

Spett. Liceo Ginnasio Statale Daniele Manin
C. A. Dirigente: Mondini Mirelva
Via Cavallotti, 2, Cremona - 26100 (CR)

PRIVACY – GDPR – DPO: LE NOVITA'

BASE GIURIDICA: dal Decreto Legislativo **196/2003** al Regolamento Europeo **679/2016**

Il **4 maggio 2016** è stato pubblicato nella *Gazzetta Ufficiale dell'Unione Europea* il nuovo **Regolamento (UE) 2016/679** del Parlamento Europeo e del Consiglio *“relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali”*.

Si tratta di una **rivoluzione** nel mondo della Privacy, attesa ormai da diversi anni e il cui percorso è stato in continua salita, essendoci in gioco milioni di euro legati soprattutto alle attività di marketing e di profilazione oltre che i rapporti tra Europa e resto del mondo (con Stati Uniti, Canada e Cina principali interlocutori interessati).

REGOLAMENTO EUROPEO: COSA È CAMBIATO DALLA BOZZA INIZIALE

Le regole introdotte vogliono adattare la legislazione UE (in vigore da 19 anni) alle **nuove tecnologie** e **all'uso sempre più disparato che si fa di internet**, ad esempio:

- ✓ **PER LE PICCOLE E MEDIE IMPRESE** ci sono novità allettanti come tagli ai costi e burocrazie più snelle e fluide, che favoriscano lo sviluppo economico e del mercato digitale.
- ✓ L'introduzione della figura del RESPONSABILE per la PROTEZIONE dei DATI (c.d. in inglese **Data Protection Officer**) **sarà facoltativa** per le piccole-medio imprese, al contrario non lo sarà per la pubblica amministrazione ai sensi dell'art. 37 del GDPR, così come la **“Valutazione d'Impatto” preventivo** del rischio Privacy per valutare e moderare le possibilità legate ad una dispersione, comunicazione o diffusione di Dati in modo non adeguato.

Inoltre, le sanzioni arriveranno fino a 20 milioni di euro o al 4% del fatturato per i trasgressori, quindi si può sicuramente affermare che **ADEGUARSI al GDPR 679/16 è nell'interesse di tutti**.

*Quali sono gli impatti principali per la **Pubblica Amministrazione**?*

1 – INDIVIDUAZIONE DEI SOGGETTI A CUI SI APPLICA IL REGOLAMENTO

Prima = la normativa era applicabile nel luogo in cui aveva sede il Titolare del trattamento dei dati.

GDPR 679/16 = la legge applicabile è quella del soggetto i cui dati vengono raccolti. Social network, piattaforme web e motori di ricerca saranno quindi soggetti alla normativa europea anche se sono gestiti da società con sede fuori dall'UE. Con il nuovo regolamento viene abolita la figura del Titolare del Trattamento Dati e rimane solo la figura di Responsabile.

2 – DOVERE DI DOCUMENTAZIONE E INFORMAZIONE

Prima = la documentazione era importante.

GDPR 679/16 = “Principio dell’accountability” (responsabilità verificabile), secondo cui **tutti i soggetti che partecipano al trattamento dati devono essere CONSCI E RESPONSABILI** e devono tenere documentazione di tutti i trattamenti effettuati. **Chi non documenta, è soggetto a possibili sanzioni**: a prescindere dall’utilizzo che si fa dei dati, è sufficiente non avere i documenti per essere perseguibili.

3 – L’INFORMATIVA PRIVACY

Prima = l’informativa era spesso lunga, incomprensibile e con richiami normativi complessi.

GDPR 679/16 = l’informativa deve essere leggibile, comunicativa, accessibile, concisa e scritta con linguaggio chiaro e semplice con un numero limitato di riferimenti normativi. Deve essere fornita per iscritto (oralmente va bene SOLO se l’interessato è d’accordo e la sua identità deve comunque essere comprovata con altri mezzi). Si propone anche l’utilizzo di icone per rendere l’informativa leggibile anche da parte di chi non conosce la lingua.

4 – CAMBIA IL CONSENSO

Prima = il consenso doveva essere libero, specifico e informato. Ci doveva essere un atto formale per accettare il trattamento dei dati.

