MANUALE PRIVACY SCUOLA

APPROFONDIMENTI IN TEMA DI SICUREZZA E PRIVACY

Informazioni in tema di sicurezza e trattamento dei dati personali nelle attività scolastiche

A cura di Progetto Privacy Srl

Responsabile della Protezione dei Dati di Istituto

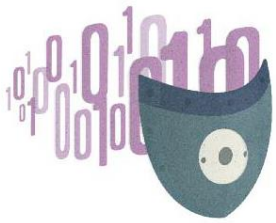
Sommario

PRESENTAZIONE

Il presente opuscolo è un contributo alla formazione del personale scolastico delle istituzioni scolastiche in cui Progetto Privacy Srl ricopre l'incarico di Responsabile della Protezione dei Dati (R.P.D.).

Per domande, dubbi o richieste di chiarimento su quanto esposto potete contattarci all'indirizzo e-mail rpd@progettoprivacy.it.

1 LA PRIVACY NELLA SCUOLA



Anche in ambito scolastico occorre riaffermare quotidianamente quei principi di civiltà, come la riservatezza e la dignità della persona, che devono sempre essere al centro della formazione di ogni cittadino.

Un documento pubblicato sul sito internet di una scuola, che riporta i dati sulla salute di uno studente, non è semplicemente una svista in tema di protezione dati, ma una violazione della normativa e un grave potenziale danno causato allo sviluppo di un giovane.

La trasparenza deve essere applicata con accortezza, nel rispetto delle linee guida del Garante: ad esempio, senza la diffusione di dati non pertinenti, come i contatti personali e altre informazioni private dei docenti, che possono essere utilizzate per furti di identità o stalking.

La normativa che regola la privacy nella scuola fa riferimento al Regolamento (UE) 2016/679 e al Codice della privacy, così come rimodulato dal D.L.gs. 101/2018, e ai provvedimenti del Garante della Privacy.

Il Regolamento (UE) 2016/679[1] del Parlamento europeo e del Consiglio, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (indicato anche con l'acronimo GDPR, o RGPD) entra in vigore il 27 aprile 2016 e diviene pienamente applicabile in tutti gli Stati membri dell'Unione Europea dal 25 maggio 2018. Il GDPR, infatti, non richiede un'apposita norma di recepimento da parte degli Stati membri poiché - contrariamente a quanto accade con le direttive europee - il regolamento è direttamente applicabile (*self-executing*).

Il "vecchio" Codice in materia di protezione dei dati personali o Codice della Privacy - D.Lgs. 196/2003 - è stato recentemente oggetto di un'intensa attività di revisione, con il D.Lgs. 10 agosto 2018 n. 101(entrato in vigore il 19 settembre), al fine di adeguare l'ordinamento interno al GDPR, e per regolamentare gli aspetti per la cui regolamentazione il GDPR rinviava al Legislatore nazionale.

Nel *corpus* normativo del GDPR si possono individuare due principi cardine: quello della c.d. *accountability* (tradotto nella versione italiana del GDPR con il termine di "responsabilizzazione") e quello relativo alla sicurezza dei dati personali (mediante l'adozione di adeguate misure tecniche e organizzative).

Il primo di questi due principi (contenuto nel secondo comma dell'art. 5 del GDPR) prevede che il titolare del trattamento debba assicurare ed essere in grado di dimostrare di aver rispettato i principi applicabili al trattamento dei dati personali. Allo stesso modo, spetterà al titolare del trattamento dei dati personali valutare i rischi incombenti sui trattamenti e individuare le misure tecniche e organizzative adeguate al fine di escludere (o, quantomeno, attenuare) tali rischi.

In secondo luogo, il GDPR, nell'occuparsi del tema della sicurezza del trattamento, prevede che il titolare e il responsabile del trattamento debbano adottare "misure tecniche e organizzative" adeguate. Nel GDPR non è più prevista un'elencazione puntuale delle misure di sicurezza (analogamente a quanto accadeva con le misure minime di sicurezza previste dall'All. B del Codice della Privacy italiano), ma ci si "limita" a offrire solamente un criterio per l'individuazione delle specifiche misure tecniche e organizzative da approntare, volta per volta, al trattamento.

Il GDPR, infatti, prescrive l'adozione di misure di sicurezza (tecniche e organizzative) che siano adeguate a fronteggiare (escludendolo o limitandolo al massimo) il rischio incombente sui dati personali oggetto di ogni singolo trattamento posto in essere. Il GDPR ha l'obiettivo di tutelare i diritti e le libertà delle persone fisiche contro i rischi che possano derivare da un trattamento non corretto dei dati personali.

Pertanto, è necessario mettere in atto, sulla base di quanto previsto dall'art. 25, par. 1 del Regolamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento, misure tecniche e organizzative adeguate volte ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie previste dal Regolamento, nonché a tutelare i diritti degli interessati. Inoltre, si devono porre in essere, sulla base di quanto previsto dall'art. 25, par. 2 del Regolamento, misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento nel rispetto del principio della minimizzazione del dato, assicurando la liceità del trattamento.

Le novità in materia di trattamento dei dati personali, per la Pubblica Amministrazione, sono significative e, di seguito verranno illustrate le altre innovazioni, gli istituti e le misure introdotte dal GDPR sulla protezione dei dati personali, con un'attenzione particolare alle misure di sicurezza e a uno degli obblighi più significativi e innovativi, vale a dire la notifica delle violazioni di dati personali (c.d. "*data breach*").

2 I DATI PERSONALI

I dati personali sono 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, uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2.1 IL TRATTAMENTO DEI DATI NELLE ISTITUZIONI SCOLASTICHE

Le istituzioni scolastiche pubbliche possono trattare solamente i dati personali necessari al perseguimento di specifiche finalità istituzionali oppure quelli espressamente previsti dalla normativa di settore.

Per tali trattamenti, non sono tenute a chiedere il consenso degli studenti. Alcune categorie di dati personali degli studenti e delle famiglie – come quelli sensibili e giudiziari o secondo il GDPR "appartenenti a categorie particolari" – devono essere trattate con estrema cautela, nel rispetto di specifiche norme di legge, verificando prima non solo la pertinenza e completezza dei dati, ma anche la loro indispensabilità rispetto alle "finalità di rilevante interesse pubblico" che si intendono perseguire.

2.2 L'AMBITO DI APPLICAZIONE

Abbiamo già visto che la disciplina si applica ai trattamenti di dati delle persone fisiche, non essendo "dati personali" quelli delle persone giuridiche. Dobbiamo però chiederci se il Regolamento si applichi a tutti i trattamenti di dati personali, o vi siano delle eccezioni.

In primo luogo, la disciplina si applica a tutti i trattamenti automatizzati di dati personali. Non bisogna però fare l'errore di pensare che i trattamenti "tradizionali" o cartacei non siano considerati dal GDPR. L'art. 2, infatti, precisa che il Regolamento si applica anche ai trattamenti non automatizzati di dati personali, purché siano "*contenuti in un archivio o destinati a figurarvi*".

Ne consegue, evidentemente, che tutti i trattamenti di dati personali, anche quelli meramente cartacei sono soggetti (almeno potenzialmente) all'applicazione del Regolamento. Anche nel contesto di un'Amministrazione sempre più digitale, pertanto, non bisogna dimenticare che i documenti cartacei continuino a circolare, e debbano essere trattati in modo corretto. Lo smarrimento o la sottrazione di un fascicolo cartaceo contenente dati personali, rappresenterà (o potrà rappresentare), pertanto, una violazione di dati personali, tanto quanto la sottrazione dei medesimi dati contenuti in un archivio informatico.

Sono invece espressamente esclusi (come peraltro accadeva già in vigenza della Direttiva 95/46) i trattamenti effettuati da una persona fisica per l'esercizio di attività a carattere "esclusivamente personale o domestico".

Quanto previsto dal Regolamento non si applica poi ai trattamenti effettuati per fini di prevenzione, indagine, accertamento o perseguimento di reati o di esecuzione delle sanzioni penali.

2.3 LE CATEGORIE DI DATI PERSONALI E LA TUTELA DIFFERENZIATA

Prima di affrontare le varie tipologie di dati, dobbiamo chiarire che cosa si intenda per "dato personale".

Per il GDPR è dato personale "qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato)"[6]. La persona fisica si considera identificabile quando possa essere individuata, direttamente o indirettamente, con riferimento a dati identificativi, quali 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.

