



ISTITUTO COMPrensIVO STATALE - CORNUDA
Prot. 0002545 del 25/05/2021
(Uscita)

POLICY PRIVACY REGOLAMENTO D'ISTITUTO

INFORMAZIONI DOCUMENTO:

Titolo	Regolamento d'Istituto Privacy		
Data di emissione	13.01.2021	Versione	A513000.05.00 rev. 02

Approvato dal C. di I. con la delibera n. 79 del 24 maggio 2021.



SOMMARIO

1. INTRODUZIONE	4
1.1 PREMessa DI CARATTERE NORMATIVO	4
1.2 PREMessa DI CARATTERE ORGANIZZATIVO	4
1.3 PREMessa DI CARATTERE METODOLOGICO	5
2. DISPOSIZIONI GENERALI	6
2.1 OGGETTO DEL REGOLAMENTO	6
2.2 FINALITA' DEL REGOLAMENTO	6
2.3 SENSIBILIZZAZIONE	6
2.4 DEFINIZIONI	7
2.5 PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI	8
2.6 TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI (DATI SENSIBILI)	9
2.7 TRATTAMENTO DEI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI (DATI GIUDIZIARI).....	10
2.8 COMUNICAZIONE DI DATI VERSO L'ESTERNO	10
3. DIRITTI DELL'INTERESSATO	11
3.1 INFORMATIVA SUL TRATTAMENTO DEI DATI	11
3.2 CONSENSO AL TRATTAMENTO DEI DATI: PRINCIPI GENERALI	12
3.3 DIRITTO DI ACCESSO DELL'INTERESSATO	12
3.4 DIRITTO DI RETTIFICA	13
3.5 DIRITTO ALLA CANCELLAZIONE (DIRITTO ALL'OBLIO)	13
3.6 DIRITTO DI LIMITAZIONE AL TRATTAMENTO.....	13
3.7 DIRITTO ALLA PORTABILITÀ DEI DATI.....	14
3.8 DIRITTO DI OPPOSIZIONE	14
3.9 PROCESSO DECISIONALE AUTOMATIZZATO (PROFILAZIONE).....	14
4. DIRITTI DI ACCESSO AGLI ATTI DELL'ISTITUTO.....	15
4.1 ACCESSO AGLI ATTI.....	15
5. TITOLARE E RESPONSABILE DEL TRATTAMENTO.....	17
5.1 TITOLARE DEL TRATTAMENTO	17
5.2 CONTITOLARI DEL TRATTAMENTO	17
5.3 DELEGATO DEL TRATTAMENTO DEI DATI.....	18
5.3 RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI EX ART. 28 DEL GDPR	19
5.4 AUTORIZZATO AL TRATTAMENTO DEI DATI.....	21
5.5 RESPONSABILE DELLA PROTEZIONE DEI DATI.....	21
6. SICUREZZA DEI DATI PERSONALI - MISURE DI CARATTERE INFORMATICO E TECNOLOGICO ...	23
6.1 PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PROTEZIONE PER IMPOSTAZIONE PREDEFINITA	23



6.2 REGISTRO ELETTRONICO DELLE ATTIVITÀ DI TRATTAMENTO	23
6.3 PROTEZIONE E SICUREZZA DEI DATI PERSONALI	23
6.4 NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITÀ DI CONTROLLO	24
6.5 VALUTAZIONE DI IMPATTO (VIP) SULLA PROTEZIONE DEI DATI.....	24
6.6 TRASFERIMENTO DI DATI PERSONALI ALL'ESTERO	25
7. ATTUAZIONE DEGLI ADEMPIMENTI EUROPEI	26
7.1 ENTRATA IN VIGORE E PUBBLICITÀ	26
7.2 DISPOSIZIONE FINALE RELATIVA AGLI "ALLEGATI TECNICI"	26



1. INTRODUZIONE

1.1 Premessa di carattere normativo

Il presente Regolamento in materia di protezione dei dati personali (così detta “privacy”) è uno strumento di applicazione del vigente Decreto Legislativo 30 giugno 2003, n. 196 (cosiddetto “Codice sulla privacy”) e, in particolare, del nuovo **Regolamento Europeo n. 2016/679**, nell'ambito dell'organizzazione dell'Istituto Comprensivo di Cornuda.

Dal 25 maggio 2018 ha trovato diretta applicazione, sul territorio nazionale, il nuovo Regolamento Europeo sulla privacy, approvato il 27 aprile 2016 e pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 04 maggio 2016.

Il Regolamento disciplina la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché la libera circolazione di tali dati. Esso abroga la precedente Direttiva 95/46/CE.

In data 19/09/2018 è entrato in vigore il Decreto legislativo 10 agosto 2018, n. 101 che adegua il Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196) alle disposizioni del Regolamento (UE) 2016/679.

È necessario pertanto, come Istituto, dotarsi sin da ora di un apposito “Regolamento” che disciplini compiti, attività e *policy* interne che garantiscano l'assolvimento degli adempimenti imposti dalle norme europee.

Il presente Regolamento d'Istituto si rende inoltre necessario per recepire, in un unico testo, i precetti normativi di maggior rilevanza, sia di carattere istituzionale che nazionale in tema di trattamento dei dati personali (*D.lgs. 196 del 30/06/2003 e ss.mm., regolamenti e codici deontologici succeduti negli ultimi anni, direttive e linee guida del Garante, Direttiva dell'UE 2000/58 sulla riservatezza nelle comunicazioni elettroniche e soprattutto Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*).

Il presente Regolamento è sottoposto ad aggiornamento periodico, in linea con le novità normative, giurisprudenziali e con le pronunce del Garante per la protezione dei dati personali.

