european informatics passport

IL REGOLAMENTO UE 679/2016 E LA "NUOVA" PRIVACY PER LA SCUOLA

Dispensa di approfondimento

certipass

ENTE ACCREDITATO DAL MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA
PER LA FORMAZIONE DEL PERSONALE DELLA SCUOLA - DIRETTIVA 170/2016

Premessa

Il Regolamento UE 2016/679 in materia di protezione dei dati personali ha introdotto nuove prassi per quel che concerne diritti e garanzie che Pubbliche Amministrazioni e imprese private devono assicurare a cittadini e clienti. In linea generale, a partire dal 25 maggio 2018 le modalità di protezione dei dati da parte degli Enti diventa più rigorosa.

Le scuole trattano quotidianamente numerose informazioni, spesso delicate (cosiddetti dati sensibili), sugli alunni, e famiglie e le relative condizioni sociali e psico-fisiche, e il nuovo Regolamento pertanto deve essere applicato anche agli istituti scolastici. Sovente la pubblicazione dei dati sensibili del minore o la pubblicazione e diffusione di foto e filmati comporta la violazione delle norme in materia di dati personali.

Sono, inoltre, da considerare numerose novità in materia di organizzazione delle informative della privacy e in tema di valutazione di impatto sulla protezione dei dati.

Centro Studi EIPASS

Disclaimer

CERTIPASS ha predisposto questo documento programmatico in base agli standard e ai riferimenti Comunitari vigenti in materia. Non si assume alcuna responsabilità derivante dall'applicazione in ambito diverso dallo stesso, neanche da informazioni elaborate da terzi in base ai contenuti del presente programma. Data la complessità e la vastità dell'argomento, peraltro, CERTIPASS non fornisce garanzie riguardo la completezza delle informazioni contenute; non potrà, inoltre, essere considerata responsabile per eventuali errori, omissioni, perdite o danni eventualmente arrecati a causa di tali informazioni, ovvero istruzioni ovvero consigli contenuti nella pubblicazione ed eventualmente utilizzate anche da terzi.

CERTIPASS si riserva di effettuare ogni modifica o correzione che a propria discrezione riterrà sia necessaria, in qualsiasi momento e senza dovere nessuna notifica.

L'Utenza destinataria è tenuta ad acquisire in merito periodiche informazioni visitando le aree del sito dedicate al Programma.

Indice

1. IL REGOLAMENTO UE 679/2016

Il Regolamento *Europeo 679 del 2016* è entrato in vigore il 24 maggio 2016 ed, essendo un atto "self-executing" è immediatamente esecutivo nell'ordinamento degli Stati membri (art. 288 TFUE); tuttavia per espressa previsione normativa sostituirà la disciplina previgente *a partire dal 25 maggio 2018* (considerando 171 e art. 99, Reg. UE n. 2016/679).

Gli Stati membri hanno avuto, pertanto, a disposizione un considerevole lasso di tempo per l'aggiornamento della disciplina interna.

Il Regolamento introduce nuovi istituti, come il diritto all'oblio e alla portabilità dei dati, e stabilisce inoltre anche criteri volti a responsabilizzare imprese ed enti in materia di protezione dei dati personali e introduce agevolazioni per chi si conforma alle *regole di tutela dei dati*.

Le norme così introdotte hanno il compito di sostituire la precedente legislazione degli anni Novanta dello scorso secolo (la Direttiva 95/46, la cosiddetta Direttiva Madre), divenuta obsoleta anche in ragione dell'introduzione di tecnologie all'epoca inesistenti.

Il recente Regolamento Europeo 679 del 2016 prende atto delle nuove sfide per la protezione dei dati che l'evoluzione tecnologica e la globalizzazione comportano, oltre a considerare che la portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. *Le recenti iniziative legislative in materia di protezione dei dati mirano ad adeguare la normativa ai mutamenti dettati dall'evoluzione tecnologica* soprattutto in tema di un aumento dei flussi transfrontalieri e dei dati scambiati tra pubblici e privati.

Pertanto, il legislatore europeo sottolinea come tale evoluzione tecnologica richieda un quadro normativo più solido e coerente in materia di protezione dei dati nell'Unione il quale, affiancato da efficaci misure di attuazione, contribuisce a creare il clima di fiducia necessario per lo sviluppo dell'economia digitale in tutto il mercato interno.

Il Regolamento UE 2016/679 non contiene una normativa differenziata in ragione dello status di titolare del trattamento pubblico o privato e non contiene neanche norme specificamente dedicate al settore pubblico. Alcune attività riguardano, tuttavia, solo lo svolgimento di attività pubbliche. Alla base della normativa non vi è, dunque, la natura pubblica o privata del titolare del trattamento ma la tipologia del trattamento stesso. Di conseguenza, l'intero provvedimento è suscettibile di essere applicato alla Pubblica Amministrazione.

Il Regolamento sulla protezione dei dati personali n. 679 del 2016, pienamente applicabile dal 25 maggio 2018, predispone una disciplina unitaria del trattamento dei dati rispondente alle attese del processo globale di digitalizzazione, e contestualmente rappresenta l'introduzione di una impostazione innovativa in materia di privacy. La normativa, infatti, introduce importanti principi tra cui quello di *"accountability" (responsabilizzazione)*.

L'*accountability* costituisce una notevole sfida per le pubbliche amministrazioni, poiché richie-

de un significativo cambio di approccio, teso a modificare i ruoli del titolare del trattamento dei dati e dell'interessato. In applicazione di tale principio spetta, dunque, al titolare del trattamento provare il rispetto delle regole in materia di trattamento dei dati, e contestualmente adattarsi ai nuovi istituti di Valutazione di impatto privacy, o notificazione delle violazioni o ancora di idoneità delle misure di sicurezza, con l'obiettivo comune di assegnare massima trasparenza all'agire amministrativo.

A titolo esemplificativo, il Regolamento statuisce che quando la violazione dei dati rappresenta una minaccia per i diritti e le libertà delle persone, il titolare dovrà informare in modo chiaro, semplice e immediato anche tutti gli interessati e offrire indicazioni su come intende limitare le possibili conseguenze negative. È evidente, dunque, che i soggetti pubblici, e pertanto anche le scuole dovranno far ricorso ad esperti competenti nella gestione dei dati, affinché realizzino le valutazioni necessarie in materia. A ciò si aggiunga che è inoltre stata prevista la figura obbligatoria del Data Protection Officer e, pertanto, la nuova regolamentazione impone alle amministrazioni, e dunque anche alle scuole, nuovi adempimenti e numerose attività di adeguamento.

1.1 Introduzione. Internet of Things

Nel 1999 Kevin Ashton, un ingegnere inglese, ha introdotto la locuzione *Internet of Things* (letteralmente internet delle cose) per indicare l'estensione di Internet anche al mondo degli oggetti. *Internet of Things* descrive un sistema in cui internet è collegato al mondo fisico mediante sensori che consentono alle applicazioni di far "comunicare" gli oggetti. L'identificazione di ciascun oggetto avviene tramite minuscoli transponder a radiofrequenza in essi inseriti, oppure mediante codici a barre o codici grafici bidimensionali impressi sull'oggetto. Le applicazioni riguardano, dunque, la gestione di beni di consumo (durante la produzione, l'immagazzinamento, la distribuzione, la vendita o l'assistenza postvendita), o anche il tracciamento di oggetti persi o rubati[1].

La portata innovativa di tali applicazioni ha benefici indiscussi, come peraltro accade per il maggior numero delle invenzioni della scienza e della tecnica. Contestualmente, le innovazioni possono entrare in conflitto, in questo campo, con l'interesse alla tutela dei dati dei soggetti e dei mezzi connessi.

Il numero dei dispositivi, connessi all'Internet of Things è in crescente aumento e in futuro la connessione riguarderà anche, a titolo esemplificativo, i termostati i dispositivi medico- diagnostici e molto altro.

A tutto ciò consegue la generazione di ingenti quantità di dati, poiché tutti i dispositivi connessi raccolgono dati capaci di fornire informazioni dettagliate sui clienti, sino a giungere alla completa profilazione degli stessi. La c.d. profilazione consente, infatti, sia di orientare la produzione, adattando il prodotto da commercializzare ad una categoria individuata di potenziali consumatori, sia di incentivare nuovi consumi, tramite la creazione di specifici prodotti funzionali ai bisogni manifestati dai consumatori.

Il risultato è la possibile ricostruzione, da parte di chiunque, delle abitudini, dei bisogni, della propensione al consumo di determinati beni, delle opinioni, in breve, della personalità dell'individuo. Di conseguenza, tra individui e informazioni, o, meglio, tra interessi dei singoli e modalità di circolazione delle informazioni si va istituendo un nuovo rapporto.

