oXFirm
Studio di Consulenza

partner
Asso Edu
Associazione Nazionale Tecnologie e Digital Media per l'Educazione

Il General Data Protection Regulation (GDPR)

oXFirm Studio di Consulenza

Sito Web: www.oxfirm.it – email: oxfirm@oxfirm.it

ROMA
Viale Antonio Ciamarra 259
00173, ROMA (RM)
tel. 06.86356274

CASERTA
Piazza Giovanni XXIII, 18
81027, S. Felice a C.llo(CE)
tel. 0823.753477 / 754996

Il General Data Protection Regulation (GDPR)

Relatore: Ing. Antonio Bove

partner
Asso Edu
Associazione Nazionale Tecnologie e Digital Media per l'Educazione

GDPR 2016/679: cos’è

GDPR (General Data Protection Regulation) in italiano RGPD (Regolamento Generale sulla Protezione dei Dati) **è il regolamento** con cui **la Commissione Europea** ha inteso **rafforzare la protezione dei dati personali dei cittadini dell'Unione Europea.**

A differenza delle direttive recepite con norme interne dagli stati membri, il regolamento è direttamente applicabile a **tutte le aziende pubbliche e private con sede UE e alle aziende con sede extra UE trattanti dati dei cittadini di uno dei 27 stati membri.**

GDPR: entrata in vigore e applicazione

- ✓ Il Regolamento **GDPR 2016/679** è entrato in vigore **il 24 maggio 2016** (20 giorni dopo la pubblicazione sulla Gazzetta Ufficiale)
- ✓ **Ha abrogato la direttiva privacy EU 95/46**
- ✓ **È stato recepito in Italia dal D.Lgs. 101/2018** del 10 Agosto che è entrato in vigore il 19 Settembre 2018 adeguando e modificando in parte il D.Lgs. 196/2003 (Codice della Privacy).

Cosa è il «diritto alla Privacy»?

L'istituto **nasce negli Stati Uniti nel 1890** come diritto "a essere lasciato solo" (*to be let alone*) e viene elaborato in Italia dagli anni '60-'70 come generico diritto alla libera determinazione nello svolgimento della propria personalità.

Con il complicarsi della comunicazione elettronica e digitale, il concetto si è evoluto e oggi si parla di **privacy** nel senso di **protezione dei dati personali**, come diritto ad impedire la rilevazione di informazioni sul nostro conto.

> *Con un'accezione più ampia, si intende anche il diritto ad esprimere liberamente le proprie aspirazioni, quindi l'autodeterminazione e la sovranità su sè stessi, il riconoscersi parte attiva nel rapporto con le istituzioni e nel rispetto reciproco delle libertà.*

Privacy e altri diritti

Il diritto alla Privacy è regolamentato da un'ampia normativa volta a garantire che il trattamento dei dati personali avvenga nel rispetto dei diritti e delle libertà fondamentali di ogni cittadino. Si deve bilanciare il diritto alla privacy con gli altri principi contemplati dall'ordinamento:

a) Principio di minimizzazione dei dati: Chi tratta i dati li deve trattare solo nella misura in cui ne ha realmente bisogno per raggiungere le finalità del trattamento rispettando:

- **L'adeguatezza** dei dati, vale a dire proporzionalità rispetto alla finalità per la quale sono raccolti;
- **Pertinenza** dei dati rispetto alle finalità precedentemente definite
- **Limitazione** dei trattamenti, solo per il raggiungimento delle finalità

b) Principio della trasparenza (accesso agli atti) La trasparenza amministrativa è un principio generale dell'attività e dell'organizzazione della pubblica amministrazione. Secondo tale principio, i dati forniti al richiedente, tramite **l'accesso civico «generalizzato»,** sono considerati «pubblici» nel rispetto dei limiti derivanti dalla normativa in materia di protezione dei dati personali.

Concetto di Privacy: le origini

Nel nostro ordinamento giuridico il primo e più importante riferimento in materia di legislazione sulla privacy è **l'art. 2 della Costituzione**:

«**La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo***- sia come singolo, sia nelle formazioni sociali ove si svolge la sua personalità - e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale»

(*) il diritto all'immagine, il diritto alla riservatezza, il diritto all'identità personale, la libertà religiosa, la libertà di associazione, etc.

FIGURE PRIVACY

I Soggetti del GDPR

Organigramma Privacy

I soggetti coinvolti nel trattamento sono indicati all'interno dell'organigramma privacy dell'Istituto scolastico così come individuati dal GDPR.

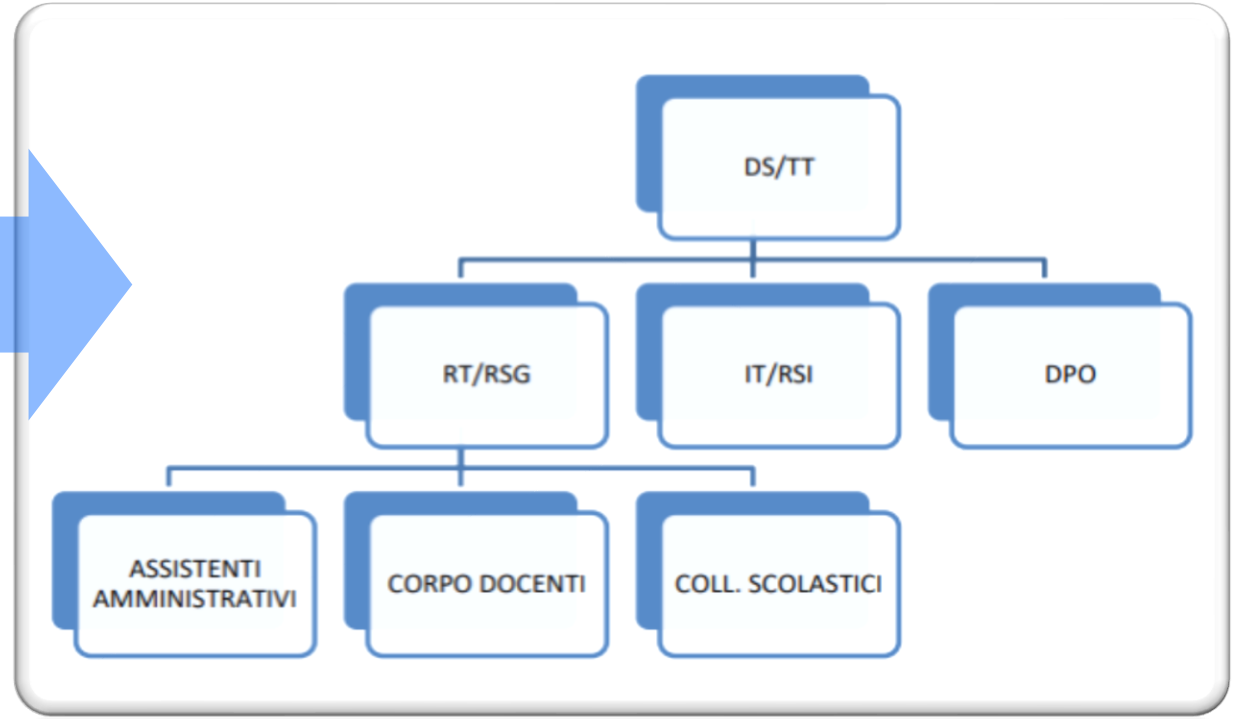
L'organigramma privacy è un **modello organizzativo** che ha la funzione di assicurare un adeguato ordinamento e classificazione dei dati personali ed un corretto utilizzo delle informazioni e dei dati.

Disciplina: Ruoli/Responsabilità/Sanzioni/Rapporto con gli interessati

La definizione dei ruoli, delle responsabilità e dei settori di competenza di ciascun soggetto dell'organizzazione costituiscono elementi imprescindibili del **sistema di gestione (presìdi)**

Esempio di organigramma Privacy

DS/TT	= Direzione/Titolare del Trattamento
RSG	= Responsabile del sistema di gestione
DPO	= Responsabile della Protezione dei dati
IT/RSI	= Responsabile informatico – Responsabile della Sicurezza delle Informazioni
ATA	= Personale non docente – amministrativo, tecnico e ausiliario
RT	= Responsabile del Trattamento
AT/I	= Addetto al Trattamento/ Incaricati



Questi soggetti operano affinché venga tutelata la privacy dell'interessato nel trattare i **dati personali.**

L’ «interessato»

L'interessato è la persona fisica a cui si riferiscono i dati personali.

Qualsiasi informazione riguardante una persona fisica identificata o identificabile è oggetto del Regolamento GDPR 2016/679.

Si considera ***identificabile*** la persona fisica che può essere individuata, direttamente o indirettamente, tramite dati anagrafici (nome), numero di identificazione (cod. fiscale), ubicazione (residenza/domicilio), contatto (numero telefonico fisso, no mobile) identificativo online (e-mail o pec) o a uno o più elementi caratteristici della sua identità fisica (fisionomia), caratteristiche psichica (carattere o patologia), economica, culturale o sociale; (art. 4, paragrafo 1, p.2)

Si definisce **DATO PERSONALE** qualsiasi informazione riguardante l'«interessato».

