
RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI

- Schema di atto di designazione del Responsabile della Protezione dei Dati personali (RDP) ai sensi dell'art. 37 del Regolamento UE 2016/679

- Modello di comunicazione al Garante dei dati dell'RPD ai sensi dell'art. 37, par. 1, lett. a) e par. 7, del RGPD - Dati del titolare/responsabile del trattamento

DATA BREACH

- Modello destinato ai titolari di trattamento di dati personali effettuati tramite dossier sanitario per la comunicazione dei casi di violazione dei dati personali (data breach)
(Provvedimento n. 331 del 4 giugno 2015)

- Violazione di dati personali che si verificano nelle banche dati della PA - Modello per la segnalazione al Garante
(Provvedimento n. 393 del 2 luglio 2015)

- Violazione di dati biometrici - Modello per la segnalazione al Garante
(Provvedimento n. 513 del 12 novembre 2014)

- Modello destinato ai fornitori di servizi di comunicazione elettronica per la comunicazione dei casi di violazione dei dati personali (data breach)
(*) ISTRUZIONI: Il modello va aperto, compilato e, dopo aver apposto la firma digitale, salvato come un file .pdf sul proprio computer. Infine, il modello va inviato al Garante unicamente tramite posta PEC all'indirizzo: dcrt@pec.gpdp.it.

TOOL GRATUITI

Tool gratuito Dpia

Software per la valutazione d'impatto del Garante Privacy

IL REGISTRO DEI TRATTAMENTI

Prendendo spunto dalla pagina dedicata dal Garante al tema, tracciamo una linea guida delle norme cui ispirarsi fino a "costruire" il registro dei trattamenti 'ideale' per un Istituzione scolastica.

L'art. 30 del GDPR (Regolamento europeo in materia di protezione dei dati personali) riguarda una delle novità e, al contempo, uno degli adempimenti più importanti concernenti **le attività di trattamento dei dati personali.**

Per rendersene conto valga **il par. 4 dell'art. 30**, per il quale 'su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.'

E' così costituito in capo al titolare **un obbligo di documentazione della conformità della propria organizzazione alle prescrizioni della legge.** Obbligo che grava anche sul responsabile, per i trattamenti che questi svolga per conto di un titolare. L'obbligo di redigere il Registro costituisce uno dei principali **elementi di accountability del titolare,** poiché rappresenta uno strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile ai fini della valutazione o analisi del rischio e dunque preliminare rispetto a tale attività.

Per fare – come suol dirsi – di necessità virtù, la redazione del registro potrebbe essere ispirata alle seguenti ulteriori finalità:

- **rappresentare l'organizzazione sotto il profilo delle attività di trattamento a fini di informazione, consapevolezza e condivisione interna**;
- costituire lo strumento di **pianificazione e controllo della politica della sicurezza di dati e banche di dati, tesa a garantire la loro integrità, riservatezza e disponibilità**. -

- **la 'funzione di Compliance**' (o regulatory compliance, ha il compito di verificare che **'le procedure interne siano coerenti con l'obiettivo di prevenire la violazione di norme di etero regolamentazione (leggi e regolamenti) e autoregolamentazione** (codici di condotta, codici etici)' **al fine di evitare rischi di 'incorrere in sanzion**i, perdite finanziarie o danni di reputazione in conseguenza di violazioni di norme legislative, regolamentari o di autoregolamentazione'. Il concetto di compliance è solitamente associato anche al concetto di onestà ed etica nei comportamenti spesso in relazione a veri e propri codici etici o principi deontologici dei settori di appartenenza.

- ´espressione del criterio **'data protection by default and by design'** (si veda art. 25), ossia dalla necessità di configurare il trattamento prevedendo fin dall´inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e 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 sostanziarsi in una serie di attività specifiche e dimostrabili.

L'autorità di controllo (Garante) è, d'altro canto, l'ente pubblico che ha titolo per richiedere la disponibilità del registro, al fine di esaminarlo.

