

VADEMECUM SUL TRATTAMENTO DATI PERSONALI

Le istituzioni scolastiche, durante lo svolgimento dei loro compiti, hanno il dovere di rispettare la privacy e proteggere i dati personali che trattano, anche in considerazione del fatto che tra questi dati vi sono anche quelli di soggetti minorenni.

Il trattamento dei dati da parte delle istituzioni scolastiche è giustificato da motivi di interesse pubblico rilevante.

Per trattamento dei dati personali si intende qualsiasi operazione, effettuata anche con l'ausilio di strumenti informatici, concernente la raccolta, la registrazione, la consultazione, l'elaborazione, l'utilizzo, la diffusione e la cancellazione dei dati.

Il Dlgs 196/2003 detta le regole per il trattamento dei dati personali, effettuato per scopi statistici, scientifici o storici.

L'art. 2 sexies del Codice Privacy (Dlgs. 196/2003) aggiornato precisa che: *“Si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle seguenti materie: istruzione e formazione in ambito scolastico, professionale, superiore o universitario”*.

Dunque, le scuole pubbliche possono trattare soltanto i dati personali necessari al perseguimento delle specifiche finalità istituzionali, che sono comunque finalità di rilevante interesse pubblico.

In particolare, si considerano di rilevante interesse pubblico i dati relativi agli esiti scolastici, intermedi e finali, per finalità legate alla formazione scolastica e universitaria.

Le scuole, quindi, sia pubbliche che private, hanno l'obbligo di comunicare agli interessati (tramite apposita informativa) le caratteristiche e modalità del trattamento dei loro dati, indicando i responsabili del trattamento. Gli interessati sono non solo gli studenti, ma anche le famiglie e gli stessi professori. È, altresì, importante che le scuole verifichino i loro trattamenti, controllando che i dati non siano eccedenti rispetto alle finalità perseguite; non possono essere, pertanto, chiesti dati non rilevanti per la finalità istituzionali.

Quindi, per tali trattamenti non occorre il consenso degli studenti, la base giuridica del trattamento è, infatti, data dall'interesse pubblico.

Occorre, tuttavia, particolare cautela nel trattamento dei dati, trattandosi di dati relativi a soggetti generalmente minorenni.

In alcuni casi si tratta anche di dati a trattamento speciale, cioè relativi alla salute o giudiziari; in questo caso le cautele devono essere massime e soprattutto occorre verificare se il trattamento di quei dati sia davvero necessario per il perseguimento delle finalità scolastiche.

La conoscenza di dati di allievi disabili o con disturbi dell'apprendimento deve essere limitata a soggetti specifici, quali docenti, genitori e operatori sanitari che congiuntamente devono predisporre il piano educativo individualizzato (L. n. 104/92, L. n. 328/2000 e D.Lgs. n. 66/2017).

I SOGGETTI COINVOLTI NEL TRATTAMENTO DEI DATI PERSONALI

Titolare del trattamento

Nella scuola il titolare del trattamento è l'istituzione scolastica stessa, nella figura del Dirigente Scolastico che determina finalità e mezzi del trattamento dei dati personali e funge da garante di sicurezza.

Le funzioni del titolare sono:

- coadiuvare la tenuta del registro delle attività di trattamento;
- coordinare l'attività di aggiornamento delle informative da rendere agli interessati;
- valutare i soggetti inquadrati come responsabili del trattamento;
- assicurare immediato riscontro alle richieste del RPD riconducibili al settore di appartenenza;
- coordinare le attività di valutazione dell'impatto privacy sugli interessati fin dal momento della progettazione dei processi di trattamento e degli applicativi informatici di supporto.

Ai sensi del Dlgs 196/2003, il Dirigente Scolastico, in qualità di titolare del trattamento dei dati personali di studenti e genitori, ha l'obbligo di autorizzare il personale al trattamento dei dati, nell'espletamento degli specifici compiti.

Senza questa autorizzazione, in teoria, non si potrebbero trattare i dati personali degli alunni, il che comporterebbe un blocco dell'attività della scuola.

Per il personale amministrativo, il Dirigente scolastico nomina il DSGA come "responsabile del trattamento", per organizzare le operazioni di trattamento dati nel rispetto del Codice della privacy (Dlgs 196/2003) e del regolamento UE sui dati sensibili e giudiziari.