La problematica relativa alla diffusione dei dati e alla conseguente profilazione non è nuova[2]

1 Treccani, lessico del XXI secolo.

2 A partire dagli anni Ottanta gli organismi internazionali e comunitari hanno preso coscienza delle problematiche connesse alla protezione dei dati personali emanando una serie di atti, alcuni normativamente rilevanti, altri di mero indirizzo, fra i quali:

- Linee giuda dell'OCSE per la tutela della riservatezza ed il flusso transfrontaliero dei dati, adottate il 23 settembre 1980 .
- Convenzione 18 settembre 1980, n. 108, del Consiglio d'Europa, per la protezione dell'individuo con riguardo al trattamento automatizzato dei dati, aperta alla firma il 18 gennaio 1981 .
- Linee guida delle Nazioni Unite adottate dall'Assemblea Generale promosse dall'Alto Commissariato per i diritti umani il 14 dicembre 1990, relative al trattamento computerizzato dei dati personali.
- Raccomandazione n. R(95)4, del Comitato dei Ministri UE agli Stati membri, relativa alla protezione dei dati a carattere personale nella gestione dei servizi di telecomunicazione, con particolare riguardo ai servizi telefonici, adottata il 7 febbraio 1995.

ed è stata da tempo affrontata mediante l'introduzione e la definizione del diritto alla riservatezza, con tutte le relative accezioni.

Lo sviluppo tecnologico più recente ha richiesto ulteriori adattamenti della disciplina a tutela della riservatezza e dei dati personali e, pertanto, nel 2016, l'Unione Europea ha emanato il Regolamento UE n. 2016/679.

L'analisi complessiva e generale dl Provvedimento suggerisce una rinnovata attenzione del Legislatore europeo al tema dei diritti della personalità e, nello specifico, della riservatezza. Dal punto di vista concreto è infatti stata introdotta la disposizione in cui si attribuisce al titolare dei dati personali un "diritto di rettifica" ovverosia di modifica dei dati personali "senza ingiustificato ritardo" n (art. 16, Reg. UE n. 2016/679.) La codificazione, inoltre del "diritto all'oblio" dei dati personali (art. 17 Reg. UE n. 2016/679), sembra rispondere al medesimo intento di accresciuta protezione della personalità. Allo stesso modo, l'interessato ha il diritto alla cancellazione "senza ingiustificato ritardo" se, i dati non siano più necessari rispetto alle finalità per cui sono stati raccolti ovvero se sia stato ritirato il consenso o fatta opposizione al trattamento, in assenza di motivi legittimi che lo giustifichino oppure se i dati sono stati trattati illecitamente oppure se la cancellazione è prescritta al responsabile del trattamento da un obbligo di legge (art. 17, Reg. n. 2016/679)[3].

3 M. L. Maddalena, *La digitalizzazione della vita dell'amministrazione e del processo in Foro amm.*, 2016, 2535 ss.

1.2 Le Novità del Regolamento: l'applicazione territoriale, l'accountability, la definizione di dato personale

1.2.1 Il nuovo campo di applicazione territoriale

Il Regolamento UE n. 2016/679 si occupa di disciplinare il trattamento dei dati personali, nonché la loro circolazione, nel rispetto del diritto alla protezione dei dati considerato come diritto e libertà fondamentale, anche perseguendo scelte di extraterritorialità per garantire la tutela dei propri cittadini.

Una delle caratteristiche più significative del Nuovo Regolamento è il relativo ambito di applicazione, che presenta caratteri innovativi sia perché modifica la tradizionale definizione del principio di stabilimento e sia perché estende l'ambito di applicazione anche ai titolari e ai responsabili del trattamento non residenti nell'Unione Europea.

La disciplina si applica dunque *"indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione" e stabilisce l'applicazione delle sue regole anche a Titolari e Responsabili non stabiliti nell'Unione Europea che*:

(i) trattino dati personali di persone fisiche che si trovano nell'UE quando il trattamento è in relazione a offerte di beni e servizi, indipendentemente dal fatto che sia richiesto o meno un pagamento;

(ii) effettuino attività di monitoraggio sul comportamento di persone fisiche che si trovano nell'UE nella misura in cui tale comportamento avvenga nell'UE.

Al contrario, la previgente Direttiva 95/46 prevedeva, l'applicazione della normativa quando il trattamento di dati personali è effettuato *"nel contesto delle attività di uno stabilimento del titolare situato nell'Unione Europea"*. Questo principio introdotto nel Codice Privacy italiano prevedeva appunto che le norme del codice si applicassero:

(i) al "trattamento di dati personali, anche detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato o in luogo comunque soggetto alla sovranità dello Stato

(ii) "anche al trattamento di dati personali effettuato da chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea e impiega, per il trattamento, strumenti situati nel territorio dello Stato anche diversi da quelli elettronici, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea".

Questo rinnovato principio di stabilimento risponde alle definizioni più recenti, sul tema, della Corte di Giustizia Europea, nonché alle indicazioni del Gruppo di lavoro articolo 29[4]. La protezione dei dati personali è, dunque, estesa a coloro che si trovino nell'Unione Europea indipendentemente dal luogo in cui il trattamento dei dati personali è effettuato[5]. L'applicazione di tale principio comporta la tutela anche dei trattamenti effettuati da Titolari che non siano stabiliti nell'Unione Europea purché tali trattamenti abbiano ad oggetto i dati personali che si trovino, anche virtualmente nell'Unione. Le norme del Regolamento sono dotate, pertanto, di una sostanziale "extraterritorialità" dell'efficacia del Regolamento.

Il Regolamento trova, dunque, applicazione se il soggetto a cui si riferiscono i dati "si trovi" realmente o virtualmente nel territorio europeo ovvero se il Titolare o il Responsabile del trattamento è stabilito nell'Unione (anche se il trattamento venga effettuato fuori dell'Unione stessa). In altre parole, l'applicazione di tale principio consente la tutela anche dei trattamenti effettuati da Titolari non stabiliti nell'Unione Europea, se ha ad oggetto dati personali di interessati che si trovano (anche virtualmente) nell'Unione e riguarda l'offerta di beni o servizi e/o con monitoraggio dei loro comportamenti all'interno dell'Unione (art.3 Reg. UE n.2016/679).

4 l gruppo di lavoro «Articolo 29» è un organo consultivo indipendente sulla protezione dei dati e sulla privacy, istituito ai sensi dell'articolo 29 della direttiva 95/46, sulla protezione dei dati. È composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal GEPD (Garante europeo della protezione dei dati), nonché da un rappresentante della Commissione.

C. Ogriseg, *Il Regolamento UE n.2016/679 e la protezione dei dati personali nelle dinamiche giuslavoristiche: la tutela riservata al dipendente in Labour & Law Issues*, 2016, n. 2, pp. 27-64.

5 Cfr. Reg. UE n. 2016/679 considerando 24: È opportuno che anche il trattamento dei dati personali degli interessati che si trovano nell'Unione ad opera di un responsabile del trattamento o di un incaricato del trattamento non stabilito nell'Unione sia soggetto al presente regolamento quando è riferito al controllo del comportamento di detti interessati, quest'ultimo inteso all'interno dell'Unione europea. Per stabilire se un'attività di trattamento sia assimilabile al controllo del comportamento dell'interessato, è opportuno verificare se le operazioni che questi esegue su Internet sono tracciate, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati volte alla profilazione dell'utente, in particolare per prendere decisioni che lo riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali.

1.3 La nuova definizione di dato personale

Uno degli aspetti più significativi del recente intervento legislativo è una definizione di dato personale arricchita dall'introduzione dell' *identificativo online*. Pertanto, la normativa definisce il *dato personale* come «*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*[6]» (art. 4 del Regolamento.)

Le nozioni di "dato genetico" e "dato biometrico" contengono delle novità[7] così come la nozione di trattamento, la quale viene ampliata e aggiornata con l'introduzione del riferimento alla Profilazione.

Il riferimento del Regolamento UE n. 679 del 2016 è esclusivamente al dato personale inerente alle persone fisiche. La direttiva 95/46/CE consentiva, invece, ai singoli Stati di introdurre una disciplina nazionale che estendesse la tutela della riservatezza anche alle persone giuridiche[8].

Nel Regolamento 2016/679 non vi sono le definizioni di dati personali sensibili e giudiziari. Gli artt. 9 e 10 ne danno una indicazione generale con l'introduzione del riferimento ai "dati relativi alla salute[9]".

