Privacy & Scuola

Come trattare i dati personali in ambito scolastico

Itconsbs s.r.l. – Giulio Angelo Fontana

Normative di riferimento

- Nuovo Regolamento Europeo 2016/679 (G.D.P.R.)
- Codice Privacy 196/2003
- D. Lgs 101/2018 che adegua il Codice Privacy al G.D.P.R.
- Decreto Ministeriale 305 del 7 dicembre 2006 - Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della pubblica istruzione
- Le decisioni della Corte Europea per i Diritti dell'Uomo e della Corte di cassazione, oltre ai provvedimenti adottati dal Garante Privacy

Normative di riferimento

- Il Parlamento Europeo, in data 14 Aprile 2016, ha approvato definitivamente, dopo un iter legislativo durato oltre quattro anni, il c.d. "pacchetto protezione dati", che si compone di due diversi strumenti:
- un nuovo Regolamento 2016/679 concernente la "**tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati**", volto a disciplinare i trattamenti di dati personali, sia nel settore privato, sia nel settore pubblico, e destinato ad abrogare la Direttiva 95/46/CE2 ("Direttiva 95/46") che ha portato in Italia, alla promulgazione del D. Lgs. 675/21996 e all'adozione del vigente D.lgs. 30 giugno 2003 n. 196 ("Codice Privacy") aggiornato al G.D.P.R. dal D. lgs. 101/2018;

SOLO LE PERSONE FISICHE SONO INTERESSATE

ALLA TUTELA DEI DATI PERSONALI

Normative di riferimento

- La Direttiva 2016/680, invece, concerne la protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati.

Normative di riferimento italiane

- recepimento della direttiva comunitaria 46/95 - Legge 675 del 31-12-1996 che provvedeva alla costituzione dell' Autorità per la protezione dei dati personali.
- Questa normativa è stata abrogata nel 2003 con l'adozione del «Codice privacy».

- **Oggi**
- Testo Unico D. Lgs. 196/03 «Codice della Privacy» adeguato al G.D.P.R. con D. Lgs 101/2018 - attualmente la normativa di riferimento unitamente al 2016/679.

- DECRETO 101 DEL 10.08.2018 PUBBLICATO IN G.U IL 4.09.2018 che ha Il fine di adeguare il quadro normativo nazionale alle disposizioni del regolamento (UE) 2016/679

Provvedimenti del garante privacy :

- Provvedimento Videosorveglianza (8 aprile 2010)
- Amministratore di Sistema (27 novembre 2008)
- Biometria e firma grafometrica (21 maggio 2014)
- Cookies (8 maggio 2014) – (20 gennaio 2020 – 13 giugno 2020)
- Posta elettronica e Internet (10 marzo 2007)
- Persone Giuridiche (20 settembre 2012)
- Spam e-mail commerciali (4 luglio 2013)

Normative di riferimento italiane

- Art. 1 (Oggetto) del nuovo Codice Privacy adeguato al G.D.P.R.
- 1. Il trattamento dei dati personali **avviene secondo le norme del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016**, di seguito «Regolamento», e del presente codice, nel rispetto della dignità umana, dei diritti e delle libertà fondamentali della persona.

Definizione di privacy

- Oggi la privacy non significa soltanto diritto ALLA RISERVATEZZA O ALLA PROTEZIONE DELLA propria sfera privata.
- E’ soprattutto il diritto di controllare l’utilizzo e la circolazione dei propri dati personali che costituiscono il bene primario dell'attuale società dell'informazione.
- Il diritto alla privacy e, in particolare, il diritto alla protezione dei dati personali costituiscono diritti fondamentali delle persone.

Definizione di privacy

› La privacy oggi più che mai è da intendersi come rispetto dei diritti fondamentali, dell'identità e dignità personale ed è un diritto sancito anche dalla Carta dei diritti fondamentali dell'Unione Europea (art. 7 «ogni persona ha diritto al rispetto della propria vita privata e familiare....» art. 8 «ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano») e dalla nostra Costituzione italiana (art. 2 «la Repubblica riconosce e garantisce i diritti inviolabili dell'uomo....»)

Finalità dell'intervento normativo

› GARANTIRE che il trattamento si svolga nel rispetto di:

- diritti e libertà fondamentali
- dignità
- diritto alla riservatezza
- Diritto alla protezione dei dati personali

DELL'INTERESSATO

Principali novità introdotte dal G.D.P.R.

- **Armonizzazione**
- **Ambito di applicazione,**
- **Accountability - obbligo di rendicontazione,**
- **Privacy by design e privacy by default,**
- **Maggiore trasparenza nelle informative,**
- **Trasferimento dati verso Paesi terzi.**

Principio di Armonizzazione

- Il nuovo "pacchetto protezione dati" **mira ad adeguare la data protection rispetto all'evoluzione tecnologica che ha determinato un aumento dei flussi transfrontalieri e, quindi, dei dati scambiati tra attori pubblici e privati, rendendo così necessari: da un lato, una più libera circolazione di dati all'interno dell'UE ma, dall'altro, un più elevato livello di protezione.**
- Merita altresì porre in rilievo la forte volontà del Legislatore europeo di eliminare la frammentazione applicativa della normativa in materia di protezione dei dati personali nel territorio dell'UE dovuta alle diverse leggi di recepimento della Direttiva 95/46.

Ambito di applicazione

1.1 Le norme precedenti.

La Direttiva 95/46/CE prevedeva che la disciplina in materia di tutela di dati personali trovasse applicazione, **per il tramite delle legislazioni nazionali**, quando il trattamento di dati personali è effettuato "nel contesto delle attività di uno stabilimento del titolare situato nell'UE".

Sulla base di tale principio, il Codice Privacy (art. 5) prevede che le sue norme s'applichino:

- (i) al "trattamento di dati personali, anche detenuti all'estero, **effettuato da chiunque è stabilito nel territorio dello Stato [italiano] o in luogo comunque soggetto alla sovranità dello Stato [italiano]**"; e
- (ii) "al trattamento di dati personali **effettuato da chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea e impiega, per il trattamento, strumenti situati nel territorio dello Stato [italiano] anche diversi da quelli elettronici, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea**".

Ambito di applicazione

1.2 Le nuove norme.

Una delle maggiori caratteristiche del Nuovo Regolamento è senz'altro il suo ambito di applicazione, che si pone in maniera innovativa sotto due profili:

A) Modifica la concezione tradizionale del principio di stabilimento; ed

B) Estende l'ambito di applicazione anche a titolari e responsabili di trattamento ("Titolari" e "Responsabili") non residenti nell'UE.

Ambito di applicazione

1.2 Le nuove norme.

Il Nuovo Regolamento infatti, **rovescia il tradizionale principio di stabilimento**, sancendo l'applicabilità della disciplina da questo dettata "indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione" e stabilisce l'applicazione delle sue regole anche a Titolari e Responsabili non stabiliti nell'UE che:

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

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

Nuovi obblighi e responsabilità (Accountability)

Il Nuovo Regolamento ridefinisce le figure di Titolare e Responsabile attribuendo loro obblighi ulteriori rispetto a quanto previsto dall'attuale Direttiva 95/46 e dal Codice Privacy.

La non concretezza e l'inefficienza delle policies sotto esposte costituisce per il Titolare fonte di responsabilità (principio di rendicontazione o di "accountability", artt. 24 e 32).

Con il Nuovo Regolamento il Titolare ha un ruolo più proattivo e obblighi più pregnanti, finalizzati non soltanto al formalistico rispetto delle regole, ma anche all'adozione di tutti gli accorgimenti tecnici e organizzativi necessari a garantire la compliance effettiva dei trattamenti, anche sotto il profilo della sicurezza.

Privacy by design e privacy by default (art. 25)

- (i) La **privacy by design** richiede che Il Titolare adotti e attui misure tecniche e organizzative sin dal momento della progettazione oltre che nell'esecuzione del trattamento, che tutelino i principi di protezione dei dati.

- (ii) La **privacy by default** presuppone invece, nella modalità operativa del trattamento, misure e tecniche che, per impostazione predefinita, garantiscano l'utilizzo dei soli dati personali necessari per ciascuna specifica finalità di trattamento.