Nella nomina al DSGA, questi riceve mandato dal Dirigente scolastico di individuare tra il personale amministrativo gli incaricati del trattamento.

Per i docenti, fa una lettera cumulativa in cui li autorizza al trattamento dei dati personali degli alunni. La lettera è allegata a questa comunicazione.

Responsabile del trattamento

È una persona fisica o giuridica, distinta dal titolare, che elabora i dati personali per conto del titolare, sotto il suo controllo.

Ogni soggetto esterno alla scuola, se tratta dati personali afferenti alla scuola, si assume la responsabilità trattamento, dovendo mettere in atto misure tecniche a tutela dei diritti e delle libertà degli interessati.

L'incarico deve essere formalizzato chiarendo obblighi, limiti e istruzioni riguardanti il trattamento, attraverso un contratto che rispetti i requisiti previsti dalla normativa vigente.

Il responsabile del trattamento, in alcuni casi, può essere chiamato a rispondere anche all'autorità di controllo.

Il Responsabile interno del trattamento dei dati personali è il DSGA.

Responsabile della Protezione dei Dati (RPD / DPO)

Ai sensi del Regolamento UE del 2016 (sul trattamento dei dati personali), ogni scuola deve nominare l'RPD, che è una figura consultiva, con specifiche conoscenze giuridiche e informatiche del settore della protezione dei dati, che vigila e dà supporto al DS e al DSGA al fine di garantire che il servizio di trattamento dei dati avvenga nel rispetto del Codice della privacy e del Regolamento UE 2016.

Si tratta di una figura completamente autonoma e indipendente, anche dal titolare, che non deve dare istruzioni.

Il titolare deve solo fornire al RPD le risorse necessarie per il corretto svolgimento delle sue funzioni. L'RPD può essere interno o esterno.

Le scuole possono nominare il RPD singolarmente o in rete.

Qualora sia interno, la scuola deve garantire che le attività richieste dal ruolo di RPD siano compatibili con le mansioni ordinariamente svolte, per non creare un conflitto di interessi.; per tale motivazione è preferibile la nomina esterna del RPD.

Accesso ai dati

Per conoscere le informazioni e i dati conservati dall'istituzione scolastica, ed esercitare, eventualmente, il diritto di rettifica e correzione, è possibile rivolgersi al titolare del trattamento, in genere lo stesso istituto scolastico.

In caso di mancata risposta ci si può rivolgere al Garante oppure alla magistratura.

Per quanto riguarda, invece, i singoli atti amministrativi, è possibile accedere alla documentazione relativa ad alunni e studenti, in base alla legge 241 del 1990 (artt. 22 e ss).

In tal caso, spetta all'istituto valutare se il richiedente ha un interesse diretto, concreto ed attuale ad ottenere l'atto in questione, ai sensi della vigente normativa in materia di accesso agli atti della Pubblica Amministrazione.

Registro dei trattamenti

Le scuole devono tenere il registro dei trattamenti.

Il Miur, con nota n. 877 del 03/08/2018, ha trasmesso alle scuole uno “Schema di Registro delle attività di trattamento” per le istituzioni scolastiche, previsto dal Regolamento europeo sul trattamento dei dati personali, fornendo anche una Guida operativa, che illustra la metodologia da applicare per la compilazione del registro.

Nella guida, sono indicati alcuni trattamenti di base, per la gestione documentale relativa a processi che si svolgono normalmente nelle scuole. Analizziamole nel dettaglio.

Attività di trattamento

Le attività di trattamento, che devono svolgere le scuole, sono 6 e sono dettagliatamente descritte nel file Excel denominato: “Registro dei Trattamenti Esempio compilazione”.