La circostanza fattuale per cui i minori sono parte integrante e attiva della società dell'informazione induce il legislatore europeo a precisare all'art. 8 che «per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale. Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni».

---

6 Cfr. art.4, n.1, Reg. UE n. 2016/679 secondo cui per dato personale si intende *"qualsiasi informazione concernente una persona fisica identificata o identificabile, l'"interessato"; si considera identificabile la persona 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 on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".*

7 Art. 4, n. 13) «*dati genetici*»: *i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;*

Art. 4, n. 14) «*dati biometrici*»: *i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.*

8 Questa possibilità è stata sfruttata dall'Italia fino al 2012 (art.40, d. l. n. 201/2011 conv. in l. n. 214/2011 che abroga l'estensione della tutela per le persone giuridiche nell'ambito delle misure di semplificazione delle imprese).

9 Art. 4, n. 15) «*dati relativi alla salute*»: *i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.*

1.4 Il Principio di Responsabilizzazione (Accountability)

Una delle novità più significative del Regolamento è l'introduzione del principio di *"responsabilizzazione"* che attribuisce ai titolari del trattamento il compito di *assicurare, ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali*.

Tale principio non trovava esplicita espressione nella Direttiva Madre, tuttavia il Garante Europeo avevano già preso in considerazione la necessità che il trattamento dei dati personali all'Interno dell'Unione fosse ispirato e guidato da un generale principio di responsabilità (parere 3/2010).

Il principio di *accountability* introduce importanti innovazioni nei sistemi di gestione dei dati, con il passaggio da un approccio formale di semplice rispetto della normativa ad uno sostanziale, e dunque, più efficace, di tutela dei dati connesso con le misure di sicurezza, con l'analisi del rischio, e con la valutazione di impatto privacy.

L'approccio applicativo del Regolamento ribalta, dunque, la prospettiva assegnando ai titolari del trattamento l'obbligo di autovalutazione in relazione al trattamento effettuato, alla tipologia dei dati personali trattati, ai rischi derivanti da tale trattamento e, alla adeguatezza delle misure tecniche e organizzative predisposte affinché il trattamento sia conforme al Regolamento.

Il principio di responsabilizzazione trova ulteriore espressione nelle esigenze di protezione dei dati "fin dalla progettazione" (il cosiddetto privacy by design) e "per impostazione predefinita" (privacy by default), previsti dall'articolo 25 del Regolamento.

Un'ulteriore applicazione del principio si rinviene nella previsione dell'obbligo del titolare di dimostrare *di aver rispettato i principio generali di cui al paragrafo 1 dell'articolo 5 e di aver adottato misure tecniche e organizzative adeguate*.

La responsabilizzazione, dunque, deve essere intesa sia come autovalutazione di conformità sia come capacità di dimostrare il rispetto delle disposizioni del Regolamento.

Tra gli strumenti operativi per l'attuazione del principio vi sono i registri delle attività di trattamento[10].

10 si veda, infra, paragrafi successivi.

1.5 La data protection by design e la data protection by default

1.5.1 La privacy by design

La teorizzazione del principio della privacy by design non è del tutto nuova ed è stata utilizzata per la prima volta da Ann Cavoukian della Information and Privacy Commissioner dell'Ontario, e adottata anche nel corso della 32ma Conferenza mondiale dei Garanti Privacy.

In linea generale, l'applicazione del principio della privacy by design comporta che le aziende e le pubbliche amministrazioni avviino i loro progetti introducendo sin dalla progettazione degli stessi gli strumenti a tutela dei dati personali. Secondo la teorizzazione della privacy by design vi sono sette principi regolatori del sistema.

- Il primo principio è "prevenire, non correggere": le questioni problematiche vanno dunque affrontate e risolte sin dalla fase di progettazione in modo da impedire il materializzarsi del rischio.
- Il secondo principio prevede la "privacy come impostazione di default". Ciò comporta che i soggetti non debbano preoccuparsi di proteggere i propri dati poiché questi sono già protetti dal sistema.
- Il terzo principio è quello della "privacy incorporata nel progetto". La tutela della privacy è dunque prevista all'interno del sistema stesso già a partire dalla sua progettazione. Dal punto di vista applicativo, ciò comporta che gli strumenti posti a tutela dei dati personali sono formati contestualmente alla tecnologia e non successivamente;
- Il quarto principio è quello della "massima funzionalità" e pertanto è indicato come uno strumento utile alla tutela degli individui ma anche ai vantaggi economici.
- Il quinto principio tende a "garantire la sicurezza per tutto il ciclo di vita del sistema di produzione del prodotto o del servizio" e infatti assicura la protezione dei dati a partire dall'inizio del trattamento fino alla fine di esso, rendendo inoltre certa la distruzione dei dati alla fine del processo.
- Il sesto principio è quello della e "trasparenza", volto a garantire massima trasparenza alle verifiche sulla tutela dei dati anche quando il sistema subisce delle modifiche.
- Il settimo principio è quello della "centralità dell'utente", e deve pertanto prevedere che l'utente sia al centro del sistema. Porre l'utente al centro implica l'attuazione di una tutela effettiva da un punto di vista sostanziale e non solo formale, nel senso che è fondamentale che l'utente sia salvaguardato e a tal fine non è sufficiente la semplice conformità del sistema alla norma.

Tale approccio è soprattutto connesso alla valutazione del rischio tenendo peraltro in considerazione la natura, il contesto, la portata e le finalità del trattamento.

Il concetto di valutazione di rischio permea numerose norme del Regolamento Europeo. L'applicazione del principio della privacy by design è, in effetti, basato sulla valutazione del rischio, e analogamente per altri obblighi le aziende devono procedere alla valutazione dei rischi. Tale valutazione deve essere effettuata al momento della progettazione del sistema e pertanto prima dell'inizio del trattamento.

Nell'effettuazione della valutazione si dovrà anche tener conto della tipologia dei dati trattati e dello stato della tecnologia pertanto il trattamento deve anche essere adattato alle diverse tecnologie e adattato nel tempo[11].

L'art. 25 del Regolamento 2016/679, rubricato "Data protection by design and by default", ovverosia "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita" introduce i principi della "privacy by design" e "privacy by default".

Il paragrafo 1 dell'art. 25 nel definire il principio della privacy by design prevede che il titolare metta in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione volte ad attuare in modo efficace i principi di protezione dei dati. Questa protezione deve riguardare non solo la fase dell'esecuzione del trattamento, ma anche quella precedente, ovverosia il momento della progettazione dello stesso. Con pseudonimizzazione si intende una metodologia finalizzata ad "allontanare" il dato dalla persona a cui si riferisce. A seguito della pseudonomizzazione, dunque, diviene complicato riferire nuovamente quel dato alla persona cui appartiene. Contestualmente, il legame tra il dato e la persona deve essere mantenuto. La pseudonomizzazione è ottenuta mediante la crittografia o la cifratura dei dati

La crittografia è una tecnica di rappresentazione di un messaggio in forma tale che l'informazione non sia intellegibile ad un qualunque osservatore esterno e possa al contrario essere compresa esclusivamente dal destinatario del messaggio stesso.

---

11 Il riferimento al rischio è peraltro presente nei considerando 75 e 76 della normativa europea del 2016. *Considerando 75 Reg. 679/2016*: I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

Considerando 76 Reg. 679/2016: La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.

1.5.2 La privacy by default

Il principio della privacy by default trova espressione nel paragrafo 2 dell'art. 25 del Regolamento Europeo, il quale prevede che il titolare deve mettere in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita ("di default"), solo i dati personali necessari per ciascuna specifica finalità del trattamento. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone senza l'intervento della persona fisica.

In altre parole, per impostazione predefinita le imprese devono trattare esclusivamente i dati personali in misura necessaria e sufficiente al raggiungimento dei propri scopi e per il periodo necessario a tale attività.

La protezione di default riguarda :

- la quantità dei dati raccolti;
- l'estensione del trattamento;
- il periodo di conservazione;
- l'accessibilità.

Le impostazioni di privacy by default garantiscono che l'utilizzo di determinati dati sia fatto dall'utente seguendo una scelta già impostata dal sistema , e dunque in automatico, pur residuando la possibilità per l'utente di modificare le impostazioni già previste.

Il concetto di privacy by default non è definito con precisione dal Regolamento del 2016, e in linea generale è inteso come un metodo di creazione di sistemi che già in origine escludono la raccolta dei dati o di alcune tipologie di essi. Il legislatore europeo non indica come debbano essere realizzati tali sistemi né vi sono ancora buone prassi già diffuse.