Privacy by design e privacy by default (art. 25)

- Il principio di privacy by design impone l'obbligo di:

- Verificare l'impatto che il trattamento può rappresentare per gli interessati (PIA),
- Limitare la raccolta dei dati facendo riferimento al principio di necessità (ex art. 3 del 196/2003),
- Verifica dei livelli di sicurezza adottati (ex art. 32 del G.D.P.R.),
- Verifica dei corretti livelli di accesso degli incaricati,
- Monitoraggio dei punti precedenti.

Privacy by default

PRIVACY BY DEFAULT

Devono essere adottati meccanismi tali che assicurino l'utilizzo e la raccolta dei soli dati necessari per una specifica finalità e la non conservazione dei dati oltre il tempo necessario al raggiungimento di tale scopo.

Valutazione d’impatto sulla protezione dei dati (art. 35) - (PIA)

Quando un determinato trattamento - tenuto conto dell’uso di nuove tecnologie e della sua natura, del contesto e delle finalità - può presentare un rischio elevato per i diritti e libertà delle persone fisiche, il Titolare deve effettuare una valutazione preventiva dell’impatto che il trattamento dati da attivare può avere sugli interessati. L’autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti che sono soggetti a Valutazione d’Impatto e di quelli che invece non vi sono soggetti, comunicandoli al Comitato europeo per la protezione dei dati, vedasi slide successiva.

La Valutazione d’Impatto deve contenere:

- una descrizione dei trattamenti previsti e delle finalità del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati e le misure ritenute idonee a mitigare i rischi individuati.

Valutazione d'impatto sulla protezione dei dati (art. 35) - (PIA)

QUANDO LA DPIA E' OBBLIGATORIA?

In tutti i casi in cui un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
Il Gruppo Art. 29 individua alcuni criteri specifici a questo proposito:

- trattamenti valutativi o di scoring, compresa la profilazione;
- decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);
- monitoraggio sistematico (es: videosorveglianza);
- trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche);
- trattamenti di dati personali su larga scala;

Valutazione d'impatto sulla protezione dei dati (art. 35) - (PIA)

QUANDO LA DPIA E' OBBLIGATORIA?

- combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);
- dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.);
- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento). La DPIA è necessaria in presenza di almeno due di questi criteri, ma - tenendo conto delle circostanze - il titolare può decidere di condurre una DPIA anche se ricorre uno solo dei criteri di cui sopra.

Valutazione d’impatto sulla protezione dei dati (art. 35) - (PIA)

QUANDO LA DPIA NON E’ OBBLIGATORIA?

Secondo le Linee guida del Gruppo Art. 29, la DPIA NON è necessaria per i trattamenti che:
- non presentano rischio elevato per diritti e libertà delle persone fisiche;
- hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;
- sono stati già sottoposti a verifica da parte di un’Autorità di controllo prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche;
- sono compresi nell’elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA;
- fanno riferimento a norme e regolamenti, Ue o di uno stato membro, per la cui definizione è stata condotta una DPIA.

Data breach (artt. 33 e 34)

Il Nuovo Regolamento estende tale obbligo di comunicazione a tutti i Titolari e Responsabili, qualsiasi siano i trattamenti posti in essere.
Nello specifico, il Responsabile deve informare il Titolare senza ingiustificato ritardo della violazione e quest'ultimo deve notificare la violazione, a sua volta senza ingiustificato ritardo, all'autorità di controllo (i.e., al Garante) e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la suesposta violazione presenti un rischio per i diritti e le libertà delle persone.
È previsto inoltre un obbligo di comunicazione, senza ingiustificato ritardo, anche a tutti gli interessati coinvolti, se la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Data breach (artt. 33 e 34)

La finalità della norma in questione, è palesemente quella di consentire all'autorità di controllo di attivarsi senza ritardo in modo da valutare quale sia la gravità della violazione e quali misure imporre al Titolare.
Da notare, che mentre per la notifica all'autorità di controllo si richiede "un rischio per i diritti e le libertà degli individui", per la notifica all'interessato è necessario che il rischio sia "elevato", dunque, in quest'ultimo caso, è richiesta una soglia di pericolo maggiore anche per evitare inutili allarmismi degli interessati a fronte di violazioni di dati meramente potenziali.

Il Garante ha l'obbligo di diffondere a tutti i canali dell'informazione ogni accesso illecito di cui viene a conoscenza.

Accresciuti obblighi di trasparenza (artt.5 e 12)

Il Legislatore europeo dedica una sezione del Nuovo Regolamento alla "Trasparenza" (Sezione 1 del Capo III) e, con riferimento alle modalità di trattamento dei dati, richiede che le informazioni all'interessato:

- a) siano rese con un linguaggio semplice e chiaro, soprattutto nel caso di minori;
- b) abbiano sempre forma scritta, l'informativa in forma orale essendo ammessa solo quando ciò è richiesto dall'interessato e l'identità di questi possa essere provata con altri mezzi o in caso di interessi maggiori es: garantire la vita dell'interessato;
- c) prevedano, inter alia,
  - (i) il periodo di conservazione dei dati personali,
  - (ii) il diritto di proporre reclamo ad un'autorità di controllo,
  - (iii) l'intenzione del titolare di trasferire dati personali a un paese terzo.

Trasferimento dati verso Paesi terzi

- In primo luogo, viene meno il requisito dell'autorizzazione nazionale (si vedano art. 45, paragrafo 1, e art. 46, paragrafo 2). Ciò significa che il trasferimento verso un Paese terzo "adeguato" ai sensi della decisione assunta in futuro dalla Commissione, ovvero sulla base di clausole contrattuali modello, debitamente adottate, o di norme vincolanti d'impresa approvate attraverso la specifica procedura di cui all'art. 47 del regolamento, potrà avere inizio senza attendere l'autorizzazione nazionale del Garante - a differenza di quanto attualmente previsto dall'art. 44 del Codice.
- Tuttavia, l'autorizzazione del Garante sarà ancora necessaria se un titolare desidera utilizzare clausole contrattuali ad-hoc (cioè non riconosciute come adeguate tramite decisione della Commissione europea) oppure accordi amministrativi stipulati tra autorità pubbliche – una delle novità introdotte dal regolamento.

Trasferimento dati verso Paesi terzi

- Il regolamento consente di ricorrere anche a **codici di condotta ovvero a schemi di certificazione** per dimostrare le "garanzie adeguate" previste dall'art. 46. Ciò significa che i **titolari o i responsabili del trattamento stabiliti in un Paese terzo potranno far valere gli impegni sottoscritti attraverso l'adesione al codice di condotta** o allo schema di certificazione, ove questi disciplinino anche o esclusivamente i trasferimenti di dati verso Paesi terzi, al fine di legittimare tali trasferimenti. **Tuttavia** *(si vedano art. 40, paragrafo 3, e art. 42, paragrafo 2)*, tali titolari dovranno **assumere**, inoltre, **un impegno vincolante mediante uno specifico strumento contrattuale o un altro strumento** che sia giuridicamente vincolante e azionabile dagli interessati.

Registro delle attività o dei trattamenti (art. 30)

- Il Titolare e il Responsabile devono tenere un registro delle attività di trattamento in forma scritta, anche in formato elettronico, contenente gli elementi di cui all'art. 30 del Nuovo Regolamento.
- Secondo il G.D.P.R., l'obbligo di tenuta del suesposto registro non si applica, in linea di principio alle imprese o organizzazioni con meno di 250 dipendenti (con limitate eccezioni).
- Rimane sempre in Italia il vincolo che consiste nel riconoscimento del trattamento Dati personali quale ATTIVITA' PERICOLOSA e quindi assoggettata all' art. 2050 del Codice Civile che prevede, per il Titolare, l'onere dell'inversione della prova.
- Non basta quindi dichiarare di non aver commesso l'illecito, ma si deve dimostrare in solido di aver adottato tutte le misure necessarie affinché l'illecito non potesse accadere.

Definizioni - Soggetti interessati al trattamento

- **Titolare o «Controller»**, “Persona fisica, persona giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali, ivi compreso il profilo della sicurezza “
- **Responsabile interno ed esterno, autonomi titolari o «Data processor»,** “Persona fisica, persona giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali ”, I compiti sono specificati per iscritto e controllati dal Titolare con verifiche periodiche.
- **Responsabile della protezione dei dati** (DPO-RPD) figura obbligatoria per tutti gli enti pubblici e organismi parificati a enti pubblici.