1.2 Premessa di carattere organizzativo

Un'attenta disamina della normativa vigente in materia di privacy ha fatto emergere una necessità imprescindibile di cambiamento della mentalità che porti alla piena tutela della stessa, da considerare non solo come un oneroso rispetto di adempimenti burocratici, ma, soprattutto, come garanzia, per il cittadino-utente che si rivolge all'Istituto, di una completa riservatezza sotto il profilo sostanziale.

Il diritto alla privacy costituisce, anche secondo il Legislatore Europeo, un vero e proprio diritto inviolabile dell'essere umano, che non si limita alla tutela della riservatezza o alla protezione dei dati, ma implica il pieno rispetto dei diritti e delle libertà fondamentali nonché dignità del singolo individuo. Per questi motivi, la “cultura della privacy” necessita di divenire un vero e proprio elemento cardine dell'organizzazione di questo Istituto. A tale scopo è necessario che L'Istituto per mezzo del proprio personale si adoperi affinché possa crescere e rafforzarsi una maggiore consapevolezza in materia e ciò, non solo con una conoscenza minima dei principi fondamentali che stanno alla base della vigente normativa nel trattamento dei dati, ma anche ponendo in essere tutti



gli adempimenti di carattere tecnico ed organizzativo per contribuire concretamente al miglioramento della qualità del rapporto con l'utenza.

1.3 premessa di carattere metodologico

Vengono allegati a questo Regolamento una serie di **documenti tecnici** atti a dare compiuta attuazione ai dettami della nuova “privacy europea”.

Tali documenti, ai quali viene data massima pubblicità e diffusione tramite la pubblicazione sul sito *internet* dell’istituto, sono:

- Regole per l’adozione delle misure di sicurezza (**Allegato n. 1**);
- Disciplinare per l’uso della rete informatica (**Allegato n. 2**);
- Regolamento per il lavoro agile “smart working” (**Allegato n. 3**);
- Disciplinare per l’autorizzato al trattamento (**Allegato n. 4**);
- Procedura per la gestione delle violazioni – data breach (**Allegato n. 5**);

Si sottolinea come il principio cardine della “responsabilizzazione” (accountability nell’accezione inglese), introdotto dal nuovo Regolamento UE, imponga al Titolare del trattamento dei dati l’obbligo di attuare delle politiche adeguate in materia di protezione dei dati, con l’adozione di misure tecniche ed organizzative, anche certificate, che siano concretamente e sempre dimostrabili, oltre che conformi alle disposizioni europee (principio della “conformità” o **compliance** nell’accezione inglese); ciò anche attraverso dei comportamenti proattivi, atti a dimostrare la concreta adozione di misure finalizzate ad assicurare l’applicazione del Regolamento.

La normativa vigente lascia al Titolare ampia autonomia decisionale in merito alle modalità, alle garanzie e ai limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento.

Pertanto questo Istituto si sta impegnando, a far propri i dettami del Legislatore europeo relativi all’*accountability* ed alla *compliance*. anche attraverso la predisposizione di questo documento.



2. DISPOSIZIONI GENERALI

2.1 Oggetto del regolamento

Il presente Regolamento disciplina, all'interno dell'Istituto, la tutela delle persone in ordine al trattamento dei dati personali, nel rispetto di quanto previsto dal Codice in materia di protezione dei dati personali (Decreto Legislativo del 30/06/2003 n. 196 e ss.mm.) ed in conformità all'emanazione della nuova normativa sovranazionale, il Regolamento UE n. 679 del Parlamento Europeo e del Consiglio del 27/04/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione degli stessi.

2.2 Finalità del regolamento

Il presente Regolamento ha come fine quello di modulare la gestione dei Dati con criteri e procedure unitarie, volte alla massima tutela delle persone fisiche alle quali gli stessi si riferiscono.

L'Istituto, in virtù di quanto suddetto pertanto, garantisce che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

La protezione delle persone fisiche, con riguardo al trattamento dei dati personali, è un diritto fondamentale. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano (articolo 8, paragrafo 1, della *Carta dei diritti fondamentali* dell'Unione Europea.)

2.3 Sensibilizzazione

L'Istituto Comprensivo di Cornuda sostiene e promuove, al suo interno, ogni strumento di sensibilizzazione che possa consolidare il pieno rispetto del diritto alla riservatezza e migliorare la qualità del servizio offerto agli studenti e ai loro familiari.

A tale riguardo, uno degli strumenti essenziali di sensibilizzazione, anche in materia di privacy, è l'attività formativa del personale dell'Istituto e l'attività informativa diretta a tutti coloro che hanno rapporti con lo stesso.

Per garantire la conoscenza capillare delle disposizioni introdotte dal nuovo Regolamento Europeo, e di conseguenza contenute nel presente Regolamento, al momento dell'ingresso in servizio è fornita, a cura dell'Ufficio Personale, ad ogni dipendente (*oltre che ad ogni collaboratore, consulente*) una specifica comunicazione in materia di privacy, con apposita clausola inserita nel contratto di lavoro (*o nella lettera di incarico per i soggetti non dipendenti poc'anzi citati*), con la quale detti soggetti (dipendenti e non dipendenti) sono nominati quali **“autorizzati al trattamento dei dati”** e **“responsabili esterni al trattamento”** ai sensi del Regolamento UE 2016/679.

Il Regolamento, pubblicato sul sito Istituzionale, contiene infatti tutti i principi fondamentali della materia, esposti in maniera semplice, chiara e puntuale e il dipendente (o il non dipendente nei termini di cui si è detto sopra), nel sottoscrivere il contratto di lavoro (o la lettera di incarico), è reso edotto dell'esistenza dell'anzidetto Regolamento e delle modalità di consultazione del medesimo.