Nella nota metodologica, il Ministero riporta esempi relativi ai seguenti processi:

- Gestione iscrizioni
- Gestione carriera scolastica alunni
- Gestione del personale docente – contrattualizzazione

Gestione Iscrizioni

Le iscrizioni a scuola avvengono, dalla primaria alla secondaria, in modalità telematica, ossia online, tramite il sito del MIM. In riferimento alle iscrizioni, in funzione della categoria di dati trattati (ad es. le categorie particolari di dati personali), delle finalità di trattamento (es. predisposizione delle graduatorie, smistamento e accettazione delle domande di iscrizione o perfezionamento dell'iscrizione), della tipologia, e della modalità di trattamento (es. applicativo SIDI o pacchetto locale), sono state individuate due attività:

1. Acquisizione e gestione domande
2. Acquisizione documentazione aggiuntiva

Tale attività prevede la raccolta delle iscrizioni presentate on line o in modalità cartacea, ove previsto, e la gestione delle stesse al fine di predisporre le graduatorie, accettare o smistare le domande di iscrizione sulla base della disponibilità di posti e dei criteri di precedenza deliberati dal Consiglio di Istituto.

Se la scuola utilizza le funzioni del portale SIDI:

- il Ministero è il Responsabile esterno del trattamento, in quanto autorità pubblica che, attraverso l'applicativo messo a disposizione, tratta dati personali per conto del titolare del trattamento, che è in questo caso, in via esclusiva, l'istituzione scolastica.

Dall'a.s.2023/2024, famiglie, docenti, studenti, personale ata hanno conosciuto ed operato con UNICA e a tal proposito si allega quanto precisato in termini di privacy <https://unica.istruzione.gov.it/it/privacy>

Anche l'INVALSI, annualmente diffonde informativa privacy alle famiglie per le prove Nazionali Invalsi.

Se la scuola utilizza pacchetti locali:

- il responsabile del trattamento è il fornitore informatico scelto dall'istituzione scolastica.

In caso di iscrizioni in modalità cartacea:

- le scuole sono in via esclusiva i titolari del trattamento e non c'è un responsabile esterno del trattamento.

Circa l'acquisizione della documentazione aggiuntiva si evidenzia che tale attività prevede la raccolta della documentazione (obbligatoria o facoltativa) per il perfezionamento dell'iscrizione e per la successiva gestione amministrativa dell'alunno.

Le informazioni raccolte contengono dati comuni e categorie particolari di dati personali (es. lo stato di salute, le convinzioni religiose, filosofiche o di altro genere).

Tali dati sono trattati in modalità cartacea e/o mediante l'utilizzo di pacchetti locali.

In tal caso, il Responsabile esterno del trattamento, ovvero la persona giuridica che tratta dati personali per conto del titolare del trattamento, è il fornitore dei sistemi informativi della scuola.

Gestione carriera scolastica alunni

In riferimento alla carriera scolastica degli alunni, l'attività individuata è una soltanto: Gestione dati alunni

Essa consiste:

- nel trattamento di dati personali relativi al percorso scolastico, formativo e amministrativo dell'alunno per la gestione dello studente, anche in relazione all'erogazione di servizi aggiuntivi
- nell'aggiornamento dell'Anagrafe Nazionale degli Studenti al fine di adempiere agli obblighi previsti dal D.M. 692/2017.

Se la scuola utilizza le funzioni del portale SIDI:

- il Ministero è il Responsabile esterno del trattamento, in quanto autorità pubblica che, attraverso l'applicativo messo a disposizione, tratta dati personali per conto del titolare del trattamento, che è, in via esclusiva, l'istituzione scolastica.

Se la scuola utilizza pacchetti locali:

- il responsabile del trattamento è il fornitore informatico scelto dall'istituzione scolastica.

Gestione del personale docente – _contrattualizzazione

La contrattualizzazione del personale docente riguarda tutte le attività di trattamento di dati che sono effettuate dalla scuola ai fini dell'assunzione del predetto personale.

In riferimento a tale processo, sono state individuate le seguenti attività di trattamento:

1. Gestione contratto a tempo indeterminato
2. Gestione contratto a tempo determinato
3. Gestione contratto per supplenze brevi e saltuarie

Gestione contratto a tempo indeterminato.

Tale attività prevede il trattamento di tutti dati personali funzionali al perfezionamento dell'assunzione del personale docente a tempo indeterminato, con riferimento agli aspetti relativi al trattamento giuridico ed economico ed alla verifica del possesso dei requisiti per l'assunzione.

La suddetta attività comporta, nel trattamento dei dati personali, una contitolarità ex art. 26 del Reg. (UE) 2016/679 del Ministero e della scuola. Considerato che l'attività si svolge tramite funzioni SIDI, il responsabile esterno del trattamento è il fornitore del sistema informativo del Ministero.