Definizioni - Soggetti interessati al trattamento

- **Incaricati al trattamento o «persone autorizzate al trattamento a cura del Titolare»,** “Persona fisica autorizzata, dal Titolare o dal Responsabile, a compiere operazioni di trattamento”
- **Interessati**, “La persona fisica, giuridica, l’ente o l’associazione a cui si riferiscono i dati personali“
- **Garante privacy**, “L’autorità di controllo, un organo collegiale, identificato nell’articolo 30 della legge 675/96, incaricato di sorvegliare sull’applicazione della legge stessa»

Definizioni - Soggetti interessati al trattamento

› L'Istituto scolastico ricopre il ruolo di "**titolare del trattamento**" in ragione della sua autonomia organizzativa rispetto al Ministero dell'Istruzione.

› Al dirigente scolastico, in quanto legale rappresentante dell'Istituto scolastico, spetta in concreto l'onere di prendere decisioni in merito alle attività di trattamento da intraprendere e alle modalità di svolgimento a cura del personale amministrativo, docente e non docente.

Definizioni - Soggetti interessati al trattamento

› Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, **il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento.**

(GDPR: artt. 4, par. 7, 24 e 26 e considerando da 74 a 79)

ACCOUNTABILITY

Definizioni - Soggetti interessati al trattamento

ACCOUNTABILITY

› **Il titolare**:

- Individua il rischio connesso al trattamento;
- Pone in sicurezza l'attività di trattamento dei dati;
- Rilascia l'informativa all'interessato;
- Attende all'esercizio dei diritti dell'interessato;
- Nomina il Responsabile del trattamento dei dati;
- Vigila sull'osservanza del contratto di nomina del Responsabile del trattamento dei dati

(GDPR: artt. 4, par. 7, 24 e 26 e considerando da 74 a 79)

Definizioni - Soggetti interessati al trattamento

ACCOUNTABILITY

› **Il titolare**:

- Compila il registro del trattamento dei dati;
- Nomina il Responsabile della Protezione dei dati (DPO/RPD);
- Coopera con l'Autorità di controllo;
- Effettua la «valutazione d'impatto» (DPIA);
- Effettua la «consultazione preventiva».

(GDPR: artt. 4, par. 7, 24 e 26 e considerando da 74 a 79)

Definizioni - Soggetti interessati al trattamento

ACCOUNTABILITY

› **Il titolare**:

- Notifica l'eventuale violazione dei dati personali (data breach);
- Documenta la violazione dei dati personali (data breach);
- Comunica la violazione dei dati personali (data breach);

(GDPR: artt. 4, par. 7, 24 e 26 e considerando da 74 a 79)

Definizioni - Soggetti interessati al trattamento

ACCOUNTABILITY

- **Il responsabile:**
  - La base giuridica del trattamento è il contratto.

Responsabilità del «responsabile»

Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato (art. 28).

Definizioni - Soggetti interessati al trattamento

ACCOUNTABILITY

› **Il responsabile:**

IL RESPONSABILE SI IMPEGNA A:

- trattare dati soltanto su istruzione documentata del titolare;
- consentire i trattamenti solo a persone autorizzate con impegno alla riservatezza o che abbiano un adeguato obbligo legale di riservatezza;
- adottare tutte le misure di sicurezza (es. cifratura, pseudonimizzazione, recupero da backup);

Definizioni - Soggetti interessati al trattamento

ACCOUNTABILITY

› **Il responsabile:**

IL RESPONSABILE SI IMPEGNA A:

- assistere il titolare per dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
- cancellare o restituire tutti i dati e cancellare le copie esistenti;
- mettere a disposizione del titolare le informazioni per dimostrare il rispetto dei suddetti obblighi e consentire le ispezioni.

Definizioni - Soggetti interessati al trattamento

ACCOUNTABILITY

› Il responsabile della protezione dei dati:

Tutti i soggetti pubblici, devono nominare il Responsabile della protezione dei dati personali

E’ la nuova figura di riferimento per le imprese e la Pubblica Amministrazione, per utenti e clienti, ed è l’interfaccia per le Autorità garanti (esclusi i tribunali).

Definizioni - Soggetti interessati al trattamento

ACCOUNTABILITY

› Il responsabile della protezione dei dati:

L'RDP deve essere designato in base alla sua professionalità e, in particolare, alla sua conoscenza della legislazione di protezione dei dati, conoscenze in campo informatico ed è tenuto, inter alia a:

• informare e consigliare il Titolare o il Responsabile in merito agli obblighi derivanti dal Nuovo Regolamento e da altre disposizioni dell'UE;

• sorvegliare che il Nuovo Regolamento sia osservato;

• fornire, se richiesto, un parere in merito alla Valutazione d'Impatto;

• cooperare con l'autorità di controllo;

Definizioni - Soggetti interessati al trattamento

ACCOUNTABILITY

› Il responsabile della protezione dei dati:

L'RDP deve operare in completa autonomia, e per questo preferibilmente una figura esterna alla struttura, così da non incorrere in conflitti di interesse.

É tenuto a:

• supportare il Titolare nella gestione di tutti i rapporti interni ed esterni;

• sorvegliare che le misure adottate e gli eventuali adeguamenti necessari vengano mantenuti nel tempo;

• verificare periodicamente la documentazione in uso, informative, consensi, lettere di incarico, nomine delle figure necessarie a garantire l'integrità, la disponibilità e la riservatezza dei dati trattati;

• eseguire degli audit interni di verifica periodici e presso i responsabili esterni e/o autonomi titolari nominati dal Titolare del trattamento.

Definizioni - Soggetti interessati al trattamento

ACCOUNTABILITY

› Incaricati al trattamento:

L'art. 2-quaterdecies del Codice prevede che titolare e responsabile possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifiche funzioni siano attribuite a persone fisiche espressamente designate.

Per incaricato si intende il personale, autorizzato dal titolare, direttamente coinvolto nel processo formativo ed educativo o nelle attività amministrative e di gestione della scuola.

Le persone autorizzate al trattamento dei dati personali non possono trattare tali dati se non sono formate in tal senso dal titolare o dal responsabile con istruzioni mirate al contesto (trattamento dati minori, rendimento scolastico).

Definizioni - dati personali (ex comuni)

- Dato personale (art. 4):
- qualsiasi informazione concernente una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, con particolare riferimento ad un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo on line (nickname), o a uno o più elementi caratteristici della sua identità fisica, genetica, psichica, economica, culturale, sociale, GIUDIZIARIA.

Definizioni - dati personali particolari

› Dato personale (ex art. 9):

Dati personali che rivelino l'origine razziale, etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati genetici, biometrici, dati relativi alla salute, vita sessuale o orientamento sessuale della persona.

Definizioni - dati personali particolari

› Dato personale (art. 10):

Il Nuovo Regolamento integra anche le tipologie di dati riferiti ai dati giudiziari in ambito penale, ovvero idonei a rivelare:

- provvedimenti di cui all'art. 3 del T.U. del Casellario giudiziale,
- la qualità di indagato (ex art. 335 c.p.p.)
- la qualità di imputato (artt. 60 e 61 del Codice di procedura penale).
- anagrafe delle SANZIONI AMMINISTRATIVE DIPENDENTI DA REATO

Definizioni - dati personali riferiti a minori

I minori, in quanto "persone fisiche vulnerabili" (Considerando n. 75 del Regolamento) meritano, infatti, "una specifica protezione relativamente ai loro dati personali, in quanto possono essere **meno consapevoli dei rischi, delle conseguenze** e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali" (Considerano n. 38 del Regolamento).

Al fine di tutelare i soggetti in condizione di particolare vulnerabilità, quali i minori, "i titolari del trattamento devono prestare particolare attenzione alla situazione del minore, di cui devono rispettare **sempre l'interesse superiore**". (**Gruppo di Lavoro Art. 29, "Parere 2/2009 sulla protezione dei dati personali dei minori", adottato l'11 febbraio 2009, WP 160)**

Linee guida DPIA e rischi elevati 4 aprile 2017 (WP 248 rev. 01) – soggetti vulnerabili

Definizioni - trattamento

› Per trattamento si intende:

› "qualunque operazione o complesso di operazioni svolte con o senza l'aiuto di mezzi elettronici o comunque automatizzati riguardanti:

- la raccolta,
- la registrazione,
- l'organizzazione,
- la conservazione,
- la consultazione,
- l'elaborazione,
- la modifica,
- la selezione,
- l'estrazione,
- il raffronto,
- l'utilizzo,
- l'interconnessione,
- il blocco,
- la comunicazione,
- la diffusione,
- la cancellazione,
- la distruzione dei dati".