Quando invece non è possibile, neanche indirettamente, risalire a una persona fisica identificata o identificabile, si parla di "dati anonimi", come vedremo tra poco.

Il GDPR distingue nettamente tre categorie di dati personali. Questa distinzione era già presente nella precedente disciplina, ma adesso viene articolata in maniera parzialmente diversa. Si devono pertanto distinguere i dati "comuni", dalle "categorie particolari di dati" e dai dati relativi a condanne penali e reati.

I dati comuni sono individuati in negativo, in quanto sono tutti quei dati personali che non rientrano nelle "categorie particolari", o che non siano dati inerenti a condanne penali e reati.

Le "categorie particolari di dati" (che coincidono - seppur parzialmente - con i "vecchi" dati sensibili) sono rappresentate da: dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici, dati biometrici (intesi a identificare in modo univoco la persona), e dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

L'art. 9 stabilisce un generale divieto di trattamento, temperato da alcune eccezioni, che esamineremo più avanti, quando andremo a occuparci della base legale necessaria per poter trattare i dati. La disciplina è completata, a livello italiano, dagli artt. 2-*sexies* e 2-*septies* del Codice Privacy, che esamineremo più avanti.

I dati giudiziari (art. 10 del GDPR e art. 2-*octies* del Codice Privacy), sebbene non rientrino tra le particolari categorie di dati, meritano particolare attenzione. Concernono i dati relativi alle condanne penali e ai reati o connesse a misure di sicurezza. Anche il loro regime è caratterizzato da importanti restrizioni, previste sia dal GDPR che dalla normativa nazionale, e che esamineremo più avanti.

2.3.1 DATI ANONIMI E PSEUDONIMI

È bene chiarire il concetto di "dati anonimi". Essi infatti non sono dati personali. Se il dato personale è quel dato riconducibile ad una persona fisica identificata o identificabile, il dato anonimo è quello che non consente tale identificazione.

Il dato anonimo nasce originariamente tale, oppure lo diventa in forza di un processo di oscuramento del dato personale "in chiaro". Si tratta, in questo caso, di un dato che era "personale" in origine e che è stato in seguito privato di tutti gli elementi capaci di ricondurlo ad una persona fisica determinata o determinabile.

I dati pseudonimi sono invece quei dati personali che non consentono l'identificazione di una persona fisica determinata senza l'utilizzo di informazioni aggiuntive. Condizione imprescindibile è che tali informazioni aggiuntive siano conservate separatamente e custodite con misure adeguate a evitare che vengano ricondotte a una persona specifica.

Per fare un esempio, si pensi a una banca dati in cui i dati identificativi dei soggetti sono sostituiti da una sigla alfanumerica. Il soggetto che elabora questi dati non sarà in grado di sapere a quali persone essi si riferiscano, in quanto la connessione tra le sigle e le persone è contenuta in altra banca dati, separata e distinta.

Il trattamento di dati pseudonimi è pur sempre un trattamento di dati personali, come è chiarito nel "Considerando" 28. La pseudonimizzazione può ridurre i rischi per gli interessati e aiutare i titolari e i responsabili del trattamento a rispettare i loro obblighi di protezione dati, ma ciò non esime dall'adottare altre misure a protezione.

2.4 LA COMUNICAZIONE E DIFFUSIONE DI DATI PERSONALI

L'art. 2-*ter* disciplina poi (in maniera sostanzialmente analoga al precedente assetto) due modalità particolari di trattamento: la comunicazione[8] di dati personali e la loro diffusione[9].

La comunicazione presuppone una "fuoriuscita" del dato personale dalla sfera di controllo del titolare, in conseguenza della quale il dato stesso viene reso conoscibile (senza necessità che lo stesso venga trasferito) ad altri soggetti determinati (diversi dall'interessato, dai designati, dagli autorizzati o dai responsabili). Si pensi, ad esempio, alla comunicazione di dati tra il MIUR e un altro Ente pubblico, o tra una Scuola e un Ente locale. Si individuano tre ipotesi distinte di comunicazione:

1) La comunicazione tra titolari che trattino i dati nell'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è lecita se **prevista da norma di legge** (o, nei casi previsti dalla legge, di regolamento). Occorre dunque, anche in questo caso, una norma espressa che preveda la comunicazione stessa.

2) Se invece, anche in **assenza di norma**, la comunicazione è comunque necessaria per lo svolgimento di compiti di interesse pubblico e di funzioni istituzionali, occorre attivare una procedura che prevede una sorta di silenzio-assenso: l'attività può essere iniziata se si effettua una comunicazione al Garante, e decorrono quarantacinque giorni, senza che quest'ultimo abbia adottato una diversa determinazione delle misure da adottarsi a garanzia degli interessati.

3) La comunicazione (sempre da parte di un soggetto che tratti i dati nell'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri) a un soggetto che intenda trattare i dati per **finalità diverse** è infine lecita soltanto se prevista da norma di legge o (nei casi previsti dalla legge) di regolamento.

La diffusione di dati presuppone il dare conoscenza dei dati personali a soggetti indeterminati in qualunque forma, anche mediante la loro messa a disposizione o consultazione. Tale diffusione da parte di un soggetto che li tratti nell'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è, invece, lecita (ai sensi dell'art. 2-*ter*, comma 3) soltanto se prevista da norma di legge o - nei casi previsti dalla legge - di regolamento.

Anche in questo caso non vi è alcuna sostanziale novità rispetto al passato: perché vengano diffusi dati personali da parte del MIUR (o delle Scuole), occorre una base normativa specifica. In assenza di una norma *ad hoc*, è vietato diffondere dati personali (o si deve procedere alla loro irreversibile anonimizzazione).

In conclusione, è fondamentale, per ogni trattamento, individuare correttamente quale sia la fonte normativa che consenta al Ministero di trattare, comunicare o diffondere i dati personali: in questa operazione, è di grande aiuto una corretta compilazione del Registro delle attività di trattamento con riguardo alla individuazione della base giuridica di ogni attività di trattamento.

2.5 IL CONSENSO

Il consenso, ex art. 4 par. 1, n. 11 del GDPR, è qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato che esprime il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, al trattamento dei suoi dati. Si presuppone che il soggetto che conferisce il consenso abbia la capacità giuridica per farlo.

Come visto, il consenso è solo una delle basi giuridiche del trattamento. E dunque non è affatto richiesto quando esista un'altra condizione legittimante, quale ad esempio l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, ovvero l'obbligo di legge.

Nell'ambito delle attività delle Istituzioni Scolastiche, pertanto, il consenso, quale base legale, troverà un'applicazione decisamente marginale. L'art. 29 WP (Gruppo dell'articolo 29 per la tutela dei dati - *Article 29 Working Party*), nelle sue linee guida, ritiene che sia improprio ritenere che le Autorità pubbliche nello svolgimento delle proprie finalità istituzionali possano basarsi sul consenso per effettuare il trattamento dei dati personali, poiché quando il titolare del trattamento è un'Autorità pubblica sussiste un evidente squilibrio di potere nella relazione tra il titolare del trattamento e l'interessato. Nella maggior parte dei casi, infatti, l'interessato non dispone di alternative realistiche all'accettazione per poter usufruire di quel determinato servizio pubblico. Pertanto, nell'esercizio delle finalità istituzionali le pubbliche amministrazioni svolgono l'attività di trattamento facendo ricorso ad altre basi legittime per il trattamento. Comunque il consenso non è sempre escluso, ma che possa essere appropriato soltanto in quelle circostanze in cui è pacifico che sia assolutamente libero e laddove l'eventuale diniego non pregiudichi in alcun modo l'erogazione dei servizi. In particolare, si fa l'esempio della richiesta di consenso, da parte di una Scuola, per l'utilizzo delle fotografie degli studenti in una rivista studentesca. Il consenso sarà libero, qualora sia chiaro che agli studenti non vengano negati l'istruzione o altri servizi e che essi possano liberamente rifiutare senza subire pregiudizio.

3 I SOGGETTI DEL TRATTAMENTO

Nel Regolamento europeo alcune figure soggettive fondamentali nell'ambito del trattamento dei dati personali: la comprensione dei diversi ruoli e funzioni (e la ripartizione dei compiti anche all'interno dell'Ente) è imprescindibile al fine di costruire un organigramma coerente e funzionale al rispetto dei principi del Regolamento e dei diritti degli interessati. Più avanti esamineremo, in sintesi, le figure principali.