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

Si invita altresì a consultare il documento interpretativo del 19 aprile 2018 del Gruppo ex art. 29 (Ora Comitato europeo per la protezione dei dati) reperibile al seguente link:

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045

2. Chi è tenuto a redigerlo?

3. Quali informazioni deve contenere?

Il Registro dei trattamenti è un documento di censimento e analisi dei trattamenti effettuati dal titolare o responsabile. In quanto tale, il registro deve essere mantenuto costantemente aggiornato poiché il suo contenuto deve sempre corrispondere all'effettività dei trattamenti posti in essere. Qualsiasi cambiamento, in particolare in ordine alle modalità, finalità, categorie di dati, categorie di interessati, deve essere immediatamente inserito nel Registro, dando conto delle modifiche sopravvenute.

Il Registro può essere compilato sia in formato cartaceo che elettronico ma deve in ogni caso recare, in maniera verificabile, la data della sua prima istituzione (o la data della prima creazione di ogni singola scheda per tipologia di trattamento) unitamente a quella dell'ultimo aggiornamento. In quest'ultimo caso il Registro dovrà recare una annotazione del tipo:

'- scheda creata in data XY'

'- ultimo aggiornamento avvenuto in data XY'

NOTA CIRCOLARE 877 DEL 3 AGOSTO 2018

Il Miur, con nota n. 877 del 03/08/2018, ha trasmesso alle scuole uno schema di Registro delle attività di trattamento per le istituzione scolastiche, previsto dal Regolamento europeo sul trattamento dei dati personali.

Insieme allo schema di registro e alla guida operativa, è stata pubblicata una nota metodologica, che illustra la metodologia utilizzata per la compilazione del Registro delle attività di trattamento rispetto ad un Sotto insieme di processi gestiti dalle istituzioni scolastiche.

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'.

Il Miur nella nota metodologica riporta esempi relativi ai seguenti processi:

1. Gestione Iscrizioni

Le iscrizioni a scuola avvengo, dalla primaria alla secondaria, in modalità telematica, ossia online, tramite il sito del Miur.

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 vs perfezionamento dell'iscrizione),

della tipologia, e della modalità di trattamento (es. applicativo SIDI vs pacchetto locale), sono state individuate due attività:

a. Acquisizione e gestione domande

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 dai singoli Consigli di Istituto.

Se la scuola utilizza le funzioni del portale SIDI:

il Miur 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; il titolare del trattamento 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.

In caso di iscrizioni in modalità cartacea:

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

b. Acquisizione documentazione aggiuntiva

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.

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

La gestione dei dati degli alunni 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 Miur 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;

il titolare del trattamento 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 Personale docente
2. Gestione contratto a tempo determinato Personale docente
3. Gestione contratto per supplenze brevi e saltuarie Personale docente

Gestione contratto a tempo indeterminato Personale docente

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 MIUR e della scuola.

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

Gestione contratto a tempo determinato Personale docente

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 una contitolarità ex art. 26 del Reg. (UE) 2016/679 del MIUR 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 MIUR.

Gestione contratto per supplenze brevi e saltuarie Personale docente

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 MIUR 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.

Un software per la valutazione di impatto

La CNIL, l'Autorità francese per la protezione dei dati, ha messo a disposizione un software di ausilio ai titolari in vista della effettuazione dellavalutazione d'impatto sulla protezione dei dati (DPIA).

Il software - gratuito e liberamente scaricabile dal sito www.cnil.fr (https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de...) - offre un percorso guidato alla realizzazione della DPIA, secondo una sequenza conforme alle indicazioni fornite dal WP29 nelle Linee-guida sulla DPIA.

IMPORTANTE

Il software qui presentato **NON costituisce un modello** al quale fare riferimento in ogni situazione di trattamento, essendo stato concepito soprattutto come ausilio metodologico per le PMI. **Offre in ogni caso un focus** sugli elementi principali di cui si compone la procedura di valutazione d'impatto sulla protezione dei dati.