Obblighi per i Titolari e Responsabili del trattamento

- Si introduce l'obbligo, per tutti i Titolari del trattamento, di garantire tre principi fondamentali nelle attività di trattamento di dati personali :
- **L'integrità,**
- **La disponibilità,**
- **La riservatezza.**

Obblighi per i Titolari e Responsabili del trattamento

› Ai sensi dell'articolo 5 i dati personali sono:

a) Trattati in modo lecito, corretto e trasparente (liceità, correttezza, trasparenza)

- tutte le scuole hanno l'obbligo di far conoscere agli interessati come vengono trattati i loro dati personali

b) Raccolti per finalità determinate, esplicite e legittime (limitazione delle finalità)

- tutte le scuole hanno l'obbligo di trattare solamente i dati personali necessari al perseguimento di finalità istituzionali oppure previste dalla normativa di settore – nell'ambito della scuola pubblica non serve il consenso,
- dati riguardanti le origini razziali o etniche per favorire l'integrazione degli alunni,

Obblighi per i Titolari e Responsabili del trattamento

- convinzioni religiose: per garantire la libertà di culto,
- stato di salute: per adottare idonee misure di sostegno per alunni disabili, per gestire assenze per malattia, per l'insegnamento domiciliare o ospedaliero, per attivitá sportive o viaggi di istruzione,
- opinioni politiche: per garantire il funzionamento degli organismi di rappresentanza,
- dati giudiziari: per assicurare il diritto allo studio anche a soggetti sottoposti a regime di detenzione o protezione
- contenziosi: per gestire i contenziosi con dipendenti e famiglie,

Obblighi per i Titolari e Responsabili del trattamento

- c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (minimizzazione dei dati)
- d) Esatti e aggiornati (esattezza)
- e) Conservati per un tempo non superiore al conseguimento delle finalità per le quali sono stati raccolti (limitazione della conservazione)
- f) Trattati in maniera da garantire un'adeguata sicurezza dei dati personali (integrità e riservatezza)

- Il Titolare del trattamento è competente per il rispetto di tali principi ed è in grado di comprovarlo attraverso la redazione di un registro delle attività (ex. Art. 30 del G.D.P.R.)

Basi giuridiche (Art. 6 condizioni di liceità)

› Il trattamento dei dati personali è lecito solo se basato su una delle seguenti condizioni di liceità:

- ❖ Consenso (NELLA SCUOLA PUBBLICA NON SERVE PER LE FINALITÀ ISTITUZIONALI),
- ❖ Esecuzione di un contratto in cui l'interessato è parte,
- ❖ Adempimenti ad obblighi di legge al quale è soggetto il titolare,
- ❖ Salvaguardia degli interessi vitali dell'interessato,
- ❖ **Esecuzione di un compito di interesse pubblico**,
- ❖ Interesse legittimo del titolare (purché non prevalga sui diritti fondamentali dell'interessato),

Basi giuridiche (Art. 6 condizioni di liceità)

- Il trattamento dei dati da parte delle istituzioni scolastiche, **compresi i dati particolari**, è giustificato **per motivi di interesse pubblico rilevante**. L'art. 2 sexies del Codice Privacy, aggiornato al G.D.P.R. dal D. Lgs 101/2018, precisa che: "I trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g), del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, **le operazioni eseguibili e il motivo di interesse pubblico rilevante**, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Basi giuridiche (Art. 6 condizioni di liceità)

› Fermo quanto previsto dal comma 1, 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».

Le scuole, quindi, sia pubbliche che private, hanno l'obbligo di informare (tramite apposita informativa) gli interessati delle caratteristiche e modalità del trattamento dei loro dati, indicando i responsabili del trattamento.

Si intende che gli interessati non sono solo gli studenti, ma anche le famiglie, gli stessi professori e tutti i soggetti che operano nelle strutture scolastiche su incarico del titolare. E' altresì importante che le scuole verifichino i loro trattamenti controllando se i dati siano eccedenti rispetto alle finalità perseguite.

Basi giuridiche (Art. 6 condizioni di liceità)

- Il consenso non dovrebbe costituire un valido presupposto di liceità «qualora esista un evidente squilibrio tra l'interessato e il titolare [...] in quanto ciò rende improbabile che il consenso sia stato espresso liberamente» (considerando 43).
- Comitato per la protezione dei dati, Linee Guida sul consenso ai sensi del Regolamento UE 2016/679 (WP 259- del 4 maggio 2020)

Attività relative a studenti e famiglie e relativa base giuridica

- iscrizione
- Processi didattici educativi
- Valutazioni e pagelle
- Rapporto con le famiglie
- Procedure disciplinari
- Rilascio titoli di studio con valore legale

di studenti e famiglie

Finalità istituzionali esecuzione compiti pubblici e motivi di interesse pubblico rilevante

IL CONSENSO DELL'INTERESSATO NON È NECESSARIO

Attività relative a comunicazioni interne e relativa base giuridica

Alcune attività richiedono la comunicazione dei dati degli studenti e del personale nelle bacheche dedicate.
Per esempio:

- Esiti degli scrutini (i dati sono pubblici),
- Pubblicazione delle pagelle (i dati sono pubblici),
- Graduatorie,
- Rapporti con le OOSS.
- Circolari docenti
- Atti organizzativi e di programmazione
- Orario lezioni
- Convocazioni collegio docenti
- Riunioni con i genitori e rappresentati di classe
- Comunicazioni generali (sicurezza, chiusura locali, direttive, documenti di varia natura…)

IL CONSENSO DELL'INTERESSATO NON È NECESSARIO

Attività relative a comunicazioni interne e relativa base giuridica

NB: Il riferimento alle “prove differenziate” sostenute, ad esempio, dagli studenti con disturbi specifici di apprendimento (DSA) non va inserito nei tabelloni, ma deve essere indicato solamente nell’attestazione da rilasciare allo studente.

IL CONSENSO DELL’INTERESSATO NON È NECESSARIO

Nelle comunicazioni scuola-famiglia possono essere inseriti dati personali degli alunni/studenti?

Nelle circolari, nelle delibere o in altre comunicazioni non rivolte a specifici destinatari non possono essere inseriti dati personali che rendano identificabili gli alunni (ad esempio, quelli coinvolti in casi di bullismo o quelli cui siano state comminate sanzioni disciplinari o interessati da altre vicende delicate).

IL CONSENSO DELL'INTERESSATO NON È NECESSARIO

Attività relative a comunicazioni all'esterno e relativa base giuridica

Alcune attività richiedono la comunicazione dei dati degli studenti a soggetti esterni.

Per esempio:

- L'organizzazione di gite scolastiche,
- L'alternanza scuola/lavoro,
- stage e tirocini presso strutture esterne,
- La segnalazione ad aziende di nominativi di studenti al fine di agevolare il successivo inserimento nel mondo del lavoro
- Comunicare eventuali intolleranze alimentari ai gestori del servizio mensa.

IL CONSENSO DELL'INTERESSATO NON È NECESSARIO

Attività relative a diffusione all'esterno e relativa base giuridica

La pubblicazione sul sito internet istituzionale di immagini e video relativi alle attività svolte durante l'orario scolastico e/o extrascolastico, trattandosi di diffusione, ovvero non si è in grado di identificare preventivamente chi verrà a conoscenza dei dati pubblicati, richiede il consenso degli interessati e/o dei loro familiari.
Determinante rispettare i principi di pertinenza e non eccedenza, secondo i quali, una volta terminata la frequentazione della struttura scolastica viene meno anche il consenso prestato.

In ogni caso non possono essere diffusi i dati relativi alla salute: **non è consentito**, ad esempio, **pubblicare online una circolare contenente i nomi degli studenti con disabilità oppure quegli degli alunni che seguono un regime alimentare differenziato per motivi di salute**.

IL CONSENSO DELL'INTERESSATO È NECESSARIO

Attività relative a diffusione all'esterno e relativa base giuridica

È da considerarsi lecita la pubblicazione sul sito internet istituzionale delle graduatorie di docenti e personale ATA?