3.1 IL TITOLARE E IL CONTITOLARE

Il titolare del trattamento (Data Controller) è la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che decide i mezzi e le finalità del trattamento. Il titolare è dunque l'Ente, e pertanto va individuato nel MIUR quale titolare unico mentre, come approfondiremo tra breve, gli Istituti Scolastici sono titolari autonomi.

Le specifiche attività in capo al titolare possono essere espletate dalle varie Direzioni e Uffici del MIUR, nella sua articolazione centrale e periferica che include gli Uffici Scolastici Regionali (art. 8 del D.P.C.M. 11 febbraio 2014, n. 98).

Gli Istituti Scolastici, come abbiamo anticipato, sono invece titolari distinti dal MIUR in quanto dotati di autonomia. Il percorso di conformità al GDPR del Ministero ha portato a concludere che Amministrazione Centrale e Istituti Scolastici hanno distinte competenze per Legge o Regolamento nel determinare finalità e mezzi del trattamento di dati personali (art. 4, n. 7 del Regolamento UE 679/2016).

La titolarità è uno *status* che deriva dal potere decisorio in ordine alle modalità e finalità del trattamento, e non ha bisogno di essere formalizzata in alcun modo.

Ne consegue che ciascun Istituto Scolastico è da intendersi quale titolare dei trattamenti per i quali decide modalità e finalità. Si pensi, ad esempio, ai trattamenti di dati effettuati mediante il registro elettronico, o alle pubblicazioni sul sito della Scuola, o all'eventuale pagina che la Scuola attivasse sui social network (ad esempio Facebook).

Bisogna evitare l'errore di ritenere che il titolare del trattamento sia il legale rappresentante dell'Ente (e dunque, per gli Istituti Scolastici, il Dirigente Scolastico): è l'Ente stesso, nel suo complesso, e non il legale rappresentante, ad essere il titolare. Il Dirigente scolastico si porrà come soggetto che esercita le funzioni di titolare.

Vi possono essere delle ipotesi in cui siano più soggetti a decidere congiuntamente i mezzi e le finalità del trattamento. In questo caso, regolato dall'art. 26 del GDPR, occorre procedere alla formalizzazione di un accordo interno tra i contitolari, che regoli i profili essenziali del trattamento di dati personali. Nell'accordo si può anche (è una facoltà e non un obbligo) individuare il "punto

di contatto", vale a dire il soggetto a cui gli interessati possono fare riferimento per l'esercizio dei loro diritti.

Nell'ambito delle attività del MIUR vi sono vari esempi di contitolarità. Ad esempio, possono individuarsi due ipotesi di contitolarità tra il MIUR e gli Istituti Scolastici, con riguardo alla gestione dei contratti a tempo indeterminato e determinato del personale docente. I mezzi e le finalità di questi trattamenti (funzionali al perfezionamento dell'assunzione del personale docente, con riferimento agli aspetti relativi al trattamento giuridico ed economico, nonché alla verifica del possesso dei requisiti per l'assunzione) non sono infatti decisi esclusivamente dal MIUR o dall'Istituto Scolastico, e pertanto ci si trova in una situazione di contitolarità.

3.2 IL RESPONSABILE DEL TRATTAMENTO

Il responsabile del trattamento (*Data Processor*) è la persona fisica o giuridica che tratta i dati per conto del titolare. Il Responsabile, nell'ambito della sistematica del GDPR, è sempre un soggetto esterno rispetto all'organizzazione del titolare, contrariamente a quanto accadeva nella vigenza dell'art. 29 del Codice Privacy. Il titolare deve scegliere esclusivamente dei responsabili che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, affinché il trattamento soddisfi i requisiti del regolamento e garantisca la tutela dei diritti dell'interessato.

Per fare alcuni esempi, si pensi al fornitore di un servizio di posta elettronica, o al soggetto esterno a cui è affidata l'elaborazione e gestione di una graduatoria, o al fornitore di servizi *cloud* (ad esempio il registro elettronico): tutti questi soggetti, in quanto trattano dati per conto del titolare, sono da individuarsi come "responsabili".

Il rapporto tra titolare e responsabile deve essere regolato, secondo quanto prevede l'art. 28 del GDPR, da un "*contratto o altro atto giuridico*", che sia vincolante, e che individui con precisione l'oggetto del trattamento, la sua durata, la natura, le finalità, il tipo di dati personali, nonché gli obblighi e i diritti del titolare.

Occorre pertanto provvedere a stipulare idonei accordi ovvero, laddove l'attività di trattamento sia acquisita mediante evidenza pubblica, a integrare i bandi e i capitolati per includervi quanto richiesto dall'art. 28 stesso.

3.3 I DESIGNATI E GLI AUTORIZZATI

Nel previgente impianto del Codice Privacy, l'art. 29 individuava i c.d. "responsabili interni".

Ai responsabili (figura facoltativa e rimessa alla discrezionalità del titolare) potevano essere affidati dei compiti, che andavano analiticamente descritti. Normalmente ai responsabili (interni) venivano affidati compiti di supervisione e controllo dei trattamenti di dati personali per le aree di loro competenza, compresa la nomina degli "incaricati". Questi soggetti oggi vengono, per lo più, indicati con il termine "designati".

L'art. 30 regolava invece la figura degli "incaricati", le persone fisiche che procedevano materialmente al trattamento di dati personali, e che dovevano operare sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite. Questi soggetti, invece, sono oggi per lo più indicati con il termine "autorizzati".

Il GDPR, in coerenza con il principio di responsabilizzazione, non individua specifiche disposizioni, lasciando al titolare l'onere di regolamentare, con proprie misure organizzative, l'organigramma relativo al trattamento di dati personali, e limitandosi a prevedere (artt. 29 e 32) che chiunque abbia accesso ai dati personali, sotto l'autorità del titolare o del responsabile, debba essere debitamente istruito.

Il D.Lgs. 101/2018, introducendo nel Codice Privacy l'art. 2-*quaterdecies*, ha provveduto a individuare in maggiore dettaglio le attribuzioni di funzioni e compiti in materia di trattamento di dati personali.

I "soggetti designati", previsti dal primo comma dell'art. 2-*quaterdecies*, sono le persone fisiche a cui il titolare o il responsabile attribuiscono specifici compiti e funzioni connessi al trattamento. Questi compiti e funzioni, nel rispetto del principio di responsabilizzazione, devono essere esplicitamente indicati, delimitando in tal modo l'ambito del trattamento. Questa figura è dunque, come anticipato, simile al "vecchio" responsabile interno. Potranno quindi essere attribuiti al designato, ad esempio, i compiti legati alla conclusione dei contratti con i responsabili esterni, alla supervisione e controllo del rispetto dei principi in materia di trattamento, per le aree o i servizi di competenza, o la nomina degli "autorizzati" al trattamento.

Il secondo comma dell'art. 2-*quaterdecies*, ricollegandosi agli artt. 29 e 32 del GDPR, prevede che il titolare (o il responsabile) debbano individuare le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la loro autorità diretta. Si tratta, appunto dei "soggetti autorizzati", figura che appare accostabile, come già anticipato, alla vecchia definizione di "incaricato al trattamento". Occorre pertanto prevedere che chiunque tratti dati personali sotto l'autorità diretta del titolare riceva specifiche istruzioni, accompagnate da idonea formazione.

Nell'ambito delle organizzazioni complesse, pertanto, occorre individuare i soggetti designati, a cui attribuire specifici compiti e funzioni, e provvedere a fornire idonee e dettagliate istruzioni a tutti coloro che trattano i dati sotto l'autorità del titolare stesso.

Il singolo Istituto Scolastico, quindi, nell'ambito della sua autonomia organizzativa, potrà individuare - ai sensi dell'art. 2-*quaterdecies* del D.Lgs. 196/2003 così come modificato dal D.Lgs. 101/2018 - la soluzione più idonea a gestire, dal punto di vista organizzativo interno, la tutela dei dati personali di cui l'Istituto stesso sia titolare. In questa sua qualità, pertanto, l'Istituto Scolastico, a mezzo del Dirigente Scolastico, adotta gli opportuni provvedimenti relativi all'ambito tecnico e organizzativo. Il Dirigente Scolastico potrà, pertanto, decidere di individuare uno o più designati al trattamento dei dati personali, oltre a dover individuare specificamente i soggetti autorizzati al trattamento dei dati personali di cui l'Istituto Scolastico sia titolare, fornendo a questi ultimi idonee e specifiche istruzioni sul trattamento dei dati personali.