CODICE DELLA PRIVACY D.Lgs. 196/2003

- ✓ **Dati «sensibili»** (origine razziale, etnica, orientamento sessuale, politico, religioso/filosofico, dati relativi allo stato di salute, appartenenza sindacale,..)

REGOLAMENTO GDPR 2016/679

- ✓ **Dati «particolari» (art.9) *ex dati sensibili*** (origine razziale, etnica, orientamento sessuale, politico, religioso/filosofico, dati relativi allo stato di salute, appartenenza sindacale,..)
- ✓ **Dati genetici**
- ✓ **Dati biometrici**
- ✓ **Dati giudiziari (art.10)**

Il trattamento dei «dati particolari»

IL DIVIETO del trattamento di dati personali (art. 9) ["*che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*."]

è DIVIETO DEROGABILE in presenza di una delle condizioni a seguire:

- ✓ consenso esplicito
- ✓ trattamenti dati nel rapporto di lavoro (Servizio sanitario in occasione delle visite fiscali, organi preposti alla vigilanza igienico-sanitaria, per profilassi anticontagio Covid-19 ad es, …)
- ✓ trattamenti di dati nell'ambito delle associazioni
- ✓ stato di necessità, indagine o di polizia
- ✓ dati personali resi manifestamente pubblici dall'interessato
- ✓ dati sanitari

Trattamento dati, significato pratico

Per «**trattamento dei dati**», s'intende qualsiasi operazione fatta su uno o più dati **personali**, sia in modalità informatica che cartacea – ad es.:

- ✓ raccolta dati dall'interessato (colui che mette a disposizione del Titolare i propri dati)
- ✓ conservazione dei dati, archiviazione
- ✓ adattamento dei dati, manipolazione
- ✓ raffronto dei dati raccolti da più fonti
- ✓ messa a disposizione dei dati a favore di terzi autorizzati
- ✓ estrazione dei dati
- ✓ cancellazione o distruzione dei dati

Il Titolare del trattamento

Secondo il **GDPR il «Titolare del Trattamento» è: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che determina le finalità e i mezzi del trattamento di dati personali.**

Quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione sono stabiliti dal diritto dell'Unione o degli Stati membri (art. 4, punto 7).

Nella **SCUOLA il Titolare del trattamento** è la scuola stessa nel suo complesso

Il Titolare del trattamento

Il Titolare del trattamento è **responsabile** del rispetto dei **princìpi** applicabili al trattamento di dati personali stabiliti **dall'art. 5 del GDPR**

Il Titolare del trattamento: i compiti

Il titolare del trattamento deve dimostrare: **INTENSA ATTIVITÀ DI ADEGUAMENTO:**

- ✓ rispetto dei principi del trattamento **(art. 5)** e della **privacy by design e by default**
- ✓ **valutazione di impatto** e **consultazioni preventive (art. 35)**
- ✓ applicazione delle **procedure di sicurezza**
- ✓ **valutazione dei rischi**
- ✓ **tenuta del registro dei trattamenti** e **gestione dei *data breach**
- ✓ **designazione del Data Protection Officer (DPO)**
- ✓ gestire **Audit**

(*) ***data breach*** **=** *una violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.*

Il Responsabile del trattamento: esterno

Si definisce «Responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che **tratta dati personali per conto del Titolare del trattamento** (art. 4, punto 8 GDPR).

Il Responsabile del Trattamento, deve essere sempre ESTERNO e legato al titolare da contratto o atto giuridico vincolante per entrambi.

-Ha obblighi di trasparenza

- Deve garantire la sicurezza dei dati
- Ha l'obbligo di conservare il registro dei trattamenti del Responsabile

Nella **SCUOLA** il **responsabile del trattamento esterno è il fornitore** che gestisce i servizi Cloud/non (es. gestione il sito web, il software di segreteria, il Registro Elettronico, contatti con agenzie di viaggio, ecc…) e tratta i dati personali per conto della scuola (**GDPR Compliant**)

Il «referente interno» responsabile del trattamento

Il **referente interno** responsabile della procedura è designato **dal Titolare:**

1. è individuato tra i soggetti che, per esperienza, capacità ed affidabilità, siano in grado di fornire **idonea garanzia** del **pieno rispetto delle vigenti disposizioni** in materia di trattamento, ivi compreso il profilo relativo alla **sicurezza**.
2. ove necessario, per esigenze organizzative, possono essere designati responsabili **più soggetti**, anche mediante suddivisione di compiti.

Nella **SCUOLA** può essere designato il DSGA, il Vicario o un Responsabile di Plesso.

L’Amministratore di Sistema

L’amministratore di sistema non è previsto direttamente dal GDPR ma è colui che si occupa, a livello operativo, di mettere in atto le MISURE TECNICHE adeguate per garantire la sicurezza dei dati, ovvero si occupa della **gestione e alla manutenzione di impianti di elaborazione** con cui vengano effettuati trattamenti di dati personali:

a. sistemi di gestione delle basi di dati

b. sistemi *software* complessi: sistemi ERP (*Enterprise resource planning*) utilizzati in grandi aziende e organizzazioni

c. reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali.

Data Protection Officer (DPO)

La nomina del responsabile della protezione dati (RPD) o Data Protection Officer (DPO), deve essere comunicata al Garante della Privacy per via telematica.

Il DPO ha l'obbligo di vigilare in via generale sui trattamenti posti in essere dal titolare del trattamento.

Il DPO deve tempestivamente e adeguatamente coinvolto, dal titolare e dal responsabile del trattamento, in tutte le questioni inerenti la protezione dei dati nonché sostenuto nell'esecuzione dei suoi compiti

Data Protection Officer, **DPO**: il ruolo

a. ha **conoscenza specialistica** della normativa GDPR e delle prassi

b. si relaziona **con gli interessati**, **fornisce consulenza** al titolare, al responsabile nonché ai dipendenti

c. é **coinvolto in modo tempestivo e adeguato**

d. lavora in **autonomia** senza ricevere istruzioni

e. riferisce direttamente al vertice gerarchico

f. verifica l'osservanza della normativa, l'attribuzione delle responsabilità interne, la sensibilizzazione e la formazione del personale

g. fornisce un **parere in merito alla valutazione d'impatto** e ne segue lo svolgimento

h. si **relaziona col Garante della Privacy**

Data Protection Officer, **DPO**:le responsabilità

Linee guida gruppo dei Garanti europei art. 29 sul DPO dicembre e aprile 2017:

In caso di trattamenti NON conformi al regolamento europeo, **IL DPO NON È PERSONALMENTE E DIRETTAMENTE RESPONSABILE,** in quanto gli **obblighi** sono **a carico del titolare e del responsabile del trattamento**

Si parla di:

a. **responsabilità contrattuale**, se il DPO è esterno per inadempimento contrattuale
b. **responsabilità amministrativa,** se il DPO opera negli enti pubblici, nei casi di azione di rivalsa nel caso di dolo o colpa grave

Trasparenza e DPO

a. I **dati di contatto del DPO** devono essere comunicati, da parte del titolare o del responsabile, all'autorità di controllo competente

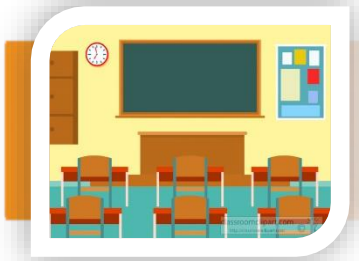
b. Il **registro dei trattamenti** deve contenere il nome e i contatti del responsabile della protezione dei dati personali DPO

c. L'**informativa privacy** deve riportare i riferimenti del DPO (trasparenza e accountability)

Autorizzati ex Incaricato al trattamento

Non viene previsto in modo espresso la figura dell'**incaricato** ma non se ne esclude la presenza (Guida applicativa del Garante privacy) .

Le persone autorizzate al trattamento dei dati personali sono sotto l'autorità diretta del titolare o del responsabile (art. 4, n. 10 del Regolamento)



Nella **SCUOLA** possono essere designati incaricati del trattamento: docenti, assistenti amministrativi, collaboratori scolastici, ecc.

Principi cardine del GDPR

Privacy ovunque e comunque

L’ «Accountability»

Il principio di «**responsabilizzazione (Accountability)**» **del Titolare del trattamento** è il cardine del Regolamento GDPR.

Impone **l’adozione di politiche adeguate** derivanti dalla **valutazione del rischio** annesso al trattamento di dati personali, in termini di **tutela dei diritti e le libertà degli «interessati».**

IL GDPR: misure tecniche e organizzative

Per ottemperare agli obblighi del **GDPR,** all'**art. 25**, introduce il principio di privacy by design e privacy by default, un approccio concettuale innovativo che impone alle aziende l'obbligo di avviare un progetto prevedendo, fin da subito, gli strumenti e le corrette impostazioni a tutela dei dati personali:

A. **«Privacy by design»:** misure tecniche e organizzative messe in atto già **in fase di progettazione** dei sistemi informativi e dei mezzi per il trattamento dei dati.

B. **«Privacy by default»:** Il titolare del trattamento mette **in atto misure tecniche e organizzative adeguate** per garantire che, per impostazione predefinita, i dati personali siano resi accessibili dati personali ad un numero definito di soggetti interessati.