I principi di protezione della privacy introdotti dall'art. 25 del Regolamento Europeo sono molto significativi, poiché impongono alle pubbliche amministrazioni e alle imprese un approccio strategico e di valutazione già dal momento della progettazione di nuove procedure e di prodotti e servizi.

2. LA TUTELA DELLA PRIVACY NELLE ISTITUZIONI SCOLASTICHE

2.1 I concetti chiave: titolare- responsabile e incaricati del trattamento

I soggetti che effettuano il trattamento dei dati sono :

- *il titolare del trattamento*, ovverosia il rappresentante legale dell'Istituto scolastico *(Il Dirigente scolastico);*
- *il responsabile del trattamento*, che può essere nominato dal titolare ovvero può coincidere con il Titolare medesimo. Generalmente il responsabile è il Direttore dei servizi generali e Amministrativi, pur essendo prevista la possibilità che i responsabili siano in numero maggiore di uno, soprattutto in ragione di una particolare complessità organizzativa che comporti una suddivisone dei compiti;
- il responsabile nomina *gli incaricati* del trattamento (Docenti, referenti di Plesso i quali seguono le direttive ricevute dal responsabile).

Alcune definizioni. Art. 4 del Reg. 679/2016:

7) *«titolare del trattamento»*: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

8) *«responsabile del trattamento»*: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

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

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

2.2 I principi di liceità, correttezza, trasparenza nell'utilizzo dei dati

I principi di *liceità, correttezza e trasparenza* nell'utilizzo dei dati sono alla base della normativa in materia di trattamento dei dati (art. 5 del Regolamento),[12] così come *la necessità del consenso* al trattamento da parte dell'interessato, in coerenza con quanto previsto dalle regolamentazioni precedenti (codice della privacy).

L'articolo 5, al paragrafo 1, elenca i principi applicabili al trattamento dei dati personali: *liceità*[13] *e correttezza* (già presenti nella Direttiva del 1995) e specifica ulteriormente gli altri : trasparenza, minimizzazione, esattezza, limitazione di conservazione, integrità e riservatezza.

Sono, inoltre, indicati i criteri da rispettare al fine della redazione delle informative, volte ad ottenere un consenso "informato" e "consapevole" (art.12, Reg. UE n. 2016/679). I requisiti fondamentali delle informative sono: puntualità, efficacia, intelligibilità e comprensibilità delle informazioni fornite sulle modalità di trattamento dei dati.

---

12 Articolo 5, Reg. Europeo 679 del 2016

Principi applicabili al trattamento di dati personali

1. 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, considerato incompatibile con le finalità iniziali («limitazione della finalità»);

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

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

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

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

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

13 Liceità del trattamento.

Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

2.3 Le categorie particolari di dati personali

Alcune definizioni. Art. 4 del Reg. 679/2016:

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

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

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

L'articolo 9 del Reg. 679/2016 ribadisce il principio generale per cui *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.*

Il divieto non si applica se, tra le altre ipotesi, l'interessato ha prestato il proprio consenso esplicito al trattamento dei dati personali.[14]

14 Articolo 9 Reg. 679/2016

Trattamento di categorie particolari di dati personali

1. 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.

2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi:

a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;

b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;

c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;

e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;

f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

2.4 L'informativa privacy

La Direttiva n. 95/46 e il Codice della Privacy già avevano riconosciuto la funzione fondamentale dell'informativa, e tale importanza è confermata e potenziata nel recente provvedimento europeo.

Il diritto a ricevere una informativa adeguata ha ora rilevanza autonoma (artt. 12, Reg. UE n. 2016/679) e non è più esclusivamente il mezzo per ottenere il consenso al trattamento dei dati.

Il contenuto dell'informativa è poi differente a seconda che i dati siano raccolti presso l'interessato oppure no, e in questa ultima ipotesi sono previste informazioni aggiuntive (artt.13 e 14, Reg. UE n. 2016/679).

2.5 La "nuova informativa"

Il regolamento specifica molto più in dettaglio rispetto al Codice della privacy le caratteristiche dell'informativa che deve essere rilasciata al momento della raccolta dei dati presso l'interessato.

Gli articoli 13, paragrafo 1, e 14, paragrafo 1, del regolamento elencano i contenuti dell'informativa, che ne risulta ampliata rispetto alla normativa italiana.

---

g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;

h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3;

i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;

j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

3. I dati personali di cui al paragrafo 1 possono essere trattati per le finalità di cui al paragrafo 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti.

4. Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute.

Articolo 13 Regolamento UE 2016/679

Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato.

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, ove applicabile;
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), 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 o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

(Art. 13 segue)

2. In aggiunta alle informazioni di cui al paragrafo 1, 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:

a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
b) 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;
c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
d) il diritto di proporre reclamo a un'autorità di controllo;
e) 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;

f) 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.

3. 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 e ogni ulteriore informazione pertinente di cui al paragrafo 2.

4. I paragrafi 1, 2 e 3 non si applicano se e nella misura in cui l'interessato dispone già delle informazioni.

2.6 Le modalità di prestazione dell'informativa

Il Regolamento indica in maniera più dettagliata rispetto al Codice della Privacy le modalità dell'informativa da fornire all'interessato, e specifica che questa debba essere *concisa, trasparente, intelligibile per l'interessato e facilmente accessibile.*

È richiesto un linguaggio chiaro e semplice, e per i minori occorre prevedere informative idonee. [15]

L'informativa è generalmente fornita per iscritto.

2.7 Le ipotesi di esonero dall'informativa

Le fattispecie in cui è previsto l'esonero della presentazione dell'informativa non sono del tutto coincidenti con quanto previsto dal Codice Privacy.

Il Codice Privacy individua tre ipotesi nelle quali il titolare non è tenuto a informare l'interessato, ovverosia quando:

- il trattamento è da eseguire in base ad un obbligo di legge o di regolamento ovvero in base ad una norma comunitaria;
- i dati sono da trattare ai fini dello svolgimento delle investigazioni difensive ovvero per far valere/difendere un diritto in sede giudiziaria;
- l'informativa all'interessato comporti un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiari manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, sempre per il Garante, impossibile.

15 Considerando n. 58, Regolamento 2016/679: *Il principio della trasparenza impone che le informazioni destinate al pubblico o all'interessato siano concise, facilmente accessibili e di facile comprensione e che sia usato un linguaggio semplice e chiaro, oltre che, se del caso, una visualizzazione. Tali informazioni potrebbero essere fornite in formato elettronico, ad esempio, se destinate al pubblico, attraverso un sito web. Ciò è particolarmente utile in situazioni in cui la molteplicità degli operatori coinvolti e la complessità tecnologica dell'operazione fanno sì che sia difficile per l'interessato comprendere se, da chi e per quali finalità sono raccolti dati personali che lo riguardano, quali la pubblicità online. Dato che i minori meritano una protezione specifica, quando il trattamento dati li riguarda, qualsiasi informazione e comunicazione dovrebbe utilizzare un linguaggio semplice e chiaro che un minore possa capire facilmente.*

Il Regolamento Europeo 2016 individua le seguenti ipotesi in cui il titolare non è tenuto a informare l'interessato, ovverosia quando:

- l'interessato dispone già delle informazioni;
- comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato;
- i dati personali debbano rimanere riservati per obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri;
- l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare.

Nelle ipotesi di dati personali raccolti da fonti diverse dall'interessato spetta al titolare valutare se la *prestazione dell'informativa agli interessati comporti uno sforzo sproporzionato* (*art. 14, paragrafo 5, lettera b*) – a differenza di quanto prevede l'art. 13, comma 5, lettera c del Codice Privacy.

In maniera non dissimile da quanto previsto dal Codice Privacy:

- L'informativa deve essere fornita prima di effettuare la raccolta dei dati (se raccolti presso l'interessato);
- Se i dati non sono raccolti direttamente presso l'interessato, come previsto dall'art. 14 del Regolamento, l'informativa deve comprendere anche le categorie dei dati personali oggetto di trattamento. In tutti i casi, il titolare deve specificare la propria identità e quella dell'eventuale rappresentante nel territorio italiano, le finalità del trattamento, i diritti degli interessati (compreso il diritto alla portabilità dei dati), se esiste un responsabile del trattamento e la sua identità, e quali sono i destinatari dei dati.

2.8 Il diritto all'oblio

Il Regolamento Europeo del 2016 attua il riconoscimento normativo del diritto all'oblio, sinora elaborato dalla giurisprudenza e definito come il diritto del soggetto ad "essere dimenticato" e, dunque, a vedere i propri dati cancellati dalle banche, o dai mezzi di informazione e dai motori di ricerca.

