REGOLAMENTO EUROPEO «PRIVACY»
UE 2016/679

Istituzione Scolastica

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

INTRODUZIONE

Il Regolamento UE 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, in materia di protezione dei dati personali (GDPR), che ha acquistato piena efficacia il 25 maggio del 2018, è un'evoluzione e non una rivoluzione, rispetto al Codice della Privacy italiano (D.Lgs. 196/2003)

Il Regolamento reca, comunque, alcune rilevanti innovazioni in tema di trattamento di dati personali, e sarà applicabile in maniera generalizzata e immediata in tutta l'Unione europea, sostituendo la Direttiva 95/46/CE.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

.

Il GDPR, essendo un Regolamento, è direttamente applicabile in tutti gli Stati dell'Unione (self executing), senza bisogno di essere implementato da un'apposita norma nazionale (come è accaduto invece per la direttiva 95/46), e ciò nonostante lascia dei "margini di manovra" ai singoli Stati.

In particolare, il Legislatore nazionale potrà, con riguardo ai trattamenti di dati effettuati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (e dunque per i trattamenti effettuati da soggetti pubblici), mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione del GDPR.

In Italia, con l'art. 13 della cd. "Legge comunitaria" (L. 25 ottobre 2017, n. 1633) si è delegato il Governo a emanare uno o più decreti legislativi per l'adeguamento e l'armonizzazione della normativa nazionale al GDPR. Il 4 settembre 2018 è stato pubblicato il Decreto Legislativo 101/2018 che contiene le disposizioni per l'adeguamento della normativa nazionale al GDPR in materia di protezione dei dati personali

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

.

Oltre alla normativa primaria, dovranno necessariamente essere aggiornati (o sostituiti) i provvedimenti e le Linee guida del Garante Privacy, che rivestono un'importanza fondamentale in questa materia. Quest'operazione di revisione normativa riguarderà, ovviamente, anche i provvedimenti via via emanati (dal legislatore, dal Ministero e dal Garante) nell'ambito dell'attività del MIUR.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

PERCHE' UN NUOVO REGOLAMENTO?

L'esigenza di una nuova disciplina sorge, soprattutto, da due ordini di ragioni:

- La rapidità dell'evoluzione tecnologica e la globalizzazione hanno comportato nuove sfide per la protezione dei dati personali, anche perché la condivisione e la raccolta di dati personali è aumentata in modo esponenziale e la tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività.
- Esigenza di dotarsi di uno strumento che eliminasse la frammentazione e le diversità normative stratificatesi nei singoli Stati membri. La Direttiva 95/46/CE, infatti, era stata recepita (e applicata) in maniera non uniforme, e ciò ha comportato evidenti conseguenze sia in tema di libera circolazione dei dati personali, che di concretezza e omogeneità della tutela in ambito europeo. Si è pertanto optato per l'adozione di un Regolamento, direttamente applicabile in tutti gli Stati membri, "al fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione" (come precisa il decimo Considerando).

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

SINTESI DELLE PRINCIPALI NOVITA'

- La principale novità del Regolamento è certamente costituita dalla centralità del principio di responsabilizzazione (accountability), previsto dall'art. 5. In forza di questo principio, è rimesso al titolare del trattamento il compito di assicurare, ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali. Non vi è più una serie predefinita di adempimenti da rispettare, ma dev'essere ciascun titolare, nell'ambito della propria autonomia e previa accurata valutazione dei rischi, a dover individuare le più idonee (e adeguate) misure organizzative e tecniche, e a doverne dimostrare l'applicazione e l'efficacia.

- Centralità dei profili di sicurezza dei dati. Infatti l'art. 5 del GDPR, che individua i principi generali in tema di trattamento, menziona espressamente l'"integrità e riservatezza" dei dati, stabilendo che il trattamento debba avvenire "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".

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

SINTESI DELLE PRINCIPALI NOVITA'

- Contenuti delle informative: dovranno essere arricchite delle seguenti informazioni :
  - i dati di contatto del Data Protection Officer;
  - la base giuridica del trattamento;
  - l'indicazione se sia previsto il trasferimento di dati in Paesi terzi (vale a dire al di fuori dell'Unione europea), e, in caso affermativo attraverso quali strumenti;
  - il periodo di conservazione dei dati o i criteri stabiliti per determinarne la durata;
  - il diritto di presentare reclamo all'Autorità di controllo;
  - se il trattamento comporti processi decisionali automatizzati e, nel caso, la logica applicata ai processi decisionali e le possibili conseguenze per l'interessato.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

SINTESI DELLE PRINCIPALI NOVITA'

Modifiche in tema di diritti dell'interessato:

- Disciplina dettagliata sul diritto alla cancellazione ("diritto all'oblio")
- "Diritto alla portabilità del dato" (regolato dall'art. 20). In base a tale diritto, l'interessato gode della facoltà di ricevere i dati personali forniti a un titolare, in formato strutturato, di uso comune e leggibile da un dispositivo automatico, e di trasmettere tali dati a un altro titolare, per le ipotesi di trattamenti effettuati con mezzi automatizzati, basati sul consenso o su un contratto. In pratica, il livello di "signoria" sui propri dati personali arriva al punto di poter migrare liberamente da un titolare all'altro. Questo innovativo "diritto alla portabilità" non si applica ai trattamenti di dati necessari per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, e quindi non potrà essere esercitato nei confronti delle pubbliche amministrazioni, quali il MIUR.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

SINTESI DELLE PRINCIPALI NOVITA'

- "privacy by design" e "privacy by default", o, per dirla secondo la versione italiana, "protezione dei dati fin dalla progettazione" e "protezione per impostazione predefinita". Si tratta di due importanti presidi, a tutela del corretto trattamento dei dati personali, che devono iniziare a fare parte del bagaglio di cognizioni di chiunque debba realizzare - e utilizzare - sistemi che trattino dati personali.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

SINTESI DELLE PRINCIPALI NOVITA'

Il Registro dei Trattamenti è una delle principali novità del GDPR. E' importante sottolineare come la predisposizione del medesimo non debba essere considerata alla stregua di un nuovo adempimento burocratico, ma come strumento che consente una gestione più efficace della data protection all'interno dell'organizzazione, oltre a rappresentare un elemento imprescindibile per l'individuazione e la realizzazione di un numero significativo di azioni inserite nell'Action Plan per l'adeguamento al GDPR. Difatti, tale nuovo adempimento consente alle singole organizzazioni di rispondere a una pluralità di finalità, tra cui:

- tenere traccia delle operazioni di trattamento effettuate all'interno della singola organizzazione;
- costituire uno strumento operativo di lavoro mediante il quale censire in maniera ordinata le banche dati e gli altri elementi rilevanti per assicurare un efficace «ciclo di gestione» dei dati personali;
- dimostrare di aver adempiuto alle prescrizioni del regolamento, nell'ottica del principio di "accountability"