Privacy ‘by design’

L’utente è il centro del «sistema Privacy»:

Qualsiasi progetto, sia strutturale che concettuale, deve essere realizzato considerando, sin dalla sua implementazione (by design), nel rispetto della **riservatezza** e la **protezione dei dati personali**.

La Privacy by design contempla una trilogia di applicazioni:

1. sistemi informatici
2. pratiche amministrative corrette
3. progettazione strutturale e infrastrutture di rete

1. Privacy by design: sistemi informatici

1. Privacy by design: sistemi informatici

1. **Le Password per tutte le postazioni PC devono essere conservate**, in busta chiusa e custodite con riservatezza (*possibilmente non sotto la tastiera del computer*) - **oltre che dal singolo assistente amministrativo, anche dal DSGA.**

2. **Le Password devono essere modificate generalmente ogni 3 – 6 mesi.**

NB: nel caso in cui siano cedute temporaneamente ad altri utenti, devono essere modificate tempestivamente entro il giorno successivo, onde evitare un eventuale accesso abusivo al sistema informatico da parte di terzi non autorizzati. (ex art. 615 cod. penale)

1. Privacy by design: sistemi informatici

3. Si consiglia di avere **stampanti multifunzione separate**: una per la didattica ed una per la segreteria; di collocare la **multifunzione all'esterno degli uffici** di segreteria.

Quando questa dovesse essere allocata in una zona di passaggio e non vigilata fisicamente da un collaboratore scolastico, **per garantire la riservatezze dei documenti si consiglia di aver un apposito PIN** (unico per tutto l'ufficio di segreteria) e di digitarlo quando è fisicamente vicino alla stampante.

2. Privacy by design: pratiche amministrative

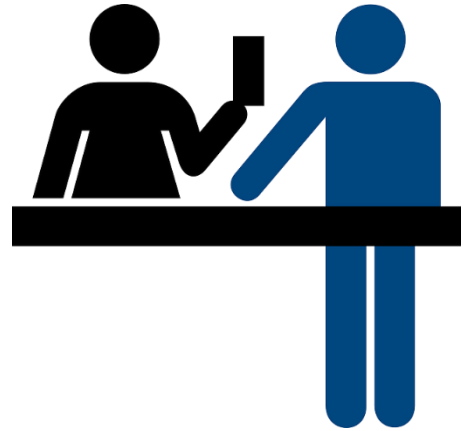
4. Archiviazione Fascicoli dati: con la **pseudonimizzazione** dei dati è garantita **la non identificazione del soggetto**, omettendo le informazioni sensibili e identificando i fascicoli con una lettera ed un numero, codice alfanumerico (**cifratura dei dati** personali)

5. Pulizia Uffici: si consiglia, ove possibile, di impiegare collaboratori scolastici, personale autorizzato e dipendente dello stesso titolare del trattamento, piuttosto che ricorrere al personale esterno (LSU)

6. Accesso Uffici: regolamentare l'accesso negli uffici di segreteria a professori e genitori con orari differenziati, nel rispetto della massima riservatezza.

3. Privacy by design: progettazione strutturale

7. Front Office: per disciplinare gli accessi presso le segreterie e garantire massima riservatezza sarebbe opportuno utilizzare un front office e delimitare con una linea segnaletica la distanza di sicurezza (es. ufficio postale).



8. Sistemi di Antifurto e Videosorveglianza

9. Grate alle finestre

10. Armadi chiusi a chiave

Privacy by default

Il principio di ***privacy by default*** stabilisce che, per impostazione predefinita, i **dati personali devono essere trattati soltanto in misura necessaria e sufficiente, allo scopo e per il periodo strettamente necessario.**

Occorre, dunque, progettare il sistema di trattamento di dati personali garantendo la **non eccessività delle informazioni raccolte**

Strumenti per garantire la «sicurezza»

Titolare e Responsabile del trattamento devono mettere in atto una serie di misure tecniche e organizzative volte a garantire il livello di sicurezza adeguato al rischio:

a. la **pseudonimizzazione** e la **cifratura dei dati** personali
b. la **capacità di assicurare, su base permanente,** la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento
c. la **capacità di ripristinare tempestivamente** la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico
d. una **procedura** per testare, verificare e valutare regolarmente **l'efficacia** delle misure tecniche e organizzative adottate, a garanzia di ogni eventuale distruzione, perdita, modifica, divulgazione non autorizzata oppure dall'accesso in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati e rischi annessi.

Le misure «adeguate» di sicurezza

Il **GDPR** ha spazzato via il requisito di **misure "minime" di tutela della Privacy** prevedendo che i titolari adottassero **misure «adeguate»** alla protezione dei dati - che tengano in dovuto conto:

- ✓ **della natura, dell'oggetto, del contesto e delle finalità del trattamento**
- ✓ **dei costi** di attuazione
- ✓ **del rischio** di varia probabilità e gravità per i diritti e libertà delle persone fisiche

La Documentazione prevista dal GDPR

Informative e consenso nella Scuola

La «GDPR Compliance»:cos'è

GDPR compliant è uno dei principi fondamentali, significa essere **«conformi al GDPR - Regolamento europeo per la protezione dei dati» -**, rispettarne i princìpi e adottare procedure organizzative e di sicurezza, verificando che anche tutta la catena dei responsabili sia *compliant*, dai titolari ai responsabili esterni, ovvero agisca con ***accountability*** (senso di responsabilità)

In particolare, il fornitore responsabile del trattamento ha **l'obbligo di conservare il registro dei trattamenti e le eventuali violazioni di dati.**

Informativa: art 13 e 14 GDPR

Il rapporto con gli interessati (alunni, famiglie, fornitori, personale dipendente) è disciplinato dalle **informative idonee per minori** **(art.13, e 14 del GDPR)**

Il titolare del trattamento DEVE SEMPRE specificare:

- ✓ i **dati di contatto del DPO** (Data Protection Officer);
- ✓ la **base giuridica** del trattamento,
- ✓ **qual è il suo interesse legittimo,** se quest'ultimo costituisce la base giuridica del trattamento
- ✓ **se trasferisce i dati personali in Paesi terzi** e **attraverso quali strumenti;**
- ✓ **il periodo di conservazione dei dati** e
- ✓ i criteri seguiti per stabilire tale periodo di conservazione;
- ✓ il diritto di **presentare un reclamo** all'autorità di controllo.

Informativa: art 14 GDPR

Nel caso di **dati personali non raccolti direttamente** presso l'interessato (art. 14 GDPR), l'informativa deve essere:

- ✓ fornita **entro un termine ragionevole che non può superare 1 mese** dalla raccolta, oppure **al momento della comunicazione** dei dati a terzi o all'interessato.
- ✓ **concisa, trasparente, intelligibile per l'interessato e facilmente accessibile**
- ✓ espressa in un linguaggio **chiaro e semplice, soprattutto se coinvolti minori**
- ✓ fornita per **iscritto e preferibilmente in formato elettronico**

Preferibile che gli interessati forniscano in qualche modo la prova di aver preso visione dell'informativa

Il «consenso» al trattamento dati

Il GDPR identifica 6 basi giuridiche della raccolta ed trattamento dei dati in Europa, dove non è necessario fornire **il consenso** per ognuno:

1. L'interesse vitale dell'individuo
2. L'interesse pubblico rilevante
3. L'esigenza contrattuale
4. La conformità a obblighi legali
5. Il consenso non ambiguo dell'individuo
6. L'interesse legittimo del titolare del trattamento

Il consenso: linee guida art 29 (WP259)

Il Consenso esplicito al trattamento dei dati non occorre per la stragrande maggioranza dei procedimenti. E' previsto invece il *diritto di opposizione* che la Pubblica Amministrazione può neutralizzare con adeguata motivazione

Il Dirigente scolastico può trattare i dati **SENZA CONSENSO**:

a. quando il trattamento dati interessa l'esecuzione di un contratto di cui l'interessato è parte (fornitori, esperti esterni, ecc)
b. per tutte le attività che è obbligato per legge ad effettuare
c. quando il trattamento è necessario alle finalità istituzionali (es. attività entro PTOF).

Il Dirigente scolastico NECESSITA DEL CONSENSO in tutti gli altri casi, ad es:

a. trattamento foto / video
b. trasmissione dati per scopo di inserimento in scuole di ordine superiore
c. attività di allocazione post-diploma
d. attività progettuali non riportate nel PTOF

Diritti degli interessati art 11 e 12

Il **termine** entro il quale il titolare deve dare un riscontro all'interessato è di **1 mese**, per tutti i diritti, incluso il diritto di accesso.

Termine estendibile fino a 3 mesi in casi di particolare complessità.

Il titolare deve fornire un riscontro all'interessato entro 1 mese dalla richiesta anche in caso di diniego.

La risposta fornita all'interessato deve essere non solo "intelligibile", ma anche **concisa, trasparente e facilmente accessibile**, espressa in un **linguaggio semplice e chiaro**.