L'art. 17 Regolamento (UE) 2016/679 prevede espressamente che l'interessato abbia il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo, e che il titolare del trattamento abbia l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

- i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
- l'interessato revoca il consenso su cui si basa il trattamento e se non sussiste altro fondamento giuridico per il trattamento;
- l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento;

- i dati personali sono stati trattati illecitamente;
- i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
- i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione.

In termini generali, il diritto all'oblio è il diritto *"ad essere dimenticati"*, relativamente ai dati risalenti nel tempo, con riguardo soprattutto ai precedenti giudiziari o ad eventuali condanne penali.

La tutela del diritto all'oblio ha avuto, di recente, significativa diffusione ed è considerata una espressione del diritto alla riservatezza, nella accezione di diritto a veder "restaurata la propria intimità". Accogliendo queste istanze di protezione il Regolamento Europeo ha introdotto una disposizione normativa che tutela il diritto dell'interessato alla cancellazione dei dati personali che lo riguardano e che sono detenuti dal titolare del trattamento.

Dal punto di vista pratico l'attuazione di tale diritto prevede due fattispecie:

- Se il trattamento dei dati è effettuato in relazione al preventivo rilascio del consenso da parte dell'interessato, la revoca di questo sarà sufficiente ai fini della cancellazione dei dati in possesso del titolare del trattamento;
- Se il trattamento dei dati è effettuato in relazione ad una raccolta senza il preventivo e necessario rilascio del consenso, la cancellazione dei dati può attuarsi se questi non siano più necessari rispetto alle finalità per le quali sono stati raccolti.

Nel caso in cui sia pervenuta al titolare una richiesta di cancellazione dei dati, questi è tenuto sia alla rimozione presso gli archivi sia - ove i dati siano stati resi pubblici in altre piattaforme - alla comunicazione di rimozione dei dati ai soggetti terzi e titolari di differente trattamento dei medesimi dati di cui l'interessato ha richiesto la cancellazione "tenendo conto della tecnologia disponibile e dei costi di attuazione".

Sono escluse dal diritto all'oblio le ipotesi in cui il trattamento dei dati è necessario ad esempio per l'esercizio del diritto alla libertà di espressione e di informazione oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria (art. 17 del Regolamento, terzo comma.)

Il confronto con la normativa italiana sulla Privacy evidenzia l'intenzione del Legislatore Europeo di assegnare al diritto all'oblio un ruolo rafforzato. Sul punto, rispetto all'art. 7, comma 3, lettera b) del Codice della Privacy, il "nuovo" diritto all'oblio, prevede che l'interessato ha il diritto di richiedere la cancellazione dei propri dati personali anche dopo la revoca del consenso al trattamento.

2.9 Il diritto di Opposizione

L'Art. 21 del Regolamento disciplina il "Diritto di opposizione", che attribuisce all'interessato il diritto di opporsi "in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano". A seguito dell'esercizio del diritto, il titolare potrà continuare a trattare i dati in suo possesso solo ove 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. GLI ADEMPIMENTI E GLI OBBLIGHI PER LE ISTITUZIONI SCOLASTICHE.

3.1 La proceduralizzazione degli obblighi di Titolari e Responsabili

L'intento del Legislatore Europeo di rafforzare la protezione dei dati personali trova ulteriore espressione nella proceduralizzazione degli obblighi di Titolari e Responsabili, a seguito dell'introduzione del Nuovo Regolamento. Le norme del 2016 impongono, infatti, ai Titolari del trattamento l'Analisi e la Valutazione dei Rischi e la conseguente adozione di Misure di Sicurezza Tecniche e Organizzative "adeguate" (art. 5 e 32, Reg. UE n.2016/679.) La Direttiva 95/46/CE aveva invece previsto l'adozione di misure minime di sicurezza, così come, peraltro artt.33 e ss. e Allegato B del d.lgs. n. 196/2003.

Per quel che concerne, dunque, i processi considerati dal Regolamento e dalle Autorità Garanti "pericolosi" per i dati personali[16] è anche obbligatoria la valutazione d'impatto sulla protezione della riservatezza (cd. Privacy Impact Assessment.) L'Oggetto di tale valutazione è l'impatto sulla protezione della privacy di soluzioni tecnico-organizzative adottate in relazione all'attività svolta.

L'art. 35 al punto 3 prevede, in proposito, ipotesi specifiche: *La valutazione d'impatto sulla protezione dei dati è richiesta in particolare nei casi seguenti:*

a) *una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;*
b) *il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o*
c) *la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.*

Spetta all'autorità di controllo (il Garante privacy) il compito di redigere e rendere pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati.

16 Articolo 35. Valutazione d'impatto sulla protezione dei dati1. 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.

3.2 La valutazione di impatto sulla protezione della privacy nelle scuole

Il legislatore europeo ha previsto la necessità di realizzare una valutazione d'impatto sulla protezione dei dati esclusivamente quando la tipologia di trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche"[17] (articolo 35, paragrafo 1).

L'applicazione pratica di tale principio comporta che i titolari del trattamento devono continuamente valutare i rischi creati dalle loro attività al fine di stabilire quando una tipologia di trattamento "possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche." La valutazione d'impatto sulla protezione dei dati va effettuata "prima del trattamento".

Alcune istituzioni scolastiche potrebbero essere tenute a realizzare la valutazione di impatto sulla protezione dei dati, nelle ipotesi in cui svolgano il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 del Regolamento (trattamento dei cosiddetti dati sensibili), ovvero se applichino la sorveglianza sistematica su larga scala di una zona accessibile al pubblico. La definizione di larga scala si presta a numerose interpretazioni[18] e il Regolamento riferisce comunque il concetto ad una *notevole quantità di dati personali trattati a livello regionale, nazionale o sovranazionale*. In linea generale non può escludersi che gli istituti scolastici mettano in atto trattamento dei dati con rischi elevati: si pensi ad esempio ad attività che prevedano soggiorni all'estero degli studenti, soprattutto in Paesi estranei all'Unione Europea.

La valutazione di impatto, inoltre, è particolarmente importante quando è introdotta una nuova tecnologia di trattamento dei dati, e si pensi, nello specifico, all'uso oramai diffuso nelle scuole di lavagne e registri elettronici, tablet, classi 2.0, aule 3.0, applicazioni per l'apprendimento e servizi digitali per gli studenti. In mancanza delle indicazioni più precise da parte del Garante Europeo, nei casi in cui non è chiaro se sia richiesta una valutazione d'impatto sulla protezione dei dati o meno, il WP29[19] raccomanda di effettuarla comunque, in quanto detta valutazione è uno strumento utile che assiste i titolari del trattamento a rispettare la legge in materia di protezione dei dati[20].

---

17 GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679adottate il 4 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017.

18 Il Regolamento Europeo riferimento al concetto di larga scala nel Considerando 91, che, sul punto, prevede: "trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato".

19 Il Regolamento Europeo riferimento al concetto di larga scala nel Considerando 91, che, sul punto, prevede: "trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato".

20 GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679adottate il 4 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017.

Approfondimento

Il Gruppo di Lavoro Art.29, ha emanato alcune Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679adottate il 4 aprile 2017.

In questo documento si legge espressamente che al fine di fornire un insieme più concreto di trattamenti che richiedono una valutazione d'impatto sulla protezione dei dati in virtù del loro rischio elevato intrinseco, si devono considerare alcuni criteri, in particolare in considerazione di "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato" (considerando 71 e 91) . In relazione a tali criteri i seguenti possono riguardare più nello specifico le istituzioni scolastiche

Valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato" (considerando 71 e 91).

Monitoraggio sistematico: trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o "la sorveglianza sistematica su larga scala di una zona accessibile al pubblico" (articolo 35, paragrafo 3, lettera c))15 . Questo tipo di monitoraggio è un criterio in quanto i dati personali possono essere raccolti in circostanze nelle quali gli interessati possono non essere a conoscenza di chi sta raccogliendo i loro dati e di come li utilizzerà. Inoltre, può essere impossibile per le persone evitare di essere soggette a tale trattamento nel contesto di spazi pubblici (o accessibili al pubblico).

Dati sensibili o dati aventi carattere altamente personale: questo criterio include categorie particolari di dati personali così come definite all'articolo 9 (ad esempio informazioni sulle opinioni politiche delle persone).