Gestione contratto a tempo determinato

Questa attività prevede il trattamento di tutti i dati personali funzionali all'assunzione del personale docente a tempo determinato, con riferimento agli aspetti relativi al trattamento giuridico ed economico ed alla verifica del possesso dei requisiti per l'assunzione.

Come nel caso del personale di ruolo, vi è una contitolarità ex art. 26 del Reg. (UE) 2016/679 del Ministero e dell'istituzione scolastica nel trattamento dei relativi dati personali.

Considerato che l'attività si svolge tramite funzioni SIDI, il responsabile esterno del trattamento è il fornitore del sistema informativo del Ministero.

Gestione contratto per supplenze brevi e saltuarie

Tale attività prevede il trattamento di tutti i dati personali funzionali all'assunzione del personale docente per supplenze brevi e saltuarie, con riferimento agli aspetti relativi al trattamento giuridico ed economico ed alla verifica del possesso dei requisiti per l'assunzione.

L'attività comporta la titolarità esclusiva della scuola nel trattamento dei relativi dati personali, mentre il Ministero si pone come responsabile esterno del trattamento, in quanto autorità pubblica che, attraverso l'applicativo del portale SIDI, tratta dati personali per conto del titolare del trattamento.

Come avviene la gestione della privacy in caso di utilizzo di foto e telecamere?

Foto degli alunni

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 o dei genitori.

In tale ottica la pubblicazione di foto degli alunni sui siti istituzionali o sui social afferenti alla scuola può essere considerata lecita in quanto tra le attività istituzionali rientra anche la realizzazione di eventi quali teatri, festival letterari o scientifici, open day, attività di orientamento, progetti e attività scolastiche.

La riproduzione dei dati deve però rispondere alla sola esigenza di documentazione dell'attività didattica, in ossequio al principio di proporzionalità.

Per cui le riprese degli eventi dovrebbero essere limitate al gruppo nello svolgimento dell'attività, evitando i primi piani.

Gli studenti devono essere sempre ripresi in atteggiamenti positivi o costruttivi, mai negativi.

La diffusione delle immagini (su internet) deve essere, invece, soggetta al consenso dei genitori.

Telecamere a scuola

L'installazione di sistemi di videosorveglianza nelle scuole deve comunque garantire i diritti degli studenti.

È ammissibile nei casi in cui sia indispensabile, al fine di tutelare l'edificio e i beni scolastici da atti vandalici, restringendo le riprese alle sole aree interessate.

Ovviamente la presenza delle telecamere va segnalata con appositi cartelli e, comunque, le telecamere all'interno della scuola vanno attivate solo dopo la chiusura degli orari scolastici e non in coincidenza delle attività scolastiche ed extrascolastiche.

Gestione del Rischio Data breach

MISURE DI ACCOUNTABILITY (RESPONSABILIZZAZIONE) DI TITOLARI E RESPONSABILI

Il Data breach è una violazione dei dati personali, causata, accidentalmente o in modo illecito, dalla distruzione, dalla perdita, dalla modifica, dall'accesso o dalla divulgazione non autorizzata dei dati personali conservati o trattati.

Il Regolamento per la protezione dei dati personali pone con forza l'accento sulla "responsabilizzazione" (accountability) di titolari e responsabili – ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad

assicurare l'applicazione del regolamento (*artt. 23-25, in particolare, e l'intero Capo IV del regolamento*).

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

Il primo fra tali criteri è sintetizzato dall'espressione inglese “data protection by default and by design” (*art. 25*), ossia la necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili per tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio (“sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso”, secondo quanto afferma l'art. 25 del regolamento) e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che devono attivare una serie di misure specifiche e dimostrabili.

La stessa designazione di un “responsabile della protezione dati” (RPD, ovvero DPO se si utilizza l'acronimo inglese: Data Protection Officer) riflette l'approccio responsabilizzante che è proprio del regolamento (*si veda art. 39*), essendo finalizzata a facilitare l'attuazione del regolamento da parte del titolare/del responsabile. Non è un caso, infatti, che fra i compiti del RPD rientrino “la sensibilizzazione e la formazione del personale” e la sorveglianza sullo svolgimento della valutazione di impatto di cui all'art. 35.