Diritti degli interessati: art 11 e 12

E' opportuno che i titolari di trattamento adottino le **misure tecniche e organizzative eventualmente necessarie** per favorire **l'esercizio dei diritti e il riscontro alle richieste** presentate dagli interessati che dovrà avere forma scritta per impostazione predefinita (anche elettronica)

Diritto di «accesso» art 15: cosa cambia

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

Fra le informazioni che il titolare deve fornire **occorre indicare il periodo di conservazione** previsto o, se non è possibile, i criteri utilizzati per definire tale periodo, nonché le **garanzie** applicate **in caso di trasferimento dei dati verso Paesi terzi**.

Non rientrano invece tra gli obblighi le informazioni in merito alle modalità in cui viene effettuato il trattamento

Valutazione di Impatto

I rischi e la gestione del Data Breach
I registri del Trattamento

La «Valutazione dell'impatto» DPIA

il GDPR obbliga i titolari a svolgere una **valutazione di impatto DPIA (Data Protection Impact Assessment),** quando le attività in corso relative al trattamento dei dati possono determinare **rischio elevato** per i diritti e le libertà delle persone interessate, attraverso consultazione dell'Autorità di controllo, Garante Privacy.

La DPIA è una procedura di verifica dei rischi eventuali in cui incorre il Titolare del trattamento, in termini di violazione di diritti e libertà fondamentali, secondo i principi della privacy by design e privacy by default

Il registro del trattamento

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti, ma solo se non effettuano trattamenti a rischio *(si veda art. 30, paragrafo 5)*, devono tenere un **Registro delle operazioni di Trattamento**: **strumento fondamentale** ai fini dell'eventuale supervisione da parte del Garante, che consente di disporre di un quadro aggiornato dei trattamenti in essere all'interno della scuola, **indispensabile per ogni valutazione e analisi del rischio**.

Si aggiorna al mutare degli elementi essenziali, non si pubblica, deve essere stampato e protocollato

Il registro del trattamento

L'art. 30, quinto comma non si applica alle imprese o organizzazioni private con meno di 250 dipendenti a meno che:

- ✓ il trattamento **possa presentare un rischio per i diritti e le libertà dell'interessato;**
- ✓ il **trattamento non sia occasionale**;
- ✓ includa il **trattamento di categorie particolari di dati (art. 9.1), o relativi a condanne penali e a reati** (art. 10).

Il registro del trattamento

Non dovrebbe necessariamente trattarsi di un mero obbligo; **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.

Il registro del trattamento: il Titolare

Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolto per conto di un titolare del trattamento.

Tale registro contiene tutte le seguenti informazioni:

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;

b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;

c) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento ;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 .

La doppia anima del registro

Il registro svolge una doppia funzione:

- ✓ funge da "***strumento operativo di lavoro*** *(ex ante e durante)*
- ✓ *funge da* ***"documento probatorio (ex post) degli adempimenti***" prescritti dal Regolamento europeo in materia di protezione dei dati personali *"su richiesta il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare o del responsabile … mettono il registro a disposizione dell'autorità di controllo".*

  il registro sarà dettagliato, aggiornato e corrispondente all'organizzazione aziendale o delle pubbliche amministrazioni ai fini di una reale tutela della persona, delle sua libertà e della sua dignità.

Registri a confronto

Informazioni richieste	Titolare *art. 30(1)*	Responsabile *art. 30(2)*
a) Nome e **dati di contatto** del titolare, contitolare, rappresentanti del tit., DPO	X	*Nomi di contatto del responsabile e del titolare per conto del quale si agisce*
b) Finalità del trattamento	X	**No**
c) Categorie di interessati e dati personali	X	**No**
c) Categorie di trattamenti effettuati per il titolare	**No**	X
e) Trasferimenti verso **paesi terzi**	X	X
f) Termini per **cancellazione** dati	X	***No*** *(cfr. art. 28.3.g)*
g) Misure di sicurezza tecniche e organizzative	X	***Si*** *(cfr. art. 28.3.c)*

Registro ed altri adempimenti del GDPR

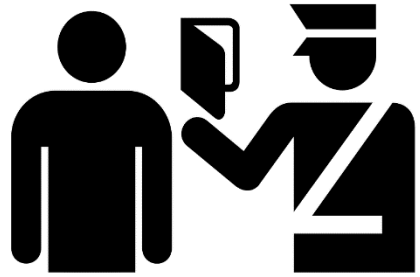
Il registro dei trattamenti costituisce uno strumento di lavoro che consente all'organizzazione di disporre di un **censimento dei trattamenti effettuati, delle relative finalità, degli interessati e delle categorie dei dati personali, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, di una descrizione generale delle misure di sicurezza tecniche e organizzative.**

La redazione dei registri dei trattamenti consente al titolare **di dimostrare quali misure ha utilizzato per garantire un livello di sicurezza adeguato al rischio e soprattutto che le misure sono state adottate.**

La redazione e l'aggiornamento dei registri dei trattamenti devono essere coordinati con gli altri adempimenti previsti dal regolamento privacy europeo (l'informativa privacy, la valutazione di impatto privacy, le istanze di consultazione preliminare; le comunicazioni delle violazioni di dati *"**data breach**")

Rischi e sanzioni

La violazione delle disposizioni dell'art. 30 rubricato:



"*Registri dei trattamenti*" del regolamento privacy europeo comporta significative sanzioni pecuniarie (**fino a euro 10.0000.000, o per le imprese fino al 2% del fatturato** mondiale totale annuo dell'esercizio precedente se superiore).

Misure di sicurezza e Rischi:

distruzione, perdita, modifica, divulgazione non autorizzata derivanti dall'accesso in modo accidentale o illegale

«Data breach»

I titolari del trattamento dovranno **documentare le violazioni** di dati personali subite e in alcuni casi notificarle all'autorità di controllo, indicando le relative circostanze, conseguenze e i provvedimenti adottati *(art. 33, paragrafo 5); devono poter* fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

Tipologie:

- ✓ Notifica - comunicazione delle violazioni all' autorità di controllo (autorità Garante privacy) art. 33
- ✓ Notifica -comunicazione delle violazioni all'interessato art. 44

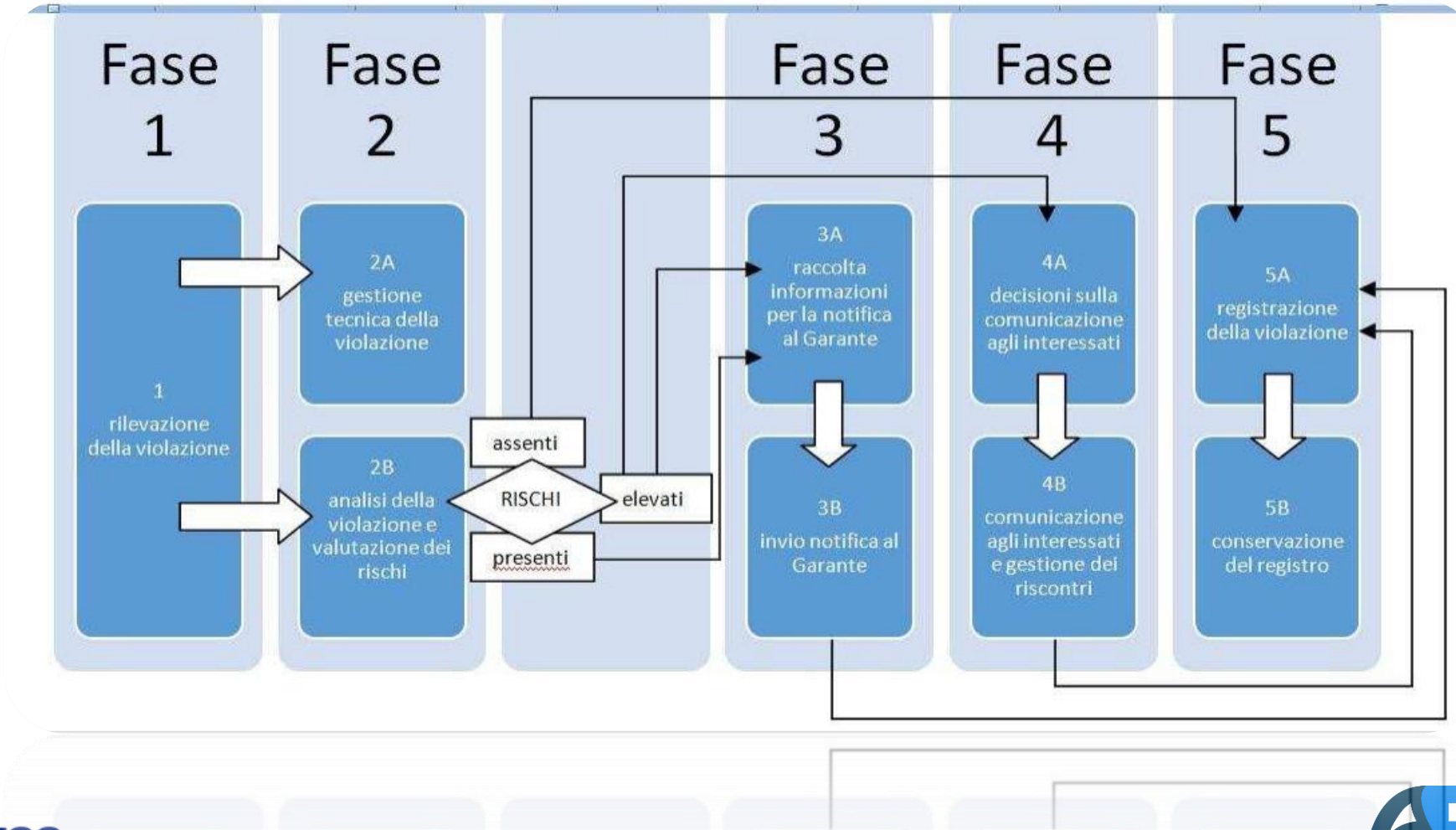
Data breach e valutazione del rischio

La notifica all'autorità dell'avvenuta violazione **non è obbligatoria**, ma subordinata **alla valutazione del rischio per gli interessati** che spetta, ancora una volta, al titolare: il rischio di pregiudizio per i diritti e le libertà degli interessati è probabile o non è probabile? Se è probabile, si è in presenza di una violazione e dunque occorre attivare la procedura legata al «*data breach*» nei confronti degli interessati e l'autorità Garante.