2.4 Definizioni

Come stabilito dall'articolo n. 4 del Regolamento Europeo n. 2016/679, ai fini di questo disciplinare d'istituto si intende per:

- a) «**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;
- b) «**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;
- c) «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- d) «**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;
- e) «**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;
- f) «**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;
- g) «**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;
- h) «**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;
- i) «**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;

- j) «**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;
- k) «**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;
- l) «**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;
- m) «**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; a proposito delle tipologie di "dati" sopra indicate, si fa presente che il Regolamento europeo non utilizza la definizione "**dati sensibili**" per la quale, quanto meno sino all'emanazione della legge italiana di revisione del D.lgs. 196/20013, si fa espresso rinvio all'articolo n. 4 del vigente Codice della privacy (D.lgs. 196/2003): definizione che, quindi, al momento rimane nell'utilizzo e nel linguaggio corrente per la materia di cui si tratta.
- n) «**autorità di controllo**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento UE.

Quelle sopra riportate, di cui si è data evidenza, rappresentano le "definizioni" su cui ha inciso maggiormente il nuovo Regolamento europeo: per le altre "definizioni" si fa espresso rinvio al testo dell'articolo n. 4 del Regolamento Europeo n. 2016/679.

2.5 Principi applicabili al trattamento dei dati

Come stabilito dall'articolo n. 5 del Regolamento Europeo n. 2016/679, i dati personali 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 del Regolamento UE, 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**»). A tale proposito, il Regolamento UE ricalca i principi sostanziali di "**necessità, pertinenza, indispensabilità e non eccedenza**" (rispetto alle finalità del trattamento) contenuti negli articoli 4 e 11 del D.lgs. 196/2003.



- 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 del Regolamento UE, 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**»).

Come stabilito dal Regolamento UE, il Titolare del trattamento è competente per il rispetto di quanto sin qui esposto ed è in grado di provarlo verso l'esterno (principio europeo dell'«**accountability**» o «**responsabilizzazione**»).

2.6 Trattamento di categorie particolari di dati (dati sensibili)

Come stabilito dall'articolo n. 9 del Regolamento Europeo n. 2016/679, è vietato trattare dati personali 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*.

Detta disposizione non si applica, secondo il Regolamento UE, quando incorrono alcune condizioni, riportate al summenzionato articolo n. 9, tra le quali si evidenzia quella di cui alla lettera "g" applicabile a questo Istituto, ai sensi della quale *"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"*

Si fa presente, inoltre, che il Regolamento UE consente di *"mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute"* (articolo n. 9, paragrafo n. 4).

Posto quanto sopra, si fa rinvio alle vigenti disposizioni emanate, in materia di dati sensibili, biometrici e genetici e in particolare al "Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art.21, comma 1 del D.Lgs. 10 Agosto 2018, n. 101" del Garante della Privacy, pubblicato in Gazzetta Ufficiale il 05 Giugno 2019.



2.7 Trattamento dei dati personali relativi a condanne penali e reati (dati giudiziari)

Come stabilito dall'articolo n. 10 del Regolamento Europeo n. 2016/679, *“il trattamento dei dati personali 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.”*

Il Regolamento UE 2016/679 pertanto ravvisa quali condizioni necessarie per il trattamento suddetto la presenza di una base giuridica che lo giustifichi (l'art. 6, paragrafo 1 del GDPR) ed altresì il controllo dell'autorità pubblica o l'autorizzazione del diritto dell'Unione o degli Stati membri, nel rispetto delle garanzie appropriate per i diritti e le libertà degli interessati.

Sul tema si sottolinea come la dottrina prevalente, in merito al fondamento giuridico che consenta di trattare i dati relativi a condanne penali e reati per valutare l'attitudine lavorativa, ha ritenuto che l'autorizzazione da parte del diritto nazionale già risulti presente ai sensi dell'art. 8 del c.d. “Statuto dei Lavoratori” (L. 300/1970) che ne prevede il trattamento nell'ambito della valutazione dell'attitudine lavorativa.

2.8 Comunicazione di dati verso l'esterno

La comunicazione a soggetti terzi di dati di carattere personale e particolare, detenuti dal Titolare del Trattamento, deve avvenire unicamente in ragione delle finalità per le quali gli stessi sono stati acquisiti e di cui si è data contezza nell'informativa privacy consegnata e sottoscritta dagli interessati.

La diffusione di dati che ecceda quanto su indicato, deve considerarsi illecita.

L'eventuale **comunicazione di dati particolari e giudiziari tra soggetti pubblici**, è ammessa solo in presenza di una normativa o di un regolamento che la giustifichino e, in ogni caso, qualora risulti necessaria per lo svolgimento di funzioni istituzionali, anche a seguito di un bilanciamento degli interessi.



3. DIRITTI DELL'INTERESSATO

3.1 Informativa sul trattamento dei dati

Come stabilito dall'articolo n. 13 del Regolamento Europeo n. 2016/679, in caso di raccolta presso l'interessato di dati che lo riguardano, il Titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti **informazioni**:

- a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
- b) i dati di contatto del Responsabile della protezione dei dati (D.P.O.);
- c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f) del Regolamento UE, i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
- e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione, nei termini previsti dal Regolamento UE.

In aggiunta alle informazioni di cui sopra, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti **ulteriori informazioni necessarie** per garantire un trattamento corretto e trasparente:

- g) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- h) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al *diritto alla portabilità* dei dati;
- i) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a) del Regolamento UE, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- j) il diritto di proporre reclamo a un'autorità di controllo;
- k) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l) l'eventuale esistenza di un *processo decisionale automatizzato*, compresa la *profilazione* di cui all'articolo 22, paragrafi 1 e 4 del Regolamento UE, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Per quanto concerne il periodo di conservazione dei dati personali raccolti da questo Istituto, i dati verranno conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello strettamente necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

A tale riguardo, sia fa rinvio al massimario di conservazione e scarto in uso presso l'Istituto.