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

SINTESI DELLE PRINCIPALI NOVITA'

La valutazione d'impatto sulla protezione dei dati personali:

essa costituisce un processo strutturato di valutazione e gestione del rischio legato ai trattamenti di dati personali, da effettuarsi obbligatoriamente in specifiche situazioni, laddove il trattamento, anche per l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Vi sono delle ipotesi, espressamente individuate dal GDPR, nelle quali la valutazione d'impatto deve essere effettuata: il trattamento su larga scala di categorie particolari di dati o di dati relativi a condanne penali e a reati; la valutazione sistematica e globale di aspetti personali, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici; infine il monitoraggio sistematico di aree pubbliche su vasta scala.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

SINTESI DELLE PRINCIPALI NOVITA'

L'obbligo di notificazione e comunicazione delle violazioni di dati personali (c.d. data breach)

Il GDPR introduce infatti l'obbligo di notificazione al Garante dei data breach, entro settantadue ore dalla scoperta; obbligo a cui si aggiunge anche la comunicazione agli interessati, laddove ci sia un rischio elevato per i diritti e le libertà fondamentali.

Questo impone di dotarsi di sistemi di adeguata segnalazione e reportistica delle intrusioni e delle diffusioni e perdite, anche accidentali, di dati, per essere in grado di adempiere correttamente all'obbligo.

Non si tratta di una novità assoluta per le pubbliche amministrazioni, ma certamente la sua portata è molto estesa rispetto al passato, per cui tutti i dipendenti devono essere a conoscenza dell'obbligo di attivarsi in caso di violazioni di dati personali.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

SINTESI DELLE PRINCIPALI NOVITA'

La Figura del Data Protection Officer (DPO) o RPD (Responsabile Protezione dei dati): si tratta di una figura sostanzialmente nuova, che deve essere nominata obbligatoriamente da enti od organismi pubblici (sia dal titolare che dal responsabile). Per i privati l'obbligo della nomina scatta solo se l'attività principale consiste in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala, oppure se l'attività principale consiste nel trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati.

Il DPO (che può essere sia interno che esterno) è designato in funzione delle qualità professionali, e in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti espressamente individuati dal GDPR. Il DPO deve essere autonomo e non deve subire ingerenze, inoltre, tra i suoi compiti, vi è quello di fornire consulenza e pareri, sorvegliare sul rispetto delle disposizioni del GDPR, cooperare e fungere da punto di contatto con l'Autorità Garante. I dati di contatto del DPO devono essere, infine, pubblicati sul sito, inseriti nell'informativa e comunicati al Garante (anche nel caso di data breach).

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

Obblighi delle scuole

In Relazione alle novità introdotte dal GDPR, le scuole in particolare sono tenute:

- a nominare il DPO: Art. 37 comma 1
- ad elaborare il registro dei trattamenti del titolare e del responsabile del trattamento: sulla base di quanto definito dall'articolo 30
- ad elaborare il DPIA: sulla base di quanto definito dall'articolo 35, 9 e 10 del regolamento Europeo
- Gestione Data Breach

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

I PRINCIPI INTRODOTTI DAL NUOVO REGOLAMENTO EUROPEO SULLA PROTEZIONE DEI DATI

- Principio di liceità del trattamento
- Principio di correttezza
- Principio di trasparenza
- Principio di pertinenza
- Principio di necessità
- Principio di sicurezza
- Principio di responsabilizzazione

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

I PRINCIPI INTRODOTTI DAL NUOVO REGOLAMENTO EUROPEO SULLA PROTEZIONE DEI DATI

Principio di liceità del trattamento (art. 6)

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.

La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

I PRINCIPI INTRODOTTI DAL NUOVO REGOLAMENTO EUROPEO SULLA PROTEZIONE DEI DATI

Principio di correttezza

Accanto al principio di liceità del trattamento, il legislatore comunitario enuncia all'art. 5 par. 1 lett. a) quello della correttezza. Già presente nel D.Lgs. 196/2003, il principio di correttezza è da intendere come buona fede da osservare in tutte le fasi in cui si articola il trattamento dei dati personali

Principio di Trasparenza

Per poter consentire al soggetto interessato di avere il controllo sui dati che lo riguardano (a prescindere e prima ancora della valutazione circa la eventuale illiceità del trattamento) e per rendere effettivo tale controllo è necessario fornirgli tutte le informazioni relative ai dati trattati, alle finalità del trattamento, all'identità e ai dati di contatto del titolare, del responsabile del trattamento e del Responsabile della Protezione dei Dati (DPO o RPD), agli eventuali destinatari dei dati, alla possibilità che i dati vengano trasferiti a un Paese extra UE (cfr. artt. 13 e 14 GDPR). Altrettanto importante (e sempre nell'ottica della trasparenza nel trattamento) è informare l'interessato dei diritti che il GDPR riconosce e garantisce e delle modalità attraverso cui esercitarli.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

I PRINCIPI INTRODOTTI DAL NUOVO REGOLAMENTO EUROPEO SULLA PROTEZIONE DEI DATI

Principio di pertinenza

Il dato è pertinente quando la sua trattazione è assolutamente necessaria per il perseguimento della finalità, ossia quando fra dato e finalità vi è un nesso inscindibile e dunque quando la finalità prefissata non si può raggiungere senza il trattamento di quel determinato dato personale.

Principio di Necessità

Il GDPR ha ribadito nell'art. 5 par. 1 lett. c) che i dati personali sono, non solo adeguati e pertinenti, ma anche "limitati a quanto necessario rispetto alle finalità per le quali sono trattati" sempre nell'ottica di quella minimizzazione dei dati che impone a colui che effettua il trattamento di ridurre al minimo il trattamento stesso ed evitare che si renda possibile identificare l'interessato tutte quelle volte in cui il raggiungimento della finalità perseguita non lo richieda

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

I PRINCIPI INTRODOTTI DAL NUOVO REGOLAMENTO EUROPEO SULLA PROTEZIONE DEI DATI

Principio di Sicurezza

La lettura della lettera f) dell'articolo -5 - secondo cui "i dati personali sono trattati in maniera da garantire un'adeguata sicurezza [...] compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali" - conferma che la sicurezza è principio che permea l'intera attività di trattamento. Un livello di sicurezza che il GDPR definisce "adeguato" al rischio deve essere garantito tanto a livello tecnico-informatico, quanto a livello giuridico e organizzativo ("misure tecniche e organizzative adeguate", art. 32 par.1).