Sì , amministrazione trasparente.
Questo consente a chi ambisce a incarichi e supplenze di conoscere la propria posizione e il proprio punteggio.

Tali liste devono però contenere solo il nome, il cognome, il punteggio e la posizione in graduatoria.

È invece eccedente la pubblicazione dei numeri di telefono e degli indirizzi privati dei candidati.

IL CONSENSO DELL'INTERESSATO È NECESSARIO

Chi può trattare i dati degli allievi disabili o con disturbi specifici dell'apprendimento (DSA)?

La conoscenza di tali dati è limitata ai soli soggetti a ciò legittimati dalla normativa scolastica e da quella specifica di settore, come ad esempio i docenti, i genitori e gli operatori sanitari che congiuntamente devono predisporre il piano educativo individualizzato (L. n. 104/92, L. n. 328/2000 e D.Lgs. n. 66/2017).

Provvedimento del Garante del 5 marzo 2020 n. 45 - Doc web n. 9365147

- "Il docente delle materie indicate annota sul registro di classe quanto segue: "XX. L'allievo XX nei giorni scorsi ha chiesto al docente di italiano e geostoria di essere dispensato dalle interrogazioni e dallo svolgimento dei compiti a casa in entrambe le discipline per tutti i mercoledì dell'anno scolastico, in quanto sostiene che ogni martedì deve sostenere una "visita medica" che lo tiene impegnato per tutto il pomeriggio. Il docente, pur in assenza di un certificato medico specifico accorda tale possibilità come gesto di disponibilità nei confronti della famiglia."
- - "l'annotazione è stata registrata nella parte del registro elettronico visibile dai Docenti della classe e dalle famiglie degli alunni;
- L'Istituto ha provveduto a rimuovere l'annotazione nel minor tempo possibile, dopo la segnalazione a cura dei genitori.

Il Garante decide di ammonire l'Istituto interessato come segue:
a) ai sensi dell'art. 57, par. 1, lett. f), del Regolamento, dichiara illecito il trattamento effettuato dal Liceo Juvarra e descritto nei termini di cui in motivazione, consistente nella violazione degli artt. 5, par. 1, lett. a) e c); 9, parr. 1, 2, lett. g), e 4 del Regolamento e 2-sexies, comma 1 del Codice, in relazione alla pubblicazione nella sezione del registro elettronico, consultabile attraverso credenziali di accesso da parte di tutti i genitori della classe, di una nota riguardante informazioni relative alla salute del figlio del reclamante;

Utilizzo degli strumenti previsti nei piani didattici

La specifica normativa di settore (L. n. 170/2010) prevede che gli studenti che presentano tali disturbi hanno il diritto di utilizzare strumenti di ausilio per una maggiore flessibilità didattica. In particolare, viene stabilito che gli studenti con diagnosi DSA possono utilizzare gli strumenti di volta in volta previsti dalla scuola nei piani didattici personalizzati che li riguardano (ivi compreso il registratore o il
pc). In questi casi non è necessario richiedere il consenso delle persone coinvolte nella registrazione.

L’utilizzo degli smartphone all’interno delle scuole è consentito?

Spetta alle istituzioni scolastiche disciplinare l’utilizzo degli smartphone all’interno delle aule o nelle scuole stesse.
In ogni caso, laddove gli smartphone siano utilizzati per riprendere immagini o registrare conversazioni, l’utilizzo dovrà avvenire esclusivamente per fini personali e nel rispetto dei diritti delle persone coinvolte.
Chi verifica tali condizioni?

È possibile registrare la lezione da parte degli studenti?

Sì. È lecito registrare la lezione per scopi personali, ad esempio per motivi di studio individuale, compatibilmente con le specifiche disposizioni scolastiche al riguardo.
Per ogni altro utilizzo o eventuale diffusione, anche su Internet, è necessario prima informare le persone coinvolte nella registrazione (professori, studenti...) e ottenere il loro consenso.

Le scuole possono consentire a soggetti legittimati di svolgere attività di ricerca tramite questionari, da sottoporre agli studenti, contenenti richieste di informazioni personali?

Sì, ma soltanto se i ragazzi e, nel caso di minori, chi esercita la responsabilità genitoriale, siano stati preventivamente informati sulle modalità di trattamento e sulle misure di sicurezza adottate per proteggere i dati personali degli alunni e, ove previsto, abbiano acconsentito al trattamento dei dati. Ragazzi e genitori devono, comunque, avere sempre la facoltà di non aderire all'iniziativa.

Violano la privacy le riprese video e le fotografie raccolte dai genitori durante le recite, le gite e i saggi scolastici?

No. Le immagini, in questi casi, sono raccolte per fini personali e destinate a un ambito familiare o amicale.

Va però prestata particolare attenzione alla eventuale pubblicazione delle medesime immagini su Internet e sui social network.

In caso di diffusione di immagini dei minori diventa infatti indispensabile ottenere il consenso da parte degli esercenti la responsabilità genitoriale.

I docenti possono richiedere informazioni sullo stato vaccinale degli studenti?

No. Il Garante privacy indica: «I docenti non possono chiedere informazioni sullo stato vaccinale degli studenti in quanto simili comportamenti potrebbero suscitare disagio per gli stessi in ragione delle scelte operate dalle proprie famiglie in merito all'adesione alla campagna vaccinale ...»

Lettera al Ministero dell'istruzione per sensibilizzare gli istituti scolastici sui rischi di alcune iniziative comunicato stampa 23.9.2021, doc web 9702160

Utilizzo della videosorveglianza e relativa base giuridica

Si possono installare telecamere negli istituti scolastici?

Può risultare ammissibile l'utilizzo di tali sistemi in casi di stretta indispensabilità, al fine di tutelare l'edificio e i beni scolastici da atti vandalici, circoscrivendo le riprese alle sole aree interessate.
È inoltre necessario segnalare la presenza degli impianti con cartelli.
Le telecamere che inquadrano l'interno degli istituti possono essere attivate solo negli orari di chiusura, quindi non in coincidenza con lo svolgimento di attività scolastiche ed extrascolastiche. Se le riprese riguardano l'esterno della scuola, l'angolo visuale delle telecamere deve essere opportunamente delimitato. [Progetti di revisione della disciplina sull'utilizzo degli strumenti di videosorveglianza negli istituti scolastici sono attualmente all'attenzione del Parlamento.]

IL CONSENSO DELL'INTERESSATO È NECESSARIO

Utilizzo registro elettronico

- Registro elettronico:
- lettera del Presidente del Garante per la protezione dei dati personali, Antonello Soro, al Ministro dell'istruzione 4 maggio 2020 https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9334326

«… Il registro elettronico costituisce, infatti, un prezioso strumento di comunicazione tra i docenti e le famiglie, tanto più nel momento attuale, caratterizzato dalla sostituzione dell'attività didattica "in presenza" con quella "a distanza", che necessita, come tale, di una più stretta interazione tra insegnanti, studenti e loro genitori, alla quale il registro on-line è sicuramente funzionale. L'inclusione, nel registro, di un novero assai rilevante – in termini quantitativi e qualitativi – di dati personali, anche di minorenni, esige tuttavia l'adozione di tutte le cautele idonee a evitare o, quantomeno, minimizzare, i rischi di esfiltrazione, trattamento illecito, anche solo alterazione dei dati stessi. …»