Per massimario di conservazione e di scarto si intende l'elenco della tipologia dei documenti con il rispettivo tempo di conservazione (limitato o illimitato); detto strumento permette di gestire in modo organizzato l'archivio d'Istituto, permettendo di conservare solo ciò che mantiene un rilievo giuridico o ha assunto un valore storico e di eliminare la documentazione non più necessaria. Qualora il Titolare del trattamento intenda trattare ulteriormente i dati personali per una **finalità** diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità.

3.2 Consenso al trattamento dei dati: principi generali

Il consenso al trattamento dei dati rappresenta la base giuridica che consente all'Ente di trattare i dati dell'interessato ogni qualvolta il trattamento non possa trovare giustificazione in basi giuridiche più specifiche, le quali vengono espressamente previste agli artt. 6 e 9 del GDPR.

- Per permettere che il trattamento di dati basato sul consenso possa considerarsi lecito è necessario che questo presenti dei requisiti che di seguito si esplicano: **il consenso deve essere "esplicito"** o il trattamento deve basarsi sul verificarsi dei casi previsti dal GDPR;
- deve essere, in tutti i casi, **libero, specifico, informato e inequivocabile** e non è ammesso il consenso tacito o presunto (non è quindi possibile utilizzare "caselle pre-spuntate" su un modulo);
- deve essere manifestato attraverso **"dichiarazione o azione positiva inequivocabile"** (per approfondimenti, si vedano considerando 39 e 42 del regolamento).

3.3 Diritto di accesso dell'interessato

Come stabilito dall'articolo n. 15 del Regolamento Europeo n. 2016/679, 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.



Oltre al rispetto delle prescrizioni relative alle modalità di esercizio di questo diritto, il Titolare può consentire agli interessati di consultare direttamente, da remoto e in modo sicuro, i propri dati personali.

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.

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.

Il diritto di ottenere una copia non deve ledere i diritti e le libertà altrui.

3.4 Diritto di rettifica

Come stabilito dall'articolo n. 16 del Regolamento Europeo n. 2016/679, 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.

3.5 Diritto alla cancellazione (diritto all'oblio)

Come stabilito dall'articolo n. 17 del Regolamento Europeo n. 2016/679, in capo all'interessato è riconosciuto il **diritto "all'oblio"**, che si configura come un diritto alla cancellazione dei propri dati personali **in forma rafforzata**.

Si prevede, infatti, l'obbligo per i Titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione" (si veda art. 17, paragrafo 2 del Regolamento UE).

Ha un campo di applicazione più esteso di quello di cui all'art. 7, comma 3, lettera b), del Codice della privacy, poiché l'interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento (si veda articolo 17, paragrafo 1).

3.6 Diritto di limitazione al trattamento

Si tratta di un diritto diverso e più esteso rispetto al "blocco" del trattamento di cui all'art. 7, comma 3, lettera a), del Codice: in particolare, è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì **anche se l'interessato chiede la rettifica dei dati (in attesa di tale rettifica da parte del titolare) o si oppone al loro trattamento ai sensi dell'art. 21 del regolamento (in attesa della valutazione da parte del titolare)**.

Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la **limitazione** è vietato a meno che ricorrano determinate circostanze (*consenso dell'interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante*).



Il diritto alla limitazione prevede che il dato personale sia **“contrassegnato”** in attesa di determinazioni ulteriori; pertanto, è opportuno che il Titolare preveda nei propri sistemi informativi (elettronici o meno) misure idonee a tale scopo.

3.7 Diritto alla portabilità dei dati

Si tratta di uno dei nuovi diritti previsti dal regolamento, anche se non è del tutto sconosciuto ai consumatori (si pensi alla portabilità del numero telefonico).

Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste **specifiche condizioni per il suo esercizio**; in particolare, sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare, per esempio), e solo i dati che siano stati **“forniti”** dall'interessato al Titolare (si veda il considerando 68 del Regolamento UE).

Inoltre, il Titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.

3.8 Diritto di opposizione

Come stabilito dall'articolo n. 21 del Regolamento Europeo n. 2016/679, 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 ai sensi dell'articolo 6, paragrafo 1, lettere e) o f) del medesimo Regolamento, compresa la profilazione sulla base di tali disposizioni.

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.

3.9 Processo decisionale automatizzato (profilazione)

Come stabilito dall'articolo n. 22 del Regolamento Europeo n. 2016/679, 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.

Tale principio non si applica nel caso in cui la decisione:

- sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
- sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà dei legittimi interessi dell'interessato;
- si basi sul consenso esplicito dell'interessato.



4. DIRITTI DI ACCESSO AGLI ATTI DELL'ISTITUTO

4.1 Accesso agli atti

L'utenza può esercitare anche i diritti connessi all'accesso agli atti e documenti dell'Istituto, mediante lo strumento di accesso agli atti.

A tale riguardosi fa presente che:

- a) per **accesso documentale** si intende la domanda di accesso (richiesta di presa visione o di rilascio copia) a delibere e provvedimenti dell'Istituto, nei termini e alle modalità previste dalla normativa vigente (Legge 07 agosto 1990 n. 241 e ss.mm.ii. e D.P.R. 12 aprile 2006 n. 184). Possono fare domanda tutti i cittadini portatori di un interesse *"diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è richiesto l'accesso"* (art. 22, Legge 241/1990). Tali termini sono sospesi (fino ad un massimo di 10 giorni) nel caso di comunicazione della richiesta al controinteressato il quale ha diritto di presentare le proprie opposizioni. Il procedimento di accesso si conclude entro 30 giorni, decorrenti dalla presentazione della richiesta all'ufficio competente (art. 6 del D.P.R. 184 del 2006).
- b) per **accesso civico** si intende il diritto di chiunque di richiedere documenti, informazioni o dati che le pubbliche amministrazioni non hanno pubblicato pur avendone l'obbligo (Decreto Legislativo 97 del 17/5/2016 *"Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione pubblicità e trasparenza delle Amministrazioni Pubbliche"*, e Decreto Legislativo 33 del 14/03/2013: *"Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni"*). L'Istituto, entro 30 giorni, procede alla pubblicazione nel sito del documento, dell'informazione o del dato richiesto e lo trasmette contestualmente al richiedente, ovvero comunica al medesimo l'avvenuta pubblicazione, indicando il collegamento ipertestuale a quanto richiesto. Se il documento, l'informazione o il dato richiesti risultano già pubblicati nel rispetto della normativa vigente, l'Istituto indica al richiedente il relativo collegamento ipertestuale. Nei casi di ritardo o mancata risposta il richiedente può ricorrere al titolare del potere sostitutivo (indicato sul sito web istituzionale) che, verificata la sussistenza dell'obbligo di pubblicazione, provvede alla pubblicazione nel sito del documento, dell'informazione o del dato richiesto e lo trasmette contestualmente al richiedente, ovvero comunica al medesimo l'avvenuta pubblicazione, indicando il collegamento ipertestuale a quanto richiesto.
- c) per **accesso generalizzato** si intende il diritto di chiunque di accedere ai dati e ai documenti detenuti dalle Pubbliche Amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del Decreto Legislativo 33/2013 ('Decreto Trasparenza') e del D.lgs. 97/2016 (così detto *Freedom of Information Act* o "FOIA"), nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico



d) Il procedimento di accesso generalizzato deve concludersi con provvedimento espresso e motivato nel termine di 30 giorni dalla presentazione dell'istanza. Se il documento risulta già pubblicato nel sito istituzionale nel rispetto della normativa vigente, l'Istituto indica al richiedente il relativo collegamento ipertestuale. Nei casi di diniego totale o parziale dell'accesso o di mancata risposta entro il termine indicato, il richiedente può presentare richiesta di riesame all'Istituto, che decide con provvedimento motivato, entro il termine di 20 giorni. Avverso la decisione dell'amministrazione competente, il richiedente può proporre ricorso al tribunale amministrativo regionale (TAR).

Le richieste dovranno essere presentate mediante i seguenti canali istituzionali:

- direttamente alla Segreteria dell'Istituto Comprensivo di Cornuda;
- attraverso mail PEC all'indirizzo TVIC85100L@pec.istruzione.it.



5. TITOLARE E RESPONSABILE DEL TRATTAMENTO

5.1 Titolare del trattamento

Il **"Titolare"** del trattamento dei dati personali è la persona fisica, giuridica, la Pubblica Amministrazione, e qualsiasi altro Ente, Associazione od organismo cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, compreso il profilo della sicurezza.

Il Titolare del trattamento dei dati personali, ai sensi e per gli effetti della vigente normativa in materia di privacy, è l'Istituto Comprensivo di Cornuda sito in via Versi, 14 a Cornuda (TV).

Il Titolare, avvalendosi della supervisione e collaborazione del **Data Protection Officer**, provvede:

- a) a richiedere al Garante per la protezione dei dati personali l'eventuale autorizzazione al trattamento dei dati personali, nei casi previsti dalla vigente normativa e ad assolvere all'eventuale obbligo di notificazione e comunicazione;
- b) a nominare con atto deliberativo i *Responsabili del trattamento dei dati personali*, impartendo ad essi, per la corretta gestione e tutela dei dati personali, i compiti e le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato previsti dall'art. 7 del Codice della Privacy e all'articolo 12 del Regolamento UE, all'adozione delle misure di sicurezza per la conservazione, alla protezione e sicurezza dei dati;
- c) a nominare il Data Protection Officer, come stabilito dall'articolo 37 del Regolamento UE;
- d) a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati;
- e) a mettere in atto misure tecniche e organizzative adeguate a garantire che il trattamento dei dati sia effettuato conformemente al presente Regolamento.

Si dà evidenza, inoltre, del fatto che il Regolamento UE pone con forza l'accento sulla **"responsabilizzazione"** (*accountability* nell'accezione inglese) di titolari e responsabili, ovvero sulla adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento (si vedano artt. 23-25, in particolare, e l'intero Capo IV del Regolamento).

Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

Questo Istituto sta lavorando attivamente per far proprio l'approccio del Legislatore europeo relativo all'*accountability*.

5.2 Contitolari del trattamento

Come stabilito dall'articolo n. 26 del Regolamento Europeo n. 2016/679, 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 Regolamento UE, con



particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni.

Tale accordo può designare un punto di contatto per gli interessati e riflette adeguatamente i rispettivi ruoli e i rapporti dei titolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

Indipendentemente dalle disposizioni dell'accordo anzidetto, l'interessato può esercitare i propri diritti ai sensi del Regolamento UE nei confronti di e contro ciascun Titolare del trattamento.

5.3 Delegato del trattamento dei dati

Secondo il D.lgs. 196/2003, s'intende per Responsabile del trattamento dei dati, *"la persona fisica, giuridica, la Pubblica Amministrazione e qualsiasi altra Associazione ed Organismo preposti dal Titolare al trattamento di dati personali"*.

Anche se il Regolamento Europeo (art. 28) disciplina i compiti del Responsabile "esterno" senza contemplare espressamente la figura ed i compiti del Responsabile "interno".

Questo Istituto, in considerazione della complessità e della molteplicità delle proprie funzioni istituzionali e della necessità di continuare a garantire, a tutti i livelli, la più efficace applicabilità dei precetti in materia di privacy, reputa necessario, come sempre avvenuto in passato, continuare a designare i **Delegati del trattamento dei dati personali**, conferendo l'incarico a quei soggetti apicali che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate a far sì che il trattamento soddisfi i requisiti del presente Regolamento e garantisca la tutela dei diritti dell'interessato.

In base all'organizzazione di questo Istituto vengono individuati quali **Delegati del trattamento dei dati personali, le seguenti figure professionali**

- DSGA;
- Assistenti amministrative.

