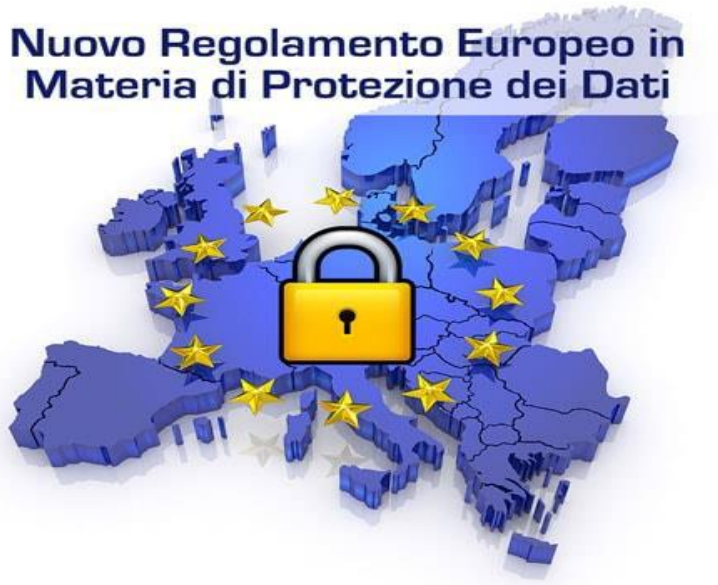
TECNOSTRUTTURA
1998 - 2018

Nuovo Regolamento Europeo in Materia di Protezione dei Dati



Rete di Comunicazione FSE
Roma, 20 novembre 2018

Perché un Regolamento UE?

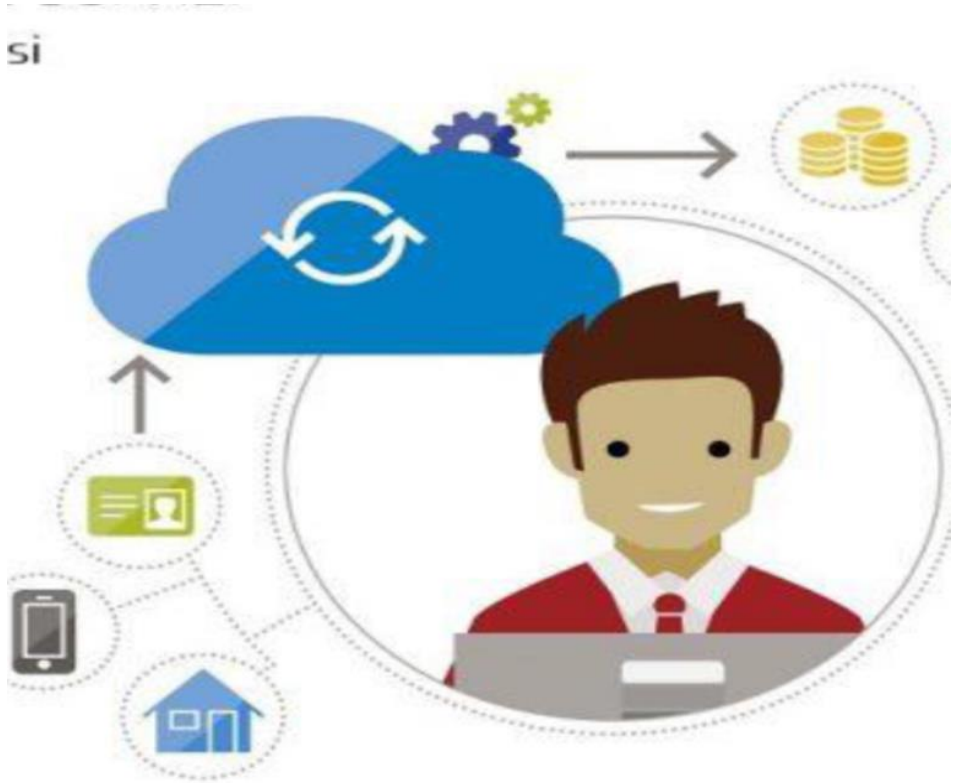
Obiettivi del Regolamento UE 2016/679, noto come GDPR