Abbiamo, infatti, già visto che chiunque abbia accesso ai dati personali, sotto l'autorità del titolare o del responsabile, debba essere preliminarmente autorizzato e debitamente istruito. L'autorizzazione e le istruzioni, per ciascun soggetto o tipologia di soggetti (siano essi designati al trattamento o autorizzati al trattamento) sono, in genere, contemplate nello stesso atto.

Per quanto riguarda gli autorizzati, le già menzionate Linee Guida del MIUR di aprile 2019 prevedono che essi siano tenuti a conformare i trattamenti a loro assegnati alla normativa in materia di protezione dei dati personali e alle istruzioni ricevute, e che, in linea generale, siano tenuti a:

☑ Trattare, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento;

☑ Verificare la legittimità e correttezza dei trattamenti, valutando, in particolare, i rischi che gli stessi presentano e la natura dei dati personali da proteggere.

Le istruzioni possono essere diversificate, disciplinando eventuali aspetti di dettaglio in relazione alle specificità dei singoli trattamenti, e devono comunque contenere un espresso richiamo alla policy del Ministero in materia di sicurezza informatica.

3.4 L'INTERESSATO

L'interessato è la persona fisica a cui si riferiscono i dati personali oggetto di trattamento. Si ribadisce che "interessato" possa essere solo e soltanto la persona fisica. Rientreranno pertanto in questa categoria i professionisti o gli imprenditori individuali, ma non le società, le Scuole o le Università, le istituzioni AFAM.

L'interessato può esercitare i diritti previsti dagli articoli da 15 a 22 del GDPR. Tra questi vanno menzionati il diritto di poter accedere ai propri dati, e alle informazioni relative alle modalità di trattamento (compresa l'esistenza di eventuali procedimenti decisionali automatizzati), il diritto di rettifica, il diritto di cancellazione, il diritto di limitazione e quello di opposizione al trattamento. Un discorso più approfondito meritano il diritto alla portabilità e il diritto a non essere sottoposti a un procedimento decisionale automatizzato.

Il titolare deve dare risposta alle richieste al massimo entro un mese, ai sensi dell'art. 12 del GDPR, ma il termine è prorogabile, previo motivato avviso all'interessato, di altri due mesi. Occorre quindi prevedere specifiche procedure (come è usuale fare in tema di accesso documentale e di accesso generalizzato) per regolamentare l'esercizio dei diritti dell'interessato, al fine di essere in grado di rispondere entro il termine previsto. Ma, ancora prima delle procedure, occorre, in applicazione del principio di *privacy by design*, prevedere che i sistemi informativi siano configurati in modo tale da consentire in maniera agevole l'esercizio dei diritti stessi.

3.5 LA FIGURA E I COMPITI DEL DATA PROTECTION OFFICER

Il GDPR, nell'ottica della responsabilizzazione, introduce la figura del Data Protection Officer (DPO) o Responsabile per la Protezione dei Dati (RPD), disciplinata agli art. 37, 38 e 39 del GDPR e dall'art. 2-*sexiesdecies* del novellato D.Lgs. 196/2003.

La nomina è obbligatoria per le pubbliche amministrazioni. Il DPO - che può essere una figura sia interna che esterna (con apposito contratto di servizi) - è designato, secondo quanto prevede l'art. 37, 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 che gli sono assegnati sulla base del GDPR.

Il MIUR ha nominato il proprio Responsabile della Protezione dei Dati con atto di designazione Prot. n. 0000282 - 16/04/2018, precisando che i compiti del Responsabile nominato attengono all'insieme dei trattamenti di dati effettuati dal Ministero dell'Istruzione, dell'Università e della Ricerca. I dati di contatto sono disponibili (oltre che nelle informative) anche nella sezione amministrazione trasparente del sito e alla voce "Privacy" del sito.

I compiti del DPO sono elencati all'art. 39 del GDPR, e, precisamente:

☑ Offrire consulenza a titolare, responsabile e dipendenti;

☑ Fornire il parere (se richiesto) sulla valutazione d'impatto ex art. 35 del GDPR;

☑ Sorvegliare sul rispetto della disciplina sulla protezione dati e sulle politiche del titolare in materia di protezione dei dati personali, compresa la sensibilizzazione e la formazione;

☑ Cooperare con l'Autorità Garante, e fungere da punto di contatto.

Il Responsabile della Protezione dei Dati deve essere tempestivamente coinvolto in tutte le questioni riguardanti il trattamento di dati personali.

Una funzione importante svolta dal DPO è quella legata al contatto con gli interessati, i quali possono interpellarlo per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti.

La figura del DPO è circondata da specifiche cautele: egli infatti non deve svolgere altri compiti e funzioni che ingenerino conflitto d'interessi, è autonomo, non può ricevere direttive o istruzioni, non può essere rimosso per l'adempimento dei propri compiti, e riferisce direttamente al vertice gerarchico.

4 LA SICUREZZA INFORMATICA NEL TRATTAMENTO DEI DATI PERSONALI

4.1 LE MISURE DI PROTEZIONE NEL GDPR

Con il GDPR si abbandona la tradizionale ripartizione tra misure minime e misure idonee per concentrarsi sulle "misure tecniche e organizzative" adeguate al trattamento. Ed è proprio il titolare (o il responsabile del trattamento) a dover comprendere - sulla base di alcuni parametri indicati nell'art. 32 del GDPR - quali siano le misure tecniche e organizzative da adottarsi. Con il principio della accountability (o "responsabilizzazione"), previsto al par. 2 dell'art. 5, infatti, il titolare è (deve essere) oltre che competente a trattare i dati personali "in maniera da garantire un'adeguata sicurezza", anche in grado di comprovarlo.

Le misure indicate spaziano dalla gestione dei dispositivi hardware a quelli software, con particolare attenzione al profilo dell'autorizzazione e autenticazione, anche con riguardo ai dispositivi mobili (laptop, server e workstation). Le misure riguardano inoltre la gestione del capitale umano che passa attraverso un controllo dei privilegi attribuiti a ogni utente in qualità di amministratore (ad esempio registrando ogni accesso effettuato, limitando i privilegi solo a coloro i quali abbiano competenze adeguate, evitando credenziali di autenticazione deboli, etc.).

4.2 IL DATA BREACH

La violazione dei dati personali è definita dall'art. 4 comma 12 del GDPR come "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". Si tratta, per l'appunto, di una violazione di sicurezza.

L'art. 29 WP (Gruppo dell'articolo 29 per la tutela dei dati - Article 29 Working Party), nelle proprie linee guida sulle violazioni di dati personali, distingue tre categorie, basandosi sui principi di sicurezza delle informazioni:

☑ Violazioni della confidenzialità: si verifica ad esempio quando un errore del sistema consente anche a terzi non autorizzati di accedere ai dati personali;

☑ Violazioni dell'integrità: consiste in una accidentale o non autorizzata alterazione dei dati;

☑ Violazione della disponibilità: si riscontra ad esempio quando l'azione di un ransomware (un software malevolo che opera cifrando i dati dei sistemi, per richiedere poi un riscatto) provochi la perdita dell'accesso o la distruzione dei dati personali.

In caso di notizia o sospetto di violazione di dati personali, occorre avvisare immediatamente e senza ritardo il Dirigente scolastico, in modo che possa attivare, in accordo con il DPO, le previste procedure privacy.

4.3 IL MALWARE: RANSOMWARE IN PARTICOLARE

I malware rappresentano uno dei maggiori pericoli per i sistemi informatici attraverso i quali siano trattati dei dati personali. Con il termine malware ci si riferisce a un'ampia categoria di software creati appositamente per danneggiare o alterare i sistemi informatici-bersaglio (spesso si fa impropriamente riferimento ai malware con il termine "virus informatico"). Il malware può colpire differenti tipologie di bersaglio (computer, dispositivi mobili, tablet, etc.) e può avere differenti finalità (danneggiamento, alterazione o introduzione abusiva nei sistemi informatici, estorsione di denaro, etc.).

Rientra nell'ampia categoria dei malware anche la sottocategoria dei ransomware, ossia quei software malevoli che, una volta introdottisi all'interno del sistema operativo-bersaglio e averne alterato in qualche modo il funzionamento o l'accessibilità ai documenti in esso contenuti, richiedono un riscatto in denaro (solitamente in valuta virtuale come, ad esempio, bitcoin) in cambio delle credenziali per ripristinare il corretto funzionamento del dispositivo o l'accessibilità ai file. In genere i ransomware rendono inaccessibili i file mediante l'uso della cifratura.