Il Titolare del trattamento dei dati deve informare ciascun delegato del trattamento dei dati, così come individuato dal presente Regolamento, delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative vigenti.

I delegati del trattamento rispondono al Titolare di ogni violazione o mancata attivazione di quanto dettato dalla normativa vigente.

Il Delegato del trattamento deve:

- a) trattare i dati personali, anche sensibili, osservando le disposizioni del presente Regolamento d'istituto nonché le specifiche istruzioni impartite dal Titolare;
- b) garantire che, presso la propria struttura, le persone autorizzate (incaricate) al trattamento dei dati personali assolvano ad un adeguato livello di riservatezza;
- c) adottare idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi presso la propria struttura, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalla normativa vigente;
- d) tenendo conto della natura del trattamento, assistere il Titolare del trattamento con misure tecniche ed organizzative adeguate, al fine di soddisfare l'obbligo del Titolare del



trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato secondo quanto previsto nella normativa vigente;

- e) mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti nel presente Regolamento;
- f) contribuire alle attività di verifica del rispetto del regolamento, comprese le ispezioni, realizzate dal titolare del trattamento o da altro soggetto da questi incaricato.

Il delegato al trattamento dei dati personali, nell'espletamento della sua funzione, deve inoltre collaborare con il **Data Protection Officer (DPO)**, al fine di:

- a) comunicare al DPO, quando questi ne faccia richiesta, ogni notizia rilevante ai fini dell'osservanza degli obblighi dettati dagli articoli da 32 a 36 del Regolamento UE 2016/679 riguardanti: *l'adozione di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio; la notificazione di una violazione dei dati personali al Garante privacy; la comunicazione di una violazione dei dati personali all'interessato, la predisposizione del Registro dei trattamenti.*
- b) utilizzare il modello d'Istituto di *Informativa e Consenso*, verificandone il rispetto e fornendo al DPO, quando questi ne faccia richiesta, le informazioni utili per l'aggiornamento del registro dei trattamenti;
- c) rispondere alle istanze degli interessati secondo quanto stabilito dal Codice della privacy e stabilire modalità organizzative volte a facilitare l'esercizio del diritto di accesso dell'interessato e la valutazione del bilanciamento degli interessi in gioco;
- d) contribuire a far sì che tutte le misure di sicurezza riguardanti i dati dell'Istituto siano applicati al suo interno ed all'esterno, qualora agli stessi vi sia accesso da parte di soggetti terzi quali Responsabili del trattamento;
- e) informare il Titolare del trattamento, senza ingiustificato ritardo, della conoscenza dell'avvenuta violazione dei dati personali.

Questo Istituto ha provveduto alla **nomina dei Delegati del trattamento dei dati**, mediante apposito atto di nomina.

5.3 Responsabile esterno del trattamento dei dati ex art. 28 del GDPR

Nell'ambito di questo Istituto, sono inoltre individuati quali **Responsabili del trattamento dei dati personali**, tutti i soggetti esterni che, per svolgere la propria attività sulla base di una convenzione o un contratto sottoscritto con l'Istituto, trattino dati di cui lo stesso è titolare e qualora siano in possesso dei requisiti previsti dall'articolo 28 del Regolamento EU (esperienza, capacità ed affidabilità).

In ottemperanza all'articolo 28 del Regolamento Europeo 2016/679, i Responsabili hanno l'obbligo di:

- trattare i dati in modo lecito, secondo correttezza e nel pieno rispetto della vigente normativa (nazionale ed europea) in materia di privacy;
- trattare i dati personali, anche di natura sensibile e giudiziaria, degli interessati esclusivamente per le finalità previste dal contratto o dalla convenzione stipulata con



Madisoft, Argo, TeamUfficio e ottemperando ai principi generali di necessità, pertinenza e non eccedenza;

- rispettare i principi in materia di sicurezza dettati dalla normativa vigente (nazionale ed europea) in materia di privacy, idonei a prevenire e/o evitare operazioni di comunicazione o diffusione dei dati non consentite, il rischio di distruzione o perdita, anche accidentale, il rischio di accesso non autorizzato o di trattamento non autorizzato o non conforme alle finalità della raccolta;
- adottare, secondo la propria organizzazione interna, misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio, nei termini di cui all'articolo 32 del Regolamento Europeo 2016/679 rubricato "Sicurezza del trattamento" che possono anche essere definite dal Titolare del Trattamento;
- nominare, al loro interno, i soggetti autorizzati / incaricati del trattamento, impartendo loro tutte le necessarie istruzioni finalizzate a garantire, da parte degli stessi, un adeguato obbligo legale di riservatezza;
- attenersi alle disposizioni impartite dal Titolare del trattamento, anche nell'eventuale caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, nei termini di cui all'articolo 28, comma 3, lettera a) del Regolamento Europeo;
- specificare, su richiesta del Titolare, i luoghi dove fisicamente avviene il trattamento dei dati e su quali supporti e le misure minime di sicurezza adottate per garantire la riservatezza e la protezione dei dati personali trattati.
- assistere, per quanto di competenza e nella misura in cui ciò sia possibile, il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del Regolamento Europeo (*sicurezza del trattamento dei dati personali, notifica di una violazione dei dati personali all'autorità di controllo, comunicazione di una violazione dei dati personali all'interessato, valutazione di impatto sulla protezione dei dati*), tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
- su scelta del Titolare del trattamento, cancellare o restituire al medesimo tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione o dello Stato membro preveda la conservazione dei dati;
- mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'articolo 28 del Regolamento Europeo e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato.

La nomina di Responsabile esterno del Trattamento avviene mediante la sottoscrizione di un contratto che integra gli accordi/convenzioni/contratti che regolano i rapporti principali in essere tra le parti.

La sottoscrizione del contratto di nomina e l'impegno a rispettare le disposizioni del presente Regolamento è condizione necessaria per l'instaurarsi del rapporto giuridico fra le Parti.