Attività relative al personale e relativa base giuridica

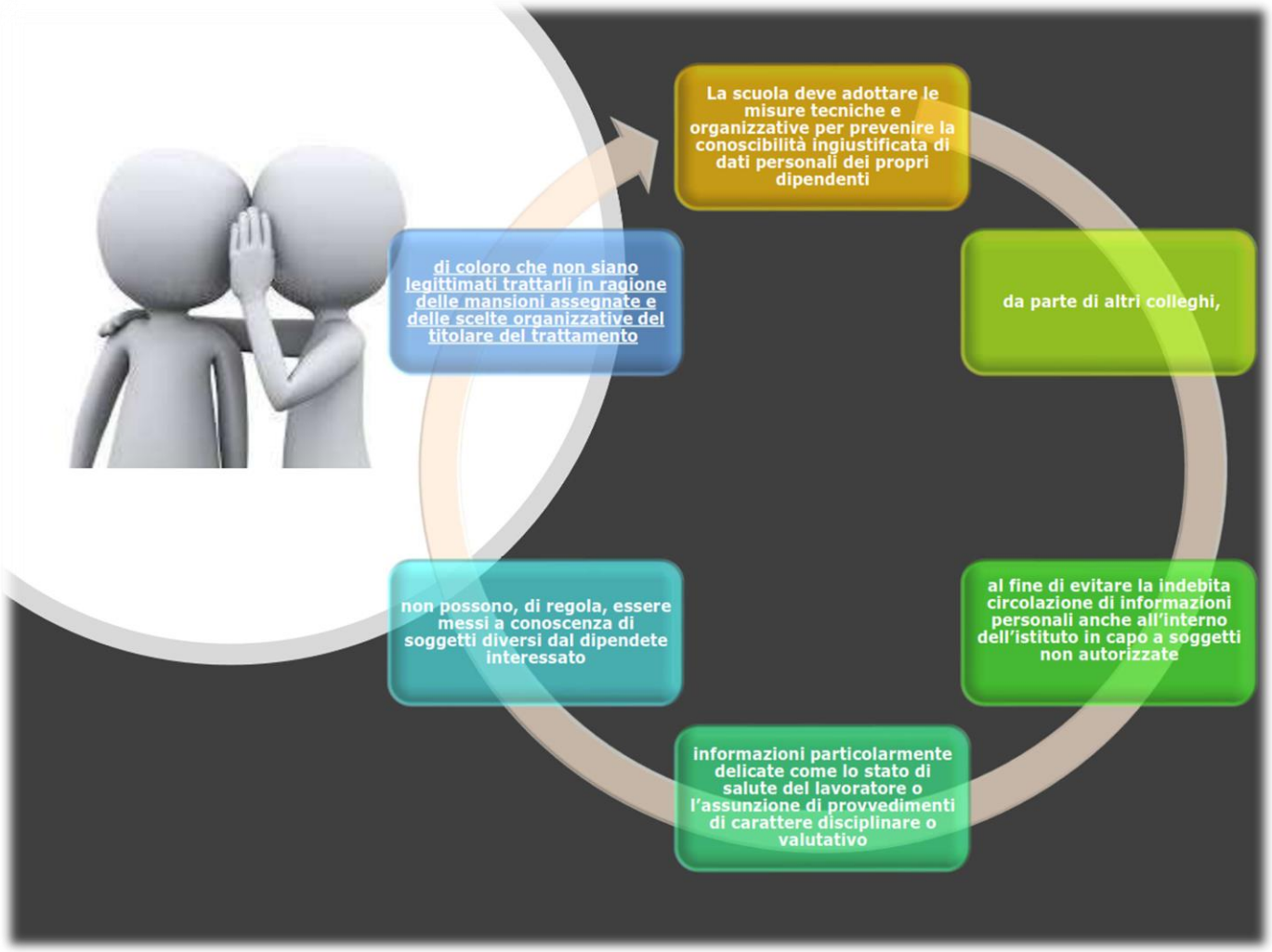
- Articolo 88 - EU RGPD - "Trattamento dei dati nell'ambito dei rapporti di lavoro«
- Gli Stati membri possono prevedere, con legge o tramite contratti collettivi, norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro, in particolare per finalità di assunzione, esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi, di gestione, pianificazione e organizzazione del lavoro, parità e diversità sul posto di lavoro, salute e sicurezza sul lavoro, protezione della proprietà del datore di lavoro o del cliente e ai fini dell'esercizio e del godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro, nonché per finalità di cessazione del rapporto di lavoro.

IL CONSENSO DELL'INTERESSATO NON È NECESSARIO

del proprio personale docente e non docente

Obblighi di legge e gestione del rapporto di lavoro (art.88 GDPR)

Attività relative al personale



Attività relative al personale

Provvedimenti che accolgono o respingono richieste individuali quali:

- Determine concessione variazione orario per esigenze personali, concessione benefici
- Provvedimenti disciplinari
- Atti valutativi
- Causali assenza (ferie, permessi, malattia, permessi sindacali)
- Lesività e gravità condotta varia se comunicazione o diffusione

Attività di comunicazione individualizzate con il dipendente

In tutte le comunicazioni all'interessato, specie se contengono categorie particolari di dati , devono essere utilizzate forme di trasmissione anche elettroniche individualizzate nei confronti di quest'ultimo o di un suo delegato:

- Indirizzo e-mail individuale e non account condivisi;
- SOLO per il tramite di personale autorizzato;
- Nel caso in cui si proceda alla trasmissione del documento cartaceo, questo dovrà essere trasmesso, di regola, in plico chiuso;
- salva la necessità di acquisire, anche mediante la sottoscrizione per ricevuta, la prova della ricezione dell'atto.

"Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati"

2. Limiti generali alla trasparenza (artt. 1 e 4 del d. lgs. n. 33/2013)

I principi e la disciplina di protezione dei dati personali – come peraltro previsto anche dagli artt. 1, comma 2, e 4 del d. lgs. n. 33/2013 (v. altresì art. 8, comma 3) – devono essere rispettati anche nell'attività di pubblicazione di dati sul web per finalità di trasparenza.

«3. Pubblicazione di dati personali ulteriori (art. 4, comma 3, del d. lgs. n. 33/2013)

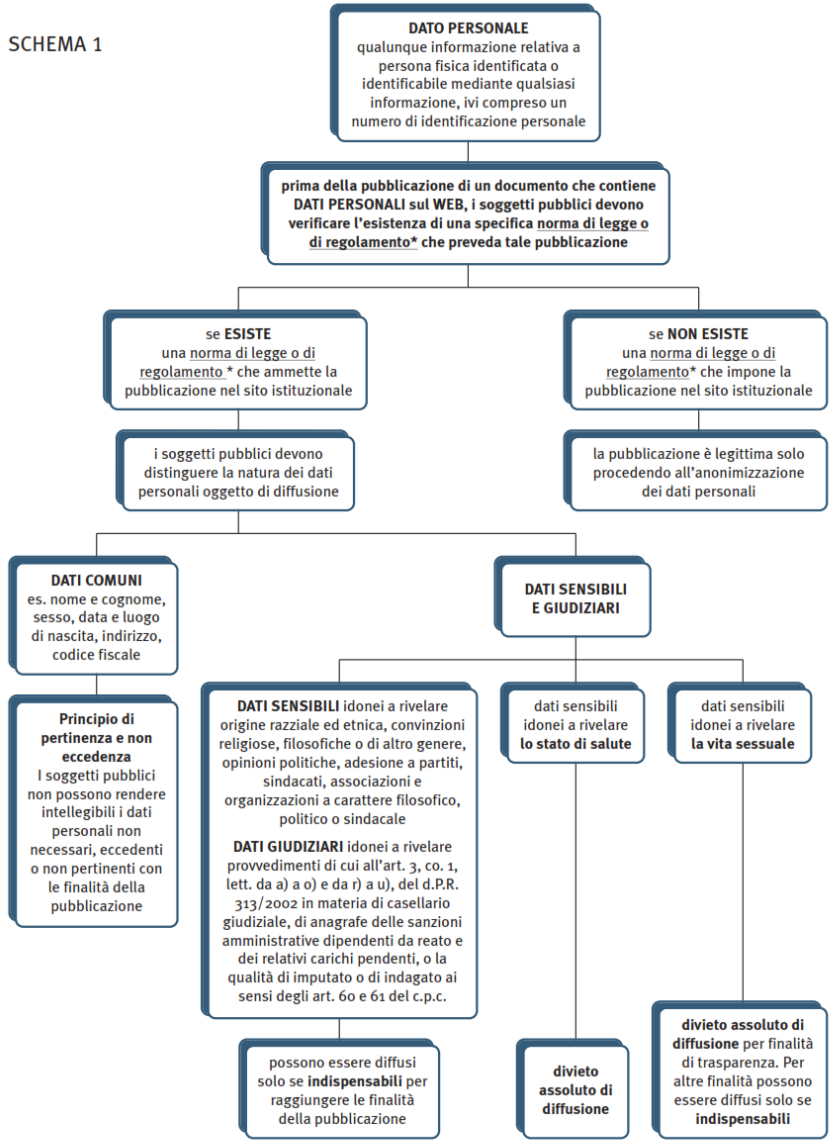
Le pubbliche amministrazioni non sono libere di diffondere "dati personali" ulteriori, non individuati dal d. lgs. n. 33/2013 o da altra specifica norma di legge o di regolamento (art. 19, comma 3, del Codice).