Principio di responsabilizzazione

Il principio di responsabilizzazione è contenuto nell'art. 5, par. 2 del GDPR. Dopo aver indicato tutti i principi che regolano il trattamento dei dati personali, il legislatore europeo afferma che "il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo". Ciò significa che il titolare del trattamento deve rispettare e applicare i principi di cui si è trattato nei precedenti punti e deve essere in grado di dimostrarlo

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

I SOGGETTI PREVISTI DAL GDPR

- L'interessato al trattamento
- Titolare del trattamento (Data controller)
- Responsabile del trattamento (Data processor)
- L'incaricato del trattamento
- Il Responsabile della Protezione dei Dati (RPD O DPO, data protection officer);

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

INTERESSATO AL TRATTAMENTO

L'interessato al trattamento è la persona fisica alla quale si riferiscono (direttamente o indirettamente) i dati personali e al quale il GDPR riconosce una serie di diritti (indicati negli artt. dal 15 al 22) finalizzati a garantire una trasparenza nei rapporti con il titolare e la possibilità di esercitare un controllo effettivo su tutte le informazioni che lo riguardano nonché delle modalità attraverso le quali le stesse sono trattate.

Diritti dell'interessato:

- Diritto all'accesso: L'art. 15 del GDPR riconosce all'interessato il diritto di "ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali".Continua a essere previsto, anche con il GDPR, il diritto dell'interessato a ottenere una copia dei dati oggetto di trattamento
- Diritto all'aggiornamento dei dati: Il diritto all'aggiornamento dei dati, previsto dall'art. 16 del GDPR, consiste nella possibilità, per l'interessato di ottenere che i suoi dati, oggetto di trattamento, siano costantemente aggiornati da parte del titolare.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

INTERESSATO AL TRATTAMENTO

- Diritto alla cancellazione (diritto all'oblio) e le sue condizioni: L'interessato ha (sulla scorta dell'art. 17 del GDPR) il diritto a chiedere la cancellazione dei dati che lo riguardano. All'esercizio di tale diritto consegue l'obbligo in capo al titolare del trattamento di provvedere alla loro cancellazione. Tuttavia tale diritto non ha una portata illimitata, ma è circoscritta al verificarsi di determinate ipotesi. In particolare potrà richiedersi la cancellazione nei casi in cui:
  - I dati non siano più necessari alla finalità per la quale sono stati raccolti o trattati;
  - L'interessato abbia revocato il consenso (nel caso in cui esso sia il solo fondamento di liceità del trattamento);
  - I dati siano stati trattati illecitamente o debbano essere cancellati per adempiere a un obbligo legale cui è soggetto il titolare del trattamento; e infine,
  - I dati siano stati raccolti nell'ambito di servizi offerti dalla società dell'informazione.

Il diritto a ottenere la cancellazione ha, poi, diverse eccezioni, fra le quali rientrano anche l'adempimento a un obbligo legale cui sia soggetto il titolare del trattamento o l'esecuzione di un compito svolto nel pubblico interesse, ovvero per l'esercizio di pubblici poteri

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

INTERESSATO AL TRATTAMENTO

- DIRITTO DI LIMITAZIONE DEL TRATTAMENTO: Con l'art. 18 il GDPR riconosce all'interessato il diritto di ottenere la limitazione del trattamento dei dati che lo riguardano, al verificarsi di determinate condizioni:
  - L'interessato contesta l'esattezza dei dati;
  - Il trattamento dei dati è illecito e l'interessato stesso si oppone alla loro cancellazione;
  - I dati sono necessari all'interessato per esercitare o difendere un diritto in giudizio benché non più necessari al titolare del trattamento in relazione alla finalità perseguita; e infine,
  - L'interessato si è opposto al trattamento in attesa della verifica circa l'eventuale prevalenza dei motivi legittimi del titolare rispetto ai suoi.

Limitare il trattamento dei dati significa, per l'interessato, poter porre un vincolo sugli stessi che rende quei dati indisponibili e non più utilizzabili, da parte del titolare, per un periodo di tempo limitato e suscettibile di revoca (in tale ultimo caso spetterà al titolare dare preventiva informazione all'interessato).

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

INTERESSATO AL TRATTAMENTO

- DIRITTO ALLA PORTABILITÀ DEI DATI: L'art. 20 del GDPR introduce un'assoluta novità: il diritto alla portabilità dei dati. In base a esso l'interessato ha il diritto di ricevere i dati personali che lo riguardano, in un formato strutturato, di uso comune e leggibile da dispositivo automatico e altresì ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti dal primo titolare qualora ricorrano cumulativamente due condizioni: il trattamento si basi sul consenso (anche in relazione alle particolari categorie di dati di cui all'art. 9) o sia necessario per eseguire un contratto e avvenga con mezzi automatizzati.

Questo diritto, come già sottolineato, non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, e non può dunque essere esercitato nei confronti delle pubbliche amministrazioni, quali il MIUR.

- DIRITTO DI OPPOSIZIONE: L'art. 21 del GDPR riconosce all'interessato il diritto di opporsi al trattamento dei propri dati personali in qualsiasi momento e per motivi anche non connessi all'eventuale illegittimità del trattamento. Quando l'interessato esercita tale diritto il titolare deve interrompere il trattamento, a meno che non riesca a dimostrare l'esistenza di motivi legittimi in grado di prevalere sugli interessi e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
-

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

INTERESSATO AL TRATTAMENTO

- IL TRATTAMENTO AUTOMATIZZATO E LA PROFILAZIONE: L'art. 22 del GDPR, rubricato "processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione", sancisce il diritto per l'interessato di non essere sottoposto a una decisione basata unicamente su un trattamento automatizzato, compresa la profilazione, se tale decisione è in grado di incidere sulla sua persona. La norma in esame non vieta l'adozione di processi automatizzati, né della profilazione (intesa come processo in grado di valutare aspetti personali relativi a una persona fisica al fine di prevederne aspetti riguardanti a esempio le preferenze o gli interessi personali, il comportamento, la situazione economica etc...), ma consente all'interessato di sottrarsi a una decisione che sia basata unicamente su tale modalità di trattamento e che si riverberi sulla sua persona o sia in grado di produrre effetti giuridici che lo riguardano. La norma si applica laddove la decisione sia unicamente basata su trattamento automatizzato, e dunque non può estendersi alle ipotesi ove vi sia un intervento umano. In secondo luogo, anche delle decisioni interamente automatizzate sono ammissibili (per quanto riguarda le pubbliche amministrazioni) qualora laddove vi sia una norma che le autorizza, e che individui anche le misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dei soggetti interessati.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

