CORSO INTRODUTTIVO
al
REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI
per il
MONDO DELL'ISTRUZIONE


GDPR
General Data Protection Regulation

Cos'è il GDPR UE 679/2016?

È il nuovo:

Regolamento: insieme coerente di norme giuridiche
Generale: che riguarda tutti: stati, imprese e persone sulla
Protezione: azione o funzione di difesa contro danni eventuali dei
Dati: informazioni *personali* codificate o codificabili

Emanato dal Parlamento dell'Unione Europea
con il numero 679, il 24 maggio 2016
divenuto operativo in tutta Europa il 25 maggio 2018.
Con il GDPR **la** Privacy (1996) è divenuta la **Protezione dei Dati (2016).**

Il GDPR UE 679/2016 è composto da 173 *considerando* e 99 *articoli*. Per sua natura è immediatamente recepibile ed applicabile (25 maggio 2018) da tutti gli Stati membri senza modifiche escluse quelle previste nel *considerando* n.8 che recita: *"ove il presente regolamento preveda specificazioni e limitazioni delle sue norme a opera del diritto degli Stati membri, gli Stati membri possono, nella misura necessaria per la coerenza e per rendere le disposizioni nazionali comprensibili alle persone cui si applicano, integrare elementi del presente regolamento nel proprio diritto nazionale".*

È proprio quanto è avvenuto in Italia. Il nostro Governo ha, infatti, firmato il giorno 10 agosto e pubblicato in GAZZETTA UFFICIALE il Decreto 101, entrato poi in vigore il 19/09/2018 (103 *articoli* in bozza – 27 nel testo definitivo) per adeguare la norma comunitaria al particolare tessuto sociale, economico e delle P.A. italiane.

Il GDPR UE 679/2016 è stato pensato per essere un work in progress, capace di adattarsi ai frenetici cambiamenti tecnologici che impongono la massima attenzione alla tutela dei nostri dati.
Pertanto la data del 25 maggio 2018 non è stata la scadenza in cui dimostrare l'adeguamento, ma l'inizio del processo di adeguamento che sarà continuo e costante.

Cos'è cambiato rispetto alla 196/2003?

1° grande cambiamento

Il Codice Privacy 2003 inquadrava l'interessato quale soggetto i cui dati (personali, sensibili, ecc.) andavano tutelati.

Il GDPR 2016 mette al centro il dato quale elemento da tutelare. Perché?

Perché grazie allo sviluppo di immensi banchi di memoria (quasi "illimitati") tutti i dati provenienti dagli smartphone, dalle app, dall'integrazione audio/video/gps/sim, tutti i messaggi whatsapp, le email, i video, le foto, ecc. di tutti noi vengono salvati e analizzati da software (big data) in grado di comprendere esattamente cosa piace/non piace, attira/non attira; cosa funziona/non funziona per la stragrande maggioranza degli esseri umani ... quindi pilotare e governare quasi tutte le nostre scelte

Cos'è cambiato rispetto alla 196/2003?

2° grande cambiamento

Il Codice Privacy 2003 definiva esattamente adempimenti e scadenze alle quali i titolari dovevano adeguarsi (il DPS con le famose misure minime di sicurezza, la privacy by default), pena importanti sanzioni.
In sostanza: le regole erano calate dall'alto su tutti noi!

Il GDPR 2016, consapevole dell'impossibilità di stabilire oggi regole pratiche realmente valide a lungo e per tutti, chiede a ciascuno di essere più responsabile e di fare sempre il massimo (misure idonee di sicurezza, la privacy by design) per garantire la protezione dei dati.
In sostanza: spinge all'autoregolamentazione consapevole.
Le sanzioni sono diventate enormi per chi viola la legge.

Il GDPR quanto riguarda il MONDO DELLA SCUOLA?

1) dati identificativi di minori e dei loro familiari

2) dati identificativi dei dipendenti e dei loro familiari

3) dati particolari (ex sensibili) degli stessi

4) trattati in modalità mista

5) con strumenti che richiedono attenzione

L'ambito di applicazione del GDPR

L'ambito materiale, descritto dall'Art. 2, riguarda le tipologie di trattamento dei dati.
L'ambito territoriale, descritto dall'Art. 3, riguarda il rapporto tra "proprietari" dei dati e "titolari" dei trattamenti in relazione a domicili/residenze/sedi degli uni e degli altri.