Prevenire il contagio da ransomware può non essere semplice, soprattutto se il contagio avvenga per il tramite di un dispositivo connesso a una rete locale in cui non tutti gli utenti siano adeguatamente formati sui rischi informatici ai quali sono continuamente esposti.

Sarà necessario dotare i sistemi informatici con i quali siano trattati dati personali di un sistema antivirus da tenere costantemente aggiornato. Potrà inoltre utilizzarsi un approccio di tipo "*endpoint security*" in cui, il sistema integrato di protezione sia in grado di identificare comportamenti anomali all'interno del sistema informatico da proteggere e blocchi quelle

attività causate, magari, da un malware non ancora conosciuto e che, quindi, un semplice antivirus tradizionale non sarebbe in grado di individuare.

4.4 DISPOSITIVI BYOD E SICUREZZA INFORMATICA

BYOD è l'acronimo di "*Bring Your Own Device*", con il quale si fa riferimento a una politica in base alla quale le aziende private o gli enti pubblici consentono ai dipendenti o agli utenti di utilizzare i propri dispositivi personali (computer, tablet, smartphone, etc.) anche in ambito lavorativo accedendo, di conseguenza, a informazioni o dati dell'Ente o dell'azienda. I BYOD se da un lato consentono all'Ente un risparmio di spesa nell'acquisto di dispositivi "aziendali" da fornire ai dipendenti, dall'altro rappresentano una fonte di rischio in considerazione della impossibilità per l'Ente o l'azienda di controllare le vulnerabilità di cui siano affetti o gli eventuali malware di cui siano portatori.

I BYOD, inoltre, sono uno strumento ritenuto utile, per le finalità didattiche, anche dal Piano Nazionale Scuola Digitale (PNSD) nel punto in cui si fa riferimento al "Piano di azione n. 6 - Linee guida per politiche attive di BYOD (Bring Your Own Device)". Si fa riferimento alle linee guida che il MIUR svilupperà in collaborazione con AgID e Garante per la protezione dei dati personali per finalità, ad esempio, di compilazione del registro elettronico o di partecipazione alle attività progettuali tra studenti e docenti. Nell'ambito di queste politiche occorre porre particolare attenzione al profilo della sicurezza informatica posto che i dispositivi personali possono essere veicolo di differenti tipologie di attacchi ai sistemi dell'Amministrazione e degli altri utenti connessi alla rete della medesima.

4.5 IL SOCIAL ENGINEERING

Con il termine "*social engineering*" (o ingegneria sociale) si fa riferimento a una serie di attività (spesso finalizzate a un attacco ai sistemi informatici) che hanno quale obiettivo non tanto il sistema informatico quanto l'utilizzatore del medesimo sistema. L'attaccante che volesse, in ipotesi, attaccare i sistemi informatici di un Istituto Scolastico potrebbe ottenere informazioni utili ad accedere a un sistema informatico pur rispettoso dello stato dell'arte della sicurezza informatica in tema di protezione. Tuttavia, la debolezza, nel sistema, potrebbe risiedere proprio nel dipendente dell'Ente pubblico che possa essere tratto in inganno al fine di consegnare credenziali di accesso o possa essere utilizzato quale veicolo della stessa infezione.

Per questo motivo si ritiene che l'unica difesa contro questo genere di attacco sia una formazione costante dei dipendenti sui profili di sicurezza informatica e sulle tipologie di attacco basate su tecniche di *social engineering*.

4.6 PHISHING

Le email di phishing, oltre a rappresentare un rischio per le risorse economiche dell'Amministrazione o dei singoli dipendenti, potrebbe essere un veicolo di malware con comprensibili contraccolpi sui sistemi informatici-bersaglio.

Per phishing, in genere, si fa riferimento a una tecnica di attacco "a strascico" (ossia un attacco non mirato ma eseguito inviando contemporaneamente a numerosi destinatari la medesima comunicazione) basata su email confezionate in modo da indurre il destinatario a cliccare sugli allegati o a seguire i link eventualmente contenuti.

4.7 RETI WI-FI

Anche le reti Wi-Fi possono essere veicolo di attacco o di infezione dei dispositivi connessi a quella medesima rete. In particolare, esistono delle tecniche di attacco che consistono nel simulare una rete Wi-Fi dell'Ente pubblico in modo da dirottare o captare i contenuti degli ignari "navigatori" che non si accorgono di non essere connessi alla rete "dell'Ente" ma a una rete Wi-Fi creata appositamente con finalità malevole.

4.8 VULNERABILITÀ ED AGGIORNAMENTO DEI SISTEMI

Con riferimento alle misure di sicurezza che ciascun titolare o responsabile del trattamento dovrebbe adottare è essenziale ribadire che il GDPR non ne individua alcuna ma impone a tali soggetti di compiere una valutazione approfondita dei rischi e, conseguentemente, di apprestare le "difese" adeguate che siano necessarie a rendere il rischio accettabile. Per questo motivo non esistono più cataloghi normativi o regolamentari di misure di sicurezza da adottare, posto che ciascun soggetto obbligato dovrà individuare le misure in base a numerosi parametri. Esistono, tuttavia, delle misure che sono ritenute utili a priori. Una di queste è quella che impone un aggiornamento costante del software a disposizione.

È importante comprendere, inoltre, che le politiche di sicurezza su qualsiasi sistema informatico non possono mai ritenersi un "punto d'arrivo" posto che vengono continuamente individuate le vulnerabilità di dispositivi, sistemi operativi o software e che queste possono essere sfruttate dagli attaccanti. Non si potrà mai, pertanto, avere una situazione di "sicurezza assoluta" dal punto di vista informatico ma si dovrà costantemente lavorare per garantire l'aggiornamento dei sistemi e delle misure di protezione (siano essi hardware o software come firewall, sistemi antintrusione, antivirus, etc.). L'aggiornamento dei sistemi operativi è essenziale e deve essere costantemente monitorato.

Occorre, tuttavia, considerare che in un sistema informatico complesso in cui operino differenti tipologie di dispositivi, differenti tipologie di sistemi operativi e software, e in cui si intersechino le attività di tali differenti sistemi è ben possibile - e anzi non è infrequente - che a un aggiornamento di uno di tali sistemi possa conseguire la mancanza di interoperabilità o di funzionamento di altri sistemi collegati. Questo problema è determinato proprio dal fatto che non sempre i sistemi sono interoperabili e compatibili tra di loro e, ad esempio, un software gestionale dell'Amministrazione, una volta aggiornati i sistemi operativi sui quali questo software viene utilizzato, potrebbe smettere di funzionare perché non riconosce l'ambiente in cui si trova a operare.

4.9 I SISTEMI DI BACKUP

Già il "vecchio" Codice della Privacy individuava nelle misure di backup una tecnica necessaria a prevenire le perdite accidentali o connesse ad attacchi mirati ai sistemi informatici e ai dati in essi contenuti. Il backup consiste nella creazione di copie (integrali o incrementali) del contenuto dei dispositivi di memorizzazione al fine di consentire un pressoché immediato ripristino dei dati nel caso di una loro cancellazione accidentale o dovuta a un attacco (ad esempio un attacco a mezzo ransomware). È importante che siano assicurate efficaci politiche di conservazione dei dati e, in particolare, che siano adottati idonei sistemi di backup e di conservazione delle copie di sicurezza.

4.10 LA CIFRATURA

Attraverso le tecniche di cifratura (che si basano su differenti algoritmi) è possibile garantire una inaccessibilità alle informazioni a soggetti non in grado di eseguire l'inverso procedimento di de-cifratura. Esistono vari algoritmi di cifratura che si differenziano tra loro essenzialmente per essere basati su algoritmi a chiave simmetrica o, al contrario, su algoritmi a chiave asimmetrica. Nella prima tipologia il medesimo algoritmo è utilizzato sia per cifrare (o criptare) che per decifrare (o decriptare) i contenuti. Nella seconda tipologia, invece, una chiave (pubblica o privata) è usata per la cifratura e l'altra (privata o pubblica) è usata, per decifrare i contenuti.

Nella seconda tipologia rientrano, ad esempio, i sistemi di cifratura basati sull'uso della firma digitale. Qualora il mittente intenda inviare telematicamente, anche avvalendosi di un sistema "non sicuro" di comunicazione (quale, ad esempio, l'email) un documento in modo da assicurarsi che solo l'effettivo destinatario possa accedere al contenuto potrà utilizzare il software di gestione della firma digitale per cifrare il documento. Tale software chiederà al mittente di ricercare la chiave pubblica della relativa firma digitale del destinatario al fine di criptare il documento. Una volta criptato potrà essere allegato e inviato al destinatario il quale, utilizzando la chiave privata della firma digitale, potrà decriptare il documento cifrato con la relativa chiave pubblica.