Tabella informative

DESCRIZIONE	CODICE DOCUMENTO	MODALITÀ DI COMUNICAZIONE	NOTE
Informativa per il trattamento dei dati personali Genitori/Alunni	Mod. 01P/P01	Consegna copia cartacea all'atto dell'iscrizione (se effettuata in manuale)(1)	Richiesta firma del Genitore/Tutore/Studente per ricevuta Richiesta firma per consenso a comunicazione/diffusione immagini/video nei casi riportati nel documento
Informativa per il trattamento dei dati personali Dipendenti	Mod. 02P/P01	Consegna copia cartacea all'atto dell'avvio del rapporto di lavoro	Richiesta firma del Dipendente per ricevuta Richiesta firma per consenso a comunicazione/diffusione immagini/video nei casi riportati nel documento
Informativa generale della politica della gestione della Privacy	Mod.03P/P01	Pubblicazione sul sito aziendale	/
Informativa sulla privacy del sito internet	Mod.04P/P01	Pubblicazione sul sito aziendale	/
Informativa video sorveglianza	Mod. 08P/P01	Pubblicazione sul sito aziendale	Se presente
Consenso al trattamento di Immagini e Riprese Filmate	Mod. 01P/P01 Mod. 02P/P01 Consensi specifici nel caso in cui immagini e riprese filmate vengano concesse a parti terze oppure non rientrino nei casi previsti e riportati nei moduli 01P/P01 e 02P/P01(2)	Vedi sopra Vedi sopra Consegna copia cartacea nell'occasione specifica	Vedi sopra Vedi sopra Richiesta firma per avvenuto consenso

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

Tabella informative

Note:

(1) Nel caso l'iscrizione venga effettuata dall'interessato tramite il portale "Iscrizioni on line" fa fede quanto previsto in tale procedura informatica.

(2) Nel caso di "PON", fa fede quanto previsto dalla piattaforma informatica. Nel caso di visite e gite, l'informativa di tipo breve e la relativa richiesta di consenso vanno inserite nel modulo di richiesta di autorizzazione di partecipazione all'evento. In ogni altro caso il Titolare del Trattamento, eventualmente con l'ausilio del RPD, elaborerà specifica informativa con richiesta di consenso.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

TITOLARE DEL TRATTAMENTO (DATA CONTROLLER)

Il titolare è la persona fisica, giuridica, autorità pubblica, servizio o altro organismo che singolarmente o insieme ad altri soggetti governa finalità e mezzi dell'intero trattamento e che disciplina le attività di raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione e, infine, cancellazione o distruzione dei dati personali.

In quanto attore principale nella scena del trattamento dei dati personali è proprio in capo a tale figura che incombono tutta una serie di obblighi e responsabilità finalizzate alla protezione concreta ed efficace dei dati personali.

Il titolare del trattamento non viene designato da nessuno, né la sua qualifica di titolare deve essere formalizzata: la titolarità, in sostanza, discende dal tipo di attività svolte che sono quelle di determinare, singolarmente o insieme ad altri (in caso di contitolarità), le finalità e i mezzi del trattamento dei dati personali (così come previsto dalla definizione di cui all'art. 4 del GDPR).

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

TITOLARE DEL TRATTAMENTO (DATA CONTROLLER)

Nell'ottica del principio di responsabilizzazione (accountability), a esempio, dovrà applicare correttamente le norme in materia di trattamento dei dati personali, oltre a dover individuare le misure adeguate tecniche e organizzative a presidio del corretto trattamento e, profilo non meno rilevante, essere in grado di dimostrare - a posteriori e qualora richiesto dall'Autorità di controllo - il rispetto e la conformità del trattamento dei dati personali di cui abbia la titolarità alla normativa in materia.

In ambito scolastico il Titolare del trattamento è l'Istituto Scolastico che manifesta la sua volontà tramite il suo rappresentante legale che è il Dirigente Scolastico.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

RESPONSABILE DEL TRATTAMENTO (DATA PROCESSOR)

Il responsabile del trattamento dei dati personali (che nella versione inglese del GDPR è chiamato “Data processor” e che non deve essere confuso con la figura del Responsabile della protezione dei dati o Data Protection Officer) è un soggetto che riveste una posizione predominante nell’impianto del GDPR per la sua funzione - sebbene soggetta alle limitazioni impostegli dal titolare mediante le istruzioni specifiche - di protezione dei dati personali.

Il responsabile del trattamento, nella definizione del GDPR, è la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Il responsabile del trattamento deve presentare garanzie sufficienti per mettere in atto le misure tecniche e organizzative adeguate alla protezione del dato personale trattato per conto del titolare, e ciò determina la necessità, per il titolare, che già in fase preliminare si accerti della “affidabilità” del responsabile del trattamento.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

RESPONSABILE DEL TRATTAMENTO (DATA PROCESSOR)

Le istruzioni al responsabile del trattamento sono conferite dal titolare mediante atto contrattuale in cui sono individuati:

- ☐ Gli obblighi per il responsabile del trattamento;
- ☐ La durata del trattamento;
- ☐ La natura e la finalità del trattamento;
- ☐ Il tipo di dati personali e le categorie di interessati;
- ☐ Gli obblighi e i diritti del titolare del trattamento.

Il rapporto tra titolare e responsabile del trattamento non deve, però, indurre a ritenere che il responsabile del trattamento di cui all'art. 28 del GDPR sia una figura omologa a quella conosciuta in Italia nella vigenza del Codice della Privacy. La nuova figura di responsabile del trattamento, infatti, si colloca necessariamente all'esterno dell'ambito organizzativo del titolare e da esso è ben distinto.

Nell'ambito Scolastico, pertanto, si dovrà procedere ad una ricognizione dei soggetti ai quali i titolari conferiscano dei dati personali di cui abbiano la titolarità per l'esecuzione di determinati compiti. Si pensi, ad esempio, alla società esterna alla quale sia affidato il compito di gestire i sistemi informatici e i database dell'Amministrazione.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

L'INCARICATO DEL TRATTAMENTO

Il GDPR non prevede espressamente la figura dell'incaricato del trattamento; tale figura può ritenersi ancora esistente anche nell'ottica del GDPR in quanto l'art. 29 prevede anche che i soggetti che si trovino sotto l'autorità del titolare o del responsabile di trattamento possano trattare i dati personali solo se istruiti in tal senso. Confermato nel D. Lgs 101/2018.

Si tratta di una categoria di soggetti che possono continuare a essere definiti, per semplicità, incaricati (o, meglio, autorizzati) al trattamento dei dati personali da parte del titolare o del responsabile.