Dunque, il titolare del trattamento ha due obblighi: tutela diritti degli interessati e la gestione del rischio di Data breach.

Fondamentale, fra tali attività, è la gestione del rischio inerente al trattamento, da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati; tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (*artt. 35-36*) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi (vedi le linee-guida in materia di valutazione di impatto sulla protezione dei dati adottate dal Gruppo “Articolo 29”, qui disponibili: www.garanteprivacy.it/regolamentoue/DPIA).

All'esito di questa valutazione di impatto il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'autorità non ha il compito di “autorizzare” il trattamento, bensì di indicare le misure

ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

Dunque, l'intervento delle autorità di controllo sarà principalmente "ex post", ossia si collocherà successivamente alle determinazioni assunte autonomamente dal titolare; infatti, a partire dal 25 maggio 2018 alcuni istituti previsti dalla direttiva del 1995 e dal Codice italiano, come la notifica preventiva dei trattamenti all'autorità di controllo e il cosiddetto *prior checking* (o verifica preliminare), sono stati sostituiti dagli obblighi di tenere un registro dei trattamenti da parte del titolare/responsabile e, appunto, di effettuazione di valutazioni di impatto in piena autonomia, con successiva eventuale consultazione dell'Autorità.

Nell'ambito della tutela e della gestione del rischio, si analizzano i principali adempimenti da parte del titolare e del responsabile del trattamento dei dati.

Aggiornamento delle informative privacy a scuola

La prima operazione da eseguire per l'adeguamento al GDPR (n°679/2016, promulgato il 25 maggio 2018) è l'aggiornamento delle informative da comunicare agli interessati.

Si ricorda poi che le informative devono contenere le informazioni relative al periodo di conservazione di dati, la base giuridica, i diritti dell'interessato e i contatti del responsabile della protezione dei dati, così come soddisfare tutti i requisiti previsti dagli artt. 12, 13 e 14 del GDPR.

Lo scopo è quello di informare la persona dell'esistenza del trattamento, nonché di mettere a sua disposizione tutte le informazioni necessarie.

Ogni volta che vengono raccolti dati – ad esempio per l'iscrizione o per un contratto – va perciò consegnata all'interessato un'informativa per la privacy.

Relativamente ai tempi di conservazione delle informazioni, si ricorda che la scuola deve archiviare i dati secondo i tempi definiti dal nuovo "Massimario di conservazione e di scarto per le istituzioni scolastiche".

È sufficiente pubblicare l'informativa sul sito web dell'istituto.

Queste informative devono contenere informazioni relative al periodo di conservazione dei dati, la base giuridica, i diritti dell'interessato e tutti i requisiti previsti dagli artt. 12, 13 e 14 in merito all'obbligo informativo.

Il consenso non è obbligatorio per la fruizione di servizi per prevenzione e consulenza fornita direttamente ai minori, come lo sportello di ascolto e sostegno all'infanzia.

Per trattamenti speciali dei dati, come foto, riprese, audio e video, e relativa diffusione, occorre l'esplicita autorizzazione degli interessati. Nella pubblica amministrazione, i tempi di

conservazione dei dati personali raccolti sono stabiliti dal Ministero dei Beni e delle Attività Culturali.

Registro dei trattamenti

È un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30.

Tra i vari obblighi del titolare vi è anche la tenuta del registro delle attività di trattamento, documento che va aggiornato con regolarità (si consiglia in ogni caso una prima revisione già all'inizio dell'anno scolastico).

Nel registro vengono annotate le informazioni su tutti i trattamenti effettuati dall'istituto.

Questo documento svolge un duplice ruolo: oltre a permettere e agevolare eventuali verifiche da parte del Garante della privacy, risulta estremamente utile anche per chi lo redige, poiché consente di avere una visione d'insieme, sempre aggiornata, dei trattamenti sui dati personali messi in atto sotto la propria responsabilità, dettagliandone ogni caratteristica.

Il registro delle attività di trattamento è anche uno strumento indispensabile per la valutazione e l'analisi del rischio, in quanto consente la ricognizione, la mappatura e la valutazione di conformità di tutte le attività svolte dalla scuola sui dati degli utenti, nonché prova che l'azione del titolare sia pienamente rispondente alle richieste della normativa europea.