Allo stesso modo un soggetto potrebbe voler inserire un documento all'interno di un dispositivo portatile (come, ad esempio, una pennina USB) ed essere sicuro che, dovendosi spostare dal posto A (ad esempio dal luogo di lavoro) al posto B (ad esempio la propria abitazione), qualora dovesse smarrire la pennina USB nessuno possa accedere ai contenuti del documento memorizzato sulla medesima pennina USB. Per far ciò potrà utilizzare la chiave pubblica della propria firma digitale per cifrare il documento mentre si trova nel posto A e, poi, una volta giunto nel posto B, decifrare il documento utilizzando la chiave privata della propria firma digitale.

Si noti che il GDPR fa spesso riferimento alla cifratura come uno dei possibili strumenti per assicurare l'esistenza di garanzie adeguate nella protezione dei dati (ad esempio si veda l'art. 6, par. 4, lett. e, oppure, ancora, l'art. 32, par. 1, o l'art. 34, par. 3, lett. a). Inoltre, il Considerando 83, in modo ancor più esplicito, prevede che "*per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura*".

4.11 LA DISMISSIONE DELL'HARDWARE E LA CANCELLAZIONE DEI DATI

Ulteriore profilo da considerare in caso di dismissione di sistemi di memorizzazione delle informazioni è quello relativo alla cancellazione sicura dei dispositivi. È noto, infatti, che la semplice cancellazione dei file mediante ricorso al "cestino" del sistema operativo non è in grado di eliminare realmente dal supporto di memorizzazione le informazioni in esso contenute. Poiché una dismissione non corretta di sistemi di memorizzazione (quali memorie USB, hard disk delle postazioni lavorative, smartphone, etc.) può integrare un'ipotesi di *data breach*, allora sarà necessario ricorrere, prima della dismissione dell'hardware in questione, a sistemi di cancellazione sicura dei dati (*wiping*).

4.12 LE POLICY SULLA SICUREZZA INFORMATICA

È possibile aumentare il livello di consapevolezza dei rischi, in capo a tutti i dipendenti dell'Ente, attraverso un documento contenente le politiche sulla sicurezza informatica stabilite dall'Ente stesso, previa verifica delle aree, dispositivi e strumenti esposti a rischio informatico. Una volta individuate le aree a rischio - con la collaborazione di personale altamente specializzato nel tema della sicurezza informatica - sarà possibile descrivere, all'interno di tale documento, le misure da adottarsi al fine di prevenire qualsiasi incidente informatico, nonché quelle di contenimento dell'impatto dell'incidente informatico una volta verificatosi.

Le policy sulla sicurezza, che devono essere distribuite e rese note a tutta l'Amministrazione, possono rappresentare, infatti, un'occasione per definire in modo chiaro le istruzioni per i dipendenti che abbiano ricevuto, per l'adempimento della propria prestazione lavorativa, strumenti informatici (quali computer, tablet, smartphone), esposti ai rischi informatici più diffusi.

(Regolamento informatico scolastico, disponibile presso la segreteria, inviato per email e pubblicato in area riservata / registro elettronico).

5 APPROFONDIMENTI OPERATIVI

5.1 IL CRITERIO DI RIDUZIONE DEL RISCHIO

In ogni trattamento occorre cercare di diminuire i rischi per i DIRITTI E LE LIBERTA' DELLE PERSONE FISICHE coinvolte. Ad esempio:

- Non comunicare a terzi, al di fuori dell'ambito lavorativo, o in difformità dalle istruzioni, qualsiasi dato personale;
- Non fornire telefonicamente o a voce informazioni relativi a terzi, senza una specifica autorizzazione del Titolare e, comunque, senza avere la certezza della loro identità;
- Non lasciare a disposizione di estranei documenti o supporti di memorizzazione (cd, dvd, pen drive) che contengono dati personali;

- Non abbandonare la postazione di lavoro senza aver provveduto a custodire in luogo sicuro i documenti e files contenenti dati personali.

5.2 VOTI ED ESAMI

Gli esiti degli scrutini o degli esami di Stato sono pubblici. Le informazioni sul rendimento scolastico sono soggette ad un regime di conoscibilità stabilito dal Ministero dell'Istruzione dell'Università e della Ricerca.

È necessario però che, nel pubblicare i voti degli scrutini e degli esami nei tabelloni, l'istituto scolastico eviti di fornire, anche indirettamente, informazioni sulle condizioni di salute degli studenti, o altri dati personali

5.3 TEMI IN CLASSE

Non lede la privacy l'insegnante che assegna ai propri alunni lo svolgimento di temi in classe riguardanti il loro mondo personale o familiare. Nel momento in cui gli elaborati vengono letti in classe – specialmente se riguardano argomenti delicati - è affidata alla sensibilità di ciascun insegnante la capacità di trovare il giusto equilibrio tra le esigenze didattiche e la tutela dei dati personali. Restano comunque validi gli obblighi di riservatezza già previsti per il corpo docente riguardo al segreto d'ufficio e professionale, nonché quelli relativi alla conservazione dei dati personali eventualmente contenuti nei temi degli alunni.

5.4 CUSTODIA DEI DOCUMENTI CARTACEI

Conservare la documentazione contenente dati personali sempre in armadi chiusi a chiavi con chiavi affidate al soggetto autorizzati.

Non lasciare documenti abbandonati sulle scrivanie dove tutti possano prenderne visione. Non gettare nel cestino dei rifiuti documenti cartacei se non siano stati prima resi illeggibili, anche tramite l'uso di un apparecchio distruggi documenti.

Non lasciare documenti sulla fotocopiatrice, in caso di scansione di documenti accertarsi di rimuoverli dalla cartella scansioni.

5.5 UTILIZZO DEI REGISTRI ELETTRONICI

I registri elettronici, come qualsiasi altro software, sono esposti - soprattutto quando connessi alla rete Internet (o anche in una LAN - *Local Area Network*) - ai medesimi rischi ai quali sono comunemente esposti tutti gli altri sistemi informatici della Scuola. Considerando che esistono, allo stato, diversi tipi di registro elettronico, non si possono offrire risorse tecniche circa la sicurezza di tali strumenti. Le regole basilari della sicurezza informatica, comunque, rappresentano una buona base di partenza per ridurre i rischi legati, appunto, all'utilizzo del registro elettronico.

Qualora, inoltre, la gestione del registro elettronico si basi su un sistema di memorizzazione in cloud, si dovrà valutare attentamente il contenuto dell'accordo tra Istituto Scolastico e fornitore del servizio del registro elettronico, dato che quest'ultimo deve essere individuato quale "responsabile del trattamento" ex art. 28 GDPR, e deve fornire idonee garanzie.

Particolare attenzione occorre porre a due aspetti:

- la riservatezza della password di accesso
- la protezione della postazione informatica (browser)

La password non deve essere troppo semplice, né riconducibile ad elementi identificativi del proprietario (nome, date varie, targhe auto, ecc). Non va annotata su post-it, foglietti volanti, ecc., non va mai comunicata ad altri soggetti quali colleghi, studenti, ecc.

Si ricorda che in caso di utilizzo della credenziale assegnata da parte di altri soggetti (es. studenti), il docente potrà dover rispondere di "abuso in atto d'ufficio".

In caso di smarrimento, occorre rivolgersi all'amministratore del sistema

Per quanto riguarda la protezione della postazione informatica, occorre prestare massima attenzione ad effettuare, al termine della sessione di lavoro, lo scollegamento dal Registro Informatico o laddove presenti da altri sistemi di autenticazione di rete, senza memorizzare alcuna password sul browser utilizzato.

5.6 UTILIZZO DI STRUMENTI DI DIDATTICA DIGITALE (GOOGLE)

Nell'attivazione di questi strumenti occorre sempre considerarne la sicurezza e l'adesione agli standard previsti dalla normativa europea GDPR.

Ad esempio, oltre alle condizioni presenti nel contratto, Google afferma di rispondere ai requisiti del GDPR e di aver predisposto un percorso di conformità, oltre a essere iscritta al programma Data Privacy Framework, accordo bilaterale USA-UE per il trasferimento dei dati personali.