Nell'ottica del rispetto del principio di accountability e, soprattutto, della necessità di dimostrare, a posteriori, la conformità al GDPR del trattamento di dati personali effettuato dal titolare o dal responsabile, sarà consigliabile tenere "traccia" sia dell'autorizzazione al trattamento sia delle istruzioni fornite a tali autorizzati. Anche nell'ambito del MIUR tale individuazione dei vari soggetti autorizzati al trattamento dovrà rispettare il principio di accountability e, soprattutto, di minimizzazione dei trattamenti individuando - una volta eseguita la scansione con il registro dei trattamenti - quali soggetti (rientranti nell'organigramma dell'Istituto scolastico) possano essere autorizzati a trattare determinati dati personali al fine di adempiere compiutamente alle mansioni lavorative.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

IL RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD O DPO, DATA PROTECTION OFFICER)

Il Responsabile della protezione dei dati (RPD), o Data Protection Officer (DPO) - disciplinato dagli artt. 37 e ss. - è, come abbiamo visto, una delle più importanti novità introdotte dal GDPR. È una figura obbligatoria per le autorità pubbliche e gli organismi pubblici13, ma più autorità pubbliche possono peraltro designare anche un unico DPO, tenuto conto della struttura organizzativa e della loro dimensione. Si tratta di una scelta che deve essere adeguatamente motivata. Pertanto si potrà, ad esempio, nominare un DPO unico per più titolari (ad esempio istituti scolastici), ma sarà imprescindibile valutare la effettività di tale nomina, sia sulla base delle strutture che delle loro dimensioni, e anche della "facile raggiungibilità" del DPO stesso.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

IL RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD O DPO, DATA PROTECTION OFFICER)

Il DPO potrà essere interno (e dunque un dipendente) o esterno, purché scelto in funzione delle sue qualità professionali, e, in particolare, della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti assegnatigli ai sensi del GPDR. Qualora si scelga di individuare la figura del DPO in una professionalità interna, occorrerà formalizzarla attraverso un apposito atto di designazione, in ordine a cui il Garante ha reso disponibile uno schema-tipo14 per la nomina a “Responsabile per la protezione dei dati”. Laddove invece si opti per un soggetto esterno, la designazione dovrà costituire parte integrante del contratto di servizi, redatto conformemente all’art. 37 del GDPR.

Il Garante ha, anche di recente, precisato che il DPO, al quale non sono richieste specifiche attestazioni formali o l’iscrizione in appositi albi, deve possedere un’approfondita conoscenza della normativa e delle prassi in materia di privacy, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

IL RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD O DPO, DATA PROTECTION OFFICER)

Il DPO è una figura particolare da coinvolgere tempestivamente e adeguatamente in tutte le questioni riguardanti la protezione dei dati personali, e al quale devono essere garantite le risorse necessarie per operare e per mantenere la propria competenza specialistica.

È autonomo nell'esecuzione dei suoi compiti, non può essere rimosso o essere oggetto di provvedimenti discriminatori per la sua attività; riferisce direttamente al vertice gerarchico, e può essere anche direttamente contattato dagli interessati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei diritti. Il DPO è, infine, tenuto al segreto, e può svolgere anche altri compiti e funzioni, purché non in conflitto di interessi

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

IL RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD O DPO, DATA PROTECTION OFFICER)

I compiti del DPO sono indicati analiticamente dall'art. 39 del GDPR, secondo cui questa figura deve:

1. Informare e fornire consulenza al titolare o al responsabile nonché ai dipendenti in merito agli obblighi derivanti dal GDPR e dalle altre disposizioni rilevanti, anche con riguardo alla tenuta del Registro dei trattamenti;
2. Sorvegliare sull'osservanza del GDPR e delle altre disposizioni rilevanti, e delle politiche adottate dal titolare o dal responsabile in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e agli audit;
3. Fornire, se richiesto, un parere in merito alla valutazione d'impatto e sorvegliarne lo svolgimento; Sempre l'art. 39 inserisce alcuni compiti del DPO di natura quasi più pubblicistica che privatistica. Il DPO deve infatti:
4. Cooperare con il Garante;
5. Fungere da punto di contatto per il Garante per questioni connesse al trattamento ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

IL RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD O DPO, DATA PROTECTION OFFICER)

Il DPO deve essere sempre “facilmente raggiungibile” e, soprattutto, deve essere agevolmente contattabile sia dagli interessati che dai dipendenti, oltre che, naturalmente, dall’Autorità Garante.

Per queste ragioni, è previsto che dei dati di contatto (e, in alcuni casi, anche del nominativo) del DPO sia data ampia pubblicità. I dati di contatto del DPO devono infatti essere pubblicati sul sito dell’Ente, comunicati all’Autorità Garante, e riportati nell’informativa.

il nome e i dati di contatto vanno comunicati all’Autorità Garante e all’interessato in caso di data breach, e sempre all’Autorità Garante nelle ipotesi di consultazione preventiva ex art. 36 del GDPR.

Tutti i dipendenti, devono quindi essere a conoscenza dell’esistenza di questa figura e delle sue funzioni.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

Tabella incarichi

FIGURA	CHI	NOMINA	MODELLO	INFORMATIVA
Titolare del trattamento dei dati	Dirigente Scolastico	NO		NO
Interessati	Alunni/Genitori	NO		SI
	Dipendenti	NO		SI
Incaricati	Dirigente Amministrativo	SI	MOD 04-P02	NO
	Personale ATA	SI	MOD 03-P02	NO
	Insegnanti	SI	MOD 03-P02	NO
RPD (Responsabile Protezione dei Dati)	Professionista esterno	SI *	MOD 01-P02 MOD 02-P02	NO
Amministratore di Sistema Servizi IT di segreteria	Personale Interno/Professionista esterno	SI	MOD 08-P02	NO
Amministratore Sito WEB	Personale Interno/Professionista esterno	SI		NO
Incaricato Sito WEB	Personale Interno/Professionista esterno	SI		NO
Amministratore Video-sorveglianza	Personale Interno/Professionista esterno	SI	MOD 06-P02	NO
Incaricato Video sorveglianza	Personale Interno/Professionista esterno	SI	MOD 07-P02	NO
Responsabile esterno del trattamento dei dati	Azienda, Professionista che effettua trattamenti dati per conto dell'istituzione scolastica	SI	MOD 05-P02	NO

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

Tabella incarichi

Note: (*) Prevista anche comunicazione al Garante per la Privacy dei dati identificativi e dei contatti del RPD

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

IL DATO PERSONALE E IL SUO TRATTAMENTO

Nel GDPR è dato personale “qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato)”.

Cosa si intende per “persona identificabile”?

La persona fisica che può essere identificata, direttamente o indirettamente, con riferimento a dati identificativi, quali 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, psichica, economica, culturale o sociale e infine, novità introdotta dal GDPR, anche genetica.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

IL DATO PERSONALE E IL SUO TRATTAMENTO

Categorie di dati personali:

Il Regolamento europeo ha introdotto delle importanti novità per quanto concerne le categorie di dati personali. Abbandonando la tripartizione “dati personali comuni”, “dati sensibili” e “dati giudiziari” (presente nel Codice Privacy)

il GDPR innova rispetto al passato introducendo le definizioni di “dati genetici”, “dati biometrici” e dedicando particolare attenzione al trattamento delle “categorie particolari di dati personali” e a quello dei “dati personali relativi a condanne penali e reati”.