5.4 Autorizzato al trattamento dei dati

Il Regolamento Europeo non fornisce rilievo autonomo alla figura dell'*incaricato* al trattamento dei dati, seppure si soffermi sul fatto che chi tratta dati, ricevendo istruzioni e formazione da parte del Titolare del trattamento debba da questi essere "*autorizzato*" al trattamento (articoli 4 e 10 del Regolamento).

Come già stabilito all'articolo 6 del presente Regolamento, al momento dell'ingresso in servizio è fornita, a cura dell'ufficio di competenza, ad ogni dipendente (*oltre che ad ogni collaboratore, consulente o titolare di borsa di studio*) una specifica documentazione in materia di privacy all'interno della quale è presente anche l'atto di nomina ad autorizzato al trattamento dei dati.

La nomina di autorizzato, costituisce un atto unilaterale ricettizio di cui il dipendente deve solo prendere atto; la non volontà di accettazione della nomina non permette l'instaurazione del rapporto lavorativo.

Solo attraverso la nomina di autorizzato al trattamento infatti, il dipendente può visionare, trattare e gestire i Dati detenuti dall'Istituto.

Contestualmente alla nomina dovrà essere data copia del presente Regolamento o, in alternativa, indicazioni per poterla scaricare dal sito internet dell'Istituto.

Il Regolamento contiene infatti tutti i principi fondamentali della materia, esposti in maniera semplice, chiara e puntuale e il dipendente (o il non dipendente nei termini di cui si è detto sopra), nel sottoscrivere il contratto di lavoro (o la lettera di autorizzato), è reso edotto dell'esistenza dell'anzidetto Regolamento e delle modalità di consultazione del medesimo.

La nomina di autorizzato al trattamento è valevole anche per le figure professionali che collaborano con l'Istituto, anche se non alle dirette dipendenze dello stesso, e che, in virtù di detta attività, possono accedere e trattare Dati stando però alle direttive dello stesso.

Ci si riferisce, a titolo esemplificativo, al *personale tirocinante* o al *personale volontario* che opera temporaneamente all'interno dell'Istituto in virtù di un accordo o di una convenzione per lo svolgimento, appunto, di tirocini formativi piuttosto che di attività di volontariato a sostegno degli alunni, dei loro genitori e del personale dell'Istituto.

Il personale di cui si parla è soggetto agli stessi obblighi cui sono sottoposti tutti gli autorizzati "interni", in modo da garantire il pieno rispetto della tutela della riservatezza dei dati.

Nel caso di Autorizzati "*esterni*", l'accesso ai dati deve essere limitato, con particolare rigore, ai soli dati personali la cui conoscenza sia strettamente necessaria per l'adempimento dei compiti assegnati e connessi all'espletamento dell'attività.

5.5 Responsabile della protezione dei dati

Il Regolamento Europeo impone la nomina del **Data Protection Officer** (DPO, in italiano: Responsabile della protezione dei dati o 'RDP'), nei termini di cui all'articolo 37, 38 e 39 del Regolamento medesimo.

Chi svolge la funzione di RDP deve aver conseguito un percorso accademico-lavorativo volto alla precisa e puntuale conoscenza della normativa e delle procedure legate alla protezione dei dati personali oltre che presentare caratteristiche di indipendenza ed autorevolezza.



Il Regolamento Ue sottolinea l'importanza del requisito di indipendenza richiesto a tale figura, pertanto risulta evidente che il DPO non deve essere in **conflitto di interessi con l'Ente per cui presta la propria assistenza**.

L'Istituto Comprensivo di Cornuda provvede al conferimento dell'incarico di cui si tratta, tenendo conto delle prescrizioni sin qui descritte.

Ai sensi dell'articolo 39 del Regolamento UE, i suoi compiti sono:

- **sorvegliare l'osservanza del Regolamento**, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione e delle finalità;
- **fornire consulenza e pareri** al Titolare, ai Responsabili del trattamento dei dati e agli incaricati relativamente all'applicazione degli obblighi europei in materia;
- collaborare con il titolare, laddove necessario, nel condurre una **valutazione di impatto sulla protezione dei dati (DPIA)**;
- **informare e sensibilizzare** il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati;
- **cooperare con il Garante e fungere da punto di contatto per il Garante** su ogni questione connessa al trattamento;
- **supportare** il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un **registro delle attività di trattamento**.

Ai sensi dell'articolo 37 del Regolamento UE, Egli deve:

- **possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali**, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati. Non sono richieste attestazioni formali o l'iscrizione ad appositi albi professionali, anche se la partecipazione a master e corsi di studio/professionali può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze;
- **adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse**. In linea di principio, ciò significa che il RPD non può essere un soggetto che ricopre ruoli gestionali e che decide sulle finalità o sugli strumenti del trattamento di dati personali;
- **operare alle dipendenze del titolare oppure sulla base di un contratto di servizio** (RPD esterno);
- **disporre di risorse umane e finanziarie**, messe a disposizione dal Titolare, per adempiere ai suoi scopi.

Il Regolamento UE prevede la pubblicazione *on line* del curriculum del RDP, nonché la pubblicazione sul sito istituzionale dell'Istituto dei **"dati di contatto" del RDP**: dati che debbono essere inseriti anche nell'informativa istituzionale sul trattamento dei dati, così che il RDP sia agevolmente contattabile dai cittadini-utenti ma anche dal Garante per la privacy.

Sia che il RDP sia interno che esterno, è necessario stipulare con il medesimo un **contratto ad hoc**. Nel caso in cui il RDP sia un "esterno" (persona o società) tutte le clausole, oltre che il compenso per l'incarico, dovranno essere inserite in un apposito contratto di servizi, ove siano anche previste le risorse necessarie a far funzionare l'ufficio del RDP.