Nella condivisione dei dati personali, occorre tenere presente che non tutti potranno accedere a tutte le informazioni ma vanno eseguite le segregazioni dei dati in base alla classe, gruppi di lavoro ecc. a seconda delle necessità.

L'utilizzo della Didattica Digitale Integrata, dovrà svolgersi secondo quanto stabilito nel Regolamento promosso dall'Istituto.

5.7 WHATSAPP

Qualora non disposto diversamente dal Dirigente Scolastico, va evitato l'uso di whatsapp per finalità istituzionali e scolastiche esistendo già diversi strumenti quali il registro elettronico e altre piattaforme di e-learning e condivisione dei dati già autorizzate dalla scuola.

Le eventuali comunicazioni con WhatsApp sono quindi sotto la responsabilità del docente titolare del numero telefonico che deve evitare di trattare dati personali senza autorizzazioni: deve chiedere l'autorizzazione per creare il gruppo ai singoli genitori, che gestirà come titolare autonomo, non coinvolgendo la responsabilità della Scuola.

Ogni diffusione o comunicazione di dati personali utilizzando whatsapp o messaggistica simile non coinvolge la responsabilità della Scuola e a rispondere a eventuali illeciti sarà chiamato l'intestatario del numero di telefono o dell'account utilizzato.

A questo proposito, si ricorda che qualsiasi utilizzo non autorizzato delle immagini o video potrà generare, nei confronti di chi lo ha effettuato, l'ipotesi di risarcimento in sede civile nonché di eventuali sanzioni penali. La legge, infatti, stabilisce quale regola generale che si possano pubblicare le immagini e i video altrui soltanto qualora chi vi è ritratto abbia precedentemente prestato il proprio consenso alla pubblicazione. Questa regola (Art. 10 cod. civ.; art. 96 L. n. 633/1941) vale per qualunque tipo di diffusione al pubblico, quindi anche per le pubblicazioni online, compresa la condivisione sul proprio profilo di un social network.

Se il numero è intestato alla scuola, va richiesta un'autorizzazione per trattare i numeri di telefono delle famiglie e inviare solo comunicazioni che non trattino dati personali.

5.8 CANALE YOUTUBE E SOCIAL MEDIA (FACEBOOK)

Qualora si intenda utilizzare un canale YouTube o pagine social per fini scolastici è opportuno effettuare la registrazione con un indirizzo e-mail istituzionale e, in caso di foto/video dove sono ripresi gli studenti in modo che siano riconoscibili, accertarsi che siano stati firmati consenso e autorizzazione da parte dei genitori/tutori, qualora non deciso diversamente dal Dirigente Scolastico.

Eliminare la possibilità di postare commenti in quanto la Scuola è responsabile di tutto ciò che viene pubblicato.

I docenti che si occupano di questi media possono ricevere una nomina specifica quali soggetti autorizzati.

Ogni diffusione o comunicazione di dati personali utilizzando account intestati non alla Scuola (privati) non coinvolge la responsabilità della Scuola e a rispondere ad eventuali illeciti sarà chiamato l'intestatario dell'account utilizzato.

A questo proposito, si ricorda che qualsiasi utilizzo non autorizzato delle immagini o video potrà generare, nei confronti di chi lo ha effettuato, l'ipotesi di risarcimento in sede civile nonché di eventuali sanzioni penali. La legge, infatti, stabilisce quale regola generale che si possano pubblicare le immagini e i video altrui soltanto qualora chi vi è ritratto abbia precedentemente prestato il proprio consenso alla pubblicazione. Questa regola (Art. 10 cod. civ.; art. 96 L. n. 633/1941) vale per qualunque tipo di diffusione al pubblico, quindi anche per le pubblicazioni online, compresa la condivisione sul proprio profilo di un social network.

5.9 FOTO E VIDEO

La Scuola è responsabile solo dei trattamenti che effettua lei stessa e di cui ha il controllo e non di foto/video effettuate da genitori o da studenti o da docenti a titolo personale (e non ufficialmente incaricati dalla scuola).

5.9.1 RECITE

Possono i genitori effettuare riprese video o foto?

Non violano la privacy le riprese video e le fotografie raccolte dai genitori durante le recite, le gite e i saggi scolastici. Le immagini, in questi casi, sono raccolte per fini personali e destinate a un ambito familiare o amicale e non alla diffusione.

Va però prestata particolare attenzione alla eventuale pubblicazione delle medesime immagini su Internet, e sui social network in particolare. In caso di comunicazione sistematica o diffusione diventa infatti necessario, di regola, ottenere il consenso informato delle persone presenti nelle fotografie e nei video.

5.9.2 GITE

Come gestire il fatto che il docente effettua le foto e video della gita col proprio smartphone, che poi consegna alla famiglia?

L'utilizzo dello strumento personale del docente deve essere autorizzato dal Dirigente o dal Regolamento d'Istituto. Il materiale deve rimanere nello smartphone del docente solo per il tempo necessario allo scarico su un computer /drive della scuola, indi cancellato. E' possibile anche salvare direttamente le foto sul drive della scuola e quindi condividerle con le famiglie, per un tempo limitato, poi vanno cancellate

5.9.3 DIFFUSIONE ONLINE SU SITO INTERNET E SOCIAL MEDIA

Salvo diversa disposizione del Dirigente Scolastico, nella diffusione di foto e video in cui sono presenti alunni sui canali istituzionali online della scuola occorre considerare i seguenti elementi:

- Si tratta di attività scolastiche inserite nel PTOF
- Nell'informativa alle famiglie si è fatta menzione di questi trattamenti
- Non ci sono primi piani, gli studenti sono ripresi in gruppo
- Il contesto è «positivo»
- Foto e video sono mantenuti online per un tempo predeterminato (fino alla fine del ciclo di studi) poi cancellate
- Salvo diversa disposizione del Dirigente Scolastico, consigliamo di chiedere un consenso al trattamento se gli alunni sono identificabili, oppure si possono «sfuocare» i volti

5.9.4 USI IMPROPRI

- Fare foto o video allo studente per poi inviarle ai genitori onde farli prendere visione dei comportamenti errati del figlio/a;
- Inviare al gruppo whatsapp della classe foto di cartelloni o situazioni in cui compaiono dati personali di tutti gli studenti (classifica buone e cattivi)
- Acquisire e/o utilizzare fotografie degli alunni per identificarli. Le fotografie rimangono memorizzate negli smartphone e tablet personali del docente e in questo modo la scuola non può garantire la sicurezza del trattamento.

5.10 SMARTPHONE E TABLET

L'uso in classe di cellulari e smartphone da parte degli alunni può essere consentito per fini strettamente personali, sempre nel rispetto delle persone. Spetta, comunque, agli istituti scolastici decidere nella loro autonomia come regolamentare o se vietare del tutto l'uso dei cellulari.

Lo studente deve sapere che non si possono diffondere immagini, video o foto sul web se non con il consenso delle persone riprese. È bene ricordare che la diffusione di filmati e foto che ledono la riservatezza e la dignità delle persone può far incorrere lo studente in sanzioni disciplinari e pecuniarie, o perfino in veri e propri reati (Cyberbullismo).

Stesse cautele vanno previste per l'uso dei tablet, se usati a fini di registrazione e non soltanto per fini didattici o per consultare in classe libri elettronici e testi on line.

5.11 REGISTRAZIONE DELLE LEZIONI

È possibile registrare la lezione esclusivamente per scopi personali, ad esempio per motivi di studio individuale. Per ogni altro utilizzo o eventuale diffusione, anche su Internet, è necessario prima informare adeguatamente le persone coinvolte nella registrazione (professori, studenti…) e ottenere il loro esplicito consenso.

Nell'ambito dell'autonomia scolastica, gli istituti possono decidere di regolamentare diversamente o anche di inibire l'utilizzo di apparecchi in grado di registrare. In ogni caso deve essere sempre garantito il diritto degli studenti con diagnosi DSA (disturbi specifici dell'apprendimento) o altre specifiche patologie di utilizzare tutti gli strumenti compensativi (come il registratore) di volta in volta previsti nei piani didattici personalizzati che li riguardano.

5.12 DATI PERSONALI ALUNNI BES/DSA

Le istituzioni scolastiche devono prestare particolare attenzione a non diffondere, anche per mero errore materiale, dati idonei a rivelare lo stato di salute degli studenti, così da non incorrere in sanzioni amministrative o penali.