L'ambito di applicazione del GDPR

L'ambito materiale, descritto dall'Art. 2, concerne il trattamento dei dati personali di persone fisiche (NON ditte o enti o associazioni o marchi o altro) contenuti in un archivio o destinati a figurarvi.

Cos'è un archivio (ambito materiale)?

" … qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico" (Art. 4.6).

N.B.1. nel Codice del 2003 non era definito il concetto di archivio che è una novità del GDPR.

N.B.2. anche se cartaceo purché non occasionale.

Dove e perché (ambito territoriale)?

L'ambito territoriale di applicazione del GDPR impone l'adeguamento alla norma per:

a) tutte le scuole di ogni ordine e grado con sede nella UE (anche se operano per soggetti extra UE);
b) tutte le scuole di ogni ordine e grado con sede extra UE che però trattano dati di cittadini UE o momentaneamente residenti in UE.

IL GDPR IN SINTESI

TIPOLOGIA	REGOLAMENTO DIRETTAMENTE APPLICABILE NEGLI STATI MEMBRI DELL'UE (consentito l'adattamento alla normativa nazionale purché non in contrasto con quella comunitaria)
SCOPO PERSEGUITO	LA TUTELA DEI DATI PERSONALI
COME PERSEGUE LO SCOPO	DISCIPLINANDO IL TRATTAMENTO DEI DATI PERSONALI
A CHI SI APPLICA	ALLE PERSONE FISICHE
SECONDO QUALI CRITERI	IL CRITERIO MATERIALE (trattamenti) E IL CRITERIO TERRITORIALE (residenze e sedi)

Dati e Profilazione

La profilazione è quell'operazione per cui, attraverso l'elaborazione dei dati conferiti dai nostri utenti, ci troviamo a suddividere gli stessi per età, residenza, sesso, titolo di studio, gusti, abitudini, attitudini, comportamenti, preferenze, ecc. Se si fanno queste operazioni bisogna dichiararle a ogni utente quando si raccolgono i suoi dati.

Questo Istituto effettua delle profilazioni?

Il titolare del trattamento

Il titolare è quella persona, giuridica o fisica, che determina le finalità ed i mezzi del trattamento dei dati personali.

In sostanza il titolare è colui che tratta i dati senza ricevere istruzioni da altri e agisce in piena e totale autonomia quando stabilisce quali dati gli servono per svolgere la sua attività, perché ne ha bisogno, come li raccoglie, come li utilizza, come li conserva, protegge, ecc.

Chi è il titolare nel mondo della scuola?

Il responsabile del trattamento

Il responsabile del trattamento è quel soggetto che, nominato dal titolare, tratta i dati unicamente per conto dello stesso.

Sono responsabili interni delle *scuole* figure professionali competenti ai fini "privacy" (anche se esterne all'amministrazione) e dotate di una certa autonomia e indipendenza dagli apicali.

Sono responsabili esterni delle *scuole*: il medico competente, il consulente ISO, il tecnico dei PC, tutti i soggetti che accedono a i dati quindi: AdV, hotel, compagnie di volo, … SOSPrivacy.net …

Il responsabile del trattamento

Il principio di responsabilità è collegato alla nozione di pericolosità delle attività che vengono operate con i dati. Si rende quindi necessaria una valutazione preliminare della pericolosità di tali attività e una descrizione delle misure che il titolare reputerà idonee (non più minime) per evitare il danno.
Il Responsabile quindi dovrà dimostrare:

di conoscere le misure disponibili/attuabili per evitare il danno

di adottare le misure stesse "disegnandole" caso per caso

di averlo fatto lasciando traccia e dandone la relativa prova

Le persone autorizzate

Sono i nostri collaboratori interni (personale ATA e docenti).
In particolare quelli che trattano i dati, cioè che hanno accesso anche solo ai dati identificativi dei nostri utenti.

Le persone autorizzate (GDPR EU 679/2016) coincidono con gli incaricati del D.Lgs 196/2003.