E' inoltre bene ricordare che la valutazione d'impatto sulla protezione dei dati deve tenere conto del rischio complessivo che il trattamento previsto può comportare per i diritti e le libertà degli interessati, alla luce dello specifico contesto. Pertanto, il concetto di rischio non si esaurisce nella considerazione delle possibili violazioni o minacce della sicurezza dei dati.

Per approfondimenti, è disponibile anche un breve tutorial realizzato dal Garante italiano.

ISTRUZIONI PER L'INSTALLAZIONE

Una volta aperta la pagina https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de... fino al titolo "Version portable" e selezionare il tipo di sistema operativo installato sul proprio computer.

Una volta scaricato il software, lanciare l'installazione che sarà effettuata automaticamente nella versione in lingua italiana.

Privacy, il GDPR applicato alle istituzioni scolastiche il D.Lgs. 101/2018 – Regolamento di attuazione del GDPR in vigore dallo scorso 25 maggio che ha adeguato, appunto, il Codice della privacy alla normativa europea – è stato pubblicato in Gazzetta Ufficiale appena lo scorso 4 settembre, è entrato in vigore dal 19 settembre, ma già si possono contare due aggiornamenti del testo negli articoli 11 e 15),

Il MIUR, con nota prot. n. 563 del 22/05/2018, ha fornito alle istituzioni scolastiche prime indicazioni in merito all’applicazione del nuovo Regolamento (UE) 2016/679. In particolare, il Ministero ha comunicato che ogni scuola deve dotarsi in via prioritaria del Responsabile della protezione dati personali: figura, interna o esterna, connotata da requisiti di autonomia e indipendenza, deve operare senza conflitto di interessi e possedere specifiche competenze in materia di trattamento dei dati personali. È consentito a più scuole di avvalersi di un unico Responsabile. Deve essere sempre soddisfatto il requisito della cosiddetta 'raggiungibilità' del Responsabile per la protezione dei dati proprio per assicurare un efficace supporto al Titolare del trattamento.

Dall’analisi del testo D.Lgs. 101/2018 emergono alcune modifiche importanti al “vecchio” Codice.

In particolare, al Capo IV – Istruzione viene abrogato l’art. 95 (Dati sensibili e giudiziari). Il successivo art. 96 (Trattamento di dati relativi a studenti) viene invece modificato come da tabella.

Un’altra modifica riguarda l’art. 50 (Notizie o immagini relative a minori), al quale viene aggiunta la parte evidenziata:

1. Il divieto di cui all’art. 13 del DPR 22/09/1988, n. 448, di pubblicazione e divulgazione con qualsiasi mezzo di notizie o immagini idonee a consentire l’identificazione di un minore si osserva anche in caso di coinvolgimento a qualunque titolo del minore in procedimenti giudiziari in materie diverse da quella penale. La violazione del divieto di cui al presente articolo è punita ai sensi dell’art. 684 del codice penale.

Il suddetto art. 684 prevede che «chiunque pubblica, in tutto o in parte, anche per riassunto o a guisa d’informazione, atti o documenti di un procedimento penale, di cui sia vietata per legge la pubblicazione, è punito con l’arresto fino a trenta giorni o con l’ammenda da cinquantuno euro a duecentocinquantotto euro».

Il consenso digitale del minore dopo il decreto Gdpr 101/2018

Differenze mondo scuola

A questo punto ci interroghiamo su come dobbiamo costruire il nostro registro dei trattamenti ;

Se deve tracciare il trattamento dei flussi di dati il registro non può esaurirsi in poche macrocategorie ma deve registrare il procedimento amministrativo anzi il processo amministrativo di tutte le istanze .

Ecco quindi un esempio di registro trattamento dati con la foma di un modulo on line, costruito a partire dall'elenco dei tipo di procedimento di ciascuna istituzione scolastica .

Si rinvia al form .....

Allegato	Dimensione
avviso-pubblico-data-officer.pdf	82.56 KB
i-o-misure-minime-di-sicurezza-informatica.pdf	123.56 KB