In base al GDPR, infatti, rientrano nelle “categorie particolari di dati personali” oltre ai dati atti a rivelare l’origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l’appartenenza sindacale, i dati relativi alla salute o alla vita sessuale o all’orientamento sessuale della persona (già “dati sensibili” per il Codice Privacy) anche i dati biometrici e quelli genetici. Il generale divieto posto dall’art. 9 del GDPR di trattare tali categorie di dati conosce delle eccezioni espressamente e tassativamente previste dal secondo comma del medesimo articolo, tra le quali, si ricorda quella relativa al trattamento necessario per motivi di interesse pubblico rilevante sulla base del diritto dell’Unione o degli Stati membri (lett. g) e quella relativa al caso in cui l’interessato abbia prestato il proprio consenso esplicito al trattamento di tali dati personali (lett. a).

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

IL DATO PERSONALE E IL SUO TRATTAMENTO

Che cosa si intende per “trattamento”?

Nel GDPR è “qualsiasi operazione o insieme di operazioni, compiute con o senza l’ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l’organizzazione, la strutturazione, la conservazione, l’adattamento o la modifica, l’estrazione, la consultazione, l’uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto”.

Si evince pertanto che la nozione di trattamento è atta a ricomprendere qualsiasi operazione che abbia a oggetto il dato personale, sia essa singola o plurima, effettuata con strumenti informatici o con altri mezzi (ad esempio cartacei).

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

IL DATO PERSONALE E IL SUO TRATTAMENTO

La pseudonimizzazione

"Pseudonimizzazione" è una nuova definizione di nuovo conio.

Il GDPR la definisce come "il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive".

La pseudonimizzazione, pertanto, è un trattamento volto a separare i dati dalla persona alla quale si riferiscono: i dati personali vengono trattati, ma non si è in grado di ricondurli direttamente all'interessato.

Come effettuare la pseudonimizzazione?

Conservando separatamente le informazioni aggiuntive che consentirebbero di ricondurre i dati alla persona alla quale si riferiscono ed effettuando tale conservazione con misure tecniche e organizzative adeguate ad evitare la riattribuzione.

Da precisare che i dati pseudonimizzati sono pur sempre dati personali (a differenza dei dati anonimi), ma non è possibile ricondurli alla persona fisica alla quale gli stessi si riferiscono e, dunque, risalire immediatamente all'identità della stessa (proprio in virtù di quella conservazione separata delle informazioni aggiuntive).

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

L'INFORMATIVA

Il GDPR dedica all'informativa gli articoli 13 e 14, indicando rispettivamente quali informazioni il titolare del trattamento debba fornire qualora i dati siano raccolti presso l'interessato e quali fornire qualora non siano stati ottenuti presso lo stesso.

Per quanto riguarda le Istituzioni scolastiche le informative accanto alle informazioni già presenti (quali i tipi di dati trattati; i riferimenti del titolare e quelli dell'eventuale rappresentante nel territorio italiano; le finalità e modalità del trattamento; le conseguenze all'eventuale rifiuto di fornire i dati personali; i diritti dell'interessato; l'eventuale responsabile del trattamento e gli eventuali destinatari dei dati personali oggetto di trattamento) devono indicarsi:

☐ I dati di contatto del Data Protection Officer;

☐ La base giuridica del trattamento;

☐ L'indicazione se sia previsto il trasferimento di dati in Paesi extra-UE (e nel caso attraverso quali strumenti);

☐ Il periodo di conservazione dei dati (o quantomeno i criteri previsti per stabilire la durata della conservazione);

☐ Il diritto di presentare reclamo all'Autorità di controllo (Garante);

☐ Se il trattamento comporti processi decisionali automatizzati (e nel caso la logica dei processi decisionali e le possibili conseguenze per l'interessato).

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

IL CONSENSO E LE ALTRE BASI GIURIDICHE PER LA LICEITÀ DEL TRATTAMENTO

Il consenso è, anche nel GDPR, una delle condizioni per la liceità del trattamento. (art.6, par.1 lettera a)

Le altri basi giuridiche per assicurare la liceità del trattamento sono:

- 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;
- il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
- il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- 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;
- 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.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

IL CONSENSO E LE ALTRE BASI GIURIDICHE PER LA LICEITÀ DEL TRATTAMENTO

Per quanto concerne la PA (incluso le Istituzioni scolastiche), la base legittimante il trattamento in generale deve essere individuata non nel consenso dell'interessato ma nell'adempimento di un obbligo legale, o nell'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, di cui è investita la P.A., la quale agisce sulla base di leggi o regolamenti.

Ciò si traduce, in pratica, nella non necessità per la PA di acquisire il consenso da parte dell'interessato qualora i dati siano raccolti e trattati per finalità istituzionali.

Ciò comporta che il consenso dell'interessato sarà necessario in particolari casi in cui i dati raccolti verranno utilizzati non per fini strettamente istituzionali .

Il consenso deve essere libero, specifico, informato e inequivocabile e, - in relazione alle particolari categorie di dati di cui all'art. 9 -, anche esplicito. Infine, per quanto concerne il consenso espresso dai minori, il GDPR prescrive all'art. 8 che, qualora lo stesso riguardi i servizi della società dell'informazione (Facebook, Google, Twitter, etc.), lo stesso sia lecito ove il minore abbia compiuto almeno 16 anni.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

REGISTRI DELLE ATTIVITÀ DI TRATTAMENTO

Tra gli obblighi ai quali il titolare del trattamento e il responsabile del trattamento sono soggetti in base al GDPR fondamentale è quello relativo alla tenuta dei registri delle attività di trattamento.

L'art. 30, a essi dedicato, indica analiticamente quali informazioni debbano essere contenute nei registri, tra le quali ricordiamo:

- ☐ Il nome e i dati di contatto del titolare del trattamento (o del responsabile) e quelli del DPO;
- ☐ La finalità del trattamento (non prevista per il responsabile per ovvie ragioni);
- ☐ Una descrizione delle categorie di interessati e dei dati personali trattati;
- ☐ I trasferimenti di dati verso Paesi terzi;
- ☐ I termini ultimi previsti per la cancellazione dei dati (ove possibile); e infine,
- ☐ Una descrizione generale delle misure di sicurezza adottate a tutela dei dati.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

REGISTRI DELLE ATTIVITÀ DI TRATTAMENTO

I registri delle attività di trattamento devono essere tenuti in forma scritta, anche in formato elettronico

Sono esonerati dall'obbligo di tenuta di tali registri le imprese e le associazioni con meno di 250 dipendenti, a meno che il trattamento effettuato possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o riguardi le categorie particolari di dati (i "dati sensibili" del Codice Privacy) o dati relativi a condanne penali o reati.

L'importanza della tenuta dei registri delle attività di trattamento è da inquadrare nell'ottica generale di accountability ed è strettamente connessa alla tutela del dato personale.

Lo strumento è fondamentale infatti per i titolari e i responsabili che vogliano dimostrare la conformità dei trattamenti a quanto previsto dal legislatore comunitario ed è indispensabile nell'attività di cooperazione con l'autorità di controllo.