Trattamento di dati su larga scala: il regolamento generale sulla protezione dei dati non definisce la nozione di "su larga scala", tuttavia fornisce un orientamento in merito al considerando 91. A ogni modo, il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala16: a. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; b. il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; c. la durata, ovvero la persistenza, dell'attività di trattamento; d. la portata geografica dell'attività di trattamento; dati relativi a interessati vulnerabili (considerando 75): uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative, quali la combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, ecc

Nella maggior parte dei casi, un titolare del trattamento può considerare che un trattamento che soddisfi due criteri debba formare oggetto di una valutazione d'impatto sulla protezione dei dati. In generale, il WP29 ritiene che maggiore è il numero di criteri soddisfatti dal trattamento, più è probabile che sia presente un rischio elevato per i diritti e le libertà degli interessati e, di conseguenza, che sia necessario realizzare una valutazione d'impatto sulla protezione dei dati, indipendentemente dalle misure che il titolare del trattamento ha previsto di adottare. Tuttavia, in alcuni casi, un titolare del trattamento può ritenere che un trattamento che soddisfa soltanto uno di questi criteri richieda una valutazione d'impatto sulla protezione dei dati.

La Valutazione d'Impatto deve contenere:

a) una descrizione dei trattamenti previsti e delle finalità del trattamento;

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

c) una valutazione dei rischi per i diritti e le libertà degli interessati e le misure previste per affrontare i rischi.

Per quel che concerne l'adeguatezza delle misure di protezione, l'obbligatorietà della adozione riguarda anche la progettazione (cd. "privacy by design") con impostazioni di Privacy predefinite chiuse (cd. "privacy by default") in maniera che siano oggetto di trattamento solo i dati personali necessari per ogni finalità e non siano invece accessibili se non ad un numero definito di persone[21] (si veda sul punto considerando 78 e art.25, Reg. UE n. 2016/679).

3.3 Il Registro delle attività di trattamento

Ulteriori adempimenti sono poi assegnati al Titolare e al Responsabile del Trattamento, i quali devono tenere dei *registri* nei quali siano documentati gli adempimenti e le procedure attinenti ad ogni trattamento. Sono esclusi dall'obbligo di tenere il registro delle attività di trattamento le imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare *un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9*, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10 (art. 30 del Reg. EU 2016/679).

3.4 Il Registro delle Attività di Trattamento nelle scuole

Il testo normativo europeo impone, dunque, a coloro che effettuano il trattamento di categorie particolari di dati (i cosiddetti dati sensibili) la tenuta dei registri delle Attività di trattamento. In tale categoria rientrano senz'altro gli istituti scolastici e pertanto, in mancanza di ulteriori indicazioni da parte del MIUR o del Garante per la privacy tali registri dovranno essere tenuti anche nelle scuole.

Il considerando 82 del Regolamento assegna al registro l'obiettivo di provare che il titolare e il responsabile del trattamento agiscano in conformità con la normativa europea. Il considerando esplicita, inoltre, la necessità di obbligare i titolari e i responsabili del trattamento ad una collaborazione attiva con l'autorità di controllo – in Italia l'Autorità Garante in materia di pro-

21 Considerando n.78: *Al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default. Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza. Art. 25, punto 2 del Regolamento: 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.*

tezione dei dati personali – affinché l'attuazione di tutte le misure disposte dal Regolamento sia formalmente e sostanzialmente dimostrata.

L'art. 30 del Regolamento Europeo indica le informazioni che devono essere contenute nel registro:

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

Il punto 2 prescrive, inoltre, che ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento.

Tali registri sono tenuti in forma scritta, anche in formato elettronico.

Su richiesta, tali registri devono essere posti a disposizione dell'autorità di controllo.

3.5 Il Data Protection Officer

Il Regolamento Europeo sulla protezione dei dati personali n. 2016/679 ha previsto in determinati casi, sia per gli enti pubblici sia per le aziende private, la designazione del Responsabile per la protezione dei dati personali (RPD), anche detto Data Protection Officer.

Il Data Protection Officer è una figura di alto livello professionale che deve essere coinvolta in tutte le questioni inerenti alla protezione dei dati personali. Il Data Protection Officer (DPO) gode di ampia autonomia ed è designato in funzione delle proprie qualità professionali, soprattutto in relazione alla conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati, e della capacità di adempiere ai propri compiti; deve, inoltre, possedere delle qualità manageriali, oltre che una buona conoscenza delle nuove tecnologie.

I compiti del Data Protection Officer sono definiti dall' art. 39 del Regolamento Europeo 679 del 2016 e sono di carattere consultivo in materia di privacy nei confronti del titolare e del responsabile del trattamento, di vigilanza sull'osservanza del Regolamento e di raccordo con l'Autorità Garante per la privacy.

La nomina del DPO nelle scuole

La nomina di un Responsabile per la protezione dei dati è obbligatoria, secondo l'art. 37 del Regolamento in tre casi:

a) *se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico*[22]*;*
b) *se le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala;*
c) *se le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento su larga scala di categorie particolari di dati*[23] *o di dati personali relativi a condanne penali e reati privacy.*

La prima ipotesi, di cui alla lettera a dell'art. 37 del Reg. Europeo è di facile interpretazione, e riguarda le ipotesi in cui il trattamento *"sia effettuato da un'autorità pubblica o da un organismo pubblico"*.

È dunque evidente che il Legislatore Europeo abbia così individuato un numero cospicuo di soggetto obbligati alla nomina del Responsabile per la protezione dei dati, tra cui figurano anche le scuole in ragione della loro qualità di ente pubblico.

La nomina del responsabile per la protezione dei dati è un compito attribuito dall'art. 37 del Regolamento sia ai titolari, sia ai responsabili del trattamento, senza una distinzione. In ragione della soddisfazione dei criteri previsti per l'obbligatorietà della nomina, questa spetterà solo al titolare del trattamento ovvero al responsabile del trattamento oppure ancora ad entrambi.

L'articolo 37, paragrafo 3, prevede la designazione di un unico RPD per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e della loro dimensione. Tale opportunità potrebbe essere utilizzata favorevolmente dai circoli di istituto i quali, in ragione delle loro dimensioni e della struttura organizzativa, potrebbero nominare un unico Responsabile per la Protezione dei dati.

Il Responsabile per la protezione dei dati deve svolgere numerose funzioni, e pertanto il titolare del trattamento o il responsabile del trattamento devono assicurarsi che un unico protection Officer, sia in grado di portare a termine le proprie funzioni, se necessario supportato anche da un team di collaboratori.

22 Ad eccezione delle autorità giudiziarie nell'esercizio delle funzioni giurisdizionali. (articolo 32 della direttiva (UE) 2016/680.

23 Ai sensi dell'articolo 9, si tratta dei dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni filosofiche o religiose, o l'appartenenza sindacale, oltre al trattamento di dati genetici, dati biometrici al fine dell'identificazione univoca di una persona fisica, e di dati relativi alla salute, alla vita sessuale o all'orientamento sessuale di una persona fisica.

3.7 La designazione Del Data Protection Officer: I requisiti

Il comma 5 dell'art. 37 indica al titolare del trattamento le modalità di scelta del Responsabile per la Protezione dei dati, prevedendo che questi debba essere designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.

Le linee Guida del Gruppo di Lavoro ex art. 29 aggiungono che tale ruolo può essere ricoperto esclusivamente da una persona fisica, supportata, se necessario, da un team.

Il par. 5 dell'art. 37 non specifica le qualità professionali necessarie al Responsabile per la protezione dei dati; tuttavia, al riguardo è senz'altro necessaria la conoscenza da parte del RPD della normativa e delle prassi nazionali ed europee in materia di protezione dei dati e un'approfondita conoscenza del Regolamento Europeo sulla protezione dei dati.

Il considerando n.97 del Regolamento specifica ulteriormente che il DPO deve avere conoscenze approfondite nell'ambito della privacy, capacità di eseguire ispezioni, consultazioni, analisi documentali in maniera del tutto indipendente

Secondo l'opinione del Garante italiano per la protezione dei dati personali nella scelta del DPO sono da tenere in attenta considerazione i requisiti normativi relativamente a:

- posizione (riferisce direttamente al vertice),
- indipendenza (non riceve istruzioni per quanto riguarda l'esecuzione dei compiti)
- autonomia (attribuzione di risorse umane e finanziarie adeguate).