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

Guida applicativa Garante privacy

Operatività in caso di **Data breach**



Esempi di Data breach

- Data Breach senza rischi e conseguenze :

Tizio assistente amministrativo invia nella chat privata di gruppo di tutto l'apparato amministrativo un file contenente il proprio certificato medico, all'istante si rende conto dell'errore commesso ed elimina il file per tutti quando ancora nessuno lo aveva visualizzato

In questo caso non ci sono state conseguenze ne rischi in quanto è stata una violazione semplice che è stata risolta nel giro di un arco di tempo breve e inoltre senza la diffusione di alcun dato particolare e quindi la violazione, se a conoscenza del dirigente scolastico, deve solo essere iscritta nel registro delle violazioni con conseguente protocollazione , senza la comunicazione al Garante.

Esempi di Data breach

Data breach con rischi presenti:

L'assistente amministrativo Tizio carica sul sito istituzionale, una circolare con all'interno la data l'ora dell'incontro di una riunione per tutto l'apparato amministrativo contenente altresì la data di nascita di 2 a.a. che sono omonimi con i relativi numeri di cellulare;

In questo caso abbiamo un data breach di 2 livello perché:

- Abbiamo un riferimento a dati particolari (data di nascita e numero di cellulare) ;
- Non è previsto che una circolare per un incontro debba detenere questi dati;
- È stato caricato il file erroneamente nella homepage del sito istituzionale

Il Dirigente ordina la cancellazione del file ma nonostante ciò i rischi ci sono (diffusione di dati particolari) per questo si deve operare con notifica al Garante (entro e non oltre le 72 ore successive all'accadimento) e compilazione del registro delle violazioni.

Esempi di Data breach

Data breach con rischi elevati presenti:

L'assistente amministrativo Tizio carica sul sito istituzionale, erroneamente, una circolare con all'interno i dati riferiti ad un a.a. che ha un trattamento particolare, ovvero orario ridotto, per la patologia del quale soffre e quindi per la normativa prevista vigente (l.104), dopo circa un'oretta si rende conto dell'errore ed elimina il file.

In questo caso abbiamo un data breach di 3 livello perché:

- Caricamento di un file che non doveva essere diffuso ;
- Diffusione di dati sanitari erroneamente;

Il Dirigente, pur se il file è stato cancellato, sa che ci sono stati rischi e sono anche elevati (diffusione di dati sanitari) per questo si deve operare con notifica al Garante (entro e non oltre le 72 ore successive all'accadimento), devono essere informati gli interessati i quali dati sono stati diffusi attendendo le eventuali azioni di risarcimento e compilazione del registro delle violazioni.

Operatività in caso di **Data breach**

Data breach (b)

Notifica di una violazione dei dati personali all'autorità di controllo (art. 33)

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la **violazione all'autorità di controllo competente a norma dell'art 55** senza ingiustificato ritardo **e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza.** Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
2. Il responsabile esterno del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

Contenuto del Data Breach all'Autorità (1)

Contenuto della Notifica di una violazione dei dati personali all'autorità di controllo:

1. **descrivere la natura della violazione dei dati personali** compresi, ove possibile e appropriato, le **categorie e il numero di interessati approssimativi** in questione nonché le categorie e il numero approssimativo di registrazioni dei dati in questione;
2. **comunicare il nome e i dati di contatto del responsabile della protezione dei dati** o di altro punto di contatto presso cui ottenere più informazioni
3. descrivere le possibili conseguenze della violazione dei dati personali;
4. **descrivere le misure adottate o di cui si propone l'adozione da parte del responsabile del trattamento** per porre rimedio alla violazione dei dati personali; e, anche se del caso, per attenuare i possibili effetti pregiudizievoli della violazione dei dati personali. **(art.33)**

Data Breach all’interessato (a)

Articolo 34: Comunicazione di una violazione dei dati personali all'interessato

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un **linguaggio semplice e chiaro** la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d):

- comunicare il nome e i **dati di contatto del responsabile della protezione dei dati** o di altro punto di contatto presso cui ottenere più informazioni
- **descrivere le possibili conseguenze della violazione dei dati personali;**
- descrivere le misure adottate o di cui si propone l'adozione da parte del responsabile del trattamento per porre rimedio alla violazione dei dati personali; e, anche se del caso, per attenuare i possibili effetti pregiudizievoli della violazione dei dati personali.

Data Breach all’interessato (b)

Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, **quali la cifratura** (la cifratura è quel processo di convertire i dati originali in un formato che non possa essere comunemente riconosciuto.

I dati così trasformati vengono detti “cifrati”).

a) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;

b) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Data Breach all’interessato (c)

Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, **l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, c**he vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta. (art. 34)

Il registro delle violazioni

Tutti i titolari di trattamento dovranno 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)*; tale obbligo non è diverso, nella sostanza, da quello attualmente previsto dall'art. 32-bis, comma 7, del Codice Privacy.

Si raccomanda, **pertanto, ai titolari di trattamento di adottare le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti**

Il registro delle violazioni

Tutte le violazioni vanno annotate nel registro delle violazioni di cui all'articolo 33 comma 5 del Regolamento e notificate prontamente al Garante se vi è un rischio per diritti e libertà fondamentali (entro 72 ore, sono violazioni della sicurezza che comportano accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati)**. In alcuni casi va fatta anche comunicazione agli interessati (no se misure adeguate e se ci sono rischi minori e se comunicazione sproporzionata).**

Principi cardine del GDPR

Pagina Privacy sito web

Pagina Privacy sito web

Il sito web scolastico deve avere la Pagina Privacy. Se questa pagina web non è presente deve essere creata;

la pagina Privacy deve essere raggiungibile mediante un link presente nel footer, ovvero nella parte bassa della home del sito istituzionale, in modo tale da essere sempre visibile durante la navigazione.

All'interno della pagina privacy devono essere inseriti i dati del:

-Titolare del Trattamento;

- I dati del DPO;

Pagina Privacy sito web

- Documenti:

- contratto e nomina DPO,
- Comunicazione del Nominativo del DPO al Garante,
- Cokkie Policy,
- Organigramma Funzionale,
- Informativa sul trattamento dei dati Personali
- Diritto all'oblio (art.17 GDPR) si intende il diritto del titolare dei dati, resi pubblici, di richiederne la cancellazione. Richiesta che deve essere inoltrata a tutti gli utilizzatori dei dati in oggetto.

Ogni qualvolta che cambieranno le informazioni l'Istituto provvederà ad aggiornare la documentazione come sopra descritta.

Pagina Privacy sito web

- Esercizio dei Diritti:

La possibilità e il modus operandi per gli interessati di far richiesta all' Isitituto della cancellazione, trasformazione in forma anonima o il blocco dei dati trattati senza consenso, nonché di opporsi per qualsiasi motivo legittimo al trattamento dati posto in essere

dallo stesso Istituto.

Proprio per questo all'interno della sezione Privacy

- devono essere indicati:
- Dirigenza ed Uffici amministrativi (indirizzo)
- Telefono scuola
- Mail scuola
- Form di contatto

GDPR
E
SITO WEB

Pagina Privacy sito web

Ancora devono essere inseriti tutti i modelli delle informative (ex GDPR 679/2016) dei trattamenti dati con la possibilità per i visitatori del sito di poterle scaricare:

- Informativa alunni/genitori, Informativa fornitori, Informativa dipendenti, Informativa didattica a distanza, Informativa lavoro agile, Informativa MAD, Informativa e comunicazione alunni Fragili.

- Riferimenti utili:

- **(conservazione_archivi)**
- **(Regolamento UE 679/16)**
- **(Informativa Invalsi)**

Il GDPR nella SCUOLA

La Formazione

La Formazione

Articolo 29: Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento.

Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali **non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri**

Nel caso di mancata formazione scatta la sanzione amministrativa prevista da art. 83 del regolamento

La Formazione

Il Regolamento privacy europeo 679/16 (GDPR) prevede **l'obbligo della formazione per le Pubbliche Amministrazioni ed imprese** in materia di protezione dei dati personali per tutte le figure presenti nell'organizzazione (sia dipendenti che collaboratori).