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

Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

Ogni anno, come primo step, le scuole devono verificare le nomine effettuate, i responsabili del trattamento designati e i contenuti dell'organigramma privacy.

Si suggerisce altresì di autorizzare e formare al trattamento dei dati il personale neoassunto, e di organizzare un corso di formazione o definire linee guida per tutti i dipendenti (anche per quelli assunti a tempo indeterminato).

Tenere questo registro è obbligatorio per tutte le imprese con almeno 250 dipendenti. Le aziende con meno di 250 dipendenti sono escluse da quest'obbligo se il trattamento dei dati non comporta un rischio per i diritti e le libertà degli interessati.

Le scuole, trattando continuamente dati, soprattutto particolari, hanno l'obbligo di tenere questo registro: un documento scritto in formato elettronico, che deve essere continuamente aggiornato ed esibito durante l'eventuale controllo del Garante.

Esso è utile anche come riepilogo completo dello stato attuale dei trattamenti per chi lo redige. Per ogni attività è opportuno specificare la base giuridica, le operazioni svolte sui dati, le modalità del trattamento, il tipo di informativa e l'eventuale presenza di responsabili esterni. Il registro deve contenere almeno:

- Nome e contatti del titolare, contitolare, rappresentante del trattamento e responsabile della protezione dei dati
- Finalità del trattamento
- Descrizione della categoria di interessati e di dati trattati
- Descrizione della categoria di destinatari dei dati, comprese terze parti
- Eventuali trasferimenti di dati
- Termini di cancellazione dei dati
- Misure di sicurezza (tecniche e organizzative)

Queste sono le informazioni minime da inserire nel registro, ma è consigliabile riportare ogni altra informazione utile a migliorare questa analisi dei trattamenti e dei relativi rischi.

Misure di sicurezza

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

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

Tuttavia, l'Autorità potrà valutare la definizione di linee-guida o buone prassi sulla base dei risultati positivi conseguiti in questi anni; inoltre, per alcune tipologie di trattamenti (quelli di cui all'art. 6, paragrafo 1), lettere d e) del regolamento) potranno restare in vigore (in base all'art. 6, paragrafo 2, del regolamento) le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili: è il caso, in particolare, dei trattamenti di dati sensibili svolti dai soggetti pubblici per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (*ex artt. 20 e 22 Codice*), ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.

Prevenzione e gestione della valutazione d'impatto

Il principio di accountability, che ha aumentato le responsabilità del titolare del trattamento dei dati personali, chiamato ad adottare misure tecniche e organizzative di sicurezza per la protezione di dati personali, basate sui principi del "risk based".

A scuola, i rischi di Data Breach possono essere legati ai seguenti fattori:

- Comportamenti errati (disattenzione, inconsapevolezza, condotte fraudolente, furto, smarrimento) del personale amministrativo scolastico, dei docenti, degli alunni o dei genitori.
- Violazione informatica (virus, malware, sabotaggio, intercettazioni, obsolescenza degrado, malfunzionamento) esterna e/o interna.
- Violazione contestuale (eventi imprevedibili naturali, dolosi, artificiali o accidentali) all'impianto scolastico.

Cosa fare in caso di Data breach a scuola?

Il verificarsi del Data breach fa scattare al titolare tre adempimenti:

- Notifica di violazione al Garante per la protezione dei dati personali
- Eventuale comunicazione della violazione all'interessato
- Aggiornamento del registro delle violazioni con circostanze, conseguenze e provvedimenti adottati per porvi rimedio.

A partire dal 25 maggio 2018, tutti i titolari devono notificare all'autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che tale violazione comporti dei rischi per i diritti e le libertà degli interessati.

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

Se la probabilità di tale rischio è elevata, si dovrà informare della violazione anche gli interessati, sempre "senza ingiustificato ritardo".

Il titolare del trattamento dovrà in ogni caso documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati (*si veda art. 33, paragrafo 5*). Pertanto, il titolare del trattamento deve adottare le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuto a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

Comportamenti da attuare in caso di perdita o hackeraggio di dati sensibili

Nel caso il dipendente verifichi la perdita di dati sensibili, relativi a personale o alunni, tramite smarrimento o furto dei dati installati in una pendrive o hard-disk esterno, lo stesso è tenuto a dare comunicazione scritta al Dirigente indicando le modalità di perdita dei dati e la natura dei dati stessi.