BASTA SAPERE –NELL'AMBITO DEI PROPRI COMPITI- NOME E COGNOME DI UN SOGGETTO E/O DEI SUOI FAMILIARI
-> PER ESSERE PERSONA AUTORIZZATA AL TRATTAMENTO DEI DATI
-> PER DOVER SAPERE/CAPIRE DI COSA SI PARLA.

La liceità del trattamento

L'art. 6 del GDPR è molto chiaro. Il trattamento è lecito quando ricorre almeno una delle seguenti condizioni:

1. L'utente ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità.
2. Il trattamento è necessario all'esecuzione del contratto.
3. Il trattamento è necessario per adempiere agli obblighi di legge.
4. Il trattamento è necessario per salvaguardare gli interessi vitali dell'utente o di altra persona fisica.
5. Il trattamento è necessario per il perseguimento dei legittimi interessi del titolare a meno che non prevalgano su questi gli interessi legittimi, i diritti e le libertà fondamentali dell'utente.

Le finalità dei dati

I dati devono essere raccolti per finalità:
a) lecite - b) precise - c) esplicite.

<table>
<tr><td rowspan="4">Finalità:

Perché raccolgo i tuoi dati?

A cosa mi servono?

Che ci faccio?</td><td colspan="2">deve essere sempre esplicitata</td></tr>
<tr><td colspan="2">deve essere sempre comunicata all’utente prima dell’inizio del trattamento</td></tr>
<tr><td>Può cambiare e la nuova finalità non è compatibile con quella iniziale</td><td>Serve un nuovo consenso da parte dell’utente</td></tr>
<tr><td>Può cambiare e la nuova finalità è compatibile con quella iniziale</td><td>Non serve un nuovo consenso da parte dell’utente</td></tr>
</table>

Caratteristiche del trattamento

MINIMIZZAZIONE	Possono essere raccolti i soli dati necessari alle finalità lecite che sono state dichiarate all'utente.
CORRETTEZZA	Ogni fase del trattamento deve essere resa trasparente.
CONSERVAZIONE	Se permettono l'identificazione dell'utente allora i dati non possono essere conservati per un tempo superiore a quello necessario per il conseguimento delle finalità del trattamento.
RISERVATEZZA	Devono essere adottate tutte le misure affinché soggetti non autorizzati NON possano accedere ai dati stessi.
INTEGRITA'	Devono essere adottate tutte le misure affinché i dati, anche accidentalmente, non vengano degradati, dispersi, distrutti.

Le misure tecniche ed organizzative

Il GDPR è chiaro: i dati personali sono qualificati come diritti fondamentali dell'uomo quindi le misure tecniche ed organizzative per proteggerli devono sempre essere adeguate, idonee ed attuali.

Se il mondo cambia, le misure devono cambiare.

Questo aggiornamento non è più tecnicamente specificato dal Legislatore (2003) che lo affida completamente al titolare del trattamento. È un grave errore pensare che il GDPR consista solo nell'aggiornare le informative e le liberatorie.

Il Consenso dell'utente

<table>
<tr><td rowspan="5">• INEQUIVOCABILE
• LIBERO
• SPECIFICO
• INFORMATO
• REVOCABILE
• VERIFICABILE</td><td>Una sola finalità</td><td colspan="2">L'utente lo rilascia per quella specifica finalità</td></tr>
<tr><td>Più finalità</td><td colspan="2">L'utente rilascia un consenso specifico per ciascuna finalità</td></tr>
<tr><td rowspan="3">Finalità che cambiano nel corso del trattamento</td><td rowspan="2">Compatibili?</td><td rowspan="2">Non serve aggiornare il consenso</td></tr>
<tr></tr>
<tr><td>Non compatibili?</td><td>Bisogna aggiornare il consenso</td></tr>
</table>

L'informativa per gli utenti

Deve contenere sempre:

- la dichiarazione che i dati verranno trattati
- gli effetti del rifiuto di fornire i dati
- la natura obbligatoria o facoltativa dei dati richiesti
- TUTTE le modalità (inclusi i tempi) del trattamento
- TUTTE le finalità del trattamento
- TUTTI i soggetti ai quali saranno comunicati i dati
- TUTTI i soggetti che potranno venire a conoscenza dei dati
- i diritti dell'utente e le modalità per esercitare gli stessi
- i contatti attivi del titolare e del DPO

La liberatoria per le immagini

ad esempio quella per pubblicare sul proprio sito o pagina fb la foto di una persona, richiede un'autorizzazione specifica (di entrambi i genitori se il soggetto ritratto è minorenne) che può anche essere verbale nell'immediatezza, ma poi deve essere confermata in maniera scritta, anche solo con un breve scambio di messaggi su whatsapp, telegram, email, ecc. (ovviamente, in caso di minori, l'autorizzazione di entrambi i genitori via whatsapp, ecc. è meno semplice e meno sicura, va evitata).

Oppure si possono anonimizzare le immagini con artifici tecnici in modo da rendere l'immagine immediatamente utilizzabile.

È invece sempre consentita la condivisione di immagini già pubblicate da altri sulla rete in quanto l'onere di raccogliere tutte le autorizzazioni è in capo al primo che pubblica una certa immagine.

Il consenso e l'informativa

Entrambi i bambini sono irriconoscibili poiché anonimizzati: quello più vicino in quanto l'inquadratura non riprende il volto/profilo; quello lontano è proprio fuori fuoco. Pubblicabile senza autorizzazione.

Tutti i bambini, sebbene di spalle, sono riconoscibili e identificabili dai numeri delle maglie. Questa immagine sarebbe pubblicabile solo con l'autorizzazione scritta di entrambi i genitori.

Quali sono i diritti dei nostri utenti?

ALLA TRASPARENZA	**Artt. 5 e 12 del GDPR**	**Conoscere, monitorare e decidere**
ALL'INFORMATIVA	**Artt. 12, 13 e 14 del GDPR**	**Entro un mese da quando ce lo richiede**
ALL'ACCESSO	**Art. 5 del GDPR**	**È il presupposto fondamentale: i dati sono del cliente e non possiamo negargli l'accesso**
ALLA RETTIFICA	**Art. 16 del GDPR**	**Se il cliente corregge o integra i dati, noi dobbiamo prontamente aggiornare i nostri archivi dandone esatta comunicazione e conservando il dato precedente.**
ALL'OBLIO	**Art. 17 del GDPR**	**Consentito solo se legittimo. In tal caso deve essere immediato ed esteso.**
ALLA LIMITAZIONE	**Art. 18 del GDPR**	**Consentito solo se legittimo. In tal caso deve essere immediato ed esteso.**
ALLA PORTABILITA'	**Art. 20 del GDPR**	**L'utente può chiederci di rendergli i suoi dati o di trasferirli ad altro titolare (digitalmente e con rimborso eventuali spese).**
ALL'OPPOSIZIONE	**Art. 21 del GDPR**	**Legittimo interesse, marketing e finalità storico/scientifiche**

La violazione dei diritti

RECLAMO	**L'utente può presentare reclamo all'Autorità Garante al fine di segnalare una violazione circostanziata della disciplina da parte di una P.A.**
SEGNALAZIONE	**Se l'utente crede o pensa che i suoi diritti siano stati violati può presentare una segnalazione all'Autorità Garante chiedendo un intervento o un controllo.**
RICORSO	**In questo caso l'utente, tramite un legale, presenta nelle sedi opportune un ricorso formale per aver creduto violati in toto o in parte i propri diritti.**

ARCHIVI CARTACEI

(cioè **tutti** i contratti firmati e tutte le liberatorie con consenso raccolte, **tutte** le copie dei documenti di identità, certificati medici, certificati anagrafici, copie di codici fiscali, ecc. ecc. "storici" che "attivi")

La regola aurea è: "**nessun estraneo deve avere**, neanche per **sbaglio** o per **caso**, la **possibilità** di **guardare questi documenti**".