La formazione dovrebbe essere finalizzata ad illustrare i rischi generali e specifici dei trattamenti di dati, le misure organizzative, tecniche ed informatiche adottate, nonché le responsabilità e le sanzioni.

La mancata formazione è motivo sanzionatorio

Il GDPR nella Scuola

La protezione dei dati personali/privacy non può declinarsi a mero adempimento burocratico tecnico-normativo ma costituisce, anche all'interno della scuola, una condizione essenziale per il rispetto e la dignità delle persone, della loro identità.

Le scuole trattano per le proprie finalità istituzionali di istruzione una mole impressionante di dati (sia dati identificativi sia dati particolari ex sensibili) relativi agli studenti ai dipendenti alle famiglie e ai fornitori.

Il GDPR nella Scuola

- le scuole come enti pubblici "devono fornire agli studenti e alle famiglie un' idonea, adeguata e preventiva **informativa privacy**: devono pertanto descrivere quali dati saranno raccolti e come saranno trattati.

- le scuole come enti pubblici non sono tenute a richiedere il **consenso scritto** al trattamento dei dati ma sono tenute a effettuare esclusivamente le operazioni di trattamento di dati necessarie al perseguimento delle specifiche finalità istituzionali o di quelle previste dalle normative di settore.

La Scuola e i dati

Le piattaforme informatiche :

- ✓ **SIDI MIUR**
- ✓ **PROTOCOLLAZIONE**
- ✓ **REGISTRO ELETTRONICO**

Altre tipologie di dati:

- ✓ **Sistemi di rilevazioni presenze**
- ✓ **Videosorveglianza**
- ✓ **Esperti esterni (RSPP, Sportello ascolto)**

I contratti con le terze parti

I contratti e i dati :

- ✓ **Dati in cloud o presso terzi**
- ✓ **Contratti di assistenza tecnica e sistemistica**
- ✓ **Mensa**
- ✓ **Agenzia di viaggi**
- ✓ **Trasporti**

Pubblicazione dati su WEB

Per pubblicare sul web dobbiamo riferirci ad una **norma di legge o di regolamento che lo consenta** (ad es. trattamento temporaneo finalizzato esclusivamente alla pubblicazione o diffusione occasionale di articoli, saggi e altre manifestazioni del pensiero anche nell'espressione artistica art. 136 c. 1 lett. c Dlgs 196/2003 modificato ed integrato dal D.Lgs. 101/2018)**, solo per gli scopi istituzionali dell'ente.**

Stesso criterio **per foto e video**, **comunicati o diffusi in qualunque altra modalità (informativa, motivazione, principio di necessità, riferimenti normativi)**

Il GDPR nella SCUOLA

La Videosorveglianza

Videosorveglianza

L'attività di videosorveglianza è stata sempre considerata invasiva proprio per questo motivo è stata sempre oggetto di regolamentazione da parte del Garante della Privacy, infatti sono stati imposti requisiti stringenti al fine di evitare che l'impiego massivo dei dispositivi di ripresa possa espandersi fino a limitare i diritti di riservatezza del cittadino e nel caso della scuola degli studenti e del personale. Sul tema sono poi intervenuti il Codice in materia di protezione dei dati personali (art.114), che afferma che *la videosorveglianza deve rispettare quanto sancito dall'art.4 dello Statuto dei Lavoratori*, e il Comitato Europeo per la protezione dei dati personali, che avvalora quanto già espresso circa l'uso della videosorveglianza mediante le Linee guida n. 3/2019.

Videosorveglianza

In un istituto scolastico è possibile installare le telecamere per prevenire furti ed atti vandalici.

Ovviamente però deve essere rispettata la normativa in tema di privacy infatti il Garante nel 2020 ha emanato delle FAQ che rispondono in modo esaustivo a tutte le domande sul tema.

Videosorveglianza e scuola

Secondo quanto stabilito dal Garante, gli istituti possono installare e utilizzare videocamere di sorveglianza (***purché in grado di garantire il diritto alla riservatezza di ogni studente***) nel caso in cui ciò risulti indispensabile al fine di tutelare l'edificio e i beni in esso contenuti da atti vandalici e furti, circoscrivendo tuttavia le riprese alle sole aree interessate.

L'installazione dell'impianto di videosorveglianza da parte della scuola appare pertanto lecita solo se avvalorata da una **concreta esigenza di prevenire situazioni di pericolo** sorte a seguito di episodi di furto o atti vandalici già verificatisi o, in alternativa, nel caso in cui la scuola custodisca beni di valore quali strumentazione informatica o somme di denaro.

Le riprese devono tuttavia risultare circoscritte alle sole aree interessate da furti o atti vandalici, e la presenza delle telecamere deve essere al contempo opportunamente e chiaramente segnalata da un'apposita cartellonistica.

Autorizzazioni per la videosorveglianza a scuola: quali aree possono essere riprese?

Secondo quanto stabilito dal Garante della Privacy le **aree** che a scuola possono essere riprese sono solo quelle **esterne** adiacenti all'Istituto anche in orario scolastico purchè non risultino pertinenti all'edificio.

Al contrario, le **aree interne** della scuola possono essere oggetto di riprese solo ed esclusivamente **negli orari di chiusura**, e non dunque durante l'ordinario svolgimento delle attività scolastiche o extrascolastiche.

Il Garante appare particolarmente attento nella gestione dei sistemi di videosorveglianza: questo poiché uno scorretto utilizzo delle telecamere può comportare un'ingerenza ingiustificata nella vita del soggetto, con conseguente violazione dei diritti e delle libertà fondamentali.

Tutte le prescrizioni indicate per l'installazione di sistemi di videosorveglianza presso gli istituti scolastici sono pertanto finalizzate a garantire "il diritto dello studente alla riservatezza"

Videosorveglianza e scuola: tempi di conservazione dei dati

Ulteriore tematica che merita un approfondimento è la conservazione dei dati personali, così come del materiale registrato mediante videosorveglianza, che ai sensi del **GDPR** deve avvenire per un tempo non superiore al conseguimento delle finalità per le quali i dati raccolti sono trattati.

In tal senso il Garante della Privacy, ha specificato che *"le immagini registrate non possono essere conservate più a lungo di quanto necessario per le finalità per le quali sono acquisite", e che "spetta al titolare del trattamento individuare i tempi di conservazione delle immagini, tenuto conto del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche"*.

Ha inoltre affermato che *"tenendo conto dei **principi di minimizzazione** dei dati e **limitazione della conservazione**, i dati personali dovrebbero essere – nella maggior parte dei casi (ad esempio se la videosorveglianza serve a rilevare atti vandalici) – cancellati dopo pochi giorni, preferibilmente tramite meccanismi automatici. Quanto più prolungato è il periodo di conservazione previsto (soprattutto se superiore a 72 ore), tanto più argomentata deve essere l'analisi riferita alla legittimità dello scopo e alla necessità della conservazione".*

Videosorveglianza: Obblighi del titolare

Il titolare del trattamento deve :

1. documentare per iscritto le ragioni delle scelte effettuate, le soluzioni operative adottate e i motivi che le giustificano.
2. informare della presenza delle telecamere tramite un'apposita informativa privacy;

L'informativa in questo caso può essere rappresentata da un modello semplificato, o in alternativa da un semplice cartello, che tuttavia deve contenere:

- le indicazioni sul titolare del trattamento

- La finalità perseguita.

L'informativa deve essere adattata a specifiche circostanze o contesti quali la presenza di più telecamere, la vastità dell'area oggetto di rilevamento o le modalità delle riprese, inoltre deve essere collocata in maniera visibile in prossimità o nelle immediate vicinanze della zona sorvegliata. Non è necessario rivelare la precisa ubicazione della telecamera, purché non vi siano dubbi su quali zone siano soggette a sorveglianza e sia chiarito in modo inequivocabile il contesto della sorveglianza stessa. L'interessato deve poter comprendere in modo chiaro quale zona sia coperta dalla telecamera a scuola, in modo da evitare la sorveglianza o adeguare il proprio comportamento, ove necessario.

Videosorveglianza: Obblighi del titolare

3. Deve iscrivere all'interno del registro del titolare del trattamento la presenza delle stesse;

4. Deve nominare per iscritto tutti i soggetti che in suo nome e conto abbiano facoltà di trattare le immagini (ritenute al pari dei dati personali) raccolte mediante impianti di videosorveglianza a scuola. Essi non sono altro che soggetti interni alla scuola che hanno accesso alle immagini e ai locali dove sono situate le postazioni di controllo o, in alternativa, i responsabili del trattamento che, secondo quanto stabilito dall'art. 28 del GDPR, sono quei soggetti esterni che hanno accesso alle immagini, quali ad esempio le società che si occupano dell'impianto di videosorveglianza e della relativa manutenzione.

