni portate a conoscenza con le presenti Istruzioni Operative. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile con provvedimenti disciplinari e/o risarcitori previsti dalla vigente normativa, nonché con tutte le azioni civili e penali consentite.

AGGIORNAMENTO E REVISIONE

La presente Politica è stata redatta tenendo conto della normativa vigente e dei Provvedimenti generali emanati dal Garante della Privacy. Per qualsiasi eventuale ulteriore indicazione, valgono oltre alla presente Politica le disposizioni della normativa vigente.

Tutti i dipendenti e collaboratori possono proporre, quando ritenuto necessario, integrazioni al presente documento. Le proposte vanno esaminate dal Titolare tramite il Responsabile della Protezione dei Dati.

La presente Politica è soggetta a revisione con frequenza periodica o qualora se ne ravveda la necessità.

Copia del presente documento verrà consegnata a ciascun dipendente o collaboratore ovvero messo a disposizione per ogni soggetto autorizzato all'utilizzo della rete scolastica interna.

Con l'entrata in vigore del presente Politica, tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi sostituite dalle presenti.

RINVIO

Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del RGPD e tutte le sue norme attuative vigenti.

Allegato A: GLOSSARIO E PRINCIPALI DEFINIZIONI

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;	RGPD
Autenticazione informatica	L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità	
Autorità di controllo	l'Autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 e, per l'Italia, il Garante per la protezione dei dati personali;	RGPD
Autorità di controllo interessata	un'Autorità di controllo interessata dal trattamento di dati personali in quanto: a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure c) un reclamo è stato proposto a tale autorità di controllo;	RGPD
Banca di dati	Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti	
Blocco	La conservazione dei dati personali con sospensione temporanea di ogni altra operazione del trattamento;	
Chiamata	La connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;	
Comunicazione	Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies (D.Lgs. 101/2018), al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;	
Comunicazione elettronica	Ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente,	

	identificato o identificabile;	
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;	RGPD
Credenziali di autenticazione	I dati e i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica	
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;	RGPD
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;	RGPD
Dati giudiziari	I dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;	
Dati identificativi	i dati personali che permettono l'identificazione diretta dell'interessato;	
Dati relativi al traffico	qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;	
Dati relativi all'ubicazione	ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;	
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;	RGPD
Categorie particolari di dati	i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, i dati genetici, i dati biometrici, nonché i dati personali	RGPD

	idonei a rivelare lo stato di salute e la vita sessuale;	
Dato anonimo	il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile	
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	RGPD
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;	RGPD
Diffusione	l dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;	
Evidenza	Nell'ambito della ISO 19011 sono definite evidenze dell'audit le registrazioni, dichiarazioni di fatti o altre informazioni, che sono pertinenti ai criteri dell'audit e verificabili. Possono essere qualitative o quantitative	ISO 19011
Impresa	la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le Scuola di persone o le associazioni che esercitano regolarmente un'attività economica	RGPD
Incaricati	le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;	
Interessato	La persona fisica cui si riferiscono i dati personali	
Limitazione di trattamento	il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;	RGPD
Parola chiave	componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;	
Politica (Policy)	Descrive, ad alto livello, la posizione di una organizzazione rispetto ad un determinato argomento. La policy, comportando un'assunzione di rischio, deve essere approvata dal top	-

	management	
Procedura	Una procedura descrive, con il livello di dettaglio adeguato, come un'organizzazione realizza uno specifico obiettivo. E' possibile che un'organizzazione si doti di un impianto documentale con procedure a diverso livello di dettaglio, dalle più generiche alle istruzioni operative. La modalità, il formato, la responsabilità di creazione e gestione, le modalità di revisione devono essere formalmente definite.	-
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;	RGPD
Profilo di autorizzazione	L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti	
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;	RGPD
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;	RGPD
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;	RGPD
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	RGPD

	raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;	
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;	RGPD
Trattamento transfrontaliero	a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro	RGPD
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;	RGPD