Per la scelta del Responsabile della protezione dei dati il Garante suggerisce di verificare le competenze ed esperienze specifiche. Per alcune categorie di trattamenti, relativi per esempio alle aziende ospedaliere, sono necessarie qualità professionali adeguate alla complessità del compito da svolgere, nonché la documentazione delle esperienze fatte, la partecipazione a master e corsi di studio/professionali (in particolare se risulta documentato il livello raggiunto). Tale indicazione è significativamente valida per gli istituti scolastici, in ragione della particolarità della attività svolta.

3.8 L'atto di designazione del RPD

L'art. 37 prevede la designazione dei RPD ad opera del titolare e del responsabile del trattamento e, pertanto, l'atto di designazione è una parte del relativo adempimento.

Se il RPD scelto è già all'interno dell'ente è necessario formalizzare un atto di designazione a "Responsabile per la protezione dei dati" .

Nel caso in cui il RPD sia un soggetto esterno all'ente, la designazione sarà parte integrante del contratto di servizi redatto secondo quanto previsto dall'art. 37 del Regolamento. Nell'atto di designazione devono essere individuate espressamente le generalità del soggetto che opererà come RPD, e devono essere indicati i compiti e le funzioni assegnate. L'assegnazione eventuale

e successiva di ulteriori compiti rispetto a quello previsti nell'atto di designazione richiede la modifica e l'integrazione delle clausole contrattuali o dell'atto di designazione.

Il Garante italiano per la Protezione dei dati personali invita anche ad indicare, nell'atto di designazione o nel contratto sia pure succintamente, anche le motivazioni che hanno indotto l'ente alla scelta della persona selezionata. Questa precisazione è utile alla verifica del rispetto dei requisiti previsti dall'art. 37 del Regolamento e può essere attuata anche mediante il rinvio agli esiti delle procedure di selezione interna o esterna effettuata.

L'indicazione dei criteri utilizzati nella scelta di tale figura, oltre a essere indice di trasparenza e di buon amministrazione, è anche elemento di valutazione del rispetto del principio di "responsabilizzazione".

3.9 Pubblicazione e comunicazione dei dati di contatto del RPD

L'articolo 37, par. 7 statuisce che "*Il titolare del trattamento o il responsabile del trattamento* ***pubblica i dati*** *di contatto del responsabile della protezione dei dati e* ***li comunica all'autorità di controllo***."

Con questa previsione il legislatore europeo ha voluto assicurare agli interessati e alle autorità di controllo la possibilità di contattare il Responsabile per la protezione dei dati facilmente e in modo diretto.

Sul punto il Gruppo dei Garanti europei suggerisce anche l'importanza della confidenzialità delle comunicazioni, sottolineando come i dipendenti possano mostrare riluttanza a presentare reclami al Responsabile in mancanza di confidenzialità.

Il responsabile della protezione dei dati è, d'altronde, tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri (articolo 38, paragrafo 5 del Regolamento Europeo 679/2016).

I dati di contatto del Responsabile per la protezione dei dati sono: recapito postale, numero di telefono dedicato e indirizzo di posta elettronica. Potrebbe essere anche utile un modulo specifico per contattare il RPD pubblicato sul sito del titolare/responsabile del trattamento. Per quanto non sia esplicitamente prevista la pubblicazione del nominativo del responsabile, il Gruppo di Lavoro dei garanti ne consiglia l'indicazione. Fermo restando, in proposito, che comunicare il nominativo del RPD all'autorità di controllo è fondamentale affinché il RPD funga da punto di contatto fra il singolo ente o organismo e l'autorità di controllo stessa (articolo 39, paragrafo 1, lettera e).

Il Gruppo di lavoro raccomanda, inoltre, che il titolare/responsabile del trattamento comunichi ai dipendenti il nominativo e i dati di contatto del RPD. Nello specifico queste informazioni (nominativo e dati di contatto) potrebbero essere pubblicate sulla intranet del titolare/responsabile del trattamento, inserite nell'elenco telefonico interno e nei diversi organigrammi della struttura[24].

24 GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, Linee guida sui responsabili della protezione dei dati Adottate il 13 dicembre 2016; Versione emendata e adottata in data 5 aprile 2017.

3.10 L'art. 38 del Regolamento: Posizione del responsabile della protezione dei dati

Secondo l'art. 38 del RGPD, il titolare del trattamento e il responsabile del trattamento assicurano che il RPD sia *"tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali"*.

Il Legislatore europeo ha espressamente previsto la necessità che il Data Protection officer sia coinvolto subito nelle questioni attinenti alla protezione dei dati. Tale principio trova concreta applicazione per quel che concerne le valutazioni di impatto sulla protezione dei dati. Sul tema, il Regolamento prevede nello specifico che il Responsabile sia coinvolto fin dalle fasi iniziali e il titolare del trattamento ha l'obbligo di consultarlo nell'effettuazione di tali valutazioni.

3.11 L'art. 38 del Regolamento, 679/2016 par. 2: le risorse necessarie

Il par. 2 dell'art. 38 prevede che il titolare del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

Di conseguenza, in relazione alla complessità (amministrativa e tecnologica) dei trattamenti e dell'organizzazione, è necessario innanzitutto valutare se è sufficiente la nomina di una sola persona per svolgere il complesso dei compiti affidati al RPD.

Come riportato anche nelle Linee guida, «in linea di principio, quanto più aumentano complessità e/o sensibilità dei trattamenti, tanto maggiori devono essere le risorse messe a disposizione del RPD. La funzione "protezione dati" deve poter operare con efficienza e contare su risorse sufficienti in proporzione al trattamento svolto».

3.12 La Posizione e I Compiti del Data Protection Officer

Il DPO ha il compito di informare e consigliare il titolare o il responsabile del trattamento e i dipendenti sugli obblighi previsti dalle norme in materia di protezione dei dati e verificare l'attuazione e l'applicazione delle stesse.

Se richiesto, ha anche il compito di fornire pareri in merito alla valutazione d'impatto sulla protezione dei dati e verificarne gli adempimenti.

Il Data Protection Officer, inoltre, è il punto di contatto con il Garante per la Protezione dei dati e anche con gli interessati al trattamento, i quali hanno facoltà di contattarlo.

Il controllo del rispetto del Regolamento sulla protezione dei dati non implica, tuttavia, che il Data Protection Officer sia personalmente responsabile in caso di inosservanza.

Spetta, infatti sempre al titolare del trattamento di essere in grado di dimostrare che il trattamento è effettuato nel rispetto del Regolamento Europeo.

3.13 Le sanzioni previste dal Regolamento Europeo

Il tema delle sanzioni nel nuovo Regolamento Europeo occupa un posto di significativo rilievo, in ragione dell'inasprimento delle stesse in relazioni al trattamenti illegittimi.

Le sanzioni penali rimangono di competenza dei singoli Stati, al contrario, alla disciplina delle sanzioni amministrative sono rivolti gli articoli 83 e 84 del Regolamento.

La normativa europea del 2016 attribuisce all'autorità di controllo il potere di imporre sanzioni amministrative per un importo pecuniario massimo predeterminato, tenendo conto, nella determinazione del quantum, di alcune circostanze- differenti rispetto ai criteri dalla legge italiana n. 689/91- quali

a. la natura, la gravità e la durata della violazione,
b. il carattere doloso o colposo della stessa,
c. le misure adottate dal Titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati, o ancora, il grado di responsabilità del Titolare o del Responsabile, anche sotto il profilo tecnico, e le misure organizzative attuate per prevenire le violazioni; eventuali rilevanti violazioni precedenti da parte del Titolare o del Responsabile;
d. il livello di cooperazione con l'autorità di vigilanza, le categorie di dati personali oggetto della violazione;
e. i benefici finanziari ottenuti, o le perdite evitate, direttamente o indirettamente, per effetto della violazione commessa.

Per quel che concerne l'entità, le sanzioni amministrative pecuniarie sono distinte a seconda della gravità dell'illecito commesso (art. 83, commi 4,5,6 Reg. UE n. 2016/679). Nella prima fascia vi sono le sanzioni amministrative fino a 10 milioni di euro, o in caso di un'impresa, fino al 2% del fatturato totale annuo mondiale dell'esercizio precedente, se superiore, connesse alla violazione degli obblighi del titolare e del responsabile del trattamento (artt. 8 e11; artt. 25-39; artt. 42-43 Reg. UE n. 2016/679);

- la violazione degli obblighi dell'organismo di certificazione (artt. 42-43 Reg. UE n. 2016/679);
- la violazione degli obblighi dell'Organismo di controllo (art. 41, par. 4, Reg. UE n. 2016/679.