Videosorveglianza: Obblighi del titolare valutazione d'impatto

Non è espressamente previsto che il titolare del trattamento ponga in essere una valutazione d'impatto prima dell'installazione delle telecamere, ma qualora il trattamento dei dati personali preveda in particolare l'uso di nuove tecnologie, quali ad esempio sistemi integrati – sia pubblici che privati – che collegano telecamere tra soggetti diversi, nonché sistemi intelligenti capaci di analizzare le immagini ed elaborarle, in quest'ultimo caso la Valutazione d'impatto preventiva risulta necessaria. Sull'argomento c'è dubbia risposta, infatti in caso di sorveglianza sistematica su **larga scala** di una zona accessibile al pubblico, come stabilito dall'art. 35, par. 3, lett. C del Regolamento Europeo, la valutazione risulta necessaria: Relativamente al concetto di "**larga scala**", è necessario specificare che il GDPR non ne dà alcuna definizione, ma aiuta semplicemente a delinearne i contorni, recitando che *"i trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato"*.

Ciascun istituto installa generalmente una sola videocamera di sorveglianza che copre un'area limitata e circoscritta, e pertanto non effettua trattamenti su larga scala. Pur non sembrando necessaria, la valutazione d'impatto rimane tuttavia altamente consigliata anche in questi casi.

Videosorveglianza e scuola: documentazione necessaria

Prima dell'Istallazione effettiva delle telecamere Il Titolare del Trattamento deve predisporre di tutti i documenti previsti dal Garante ovvero:

1. Accordo con RSU;
2. Regolamento da far approvare al Consiglio d'Istituto;
3. Informativa (modello semplificato): esposizione 'Cartello Videosorveglianza';
4. Informativa estesa;
5. Nomina qualora ci siano ulteriori autorizzati al trattamento delle immagini delle telecamere;
6. Iscrizione del Trattamento all'interno del Registro del Titolare

Il GDPR nella SCUOLA

Regole generali Scuola & Privacy

Regole generali Scuola e privacy

1) Esiti scolastici
2) Comunicazione di dati
3) Cellulari, foto e video
4) Alternanza Scuola-Lavoro
5) Sportello Ascolto
6) Pubblicazione sul sito web

Voti, scrutini, esami di Stato

In relazione alla questione della pubblicazione degli scrutini on line, l'Autorità garante per la protezione dei dati personali sentita dall'ANSA, chiarisce che a ''differenza delle tradizionali forme di pubblicità degli scrutini - che oltre ad avere una base normativa consentono la tutela dei dati personali dei ragazzi - la pubblicazione online dei voti costituisce una forma di diffusione di dati particolarmente invasiva, e non coerente con la più recente normativa sulla privacy''. Per questo sostanzialmente il Garante è d'accordo, con la linea del Miur di indicare l'ammissione degli studenti soltanto sul registro elettronico.

Una volta esposti, infatti, i voti rischiano di rimanere in rete per un tempo indefinito e possono essere, da chiunque, anche estraneo all'ambito scolastico, e per qualsiasi fine, registrati, utilizzati, incrociati con altri dati presenti sul web, determinando in questo modo una ingiustificata violazione del diritto alla riservatezza degli studenti, che sono in gran parte minori, con possibili ripercussioni anche sullo sviluppo della loro personalità, in particolare per quelli di loro che abbiano ricevuto giudizi negativi.

La necessaria pubblicità agli esiti scolastici - conclude il Garante - può essere peraltro realizzata, senza violare la privacy degli studenti, prevedendo la pubblicazione degli scrutini non sull'albo on line, ma, utilizzando altre piattaforme che evitino i rischi sopra evidenziati''.

Voti, scrutini, esami di Stato

- L'Ordinanza Ministeriale n. 53/2021 prevede (art.3 comma 2) che l'esito della valutazione è reso pubblico tramite affissione di tabelloni presso l'istituzione scolastica, nonché, distintamente per ogni classe, solo e unicamente nell'area documentale riservata del registro elettronico, cui accedono gli studenti della classe di riferimento, e riporta il voto di ciascuna disciplina e del comportamento, il punteggio relativo al credito scolastico dell'ultimo anno e il credito scolastico complessivo, seguiti dalla dicitura "ammesso".

- Per gli studenti esaminati in sede di scrutinio finale, i voti attribuiti in ciascuna disciplina e sul comportamento, nonché i punteggi del credito sono riportati nei documenti di valutazione e nel registro dei voti. Per quanto concerne le altre classi è necessario comprendere che l'ultimo punto da cui partire è la famosa nota n 9168 del 9 giugno 2020 che integra la precedente nota n. 8464 nella quale il Ministero dell'Istruzione indica un unico schema di pubblicazione, nel caso di "Pubblicità degli esiti degli scrutini delle classi intermedie delle scuole di ogni ordine e grado". Nella nota si ribadisce che "In tutti i casi la pubblicazione degli esiti degli scrutini non deve riportare informazioni che possano identificare lo stato di salute degli studenti o altri dati personali non pertinenti"; inoltre nella stessa è fatto chiaro che deve essere presente: " ... la sola indicazione per ciascun studente "ammesso" e "non ammesso", pubblicati, distintamente per ogni classe, nell'area documentale riservata del registro elettronico, cui accedono tutti gli studenti della classe di riferimento; diversamente i voti in decimi, (compresi quelli inferiori a sei decimi per le classi intermedie di ogni ordine e grado) riferiti alle singole discipline, sono riportati, oltre che nel documento di valutazione, anche nell'area riservata del registro elettronico a cui può accedere il singolo studente mediante le proprie credenziali personali;

- Il consiglio è di prediligere la pubblicazione attraverso il solo registro elettronico e valutare il "Tabellone cartaceo" all'interno dell'Albo fisico della scuola.

In sintesi:

- Sul Tabellone cartaceo → Voto, voto di condotta, crediti scolastici
- Area documentale Registro Elettronico (cui accedono tutti gli studenti della classe di riferimento) → Ammesso /Non ammesso
- Area personale dello studente sul Registro Elettronico (a cui può accedere il singolo studente mediante le proprie credenziali personali) → Voto

Pubblicazione esiti scolastici di diversamente abili

Ordinanza ministeriale 10 marzo 2008:

Presso gli albi di istituto (registro elettronico) devono comparire gli elenchi di tutti i candidati, compresi i portatori di handicap, con la sola indicazione "esito positivo" o "esito negativo" e della relativa menzione della lode. *L'eventuale indicazione dello svolgimento delle prove differenziate per i soggetti diversamente abili deve essere indicato solo nell'attestazione (nell'area personale) e non nel tabellone dei risultati*.

- Soluzione che valorizza la tutela degli interessi degli alunni disabili e anche le esigenze di trasparenza degli esiti finali degli esami di Stato (relazione Garante 2009; pag. 78).

Comunicazione di dati per attività di orientamento

Al fine di effettuare adeguate iniziative di **orientamento** per l'iscrizione alla scuola secondaria superiore, l'istituto richiede alle scuole secondarie di primo grado la **trasmissione dei dati personali** degli studenti delle terze classi.

Le scuole di istruzione secondaria, su richiesta degli interessati, possono comunicare e diffondere, anche a privati e per via telematica, dati relativi agli esiti scolastici, intermedi e finali, degli studenti e altri dati personali diversi da quelli sensibili o giudiziari, pertinenti "al *fine di agevolare l'orientamento, la formazione e l'inserimento professionale"* (cfr. art. 96 codice Privacy e confermato dal D.Lgs. 101/2018);

attività di orientamento può essere svolta dagli istituti anche attraverso la distribuzione e consultazione di *materiale informativo* disponibile presso le scuole. (es. Open Day)

Utilizzo Cellulari, foto e video in classe

L'uso dei cellulari è disciplinato nel rapporto scuola-alunno/famiglia attraverso la sottoscrizione del **Patto Educativo di Corresponsabilità.**

Gli apparecchi, smartphone, che consentono la registrazione di video o di audio o che effettuano **fotografie in ambito scolastico sono consentiti**, per professori e studenti, **solamente se rientrano nei fini didattici** e solamente se il Regolamento di Istituo permette tale possibilità (Corte Cassazione 14270/2022)

→ ad es: uno studente potrà registrare la lezione per migliorare il proprio apprendimento sulla materia, ma non potrà pubblicare o diffondere la registrazione, sia essa audio o video, senza il consenso del professore.

Utilizzo di foto e video a scuola

Foto e video **possono essere diffuse sul sito istituzionale,** bacheche all'interno della classe e dell'Istituto e/o su pubblicazioni della scuola senza la richiesta del consenso se la pubblicazione avviene per finalità istituzionali, anche se solo temporaneamente caricate, se i progetti didattici, di formazione o di orientamento a cui fanno riferimento sono indicati nel **PTOF** e **legati alla vita della scuola.**

Per qualsiasi altra pubblicazione di foto o video è necessario il consenso esplicito di chi esercita la potestà, se tratta di minori.

Utilizzo di foto e video a scuola

Il Regolamento UE 2016/679 – GDPR e D. Lgs. 196/2003 – Codice Privacy)definisce:

- le immagini e la voce sono informazioni che permettono l'identificazione diretta della persona interessata e sono pertanto da considerare "dati personali" a tutti gli effetti;
- costituisce "trattamento di dati" qualsiasi operazione compiuta con o sui dati personali (come ad esempio la raccolta, la conservazione, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, ecc.);
- anche la sola registrazione di video o foto che riprendono persone identificabili si configura come un "trattamento di dati personali", come tale assoggettabile alla citata normativa.