Non è consentito, ad esempio, pubblicare on line una circolare contenente i nomi degli studenti con diverse abilità. Occorre fare attenzione anche a chi ha accesso ai nominativi degli allievi con disturbi specifici dell'apprendimento (DSA), limitandone la conoscenza ai soli soggetti legittimati previsti dalla normativa, ad esempio i professori che devono predisporre il piano didattico personalizzato.

L'acquisizione delle certificazioni degli alunni deve essere in via ordinaria svolta dalla segreteria e i documenti archiviati presso un armadio chiuso a chiave in segreteria o presidenza.

Durante la consultazione del fascicolo dell'alunno si devono seguire le direttive del Dirigente scolastico che può disporre che non vengano fatte copie dei documenti e che gli stessi non vengano portati all'esterno della segreteria.

L'utilizzo della chiavetta USB per la memorizzazione di Piani Didattici Personalizzati o documenti analoghi, non essendo dotata di autenticazione informatica (se non cifrata), mette ad alto rischio i dati in essa contenuti che possono essere facilmente sottratti o acceduti da parte di soggetti non autorizzati. Se si vogliono usare questi supporti, occorre dotarli di cifratura.

Analogamente, si riscontra a volte che i files contenenti i PEI/PDP o altri dati sulla salute sono "salvati" sul desktop dei pc utilizzati o scaricati nella cartella "Download", al cui interno poi vengono dimenticati per lungo tempo: occorre prestare la massima attenzione a questi aspetti e non lasciare files contenenti dati personali sul desktop o nei download.

5.13 UTILIZZO DI MATERIALE PROTETTO DA COPYRIGHT

Le opere creative altrui possono esser utilizzate senza problemi, anche parzialmente, previa autorizzazione del titolare dei diritti d'autore. L'autorizzazione può anche essere espressa, specialmente in ambienti digitali, attraverso modelli standard di licenza che si ritrovano in siti web o nel documento o cartella elettronica che contiene l'opera e informa riguardo alle attività che, per volontà dell'autore e/o del titolare del relativo diritto, si è liberi di intraprendere, senza correre il rischio di violare alcuna disposizione di legge.

Le istituzioni scolastiche possono quindi utilizzare nei propri elaborati (es, presentazioni o filmati) materiale audiovisivo coperto da copyright e protetto dal diritto d'autore solo dietro autorizzazione del titolare dei diritti. La mancata osservanza di questa regola può portare a richieste di risarcimento relative all'utilizzo non autorizzato dell'opera.

Si consiglia quindi l'utilizzo di immagini e file musicali a libero utilizzo reperibili in rete e non protetti dal diritto d'autore.

6 PAROLE CHIAVE

AUTORIZZAZIONE

Il provvedimento adottato dal Garante con cui il titolare del trattamento in ambito privato (ad esempio la scuola) viene autorizzato a trattare determinati dati "sensibili" o giudiziari, oppure a trasferire dati personali all'estero. In materia di dati sensibili e giudiziari, il Garante ha emanato alcune autorizzazioni generali che consentono a varie categorie di titolari di trattare dati per gli scopi specificati senza dover chiedere singolarmente un'apposita autorizzazione al Garante.

COMUNICAZIONE

Far conoscere dati personali a uno o più soggetti determinati (che non siano l'interessato, il responsabile o l'incaricato), in qualunque forma, anche attraverso la loro messa a disposizione o consultazione.

CONSENSO

La libera manifestazione di volontà dell'interessato con cui questi accetta espressamente un determinato trattamento dei suoi dati personali, del quale è stato preventivamente informato da chi ha un potere decisionale sul trattamento (vedi TITOLARE).
È sufficiente che il consenso sia "documentato" in forma scritta (ossia annotato, trascritto, riportato dal titolare o dal responsabile o da un incaricato del trattamento su un registro o un atto o un verbale), a meno che il trattamento riguardi dati "sensibili"; in questo caso occorre il consenso rilasciato per iscritto dall'interessato (ad esempio con la sua sottoscrizione).

DATO PERSONALE

Qualsiasi informazione che riguardi persone fisiche (come uno studente o un professore) identificate o che possono essere comunque identificate tramite ulteriori dati, quali un numero o un codice identificativo (ad esempio il cosiddetto "codice studente"). Sono, tra gli altri, dati personali: il nome e cognome, l'indirizzo di residenza, il codice fiscale, la fotografia di una persona o la registrazione della sua voce, l'impronta digitale o i dati sanitari.

DATO SENSIBILE (DATO "PARTICOLARE")

Qualunque dato che può rivelare l'origine razziale ed etnica, le convinzioni religiose o di altra natura, le opinioni politiche, l'appartenenza a partiti, sindacati o ad associazioni, lo stato di salute e la vita sessuale.

DIFFUSIONE

L'atto di divulgare dati personali al pubblico o, comunque, a un numero indeterminato di soggetti in qualunque forma (ad esempio pubblicandoli su Internet), anche mediante la loro messa a disposizione o consultazione.

INCARICATO DEL TRATTAMENTO / SOGGETTO AUTORIZZATO

Il dipendente (un professore, un componente della segreteria, etc.) o il collaboratore che per conto del titolare del trattamento dei dati (ad esempio il Ministero dell'Istruzione, dell'Università e della Ricerca) elabora o utilizza materialmente i dati personali sulla base delle istruzioni ricevute dal titolare medesimo (e/o dal responsabile, se designato).

INFORMATIVA

Contiene le informazioni che il titolare del trattamento deve fornire all'interessato per chiarire, in particolare, se quest'ultimo è obbligato o meno a rilasciare i dati, quali sono gli scopi e le modalità del trattamento, l'ambito di circolazione dei dati e in che modo si possono esercitare i diritti riconosciuti dalla legge.

INTERESSATO

La persona cui si riferiscono i dati personali (ad esempio lo studente o il professore).

MISURE DI SICUREZZA

Sono tutti gli accorgimenti tecnici ed organizzativi, i dispositivi elettronici o i programmi informatici utilizzati per garantire: che i dati non vadano distrutti o persi anche in modo accidentale, che solo le persone autorizzate possano accedervi, che non siano effettuati trattamenti contrari alle norme di legge o diversi da quelli per cui i dati sono stati raccolti.

RESPONSABILE DEL TRATTAMENTO

La persona, la società, l'ente, l'associazione o l'organismo cui il titolare può affidare (previa apposita designazione), all'esterno, per la particolare esperienza o capacità, compiti di gestione e controllo del trattamento dei dati.

RECLAMO

Il reclamo al Garante è un atto circostanziato con il quale si rappresenta all'Autorità una violazione della disciplina rilevante in materia di protezione dei dati personali. Al reclamo segue un eventuale procedimento amministrativo all'esito del quale possono essere adottati vari provvedimenti.

RICORSO

Il ricorso va presentato al Garante per far valere i diritti privacy solo quando la risposta del titolare (o del responsabile, se designato) all'istanza con cui si esercita uno o più dei predetti diritti non è pervenuta o viene ritenuta non soddisfacente. In alternativa al ricorso al Garante, l'interessato può rivolgersi all'Autorità giudiziaria ordinaria.

SEGNALAZIONE

Quando non è possibile presentare un reclamo circostanziato (in quanto, ad esempio, non si dispone di tutte le notizie necessarie) si può inviare al Garante una segnalazione, fornendo elementi utili a controllare l'applicazione della disciplina rilevante in materia di protezione dei dati personali.

TITOLARE DEL TRATTAMENTO

La persona fisica, l'impresa, la pubblica amministrazione, l'associazione, etc. cui fa capo effettivamente il trattamento di dati personali e alla quale spetta assumere le decisioni fondamentali sugli scopi e sulle modalità del trattamento medesimo (comprese le misure di sicurezza). In ambito scolastico, il titolare del trattamento in genere è il Ministero dell'Istruzione, dell'Università e della Ricerca, o l'istituto scolastico di riferimento.

TRATTAMENTO

Qualsiasi operazione (raccolta, archiviazione, utilizzo, consultazione, aggiornamento, cancellazione) che può essere effettuata utilizzando i dati personali degli studenti, dei professori o di altre persone.

7 FONTI

Corsi di formazione di Progetto Privacy Srl

Corso ministeriale privacy per incaricati ATA

Vademecum "La scuola a prova di privacy" del Garante protezione dati personali (2023)

Il presente documento costituisce parte integrante della consulenza in materia di dati personali prestata dal Responsabile della protezione dei dati Progetto Privacy Srl alle proprie scuole e non è copiabile né riutilizzabile in altri contesti, salvo autorizzazione dello stesso proprietario.