Allegato 1)

CIRCOLARE N. 2/2018 PRIVACY

PRINCIPALI CONTENUTI DEL REGOLAMENTO PRIVACY (UE)

Regolamento (UE) 2016/679

DEFINIZIONI

- «**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;

- «**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;

- «**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;

- «**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;

- «**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;

- «**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;

- «**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.

PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI PERSONALI

- Principio di **«liceità, correttezza e trasparenza»:** i dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;

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

- principio di **«minimizzazione dei dati»:** i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

- principio di **«esattezza»:** i dati personali sono 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;

- principio di **«limitazione della conservazione»:** i dati personali sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato;

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

- Il Regolamento (art. 5, paragrafo 2) richiede al titolare di rispettare tutti questi principi e di essere "in grado di comprovarlo". Questo è il principio detto di **"responsabilizzazione"** o accuntability che viene poi esplicitato ulteriormente dall'art. 24, paragrafo 1 del Regolamento dove si afferma che "il titolare mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento".

PROGETTAZIONE E IMPOSTAZIONE PREDEFINITA DELLA PROTEZIONE DEI DATI

L'articolo 25, paragrafo 1 del GDPR (privacy by design) prevede che il titolare del trattamento

tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi connessi al trattamento *"sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso ... mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati*".

Pertanto, fin dalla progettazione delle attività di trattamento, è necessario considerare, in particolare per quanto riguarda la realizzazione o l'acquisizione di soluzioni informatiche, che tali soluzioni siano adeguate al fine di garantire il rispetto della suddetta disposizione.

Tra le misure da attuare dovrà essere presa in considerazione, in particolare, la pseudonimizzazione, che consiste nel *"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*".

Normalmente essa è ottenuta scorporando i dati identificativi dagli altri dati personali e attribuendo uno stesso codice ai dati anonimizzati e ai dati identificativi; i dati sono quindi resi accessibili in forma anonima, quando non è più necessaria l'identificazione dell'interessato, ma, se necessario, è comunque possibile porre fine alla pseudonimizzazione riassociando i dati anonimi ai dati identificativi.

Inoltre, è essenziale la piena applicazione del principio di minimizzazione dei dati che consiste nel trattamento dei soli dati adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

L'articolo 25, paragrafo 2 del DGPR (privacy by default) dispone che *"Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica*".

Il titolare del trattamento, quindi, deve predisporre nei mezzi informatici utilizzati le suddette impostazioni predefinite (o di default), necessarie per la protezione dei dati personali.

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

Ai sensi dell'**art. 30 del DGPR** "o*gni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità"*. Il registro deve contenere tutte le informazioni elencate in tale disposizione.

Inoltre, come chiarito al paragrafo 2, anche il responsabile del trattamento "*deve tenere un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento*".

Il registro costituisce un importante strumento di programmazione nonchè di valutazione ed analisi del rischio in quanto fornisce una visione di insieme dei trattamenti posti in essere dall'istituzione scolastica e la sua compilazione rappresenta l'occasione per effettuare una ricognizione completa di tutti gli strumenti informatici impiegati in ciascun trattamento.

Il registro dei trattamenti, che deve avere forma scritta anche elettronica, rappresenta inoltre uno degli strumenti di controllo e supervisione a disposizione del Garante. Il paragrafo 4 dell'art. 30 prevede infatti che, su richiesta, il titolare del trattamento mette il Registro a disposizione dell'autorità di controllo.

Sebbene il paragrafo 5 preveda che le disposizioni relative al registro "*non si applicano alle imprese o organizzazioni con meno di 250 dipendenti*", viene poi precisato che tale esclusione si applica "*a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1,* [dati sensibili] *o i dati personali relativi a condanne penali e a reati di cui all'articolo 10*". La portata delle eccezioni è così ampia da ricomprendere quasi tutti i trattamenti effettuati dalle istituzioni scolastiche pertanto, esse, sono soggette all'obbligo di tenuta del registro delle attività di trattamento.

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI

Il Regolamento generale sulla protezione dei dati modifica in modo sostanziale la disciplina dell'informativa, ampliandone il contenuto.

Gli articoli 13 e 14 del GDPR indicano dettagliatamente le informazioni che l'informativa deve contenere.

L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico. Deve avere una forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile. Massima attenzione deve essere prestata al linguaggio utilizzato che deve essere chiaro e semplice adottando informative idonee nel caso in cui le stesse siano rivolte a minori.