L'eventuale pubblicazione di dati, informazioni e documenti, che non si ha l'obbligo di pubblicare, è legittima solo "procedendo alla anonimizzazione dei dati personali eventualmente presenti" (art. 4, comma 3, del d. lgs. n. 33/2013).

In proposito, si evidenzia che la prassi seguita da alcune amministrazioni di sostituire il nome e cognome dell'interessato con le sole iniziali è di per sé insufficiente ad anonimizzare i dati personali contenuti negli atti e documenti pubblicati online.

Segue

SCHEMA 1



* N.B. Si precisa che la diffusione di dati comuni è ammessa solo se prevista da una norma di legge o di regolamento, mentre la diffusione di dati sensibili o giudiziari è ammessa se prevista espressamente solo da una norma di legge.

Attività di Trasmissione ad altri uffici scolastici anche territoriali

I documenti, soprattutto quelli che contengono categorie particolari di dati, ove debbano essere trasmessi ad altri uffici o funzioni della medesima struttura organizzativa in ragione delle rispettive competenze, devono contenere esclusivamente le informazioni necessarie allo svolgimento della funzione evitando di allegare, ove non strettamente indispensabile, documentazione integrale o riportare stralci all'interno del testo.

A tal fine dovranno essere selezionate e impiegate modalità di trasmissione della documentazione che ne garantiscano la ricezione e il relativo trattamento da parte dei soli uffici o strutture organizzative competenti e del solo personale autorizzato.

Prerogative sindacali: legittimità dell'accesso a dati personali dei dipendenti?

le prerogative sindacali (diritti di informazione preventiva o successiva) previsti dalle disposizioni contenute nei contratti collettivi possono, di regola, essere soddisfatte anche senza far ricorso a dati personali rendendo note solamente informazioni aggregate;

tenuto conto del quadro normativo vigente applicabile al c.d. «comparto scuola» non sia consentito agli istituti scolastici comunicare alle organizzazioni sindacali i nominativi dei docenti o di altro personale e le somme liquidate a ciascuno per lo svolgimento di attività finanziate con il c.d. fondo d'istituto.

Il solo ammontare complessivo del trattamento accessorio effettivamente distribuito, eventualmente ripartito per fasce o qualifiche, senza comunicare i nominativi e le somme erogate individualmente a titolo di compenso accessorio.

Diritti degli interessati (artt. dal 12 al 22)

- Modalità di accesso (artt. 11 e 12)
- Diritto di accesso (art. 15)
- Diritto di cancellazione (diritto all'oblio) (art.17)
- Diritto di limitazione del trattamento (art. 18)
- Diritto alla portabilità dei dati (art. 20)
- Consenso da parte dei minori a partire dai 14 anni
- Eredità del dato in caso di decesso

Modalità di accesso ai dati

Le modalità per l'esercizio di tutti i diritti da parte degli interessati sono stabilite negli artt. 11 e 12 del Regolamento.

Termine per la risposta. Per tutti i diritti, ricompreso il diritto di accesso, è di **1 mese**, estensibile fino a **3 mesi** nelle ipotesi di particolare complessità. Il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.

Riscontro. Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità, e può essere dato oralmente solo se così richiede l'interessato stesso.

La risposta fornita dall'interessato. Deve essere concisa, trasparente e facilmente accessibile, deve utilizzare un linguaggio semplice e chiaro.

Modalità di accesso ai dati

Misure per agevolare l'esercizio dei diritti. Il titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura, sia tecnica che organizzativa, a ciò idonea. Benché sia il solo titolare a dover dare riscontro in ipotesi di esercizio dei diritti, il responsabile è tenuto a collaborare col titolare ai fini dell'esercizio dei diritti degli interessati.
Gratuità per l'esercizio dei diritti. L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato, ma possono esservi eccezioni.
Informazioni. Il titolare ha il diritto di chiedere informazioni necessarie a identificare l'interessato, e quest'ultimo ha il dovere di fornirle, secondo modalità idonee.
Deroghe. Risultano ammesse deroghe ai diritti riconosciuti dal Regolamento, ma solo sul fondamento di disposizioni normative nazionali, ai sensi dell'articolo 23 nonché di altri articoli relativi ad ambiti specifici

Diritto di accesso

Il diritto di accesso prevede **in ogni caso** il diritto di ricevere una copia dei dati personali oggetto di trattamento.

Tra le informazioni che il titolare deve fornire non rientrano le “modalità” del trattamento, mentre occorre indicare il periodo di conservazione previsto ovvero, se non è possibile, i criteri utilizzati per definire tale periodo, nonché le garanzie applicate in caso di trasferimento dei dati verso Paesi terzi.

Accesso ai propri dati personali

Diritto di cancellazione o diritto all'oblio

Il diritto "all'oblio" si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata. Si prevede, infatti, l'obbligo per i titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione". Risulta più esteso di quello già riconosciuto all'art. 7, comma III, lettera b), del Codice della privacy, poiché l'interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento.

Diritto alla limitazione del trattamento

Rappresenta un diritto differente e maggiormente esteso rispetto al "blocco" del trattamento già previsto dall'art. 7, comma III, lettera a), del Codice della Privacy. In particolare risulta esercitabile non solamente in ipotesi di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì pure se l'interessato chiede la rettifica dei dati (in attesa di tale rettifica da parte del titolare) o si oppone al loro trattamento ai sensi dell'art. 21 del Regolamento (in attesa della valutazione da parte del titolare).

Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato a meno che ricorrano determinate circostanze (consenso dell'interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante).

Diritto alla portabilità dei dati

Rappresenta un diritto "nuovo" previsto dal Regolamento, pure se non è del tutto sconosciuto ai consumatori (si pensi alla portabilità del numero telefonico).
Si applica ai soli trattamenti automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio. In particolare risultano portabili soltanto i dati trattati col consenso dell'interessato ovvero sulla base di un contratto stipulato con l'interessato (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare), e solo i dati che siano stati "forniti" dall'interessato al titolare.
Il titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, qualora tecnicamente possibile.

Consenso al trattamento dei dati da parte dei minori di 14 anni

Il consenso al trattamento potrà essere espresso dai minori al compimento dei 14 anni, in relazione all'offerta diretta di servizi della società dell'informazione secondo l'art. 2-quinquies del D.lgs. 101/2018.

Al di sotto dei 14 anni di età il trattamento risulta lecito a condizione che sia prestato da chi esercita la responsabilità genitoriale (genitore legalmente esercente ovvero tutore).

Eredità del dato in caso di decesso

In realtà, il considerando n. 27 esclude che le norme del GDPR si applichino ai dati delle persone defunte ma viene lasciata agli Stati membri la possibilità di introdurre delle norme specifiche anche sul trattamento di tali dati.

L'Italia, in effetti, con il D. Lgs. n. 101/2018, ha introdotto nel Codice della Privacy (il D. Lgs. 196/03) il nuovo art. 2 terdecies che prevede che i diritti di cui agli articoli da 15 a 22 del Regolamento UE 2016/679 (concernenti il diritto di accesso, rettifica, integrazione, oblio, portabilità) riferiti ai dati personali concernenti persone decedute possano essere esercitati "da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione".

Richiesta danni e regime sanzionatorio

Danni cagionati per effetto del trattamento art. 15 e art. 82 del G.D.P.R. - Diritto al risarcimento e responsabilità.
Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art. 2050 del codice civile.

Il danno non patrimoniale è risarcibile anche in caso di violazione dell'art. 5 del G.D.P.R., ovvero se i dati personali non vengono:

- Trattati in modo lecito e secondo correttezza
- Raccolti e registrati per scopi determinati, espliciti e legittimi
- Esatti e se necessario aggiornati
- Pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti
- Conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi originari

Richiesta danni e regime sanzionatorio

CHI E' TENUTO AL RISARCIMENTO?