GDPR 679/16 = il consenso deve essere libero, specifico, informato e inequivocabile. Il consenso è valido se la volontà è espressa in modo NON equivoco, anche con un’azione positiva: non ci deve essere per forza la casella di spunta, basta un testo in cui si informa che proseguendo si accetta il trattamento dati con link all’informativa.

5 – VALUTAZIONE D’IMPATTO SULLA PROTEZIONE DEI DATI (c.d. Analisi del Rischio)

Prima = si preparava il DPS (c.d. Documento programmatico sulla Sicurezza).

GDPR 679/16 = si effettua una Valutazione degli Impatti Privacy analizzando i rischi, definendo i gap rispetto alla corretta gestione dei rischi, stabilendo un piano per colmarli e controllando annualmente gli effetti degli interventi per ridurre i rischi. Quasi sicuramente il nuovo documento sarà chiamato PIA: Privacy Impact Assessment.

6 – IL RESPONSABILE PER LA PROTEZIONE DEI DATI PERSONALI

Prima = l’RPD non era una figura contemplata.

GDPR 679/16 = bisogna istituire (per tutti gli enti pubblici e per aziende il cui core business coinvolge trattamenti di natura rischiosa) un responsabile per la protezione dei dati. L’RPD sarà una figura manageriale con rinnovo periodico, sarà referente del Garante e dovrà avere requisiti e competenze elevate. L’RPD dovrà possedere una totale autonomia di lavoro, una indipendenza dal TITOLARE del trattamento e una totale mancanza di conflitti di interesse.

7 – OBBLIGO DI SEGNALAZIONE IN CASO DI VIOLAZIONE DEI DATI

Prima = non era necessario comunicare violazioni nel trattamento dati.

GDPR 679/16 = nel caso di violazione del trattamento dati bisogna effettuare una segnalazione al Garante entro **72 ore dall'evento** e, nel più breve tempo possibile, bisogna informare anche i diretti interessati. Il mancato rispetto di quest'obbligo comporta **sanzioni penali**. È possibile prevedere delle assicurazioni per coprire il costo di comunicare la violazione a tutti gli interessati, definito "Data Breach".

8 – RICONOSCIMENTO DI NUOVI DIRITTI

Prima = pochi diritti che tutelavano l'interessato in merito alla gestione dei suoi dati.

GDPR 679/16 = nuovi diritti: **diritto alla portabilità dei dati** (posso pretendere che il soggetto a cui ho concesso l'uso dei miei dati me li restituisca su un supporto elettronico strutturato così che io possa farne ulteriore uso, anche presso un altro fornitore), diritto ad essere totalmente dimenticato (c.d. **diritto all'oblio**) da chi ha raccolto i miei dati.

INOLTRE VI SONO ALTRE IMPORTANTI NOVITÀ:

- Vengono introdotte le definizioni di "Dato Generico" e "Dato Biometrico";
- Introdotta la categoria del trattamento dati dei minori;
- Introduzione della Co-titolarità nel trattamento dei dati;
- Introduzione della figura del "Joint Controller";
- Introduzione di requisiti più stringenti per trasferire dati verso Paesi Terzi;
- **Introduzione del principio dell'applicazione del diritto UE anche ai trattamenti di dati personali non svolti nell'UE**, se relativi all'offerta di beni e servizi ai cittadini UE o tali da permettere il monitoraggio dei comportamenti dei cittadini dell'UE;
- Istituzione del Comitato Europeo per la protezione dei Dati.

FINO AL 25 MAGGIO 2018 PER ADEGUARSI

Il periodo utile per le Pubbliche amministrazioni, così come le Imprese Europee, per adeguarsi alla nuova normativa Privacy è di due anni e venti giorni a partire dal momento in cui il regolamento è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea, ovvero il **4 Maggio 2016**. Pertanto, le Pubbliche Amministrazioni avranno tempo fino al **25 Maggio 2018** per ripensare i processi di trattamento dei dati adattandosi a novità come le valutazioni di impatto e i sistemi di certificazione, e di notificazione delle violazioni e adottarsi di un **Data Protection Officer**.