- Assicurare un'applicazione coerente ed omogenea delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche, con riguardo alla tutela dei dati personali, in tutta l'Unione
- Facilitare la libera circolazione dei dati personali nel mercato interno
- Fornire una risposta, necessaria e urgente, alle sfide poste dagli sviluppi tecnologici

I dati personali oggetto del GDPR

Dati relativi a <u>persone fisiche</u> identificate o identificabili

- Nome e cognome
- Indirizzi e-mail
- Dati bancari
- Immagini (foto, video)
- …..



Dati rientranti in particolari categorie

I *cd dati sensibili*: origine razziale o etnica; stato di salute; ecc.

- Il **Regolamento fissa i principi generali di liceità del trattamento**: consenso esplicito dell'interessato; dati resi manifestamente pubblici dall'interessato; trattamento necessario per motivi di interesse pubblico rilevante ecc. (**art. 9**)
- **Spazio di manovra degli SM di precisarne le norme**, determinando con maggior precisione i vincoli in base ai quali il trattamento è lecito

Dati personali relativi alle **condanne penali** e ai **reati** o a connesse **misure di sicurezza**

Il **GDPR (art.10)** prevede **due condizioni** :

- Il trattamento deve avvenire soltanto sotto il **controllo dell'autorità pubblica**
- il trattamento è **autorizzato dal diritto dell'Unione** o **degli Stati membri**

I principi guida del GDPR

Accountability

Responsabilizzazione del titolare e del responsabile del trattamento che si configura come una sostanziale **assunzione di rischio** nell'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione delle sue prescrizioni

Privacy by design

Introduzione delle **misure di sicurezza** e delle **misure di tutela e garanzia** dell'interessato nel trattamento dei suoi dati **fin dalla progettazione** degli strumenti utilizzati

Privacy by default

Necessità che la protezione dei dati personali sia garantita "**per impostazione predefinita**".
Ne deriva che le tutte le valutazioni che il titolare del trattamento deve effettuare in tema di protezione dei dati personali devono essere compiute a monte, cioè prima di procedere al trattamento dei dati vero e proprio.

Organigramma privacy

Cosa cambia?

Titolare

- **Conferma la definizione di titolare del Dlgs 196/2003 e s.m.i**
- **Disciplina la contitolarità del trattamento (art. 26):** «*quando **due o più titolari determinano congiuntamente le finalità** e i **mezzi del trattamento** essi definiscono in un accordo interno le rispettive responsabilità in merito all'osservanza degli obblighi del GDPR*

Responsabile

- Definisce (art. 4 .8) il responsabile del trattamento come «*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che **tratta dati** personali **per conto del titolare** del trattamento*»
- Fissa, poi, più dettagliatamente (rispetto all'art. 29 del Codice) le **caratteristiche dell'atto con cui il titolare designa un responsabile** del trattamento attribuendogli specifici compiti (**art. 28)**
- Consente la **nomina di sub-responsabili** del trattamento da parte di un responsabile (**art. 28 com. 4**), per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario

Autorizzati

Non prevede espressamente la figura dell'"incaricato" del trattamento (ex art. 30 del Codice), ma non ne esclude la presenza in quanto fa riferimento a "**persone autorizzate** al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" (**art. 4 com. 10**)

Organigramma privacy: il Responsabile del trattamento

- Necessità di un **contratto o altro atto giuridico (art.28)** che vincoli il responsabile al titolare e che disciplini:
  a. materia e durata del trattamento;
  b. natura e finalità del trattamento;
  c. tipo di dati personali e categorie di interessati;
  d. obblighi e diritti del titolare del trattamento.