Da sottolineare che i registri sono un utile strumento per la gestione e il monitoraggio del "ciclo di vita" dei dati personali trattati

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

LA SICUREZZA E IL TRATTAMENTO DEI DATI PERSONALI

DATA PROTECTION “BY DESIGN” E “BY DEFAULT”

I concetti di protezione dei dati “by design” e “by default” (nella versione italiana “protezione dei dati fin dalla progettazione” e “protezione per impostazione predefinita”), contemplati dall’art. 25 del GDPR, sono espressione del principio di minimizzazione del trattamento, ossia di quel principio in base al quale il trattamento deve limitarsi ai soli dati personali necessari al soddisfacimento dello scopo legittimo per cui i dati personali siano, volta per volta, trattati.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

LA SICUREZZA E IL TRATTAMENTO DEI DATI PERSONALI

DATA PROTECTION “BY DESIGN”

il GDPR prevede che l’adeguatezza delle misure (quali ad esempio la pseudonimizzazione) tecniche e organizzative (necessarie ad attuare in modo efficace i principi di protezione dei dati e integrare nel trattamento le necessarie garanzie per soddisfare il rispetto del regolamento oltre che tutelare i diritti degli interessati) debba essere attentamente considerata sia al momento di individuare gli strumenti attraverso i quali i dati saranno trattati, sia all’atto del trattamento stesso.

I parametri che il titolare o il responsabile devono valutare al fine della individuazione delle misure tecniche e organizzative più adeguate al caso di specie sono: stato dell’arte e i costi di attuazione; natura, ambito di applicazione, contesto e finalità del trattamento; nonché i rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

LA SICUREZZA E IL TRATTAMENTO DEI DATI PERSONALI

DATA PROTECTION ““BY DEFAULT”

Consiste nella predisposizione di misure tecniche e organizzative adeguate, in modo da garantire che, per impostazione predefinita, vengano trattati soltanto i dati necessari per ogni specifica finalità del trattamento. L’obbligo si estende alla quantità dei dati personali raccolti, alla portata del trattamento, al periodo di conservazione e all’accessibilità.

In particolare, dette misure devono garantire che, per impostazione predefinita, i dati personali non siano resi accessibili a un numero indefinito di soggetti, senza l’intervento di una persona fisica.

I sistemi quindi devono essere configurati in modo da trattare soltanto i dati strettamente necessari, e in maniera tale da non essere diffusi automaticamente, se non in forza di un intervento umano.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

LA SICUREZZA IL TRATTAMENTO DEI DATI PERSONALI

DATA PROTECTION “BY DESIGN” E “BY DEFAULT”

Anche in questo ambito da sottolineare il rilievo centrale che assume il concetto di accountability (o responsabilizzazione).

Il GDPR, infatti, non descrive analiticamente le misure tecniche e organizzative che titolare e responsabile devono adottare.

Il Titolare ed il Responsabile devono quindi stabilire le misure “adeguate” al trattamento eseguito valutati i rischi che incombono sui dati personali oggetto di trattamento tenendo conto :

- dello stato dell’arte delle misure tecniche e organizzative disponibili;
- dei costi di attuazione delle misure;
- della natura, ambito di applicazione, contesto e finalità del trattamento

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

LA SICUREZZA E IL TRATTAMENTO DEI DATI PERSONALI

DATA PROTECTION “BY DESIGN” E “BY DEFAULT”

Ovviamente, come tutte le norme che hanno l’obiettivo di prevenire un rischio, bisogna essere consapevoli della impossibilità di assicurare una sicurezza assoluta dei dati personali contro la miriade di rischi che sul loro trattamento incombe.

Ciò nonostante, la disciplina è orientata a far sì che ai dati personali, in qualsiasi fase del loro trattamento, siano assicurate le migliori cautele per evitare, attenuare o ridurre il rischio di un trattamento illecito

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

LA SICUREZZA E IL TRATTAMENTO DEI DATI PERSONALI

LA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

Il GDPR individua nel titolare del trattamento il soggetto su cui incombe il compito di individuare le più adeguate misure tecniche e organizzative al fine di garantire il rispetto della disciplina e dei principi in materia di trattamento di dati personali.

Nell'impianto del Regolamento, dunque, la responsabilizzazione del titolare è centrale.

E' quindi compito del Titolare del trattamento dei dati la valutazione d'impatto sulla protezione dei dati e la consultazione preventiva.

La valutazione d'impatto sulla protezione dei dati (DPIA: Data Protection Impact Assessment) è un processo che ha la funzione di descrivere un trattamento di dati personali, valutarne la necessità e la proporzionalità, nonché contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti da esso, valutando detti rischi e determinando le misure per affrontarli.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

LA SICUREZZA E IL TRATTAMENTO DEI DATI PERSONALI

LA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA) "

Il contenuto e la procedura della valutazione sono disciplinate dall'art. 35 del GDPR, e possono essere così sintetizzati:

- ☐ Descrizione del trattamento previsto;
- ☐ Valutazione della necessità e della proporzionalità;
- ☐ Misure previste per dimostrare la conformità;
- ☐ Valutazione dei rischi per i diritti e le libertà;
- ☐ Misure previste per affrontare i rischi;
- ☐ Documentazione;
- ☐ Monitoraggio e riesame.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

DISPOSIZIONI DI SICUREZZA

Art. 32: Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

DISPOSIZIONI DI SICUREZZA

Misure Tecniche :

Nel caso di trattamento con supporto informatico per le misure tecniche si può far riferimento a quanto riportato nella CIRCOLARE 18 aprile 2017, n. 2/2017 della AGENZIA PER L'ITALIA DIGITALE, «Misure Minime di sicurezza ICT per le pubbliche amministrazioni»

AGID individua 3 livelli di applicazioni:

- Minimo
- Standard
- Avanzate

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

DISPOSIZIONI DI SICUREZZA

La Nota «MIUR.AOODGCASIS.REGISTRO UFFICIALE(U).0003015.20-12-2017» specifica che :

«Il livello minimo: è quello al quale ogni Pubblica Amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme. Questo livello può ritenersi sufficiente per gli istituti scolastici»

I livelli minimi individuati:

- Dominio di rete
- Firewall perimetrale con IPS
- Antivirus
- Back-up
- Cifratura

Per dettagli vedi slide allegate

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

DISPOSIZIONI DI SICUREZZA

Misure Organizzative

- Gestione degli incarichi
- Gestione delle Informative
- Gestione Posta elettronica e Internet
- Gestione delle protezioni fisiche
- Gestione degli accessi
- Gestione user id e password

Per la definizione delle misure organizzative si fa riferimento a specifiche procedure.