L'informativa deve essere fornita all'interessato prima di effettuare la raccolta dei dati (se raccolti direttamente presso l'interessato - art. 13 del Regolamento).

Nel caso in cui, invece, i dati non siano raccolti direttamente presso l'interessato (art. 14 del Regolamento), l'informativa deve essere fornita entro un termine ragionevole che non può superare un mese dalla raccolta, oppure al momento della comunicazione dei dati (a terzi o all'interessato).

SICUREZZA DEL TRATTAMENTO

L'articolo 32, paragrafi 1 e 2 del GDPR dispone quanto segue:

"1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio,

che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

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

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

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

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo 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".

In base a tale disposizione, il titolare del trattamento è obbligato ad approntare un efficace sistema di sicurezza dei trattamenti. Le misure di sicurezza adottate dovranno garantire un livello di sicurezza adeguato al rischio connesso al singolo trattamento e non potranno più essere previsti obblighi generalizzati di adozione di misure minime di sicurezza in quanto è rimessa al titolare e al responsabile del trattamento la valutazione, caso per caso, delle misure di sicurezza necessarie in relazione ai rischi specificatamente individuati.

Il titolare, in base al principio di responsabilizzazione (*accountability*), deve essere in grado di dimostrare di aver garantito un livello di sicurezza adeguato al rischio. L'approccio del Regolamento è quindi rivolto alla responsabilizzazione dei titolari e dei responsabili in ordine all'adozione di comportamenti proattivi tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento. A queste figure è affidato il compito di delineare e decidere in autonomia le modalità, le garanzie e i limiti del trattamento dei dati personali nel rispetto delle disposizioni e dei principi del Regolamento.

Ogni istituzione scolastica deve mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

Per quanto riguarda le applicazioni informatiche gestite in modo autonomo e i trattamenti cartacei, dovranno essere definite misure adeguate che saranno descritte nel registro dei trattamenti, con riferimento ad ogni specifico trattamento.

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

L'articolo 35, paragrafo 1 del GDPR dispone che "*Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali"*.

La valutazione d'impatto, secondo quanto stabilito dal paragrafo 3, dev'essere effettuata, in particolare e prioritariamente:

a) nel caso di valutazione sistematica degli aspetti personali relativi a persone fisiche, basata su trattamenti automatizzati, che produce effetti giuridici o incide sulle persone fisiche;

b) nel caso di trattamenti che coinvolgono particolari categorie di dati (dati sensibili) o dati relativi a condanne penali e reati (dati giudiziari);

c) nell'ipotesi in cui i trattamenti siano connessi a sistemi di videosorveglianza.

Nei casi in cui il trattamento continui a presentare un rischio elevato, è necessario consultare il Garante secondo la procedura di consultazione preventiva descritta all'articolo 36 del Regolamento.

OBBLIGO DI FORMAZIONE

L'articolo 29 del GDPR prevede che "*Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri'*.

Inoltre, **l'articolo 32 del GDPR** titolato "Sicurezza del trattamento" stabilisce, al paragrafo 4, che "*il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri*'.

Il legislatore europeo ha quindi introdotto a carico dei titolari e dei responsabili del trattamento un obbligo di formazione di tutte le persone autorizzate al trattamento. Tale obbligo costituisce una delle fondamentali misure di sicurezza propedeutiche al trattamento stesso.

RESPONSABILI DEL TRATTAMENTO

Il Regolamento europeo sulla protezione dei dati definisce 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*". La necessità di ricorrere a un responsabile del trattamento si presenta, in particolare, in caso di affidamento di servizi informatici, o altri tipi di servizi, che comportano il trattamento di dati personali forniti dall'istituzione scolastica.

Il titolare del trattamento è tenuto a ricorrere a responsabili del trattamento "*che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato"* (**articolo 28**, paragrafo 1, del GDPR).

Il paragrafo 2 stabilisce che "*il responsabile del trattamento non ricorre ad altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento*".

L'articolo 28, paragrafo 3, del Regolamento impone che il contratto (o altro atto giuridico vincolante) tra titolare e responsabile del trattamento disciplini i seguenti aspetti: oggetto, durata, natura e finalità del trattamento, tipo di dati personali trattati e categorie di interessati. Le lettere da a) ad h) del paragrafo 3

determinano, inoltre, i criteri/principi da applicare per redigere il contratto tra titolare e responsabile del trattamento.

L'articolo 28, paragrafo 3, lettera a), del Regolamento stabilisce, in particolare, che il responsabile del trattamento possa trattare i dati personali *"soltanto su istruzione documentata del titolare del trattamento";*

Le citate disposizioni rendono, dunque, necessaria la revisione degli atti attraverso i quali sono stati regolati, sino ad oggi, i rapporti con i responsabili del trattamento.