- In base al contratto **il responsabile si impegna** a:
  a. **trattare dati** soltanto **su istruzione** documentata **del titolare**;
  b. **consentire i trattamenti solo a persone autorizzate** con impegno alla riservatezza o che abbiano un adeguato obbligo legale di riservatezza;
  c. **adottare tutte le misure di sicurezza** (es. cifratura; pseudonimizzazione; recupero da backup);
  d. rispettare le condizioni per ricorrere a un sub-responsabile del trattamento;
  e. assistere il titolare per dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
  f. **cancellare o restituire tutti i dati** e cancellare le copie esistenti;
  g. mettere a disposizione del titolare le informazioni per dimostrare il rispetto dei suddetti obblighi e **consentire le ispezioni**.

Organigramma Privacy: le nuove figure

Alle consuete figure del titolare, del responsabile, dell'autorizzato/incaricato e dell'interessato il Regolamento affianca:

- **Il responsabile della protezione dei dati,** meglio noto come «Data Protection Officer (DPO)»
- **Il destinatario dei dati:** la persona fisica o giuridica (sia pubblica che privata) a cui vengono comunicati i dati personali
- **Il terzo**: in via residuale chiunque non possa essere annoverato nelle categorie soggettive previste dal Regolamento

Organigramma Privacy: il Responsabile della protezione dei dati

- Una nuova **figura altamente specializzata** e aggiornata, a tutela di dati e privacy

- Può essere un **dipendente** del titolare o del responsabile del trattamento oppure **un consulente esterno** all'amministrazione che assolve i suoi compiti in base ad un contratto di servizi (art. 37 com. 1, 5 e 6)

- Possibile nominare un **unico** responsabile della protezione **per più autorità pubbliche o organismi pubblici**, tenuto conto della loro dimensione e struttura organizzativa (art. 37 com. 3).

- Il RPD deve essere **indipendente** e avere **autonomia decisionale**, non può svolgere altre mansioni o compiti in **conflitto di interessi** con quelle proprie del RDP (art.38)

- **Compiti**: **consulenza/supporto** a titolare e a responsabile nell'applicazione del GPDR e della normativa nazionale, **sensibilizzazione e formazione del personale** che partecipa ai trattamenti, **parere in merito alla valutazione d'impatto** sulla protezione dei dati (art. 39)

Nuovi adempimenti per titolare e responsabile
Accountability

Titolare

- **Designare un responsabile della protezione dei dati** obbligatorio se:
  a. il trattamento è effettuato da autorità pubbliche o organismi pubblici
  b. si svolgono trattamenti su larga scala
- **Predisporre e implementare un registro delle attività di trattamento** che contenga gli elementi di cui all'**art. 30 com.1**
- Effettuare **un'analisi del rischio** ed adottare le **misure di sicurezza adeguate**
- Predisporre una **procedura per il data breach**
- **Eseguire la valutazione d'impatto sulla protezione dei dati personali (DPIA):** obbligatoria in caso di trattamento, su larga scala, di dati sensibili o di natura estremamente personale (**art. 35 com. 2b**) nonché quelli relativi a interessati vulnerabili quali: minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani ecc. (**considerando 75**).

Responsabile

- **Predisporre e implementare un registro delle attività di trattamento** (facoltativo per enti/imprese con meno di 250 dipendenti) che contenga gli elementi di cui all'**art. 30 com.2**
- **Effettuare un'analisi del rischio ed adottare le misure di sicurezza adeguate**
- **Designare un responsabile della protezione dei dati** se si tratta di amministrazioni pubbliche

I diritti degli interessati

Cosa cambia?

- Si rafforza la disciplina del **consenso** prevedendo che debba essere libero, specifico, informato e inequivocabile; **non è ammesso il consenso tacito o presunto**
  - ✓ Per i **dati "sensibili"** il **consenso** deve essere **«esplicito» (art. 9)**
  - ✓ **Il consenso dei minori** è **valido a partire dai 16 anni;** prima di tale età il consenso deve essere prestato dal titolare della responsabilità genitoriale o da chi ne fa le veci **(art. 8 com. 1)**