Come sottolineato dall'art. 42 del GDPR, utile riferimento per la definizione dei contenuti delle misure organizzative possono essere i requisiti previsti dalle normative internazionali per la certificazione dei «Sistema di Gestione per la sicurezza delle informazioni» quali la ISO/IEC 27001, come anche richiamato dall'art. 42 del GDPR

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

DISPOSIZIONI DI SICUREZZA

All'art. 42 viene richiamata la possibilità di dimostrare la propria compliance per quanto attiene la protezione dei dati attraverso la certificazione del proprio sistema di gestione dei dati secondo specifiche norme di riferimento.

Da sottolineare che l'eventuale certificazione non solleva il Titolare dei dati dalle proprie responsabilità

Esempio di norma di riferimento largamente utilizzata è la ISO/IEC 27001 «Requisiti per Sistemi di Gestione per la Sicurezza delle Informazioni»

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

Ulteriori Trattamenti

- Gestione Immagini e Video
  - Sito istituzionale
  - Bacheche, giornalini etc
  - Utilizzo di Social Network
- Video Sorveglianza

Per tali trattamenti vanno definite specifiche misure tecniche ed organizzative.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

NOTIFICA IN CASO DI VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

Definizione del Data Breach (Art. 4 par.12) è la seguente:

"la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".

La disciplina del data breach, pur essendo inquadrabile nell'ambito del risk management, riguarda chiaramente la gestione ex post degli eventi pregiudizievoli.

In altre parole il data breach parte dal presupposto che una violazione si sia già verificata, e si occupa di attivare le contro-misure finalizzate a minimizzarne le conseguenze.

Si deve considerare il fatto in sé, indipendentemente dalla sua imputabilità, o dalle sue cause. È irrilevante, ai fini dell'obbligo di notificazione o comunicazione, che l'evento sia imputabile ad azioni di terzi (ad esempio un criminale informatico che abbia violato i sistemi dell'ente o della società) o sia invece meramente accidentale (si pensi allo smarrimento di un supporto usb, oppure a un evento naturale che comporti la distruzione degli strumenti informatici). È dunque la mera violazione di sicurezza a generare l'applicabilità degli obblighi di cui agli artt. 33 e 34 del GDPR.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

NOTIFICA IN CASO DI VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

L'obbligo di notifica al Garante è previsto in tutte le ipotesi di violazione dei dati personali, salvo qualora sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche. Solo in quest'ultimo caso non occorre procedere alla notifica.

La notifica deve essere effettuata senza ingiustificato ritardo, e comunque entro settantadue ore dal momento in cui si è venuti a conoscenza della violazione.

La notifica stessa, che deve contenere:

- La descrizione della natura della violazione, compresi, ove possibile, le categorie e il numero approssimativo di interessati nonché le categorie e il numero approssimativo di record coinvolti;
- La comunicazione del nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- La descrizione delle probabili conseguenze della violazione;
- La descrizione delle misure adottate (o di cui si propone l'adozione) per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

NOTIFICA IN CASO DI VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

Vi è, infine, un ulteriore onere a carico del titolare, il quale deve documentare qualsiasi violazione di dati personali, ivi comprese le circostanze, le conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione è finalizzata alla verifica della compliance da parte dell'autorità di controllo (e dunque del Garante).

All'obbligo di notifica al Garante l'art. 34 del GDPR aggiunge (e questa è una novità assoluta per le pubbliche amministrazioni) l'obbligo della comunicazione del data breach anche all'interessato solamente nei casi in cui la violazione dei dati personali rappresenti un rischio elevato per i diritti e le libertà delle persone fisiche. La comunicazione è da effettuarsi "senza ingiustificato ritardo", e deve descrivere la natura della violazione con un linguaggio chiaro e preciso.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

SANZIONI

Le sanzioni amministrative possono raggiungere i 10 milioni di euro o, se superiore, il 2% del fatturato mondiale nei casi di, a titolo esemplificativo:

- violazione delle condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione;
- trattamento illecito di dati personali che non richiede l'identificazione dell'interessato;
- mancata o errata notificazione e/o comunicazione di un data breach all'Autorità nazionale competente;
- violazione dell'obbligo di nomina del DPO;
- mancata applicazione di misure di sicurezza.

L'importo delle sanzioni amministrative pecuniarie può salire fino a 20 milioni di euro, o alternativamente, sino al 4% del fatturato mondiale dell'impresa nei casi di, a titolo esemplificativo:

- inosservanza di un ordine, di una limitazione provvisoria o definitiva concernente un trattamento, imposti da un'Autorità nazionale competente;
- trasferimento illecito cross-border di dati personali ad un destinatario in un Paese terzo.

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

Principali novità introdotte dal Decreto Legislativo 101/2018

- Fissata in 14 anni l'età minima in cui un minore può prestare il consenso al trattamento dei propri dati personali in relazione ai servizi delle società di informazione (art. 2- quinquies)
- Individuato nel Garante per la Privacy l'autorità di controllo nazionale (parte 1 Art. 2 bis)
- L'art. 2 –quaterdecies consente al Titolare o al Responsabile del trattamento di prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo l'attribuzione di specifici compiti e funzioni connessi al trattamento dei dati a Persone Fisiche (incaricato) espressamente designate, che operano sotto la loro autorità
- Definito un termine entro cui il procedimento di un reclamo al garante deve essere concluso (9 mesi)
- Definito nel Garante l'organo competente per adottare i provvedimenti correttivi di cui all'art. 58, par. 2 del GDPR nonché di irrogare le sanzioni amministrative

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

Principali novità introdotte dal Decreto Legislativo 101/2018

- Sanzioni Amministrative: in aggiunte alle ipotesi sanzionate dal GDPR, sono state introdotte ulteriori condotte che danno luogo a sanzioni amministrative pecuniarie, ed in particolare:
  - Violazione dell'obbligo di redigere un'informativa con linguaggio semplificato per i minori
  - Mancata adozione delle misure indicate dal Garante per i trattamenti che presentano rischi elevati per l'esecuzione di un compito di interesse pubblico (art. 166)

- Sanzioni Penali: Rivisti gli illeciti penali:
  - Trattamento illecito dei dati (art. 167)
  - Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala (art.167 bis)
  - Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala (art.167 ter)
  - Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante (Art. 168)
  - Inosservanza di provvedimenti del Garante (Art. 170)
  - Violazione delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori (Art. 170)

La Privacy nelle Istituzioni Scolastiche

UE 2016/679

Principali novità introdotte dal Decreto Legislativo 101/2018

Infine si segnala che l'art. 22, comma 3 stabilisce che per i primi 8 mesi dalla data di entrata in vigore del D. Lgs 101/2018, il Garante tiene conto, ai fini dell'applicazione delle sanzioni amministrative, della fase di prima applicazione delle disposizioni sanzionatorie.

Il Decreto Legislativo 101/2018 entrerà in vigore il 19.09.2018