Per dati sensibili si intendono quelli che rilevano l'origine razziale o etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale.

Analoga comunicazione deve essere effettuata nel caso in cui il dipendente si accorga che dal device in uso siano stati hackerati i dati sensibili posseduti.

Di conseguenza sarà compito del dipendente produrre copia della denuncia di smarrimento/furto inoltrata alla locale Tenenza dei Carabinieri.

Che cosa va pubblicato sul sito web della scuola

La scuola deve ricordarsi di aggiornare la pagina sul sito internet con la documentazione allegata, se la stessa viene modificata.

Sul portale istituzionale vanno anche pubblicati i dati di contatto del responsabile della protezione dei dati (RPD).

Il Garante della privacy, con provvedimento n. 174 del 12 maggio 2022, ha sanzionato per la prima volta un comune per la mancanza di una valida e corretta designazione di un responsabile della protezione dei dati (RPD).

L'Autorità, tra i vari aspetti, ha evidenziato che: “il mancato aggiornamento dei dati di contatto del RPD, tanto sul sito web dell'ente quanto nella relativa comunicazione all'Autorità, costituisce una condotta sanzionabile al pari della mancata pubblicazione/comunicazione”.

Detto questo, occorre ricordare che è fondamentale che tutte le pubbliche amministrazioni, tra cui le scuole, pubblicino sul sito i dati di contatto del proprio RPD, e che tale obbligo deriva dall'art. 37, par. 7, del Regolamento Europeo 2016/679 (GDPR).

In relazione alle modalità di pubblicazione dei dati di contatto del RPD, il Garante evidenzia che tale obbligo “mira a garantire che [...] gli interessati (all'interno o all'esterno dell'ente/organismo titolare o responsabile del trattamento) [...] possano contattare il RPD in modo facile e diretto” (“Linee guida sui responsabili della protezione dei dati”).

Inoltre l'Autorità ribadisce che la “mera pubblicazione dell'atto di designazione del RPD, specialmente se effettuata indistintamente assieme a tutti gli altri atti e provvedimenti amministrativi adottati dal comune e pubblicati per finalità di trasparenza dell'azione amministrativa o di pubblicità integrativa dell'efficacia, non può, infatti, ritenersi idonea a soddisfare l'obbligo di pubblicità previsto dal Regolamento, poiché gli interessati non sono messi in condizione di reperire facilmente e direttamente i dati di contatto del RPD”.

Le scuole devono perciò pubblicare sul sito web istituzionale i dati di contatto del RPD all'interno di una sezione facilmente riconoscibile dall'utente e accessibile già dalla homepage.

Il Garante, nelle “Faq sul responsabile della protezione dei dati (RPD) in ambito pubblico”, afferma che “per quanto attiene al sito web, può risultare opportuno inserire i riferimenti del RPD nella sezione “amministrazione trasparente”, oltre che nella sezione “privacy” eventualmente già presente”.

Relativamente al sito web, si ricorda altresì che la scuola deve pubblicare online solo dati la cui diffusione risulti realmente necessaria, proporzionata alla finalità di trasparenza perseguita e prevista dalle norme.

La pubblicazione sul sito degli elenchi degli alunni suddivisi per classi

Pubblicare sul sito della scuola gli elenchi degli alunni suddivisi per classi è prassi sbagliata. Ebbene, questa è una prassi sbagliata. Già dieci anni fa, infatti, con provvedimento n. 383 del 6 dicembre 2012, il Garante per la privacy aveva sanzionato una scuola per aver diffuso sul proprio sito internet i nominativi e gli elenchi degli alunni iscritti alle classi prime.

Questo nonostante l'appello del dirigente, che si era giustificato sostenendo che la pubblicazione degli elenchi rientrasse nelle finalità di trasparenza amministrativa della scuola, in quanto pubblica amministrazione.

L'Autorità in questo caso ha affermato che non è accettabile diffondere i nominativi dei propri studenti distinti per sezioni sul sito web in assenza di una norma di legge o di un regolamento che ammetta tale operazione di trattamento dei dati personali.

La pubblicazione online dei nomi sul portale istituzionale determina infatti una diffusione illecita di informazioni da parte di soggetti pubblici.