I soggetti tenuti al risarcimento di eventuali danni causati dal trattamento dei dati personali, sono:

il «Titolare"

(ossia colui "cui competono le decisioni in ordine alle finalità del trattamento" e "della sicurezza").

il «Responsabile"

(ossia colui che è preposto dal titolare al trattamento dei dati, avendo "esperienza, capacità ed affidabilità" tale da fornire "idonea garanzia del pieno rispetto delle disposizioni di legge in materia di trattamento, ivi compreso il profilo relativo alla sicurezza").

Richiesta danni e regime sanzionatorio

CHI E' TENUTO AL RISARCIMENTO?

Il Titolare può rivalersi, in caso di dolo o colpa grave sulle seguenti figure:

L'amministratore di rete/sistema

(ossia colui che gestisce le infrastrutture di rete, i profili utente e gli strumenti in uso presso la struttura se non ottempera agli obblighi di sorveglianza) – culpa in vigilando) .

Gli incaricati

Può rivalersi anche sugli incaricati al trattamento se, dopo aver ricevuto una adeguata formazione, non rispettano le disposizioni del titolare.

Richiesta danni e regime sanzionatorio

Sanzioni amministrative e penali previste del Nuovo Regolamento Europeo

Il regolamento europeo, integrato dal Codice Privacy, distingue due gruppi di violazioni:
1) Nel primo caso (art. 83, par. 4, GDPR) le sanzioni amministrative pecuniarie possono arrivare fino a 10 milioni di euro oppure, per le imprese, fino al 2% del fatturato mondiale annuo dell'esercizio precedente, se superiore ai 10 mil., e riguardano:
a) inosservanza degli obblighi del titolare e del responsabile del trattamento a norma degli articoli 8 (consenso dei minori), 11 (trattamento che non richiede identificazione), da 25 a 39 (privacy by default, contitolari del trattamento, rappresentanti non stabiliti nell'Unione, assenza di responsabili del trattamento, ove richiesto, mancanza del registro dei trattamenti, misure di sicurezza non idonee, mancata notifica delle violazioni, assenza di una valutazione di impatto, se necessaria, mancata nomina del DPO), 42 e 43;
b) inosservanza degli obblighi dell'organismo di certificazione a norma degli articoli 42 e 43;
c) inosservanza degli obblighi dell'organismo di controllo a norma dell'articolo 41, paragrafo 4;
d) inosservanza dell'articolo 2-quinquies, comma 2, Cod. Privacy (informativa ai minori);
e) inosservanza dell'art. 2-quinquiesdecies Cod. Privacy (trattamento che presenta rischi elevati per l'esecuzione di un compito di interesse pubblico);

Richiesta danni e regime sanzionatorio

Sanzioni amministrative e penali previste del Nuovo Regolamento Europeo

f) inosservanza dell'art. 92, comma 1 Cod. Privacy (cartelle cliniche);
g) inosservanza dell'art. 93, comma 1, Cod. Privacy (certificato di assistenza al parto);
h) inosservanza dell'art. 123, comma 4, Cod. Privacy (informativa agli utenti per i dati relativi al traffico telefonico);
i) inosservanza dell'art. 128 Cod. Privacy (blocco dei trasferimenti di chiamata);
l) inosservanza dell'art. 129, comma 2, Cod. Privacy (consenso per l'inclusione negli elenchi telefonici);
m) inosservanza dell'art. 132-ter Cod. Privacy (misure di sicurezza per i fornitori di servizi di comunicazione elettronica);
n) non effettuazione della valutazione di impatto di cui all'articolo 110 Cod. Privacy, comma 1, primo periodo;
o) non sottoposizione del programma di ricerca a consultazione preventiva del Garante a norma dell'art. 110 Cod. Privacy, comma 1, terzo periodo.

Richiesta danni e regime sanzionatorio

2) Un secondo gruppo di violazioni (art. 83, par. 5, GDPR), per il quale sono previste sanzioni fino 20 milioni di euro o, per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore ai 20 mil., riguardano:

a) inosservanza dei principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9;
b) inosservanza dei diritti degli interessati a norma degli articoli da 12 a 22;
c) inosservanza dei trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49;
d) inosservanza di qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX;

Richiesta danni e regime sanzionatorio

e) inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1;
f) inosservanza degli articoli 2-ter, 2-quinquies, comma 1, 2-sexies, 2-septies, comma 8, 2-octies, 2-terdecies, commi 1, 2, 3 e 4, 52, commi 4 e 5, 75, 78, 79, 80, 82, 92, comma 2, 93, commi 2 e 3, 96, 99, 100, commi 1, 2 e 4, 101, 105 commi 1, 2 e 4, 110-bis, commi 2 e 3, 111, 111-bis, 116, comma 1, 120, comma 2, 122, 123, commi 1, 2, 3 e 5, 124, 125, 126, 130, commi da 1 a 5, 131, 132, 132-bis, comma 2, 132-quater, 157, nonché delle misure di garanzia, delle regole deontologiche di cui rispettivamente agli articoli 2-septies e 2-quater.

Richiesta danni e regime sanzionatorio

Sanzioni penali previste:

Illeciti Penali (artt.167-172) adeguati al G.D.P.R. con D. Lgs 101/2018

Art. 167 Trattamento illecito di dati personali
(mancanza del consenso espresso dell'interessato)
Diventa: «...chiunque al fine di trarre per se o per altri profitto, ovvero di arrecare danno (nocumento ovvero uso illecito di dati sensibili) all'interessato...»

Reclusione da 6 mesi a 18 mesi

In caso di dati sensibili, giudiziari o che presentino rischi specifici in violazione delle misure di garanzia, trasferisca dati ad un paese terzo senza autorizzazione

Reclusione da 1 anno a 3 anni

Richiesta danni e regime sanzionatorio

Art. 167/*bis* comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala … chiunque al fine di trarre per se o per altri profitto, ovvero di arrecare danno all'interessato…
Quando è richiesto il consenso per comunicazione e diffusione dati personali

Reclusione da 1 a 6 anni

Art. 167/*ter* «Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala»

Reclusione da 1 a 4 anni

In caso di dati sensibili, giudiziari o che presentino rischi specifici in violazione delle misure di garanzia, trasferisca dati ad un paese terzo senza autorizzazione

Reclusione da 1 anno a 3 anni

Richiesta danni e regime sanzionatorio

Art. 168 Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante

Reclusione da 6 mesi a 3 anni

Chiunque intenzionalmente cagiona un'interruzione o turba la regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti

Reclusione sino a 1 anno

Art. 169 Omessa adozione di misure necessarie alla sicurezza dei dati

Arresto sino a 2 anni ammenda da €.10.000 a €.50.000
(ravvedimento operoso)

Richiesta danni e regime sanzionatorio

Art. 170 Inosservanza dei provvedimenti del Garante

Reclusione da 3 mesi a 2 anni

Art. 171 Violazione delle disposizioni in materia di controllo a distanza e indagini sulle opinioni dei lavoratori

Ammenda di 1500 euro (estensibile fino al quintuplo nei casi più gravi)
e reclusione da 15 giorni a 1 anno

Collegamenti di riferimento

Sito ufficiale del Garante per la protezione dei dati personali:
http://www.garanteprivacy.it

Sito ufficiale del Garante per Nuovo regolamento Europeo G.D.P.R. 2016/679
http://www.garanteprivacy.it/regolamentoue

Sito ufficiale del Garante per D. Lgs 101/2018 che adegua il 196/2003 al G.D.P.R.
https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9042718

Clusit – Associazione italiana per la sicurezza informatica:
http://www.clusit.it/

Ministro per l'innovazione e le tecnologie:
http://www.innovazione.gov.it/ita/index.shtml

Grazie per l’attenzione, domande?

Relatore Giulio Angelo Fontana

- Data Protection Officer dell'Ordine degli Psicologi di Milano, Cliniche, poliambulatori , studi legali, aziende ambito produttivo e fornitori di servizi S.A.A.S. e on premise;
- Iscritto all'albo degli specialisti privacy Anorc Professioni, Federprivacy e Privacy Italia;
- Membro di Clusit: Associazione Italiana per la Sicurezza Informatica
- CTU e CTP presso gli Uffici Giudiziari, Studi Legali e Agenzie Investigative;
- Formatore ambito digital forensics di Federpol;
- Premio ISDC AWARDS 2020 per le competenze e la professionalità in ambito digital forensics.

PRIVACY ITALIA

SOCIO Clusit
Associazione Italiana per la Sicurezza Informatica