6. SICUREZZA DEI DATI PERSONALI - MISURE DI CARATTERE INFORMATICO E TECNOLOGICO

6.1 Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

L'articolo n. 25 del Regolamento Europeo n. 2016/679 introduce il criterio sintetizzato dall'espressione inglese **"data protection by default and by design"**, ossia la necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio (*"sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso"*), secondo quanto afferma l'art. 25, paragrafo 1 del Regolamento UE) e richiede, pertanto, un'analisi preventiva ed un impegno applicativo da parte del Titolare che deve sostanziarsi in una serie di attività specifiche e dimostrabili.

6.2 Registro elettronico delle attività di trattamento

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (si veda l'articolo 30, paragrafo 5 del Regolamento UE), devono tenere un **registro delle operazioni di trattamento** i cui contenuti sono indicati all'articolo 30 del medesimo Regolamento.

Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un Istituto, indispensabile per ogni valutazione e analisi del rischio.

Il Registro deve essere esibito su richiesta del Garante.

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

6.3 Protezione e sicurezza dei dati personali

Le misure di sicurezza devono **"garantire un livello di sicurezza adeguato al rischio"** del trattamento (articolo 32, paragrafo 1 del Regolamento UE); in questo senso, la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva (*"tra le altre, se del caso"*).

Per lo stesso motivo, secondo il Regolamento UE non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza (ex art. 33 Codice) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del regolamento.

Si richiama l'attenzione anche sulla possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate.

Il 05 Giugno 2019 il Garante della Privacy ha emanato il **"Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del D.Lgs. 10 agosto 2018 n.101"** contenente le indicazioni specifiche per alcune fattispecie di trattamenti.



6.4 Notifica di una violazione dei dati personali all'autorità di controllo

A partire dal 25 maggio 2018, tutti i titolari dovranno **notificare all'Autorità di controllo le violazioni di dati personali** di cui vengano a conoscenza, entro 72 ore e comunque *“senza ingiustificato ritardo”*, ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (si veda considerando 85 del Regolamento UE); questa procedura va sotto il nome di **“Data Breach”**.

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

Se la probabilità di tale rischio è elevata, si dovrà informare della violazione anche gli interessati, sempre *“senza ingiustificato ritardo”*; fanno eccezione le circostanze indicate al paragrafo 3 dell'articolo 34 del Regolamento UE. I contenuti della notifica all'Autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli art. 33 e 34 del regolamento, nonché dalle *“Linee Guida in materia di notifica delle violazioni di dati personali – WP250, definite in base alle previsioni del Regolamento UE 2016/679”* adottate dal Gruppo di Lavoro Art.29 il 03 ottobre 2017 (versione emendata e adottata il 6 febbraio 2018) e dal Provvedimento del Garante sulla notifica delle violazioni dei dati personali del 30 Luglio 2019.

Il Titolare del trattamento, sentito il Data Protection Officer, adotta quindi le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuto a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

Si ricorda, inoltre, che l'Autorità ha messo a disposizione un modello per la notifica dei trattamenti da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico (<https://www.garanteprivacy.it/documents/10160/0/Modello+notifica+Data+Breach.pdf/6d1fa433-88dc-2711-22ab-dd5d476abe74?version=1.1>).

6.5 Valutazione di impatto (VIP) sulla protezione dei dati

L'Istituto adotta le misure atte a **“garantire un livello di sicurezza adeguato al rischio”** del trattamento (articolo 32, paragrafo 1 del Regolamento UE) e ciò sulla base di quanto disposto dall'art 32, par. 1 del GDPR, che costituisce la base operativa su cui attuare la prevenzione.

fra le attività correlate alla sicurezza, di fondamentale importanza per questo Istituto sono le misure collegate al, al **rischio inerente al trattamento**.

Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati (si vedano considerando 75-77 del GDPR); tali impatti dovranno essere analizzati attraverso un apposito **processo di valutazione** (si vedano artt. 35-36 del GDPR) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi.

All'esito di questa valutazione di impatto il Titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'Autorità non avrà il compito di *“autorizzare”* il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'articolo 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.



6.6 Trasferimento di dati personali all'estero

Si fa rinvio ai principi dettati dal Regolamento Europeo agli articoli 44 e seguenti, nonché alle indicazioni che fossero dettate, in materia, dal Legislatore nazionale e dal Garante per la protezione dei dati personali.



7. ATTUAZIONE DEGLI ADEMPIMENTI EUROPEI

7.1 Entrata in vigore e pubblicità

Il Regolamento è in vigore dalla data di approvazione, mediante delibera espressa del Consiglio di Istituto.

Il Regolamento è pubblicato nel sito internet dell'Istituto (nella sezione "Privacy Europea" del menù "INFO SITO").

7.2 Disposizione finale relativa agli "allegati tecnici"

Il testo del presente Regolamento potrà essere aggiornato con atto deliberativo del CdI, a seguito di eventuali modifiche che intervengano rispetto alla vigente normativa, sia nazionale che regionale, in materia di protezione dei dati personali.

Quanto, invece, agli **Allegati tecnici** (n.1, n.2, n. 3, n. 4 e n. 5) al presente Regolamento, si stabilisce quanto segue: poiché si tratta di "strumenti di lavoro quotidiano", essi saranno inevitabilmente oggetto di continue, quanto rapide integrazioni, modifiche e revisioni, in virtù sia delle necessità che delle esigenze imposte da una realtà normativa ed organizzativa tuttora in rapidissima evoluzione. Gli eventuali aggiornamenti ai *documenti tecnici allegati* verranno, pertanto, inseriti in tempo reale sul sito internet istituzionale nell'apposita sezione dedicata alla "privacy", prescindendo dall'adozione di appositi atti deliberativi di modifica del presente Regolamento e dandone pubblicità per mezzo della mail "everyone", così da consentire una rapida consultazione on line dei medesimi ed un contenuto sempre aggiornato degli stessi.