Sul tema è intervenuto qualche anno fa anche il Ministero dell'Istruzione, il quale ha specificato che: “la diffusione dei dati relativi alla composizione delle classi sul sito web istituzionale non è consentita in quanto, secondo l'art.2-ter del Codice in materia di protezione dei dati personali, la diffusione dei dati personali è lecita solo se disposta espressamente dalla norma di legge o, nei casi previsti dalla legge, di regolamento” (oggi anche da atti amministrativi generali).

Pertanto, il Ministero suggerisce di rendere noti i nominativi degli studenti distinti per classe tramite apposita comunicazione all'indirizzo email fornito dalla famiglia in fase di iscrizione, o – se possibile – tramite l'area documentale riservata del registro elettronico, a cui accedono tutti gli studenti della classe di riferimento.

In caso di comunicazione tramite email, per evitare violazioni privacy la stessa dovrà essere inoltrata a ciascun destinatario con un messaggio personalizzato, oppure inviata utilizzando il campo denominato “copia conoscenza nascosta” (CCN) al fine di non divulgare gli indirizzi email forniti dalle famiglie.

Inoltre, si raccomanda di predisporre uno specifico “disclaimer” con cui si evidenzia che i dati personali non possono essere oggetto di comunicazione o diffusione (ad esempio mediante la loro pubblicazione su blog o social network).

Viene altresì ribadito che, per prassi, è consentita la pubblicazione al tabellone esposto nella bacheca scolastica dei nominativi degli studenti distinti per classe.

In tutti i casi, aggiunge ancora il Ministero, “gli elenchi relativi alla composizione delle classi, resi disponibili con le modalità sopra indicate, devono contenere i soli nominativi degli alunni e non devono riportare informazioni relative allo stato di salute degli studenti o altri dati personali non pertinenti (es. luogo e data di nascita, ecc.).

Sia in caso di pubblicazione nel registro elettronico sia nel caso di pubblicazione attraverso i tabelloni esposti nella bacheca scolastica, il dirigente scolastico definisce il tempo massimo di pubblicazione che comunque non deve eccedere 15 giorni”.

Senza sicurezza non c'è privacy e senza privacy non c'è sicurezza

Per implementare e aggiornare il proprio sistema privacy occorre adottare specifiche misure di sicurezza. Il legislatore europeo, nel GDPR, afferma infatti che i dati devono essere “trattati in maniera da garantire un'adeguata sicurezza... compresa la protezione, mediante misure tecniche e organizzative adeguate”.

Sicurezza e privacy sono due temi correlati: senza sicurezza non può esserci privacy e senza privacy non può esserci sicurezza.

Nel mondo dell'istruzione vengono trattati nella maggior parte dei casi dati appartenenti a minori. Spetta alla scuola il compito di proteggere questa categoria di utenti da qualsiasi tipo di minaccia, e scongiurare la perdita dei loro dati.

La sicurezza non è un tema che si può improvvisare.

Dev'essere programmata fin dal principio, “tenendo conto dello stato dell'arte e dei costi di attuazione”, in base alle proprie capacità e ai propri mezzi.

Ogni anno vanno analizzati il sistema informatico e la rete dell'istituto da parte dell'amministratore di sistema o del referente informatico.

Dev'essere adottato un sistema operativo sicuro, protetto da firewall, nonché misure volte ad attuare e implementare la politica di controllo degli accessi logici ai dati personali trattati attraverso sistemi informatici (ad es., politiche di accesso ad applicativi o a cartelle di rete condivise), secondo ruoli e responsabilità definite e profili personali attribuiti agli utenti.

Va poi limitato l'accesso a file, cartelle e applicazioni in modo restrittivo, in modo che l'accesso ai dati sia consentito solamente agli incaricati.

Inoltre, è fondamentale l'educazione e la formazione di coloro i quali trattano informazioni, affinché adottino comportamenti virtuosi in fase di gestione delle stesse.

Oltre a ciò, la scuola deve dotarsi di policy specifiche, ossia di procedure che regolino l'agire dei dipendenti nell'ambito delle diverse attività di trattamento.

Ad esempio, una policy fondamentale può riguardare l'utilizzo delle attrezzature informatiche, definendo l'uso dei PC, la gestione delle password, l'utilizzo della rete e della posta elettronica.