Se invece le riprese ovvero le foto non vengono eseguite dai genitori ma dal personale scolastico?

- In questo caso viene a mancare una delle quattro condizioni sopra elencante e per questo motivo lo scenario si presenta in modo nettamente differente:

- le riprese vengono verosimilmente effettuate in un contesto “chiuso”, che cioè non prevede la presenza di soggetti esterni all’amministrazione scolastica (genitori e parenti degli alunni, visitatori, ecc.);

- è cambiata la qualità del soggetto che effettua le riprese (egli ha responsabilità del tutto diverse da quella genitoriale e quindi non può decidere per il minore);

- è cambiata la finalità perseguita (non è più di tipo “personale” ma è semmai configurabile come “istituzionale”, “professionale”, “promozionale”, “motivazionale”, ecc.);

- i dati personali raccolti non sono destinati a circolare in un ambito “familiare o amicale” (con ogni probabilità, essi costituiranno oggetto di comunicazione o diffusione mediante trasmissione telematica).

Utilizzo di foto e video **senza consenso**

Illecito civile: nel caso in cui la pubblicazione dell'immagine di un minore avvenga senza il consenso dai genitori, gli stessi possono richiedere al Tribunale la rimozione dell'immagine e/o video all'autore o al gestore.

Azione Risarcitoria: se la pubblicazione delle immagini ha provocato un danno, anche morale, il soggetto o i genitore, se minore, possono richiederne il risarcimento

Trattamento illecito di dati (ex art.167 D.lgs.196/2003 adeguato al Codice Privacy D.lgs. 101/2018)**:** se le immagini sono utilizzate per trarne un vantaggio economico, profitto o di arrecare un danno agli interessati, procedendo in violazione al trattamento lecito di dati personali, se dal fatto deriva un vantaggio o, se il fatto consiste nella comunicazione o diffusione di dati personali, è punito con la reclusione da 6 a 24 mesi.

Reato di diffamazione (ex art. 595 c.p.): se la pubblicazione dell'immagine o del video offende o venga lesa la reputazione di un soggetto di chi vi è ritratto, si risponde del reato di diffamazione aggravata e si rischia la pena della reclusione da 6 mesi a 3 anni più multa non inferiore a 516 €

L’alternanza scuola-lavoro

L’alternanza scuola-lavoro si effettua sulla base di una convenzione (quindi rapporto contrattuale) fra i due titolari (Ente ospitante e scuola). Il trattamento dei dati avviene sulla base di tale rapporto (che legittima la scuola a fornirli e l’ente a gestirli). Fra questi dati vi sono quelli relativi agli studenti e dei docenti tutor. Quindi l’Ente ospitante non deve chiedere altro titolo di legittimazione al trattamento. Ciò detto la Scuola invece deve chiedere il consenso agli alunni (in quanto non fanno parte del rapporto contrattuale) mentre il docente tutor non può esprimere dissenso in quanto soggetto autorizzato ed obbligato in base al proprio rapporto di sevizio con la scuola stessa.

Servizio ascolto (psicologo esperto)

Il consenso del titolare della responsabilità genitoriale non dovrebbe essere necessario nel quadro dei servizi di prevenzione o di consulenza, forniti direttamente ad un minore, tenuto conto che la psicologa è vincolata al rispetto del Codice Deontologico degli Psicologi italiani ed è pertanto tenuta al segreto professionale.

Tuttavia, poiché durante la sua attività - finalizzata al benessere psicologico, al sostegno della crescita e maturazione personale ed al sostegno emotivo/affettivo, all'orientamento nei rapporti con i compagni, con i docenti e i genitori e costituisce un momento qualificante di ascolto e di sviluppo di una relazione di supporto - potrebbe venire a conoscenza di informazioni afferenti alla sfera familiare e quindi per un processo di responsabilizzazione, **si rende opportuno in ogni caso richiedere il consenso dei genitori.**

Account per le Piattaforme

In conformità alle linee guida del Piano Nazionale per Scuola Digitale, la scuola può creare un dominio@nomescuola.edu.it associato alla piattaforma **G-Suite for Education** o **Ms Office365,** spazi di conservazione conformi alla normativa sul trattamento dati.

L'utilizzo degli account personali del personale scolastico, alunni, genitori - cognomenome@nomescuola.edu.it, allo scopo di aumentare ulteriormente il livello di sicurezza e di privacy, permetterà l'accesso alla piattaforma.

Pubblicazione Graduatorie: come vanno pubblicate?

Per il Garante è possibile pubblicare le graduatorie poiché 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. **Non bisogna, invece, provvedere alla pubblicazione dei numeri di telefono e degli indirizzi privati dei candidati.** Quindi dopo aver verificato la sussistenza dell´obbligo di pubblicazione dell´atto o del documento nel proprio sito web istituzionale, il soggetto pubblico deve limitarsi a includere negli atti da pubblicare solo quei dati personali realmente necessari e proporzionati alla finalità di trasparenza perseguita nel caso concreto. Se sono dati particolari (ossia idonei a rivelare ad esempio l´origine razziale ed etnica, le convinzioni religiose, le opinioni politiche, l´adesione a partiti o sindacati, lo stato di salute e la vita sessuale) o relativi a procedimenti giudiziari, i dati possono essere trattati solo se indispensabili, ossia se la finalità di trasparenza non può essere conseguita con dati anonimi o dati personali di natura diversa.

Il caso: Pubblicazione di una circolare interna con dati particolari (Riferimenti a dati sanitari)

E' stato presentato reclamo al Garante per la pubblicazione, sul sito istituzionale del Liceo Statale nonché sul portale "CLASSEVIVA" utilizzato dall'Istituto anche con funzionalità di registro elettronico, di una circolare riguardante le ferie estive dei collaboratori scolastici recante, un prospetto del piano ferie che riportava, in corrispondenza del nominativo di più collaboratori, il riferimento alla fruizione dei benefici derivanti dalla legge 5 febbraio 1992, n. 104 e, in particolare, l'indicazione "104". La situazione è stata oggetto di decisione da parte del Garante, considerando che le pubblicazioni del piano ferie del personale avvengono normalmente nell'ambito dell'area ad accesso riservato del registro elettronico, nel caso specifico, del Liceo sul portale "CLASSEVIVA". Ciascun lavoratore dispone di credenziali di accesso che gli consentono di prendere visione della bacheca digitale interna, nella quale vengono pubblicate le comunicazioni di valenza interna ed ogni altro documento di valore organizzativo.

Il caso: Pubblicazione di una circolare interna con dati particolari (Riferimenti a dati sanitari)

Ciascuna comunicazione viene indirizzata esclusivamente al lavoratore o alla categoria interessata dalla comunicazione stessa"; in questo caso invece essendo stato pubblicato il tutto sul registro generale si è avuta una violazione;

L'istituto si è giustificato dicendo che è stato un mero errore materiale e che lo stesso dirigente non era a conoscenza della situazione prima del reclamo presentato al Garante, infatti dal momento che lo ha saputo ha subito eliminato il file erroneamente caricato.

Il caso: Pubblicazione di una circolare interna con dati particolari (Riferimenti a dati sanitari)

Ma comunque il Garante applicando la normativa vigente ovvero artt. 5, 6 e 9 del Regolamento e 2-ter e 2 sexies nonché 2-septies, comma 8, del Codice ha ritenuto che c'è stata una diffusione di dati particolari non autorizzata infatti i dati relativi alla salute, ossia quelli "attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute" (art. 4, par. 1, n. 15, del Regolamento; cfr. anche cons. 35 dello stesso), in ragione della loro particolare delicatezza, "non possono essere diffusi", Il datore di lavoro, titolare del trattamento, è, in ogni caso, tenuto a rispettare i principi generali in materia di protezione dei dati personali (art. 5 del Regolamento) e deve trattare i dati mediante il personale "autorizzato" e "istruito" in merito all'accesso e al trattamento dei dati. Per la violazione commessa l'Istituto è stato punito con sanzione amministrativa prevista dall'art. 83, par. 5, del Regolamento, ai sensi degli artt. 58, par. 2, lett. i), e 83, par. 3, del Regolamento medesimo e dell'art. 166, comma 2, del Codice. La sanzione pecuniaria, nella misura di euro 4.000,00 (quattromila) per la violazione degli artt. 5, 6, 9 del Regolamento e 2-ter, 2-sexies nonché 2-septies, comma 8, del Codice, quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva. Tenuto conto della natura dei dati oggetto di trattamento, si ritiene altresì che debba applicarsi la sanzione accessoria della pubblicazione sul sito del Garante del provvedimento sanzionatorio , prevista dall'art. 166, comma 7 del Codice e art. 16 del Regolamento del Garante n. 1/2019.

oXFirm Studio di Consulenza

Sito Web: www.oxfirm.it – email: oxfirm@oxfirm.it

ROMA

Viale Antonio Ciamarra 259
00173, ROMA (RM)
tel. 06.86356274

CASERTA

Piazza Giovanni XXIII, 18
81027, S. Felice a C.llo(CE)
tel. 0823.753477 / 754996

Grazie della Vostra cortese attenzione

privacy@oxfirm.it

partner Asso Edu
Associazione Nazionale Tecnologie e Digital Media per l'Educazione