ESERCIZIO DEI DIRITTI

Il Regolamento generale sulla protezione dei dati (**articoli da 15 a 22**) ha esteso notevolmente la portata dei diritti dell'interessato già esistenti (quali ad esempio il diritto di accesso e il diritto di informativa) e ha previsto nuovi diritti (in particolare, il diritto di limitazione del trattamento, il diritto alla portabilità e il diritto all'oblio).

Il titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura (tecnica e organizzativa) a ciò idonea.

Il termine per la risposta all'interessato è, per tutti i diritti, 1 mese, prorogabile di altri 2 mesi in casi di particolare complessità; il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego, informandolo della possibilità di proporre reclamo al Garante o di proporre ricorso giurisdizionale.

Il riscontro all'interessato di regola deve avvenire in forma scritta, anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; può essere dato oralmente solo se così richiede l'interessato stesso (articolo 12, paragrafo 1, del Regolamento). La risposta fornita all'interessato non deve essere solo intelligibile, ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.

L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato. Spetta al titolare valutare la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato, ma soltanto se si tratta di richieste manifestamente infondate o eccessive (anche ripetitive), oppure se sono chieste più copie dei dati personali nel caso del diritto di accesso (in quest'ultimo caso il titolare deve tenere conto dei costi amministrativi sostenuti).

Si indicano di seguito alcuni dei principali diritti riconosciuti all'interessato:

Diritto di accesso (art. 15 Reg) 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:

- finalità del trattamento;
- categorie di dati personali trattati;
- categorie di destinatari a cui i dati sono stati o saranno comunicati;
- periodo di conservazione o criteri per definirlo;

- sussistenza del diritto dell'interessato di chiedere rettifica o cancellazione dei dati o limitazione od opposizione al trattamento;
- diritto di proporre reclamo al Garante;
- se non raccolti presso l'interessato, presso chi sono stati raccolti i dati personali;
- sussistenza di un processo decisionale automatizzato, nonché logica dello stesso e relative conseguenze;
- nel caso di trasferimento dei dati fuori dall'Unione Europea, quali garanzie siano state applicate.

Diritto di limitazione del trattamento art. 18 Reg.

Trattasi del diritto riconosciuto all'interessato, di ottenere dal titolare del trattamento la limitazione del trattamento qualora ricorrano le ipotesi indicate dall'art. 18. Il diritto alla limitazione del trattamento è esercitabile sia in caso di violazione dei presupposti di liceità del trattamento sia nel caso in cui l'interessato chieda la rettifica dei dati (in attesa della rettifica da parte del titolare) sia nel caso in cui l'interessato si opponga al trattamento dei propri dati personali ai sensi dell'art. 21 del GDPR, nelle more della valutazione della richiesta da parte del titolare.

NOTIFICA DELLE VIOLAZIONI DI DATI PERSONALI

L'articolo 33, paragrafo 1, del Regolamento prevede che "*In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo*".

La notifica all'Autorità dell'avvenuta violazione non è quindi obbligatoria ma subordinata ad una valutazione, da parte del titolare, del rischio per i diritti e le libertà degli interessati. Per quanto riguarda i rischi legati alla violazione dei dati personali si rinvia al Considerando n. 85 del Regolamento.

In conformità al principio di responsabilizzazione, qualora il titolare valuti improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà della presone fisiche, e sia in grado di dimostrarlo, potrà omettere la notifica all'Autorità.

La notifica deve contenere almeno:

1) la descrizione della natura della violazione (inclusi, se possibile, categorie e numero approssimativo di interessati, nonché categorie e numero approssimativo di registrazioni di dati);

2) nome e dati di contatto del responsabile della struttura, o del responsabile della protezione dei dati o di chi possa fornire informazioni più complete o dettagliate;

3) le probabili conseguenze della violazione dei dati personali;

4) le misure adottate, o di cui si propone l'adozione, per contrastare la violazione e ridurne i possibili effetti negativi.

Ai sensi dell’articolo 33, paragrafo 1, del Regolamento, il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo”.

L’art. 34 del GDPR prevede che, qualora la violazione dei dati personali presenta un rischio elevato per le libertà delle persone fisiche, il titolare del trattamento comunichi la violazione all’interessato senza ingiustificato ritardo, fatta eccezione nei casi in cui si verifichino le circostanze indicate al paragrafo 3.