Nella seconda fascia sanzionatoria, che prevede sanzioni fino a un massimo di 20 milioni di euro e 4% del fatturato, in caso di aziende, rientrano :

- la violazione dei principi di base del trattamento comprese le condizioni relative al consenso (artt. 5,6,7 e 9 Reg. UE n. 2016/679);
- la violazione dei diritti degli interessati (artt. 12-22 Reg. UE n. 2016/679);
- i trasferimenti di dati a un destinatario in un paese terzo o organizzazione internazionale (artt. 44-49, Reg. UE n. 2016/679);
- la violazione di qualsiasi obbligo previsto dalle legislazioni degli Stati membri a norma del capo IX;

- l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi dei dati dell'Autorità di Controllo ai sensi dell'art. 58 par. 2 o art. 58 par.1 Reg. UE n. 2016/679);
- l'inosservanza di un ordine da parte dell'Autorità di Controllo di cui all'art. 58, par. 2 Re. UE n. 2016/679.

In tema di sanzioni, inoltre, l'art. 84 del Regolamento prevede che gli Stati membri stabiliscono le norme relative alle altre sanzioni per le violazioni del regolamento in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 83, e adottano tutti i provvedimenti necessari per assicurarne l'applicazione. *Tali sanzioni devono essere effettive, proporzionate e dissuasive*.

3.14 Data Breach e comunicazioni obbligatorie

L'art. 33 del Regolamento Europeo 679/2016 introduce un adempimento di significativa importanza per la sicurezza dei dati: l'obbligo generalizzato di notificare la violazione dei dati personali al Garante.

La normativa italiana (Legge Privacy) prevede invece che solo i "fornitori di servizi di comunicazione elettronica accessibili al pubblico" hanno l'obbligo di comunicare l'avvenuta violazione di dati personali:

(i) al Garante per la protezione dei dati personali;

(ii) in determinati casi, anche al contraente/cliente.

Innanzitutto il Regolamento Europeo Privacy EU/2016/679 considera *"Data Breach o Violazione dei Dati Personali" qualsiasi violazione di sicurezza che comporta la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzato a dati personali, indipendentemente dalla causa che l'ha generata.*

Tutti i titolari del trattamento hanno dunque l'obbligo di comunicare i casi di violazione dei dati al Garante per la Protezione dei Dati Personali entro 72 ore dalla conoscenza del fatto. Nello specifico, il Responsabile deve informare il Titolare senza ingiustificato ritardo della violazione e quest'ultimo deve notificare la violazione, senza ingiustificato ritardo, all'autorità di controllo (il garante per la Privacy). Il ritardo nella notificazione del data breach deve essere motivato al Garante Privacy, pena l'applicazione delle sanzioni previste dal Regolamento Europeo.

Il dovere di notifica nel termine di 72 ore è escluso quando è improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone. La notifica deve contenere almeno, a titolo esemplificativo:

1) la descrizione della natura della violazione e, ove possibile, il numero degli interessati;
2) il contatto del responsabile della protezione dati o di altro punto di contatto per ottenere più informazioni;

3) la descrizione delle misure adottate o che si intende adottare per porre rimedio alla violazione dei dati.

Se l'oggetto della violazione sia stato un trattamento affidato esternamene ad un responsabile del trattamento, il Regolamento impone anche al fornitore l'obbligo di comunicare tempestivamente al titolare del trattamento l'avvenuta violazione dei dati personali.

Qualora, inoltre, la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà fondamentali degli interessati, il titolare del trattamento è obbligato a comunicare l'avvenuto data breach anche a ciascun interessato (art. 34 del Regolamento), consentendo dunque di adottare le precauzioni volte a ridurre al minimo il potenziale danno derivante dalla violazione dei suoi dati personali.

La comunicazione della violazione all'interessato deve prevedere un linguaggio semplice e chiaro e contenere un'accurata descrizione della natura della violazione dei dati personali, nonché suggerimenti e raccomandazioni utili ad attenuare i potenziali effetti negativi derivanti dalla violazione dei dati personali.

L'obbligo delle suddette comunicazioni è escluso nei casi indicati dall'art. 34:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
c) la comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

La violazione degli obblighi di notificazione di *data breach* è punita dal Regolamento con sanzioni amministrative pecuniarie fino a dieci milioni di Euro o fino al 2 % del fatturato mondiale annuo dell'esercizio precedente se superiore, se riferibili ad una azienda.

Gli articoli 33 e 34 del Regolamento perseguono la finalità di consentire all'autorità di controllo di attivarsi senza ritardo e pertanto valutare e rimediare alla violazione, e si applicano anche alle istituzioni scolastiche.

CONCLUSIONI

L'applicazione del Regolamento e le indicazioni del Garante per la protezione dei dati

L'applicazione del Regolamento comporta un considerevole sforzo di adattamento da parte delle Amministrazioni Pubbliche e pertanto, anche da parte delle istituzioni scolastiche. Il Garante per la Protezione dei dati personali ha realizzato suggerimenti e linee guida in materia di applicazione concreta del Regolamento.

Il Garante suggerisce alle Amministrazioni Pubbliche di attribuire priorità alle seguenti attività:

- La designazione del Responsabile per la protezione dei Dati;
- L'istituzione del Registro delle attività di trattamento e agli adempimenti relativi alla designazione del Responsabile della protezione dei dati;
- L'istituzione del Registro delle attività di trattamento e agli adempimenti relativi alla notifica delle violazioni (*data breach*).

Il Responsabile della protezione dei dati costituisce il fulcro del processo di attuazione del principio di "responsabilizzazione". Il diretto coinvolgimento del RPD in tutte le questioni che riguardano la protezione dei dati personali, sin dalla fase transitoria, è sicuramente garanzia di qualità del risultato del processo di adeguamento in atto. Pertanto sono da tenere in attenta considerazione i requisiti normativi relativamente a:

posizione (riferisce direttamente al vertice), indipendenza (non riceve istruzioni per quanto riguarda l'esecuzione dei compiti) e autonomia (attribuzione di risorse umane e finanziarie adeguate).

Per la scelta del Responsabile della protezione dei dati il Garante suggerisce di verificare le competenze ed esperienze specifiche. Per alcune categorie di trattamenti, sono necessarie qualità professionali adeguate alla complessità del compito da svolgere, nonché la documentazione delle esperienze fatte, la partecipazione a master e corsi di studio/professionali (in particolare se risulta documentato il livello raggiunto).

Per quel che concerne il Registro delle attività di trattamento è di significativa importanza avviare la ricognizione dei trattamenti svolti e delle loro caratteristiche (finalità del trattamento, descrizione delle categorie di dati e interessati, categorie di destinatari cui è prevista la comunicazione, misure di sicurezza, tempi di conservazione, e ogni altra informazione che il titolare ritenga opportuna al fine di documentare le attività di trattamento svolte) funzionale all'istituzione del registro.

La ricognizione è utile a verificare che siano rispettati i principi fondamentali in materia di liceità del trattamento nonché l'opportunità dell'introduzione di misure a protezione dei dati fin dalla progettazione e per impostazione (privacy by design e by default, art. 25), in modo da assicurare, entro il 25 maggio 2018, la piena conformità dei trattamenti in corso (cons. 171)[25]. Infine il Garante invita ad individuare le idonee procedure organizzative per attuare le nuove disposizioni in materia di notificazione delle violazioni dei dati personali. *Dal punto di vista pratico, il Garante sottolinea l'opportunità che i titolari del trattamento verifichino la rispondenza delle informative* utilizzate con i criteri previsti dal Regolamento[26].

25 Garante Privacy: REGOLAMENTO 2016/679/UE: LE PRIORITA' PER LE PA in http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6498465

26 Cfr. Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali in www.garanteprivacy.it.

www.certipass.org

- ENTE EROGATORE DEI PROGRAMMI INTERNAZIONALI DI CERTIFICAZIONE DELLE COMPETENZE DIGITALI EIPASS
- ENTE ISCRITTO AL WORKSHOP ICT SKILLS, ORGANIZZATO DAL CEN (EUROPEAN COMMITTEE FOR STANDARDIZATION)
- ENTE ADERENTE ALLA COALIZIONE PER LE COMPETENZE DIGITALI – AGID
- ENTE ISCRITTO AL PORTALE DEGLI ACQUISTI IN RETE DELLA PUBBLICA AMMINISTRAZIONE, MINISTERO DELL'ECONOMIA E DELLE FINANZE, CONSIP (L. 135 7 AGOSTO 2012) | MEPA
- ENTE PRESENTE SU PIATTAFORMA SOFIA E CARTA DEL DOCENTE

PER INFORMAZIONI SULLE CERTIFICAZIONI INFORMATICHE **VISITA IL SITO**

www.eipass.com