Questi archivi vanno tenuti **per legge** in **armadi chiusi a chiave.**
Se non abbiamo armadi chiusi a chiave, li conserviamo in **stanze chiuse a chiave** in cui **non** si svolga **alcuna altra attività.**

ARCHIVI CARTACEI 2

*Se non abbiamo spazi simili, tali documenti vanno posti in schedari o raccoglitori che **non** permettano il **colpo d'occhio** al soggetto.*

*Se arriva un estraneo mentre stiamo lavorando la pratica di **altri soggetti**, dobbiamo **riporre** velocemente la pratica **lontana** dalla vista della persona sopraggiunta..*

La trascuratezza e l'inadeguatezza di questi punti sono sanzionate in maniera assai pesante: si rischiano **multe** di migliaia di euro.

L'autorità incaricata delle verifiche e dei controlli è la **Guardia di Finanza**, ma tutte le **Forze di Polizia** e i funzionari del Garante possono accertare eventuali violazioni.

ARCHIVI CARTACEI 3

Qualora fosse necessario **distruggere** i documenti cartacei contenenti dati di alunni, familiari e colleghi (non le pubblicità, le locandine, modulistica non usata ma scaduta, ecc.) bisogna usare il distruggi-documenti **prima** di smaltirli.

Se i locali della Scuola non sono dotati di allarme antincendio con impianto di **spegnimento**, allora è buona prassi avere almeno un **estintore** (non solo per salvare gli archivi!).

ARCHIVI DIGITALI o INFORMATICI
(sono i file del vostro "gestionale", ma anche quelli excel, word, access, qbase, ecc**. in cui avete trascritto** i dati dei vostri alunni/familiari/colleghi)

La regola aurea è: **tutti** i pc su cui ci sono i dati (anche se in word, excel, outlook, ecc.) devono avere la **password** di accensione di Windows o IOS.

Qui una breve guida su come impostare la password:
https://www.aranzulla.it/come-mettere-la-password-al-pc-945508.html

__Ogni__ utente che accede ai pc deve avere un __proprio__ profilo e una propria password … la guida di cui sopra spiega anche come creare più utenti con le relative password.

Tutti i pc su cui ci sono i dati (anche se in word, excel, outlook, assoavis, ecc.) devono avere lo **screen-saver** con **password** al ripristino impostato sui **3/5 minuti**.

Qui la guida per impostare lo screensaver:
https://www.aranzulla.it/come-creare-screensaver-9263.html

se ci allontaniamo dal pc (sebbene già dotato di screensaver con password) dobbiamo **bloccare il pc** premendo insieme i tasti **"windows"+ "L" o l'equivalente MAC**.

Qui una guida utile sui segreti del tasto "windows":
*ht*tps://www.swzone.it/Le-funzionalita-del-tasto-Win-in-Windows-10-42009.html

Se utilizziamo un “gestionale” molto probabilmente sarà già dotato di password di accesso, questo però **non esime dall’utilizzare le password del computer** perché i dati personali da proteggere potrebbero essere anche in word, outlook, ecc.

*Le password devono essere di almeno **8** caratteri tra cui una **cifra**, una **maiuscola** e un **carattere speciale** (,;.:-_çò°à§ùèé+*!”£$%&/=?^) e non **riconducibili** all’utente.*

La regola aurea è: fate i **backup almeno una volta a settimana**, indipendentemente dai programmi che utilizzate.

Inoltre fate almeno ogni mese **un'ulteriore copia dei backup** su un **hard-disk esterno** o **pennina usb** dedicati **solo a questo** (meglio se fossero dispositivi protetti da password) **criptateli** e portateveli **a casa**.

Questa procedura si chiama "**disaster-recovery**" ed ha salvato dalla distruzione colposa di dati (e relativa denuncia) decine di nostri assistiti.

*Molto efficace la disaster-recovery in **cloud** con partner affidabili*

un rischio reale

Per data breach, nella versione italiana violazione dei dati personali si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Sempre secondo il GDPR, la notifica di eventuali violazioni di dati dovrà avvenire possibilmente senza ingiustificato ritardo e, ove possibile, entro 72 ore, dal momento in cui si è venuto a conoscenza della violazione, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. L'eventuale ritardo dovrà essere motivato.

In caso di data breach è necessario contattarci per avviare le relative procedure in autotutela.

SOSPRIVACY.NET