- Viene ampliata la **tutela degli interessati** mediante **l'introduzione di nuovi diritti:**
  - ✓ **diritto alla cancellazione dei dati (diritto all'oblio)** nei casi in cui: i dati personali non siano più necessari rispetto alle finalità per le quali sono stati raccolti e trattati, sia stato revocato il consenso o l'interessato si sia opposto al trattamento **(art. 17)**
  - ✓ **diritto alla limitazione del trattamento** nelle ipotesi in cui l'interessato contesti l'esattezza dei dati o si sia opposto al trattamento **(art. 18)**
  - ✓ **diritto alla portabilità dei dati,** ossia diritto di ricevere i propri dati in un formato strutturato, di uso comune e leggibile da dispositivo automatico **(art. 20)**

- Si fissa un **termine certo per la risposta all'interessato, in caso di esercizio del diritto di accesso o degli altri diritti:** 1 mese, estendibili fino a 3 mesi in casi di particolare complessità

- Vengono **ampliati i contenuti dell'informativa** da fornire all'interessato

L'informativa all'interessato

- Il GDPR (art.13) **amplia i contenuti dell'informativa** che deve essere fornita, da parte del titolare del trattamento, all'interessato a tutela dell'esercizio della protezione dei dati.

Cosa cambia?

- ✓ l'identità e i dati di contatto del titolare del trattamento
- ✓ **i dati di contatto del responsabile della protezione dei dati** (DPO)
- ✓ la descrizione delle finalità perseguite
- ✓ **la base giuridica del trattamento** (norma, contratto ecc.)
- ✓ gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali
- ✓ l'intenzione del titolare del trattamento di trasferire i dati all'estero
- ✓ le modalità del trattamento (soprattutto se automatizzate)
- ✓ **il periodo di conservazione dei dati o i criteri** seguiti **per stabilire tale periodo**
- ✓ **il diritto dell'interessato di ottenere la limitazione del trattamento**
- ✓ **Il diritto alla portabilità dei dati**
- ✓ **Il diritto di presentare un reclamo all'autorità di controllo**

Le sanzioni amministrative

- **Sanzioni pecuniarie fino a <u>€ 10.000.000</u> (art. 83 com.4)** in caso di violazione delle seguenti disposizioni:
  - ✓ **Obblighi del titolare e del responsabile del trattamento** a norma degli articoli 8,11, da 25 a 39, 42 e 43
  - ✓ ….

quindi: violazione obblighi in materia di consenso dei minori, privacy by design, misure di sicurezza, designazione DPO …

- **Sanzioni pecuniarie fino a <u>€ 20.000.000</u> (art. 83 com.5)** in caso di violazione delle seguenti disposizioni:
  - ✓ **i principi di base del trattamento,** comprese le condizioni relative al **consenso**
  - ✓ **i diritti degli interessati**
  - ✓ **i trasferimenti di dati personali all'estero**
  - ✓ **……..**

Il percorso di adeguamento interno

- **6 novembre 2017:** pubblicazione in GURI Legge delega al governo per l'adeguamento, entro 6 mesi, della normativa nazionale alle disposizioni del GDPR (L. 163/2017 art. 13)
- **maggio 2018:** proroga al 21 agosto della scadenza della delega
- **10 agosto 2018:** approvazione in CdM decreto legislativo di adeguamento al Regolamento UE 2016/679 (D.lgs. 101/2018)
- **4 settembre 2018**: pubblicazione D.lgs. 101/2018 in GURI (GU Serie Generale n.205 del 04-09-2018)
- **19 settembre 2018:** entrata in vigore del provvedimento

L’approccio del legislatore italiano

- Abrogazione delle disposizioni del previgente codice in contrasto con il GDPR
- Non duplicazione di alcune disposizioni molto simili ma non coincidenti, presenti sia nel regolamento sia nel codice (es. le definizioni, l’informativa da rendere all’interessato ecc.)
- Mancato richiamo di alcune previsioni contenute nel previgente codice assorbite dalle norme del regolamento europeo
- Abrogazione delle misure minime di sicurezza in coerenza con il principio di «*accountability*»

Le principali novità del D.lgs 101/2018

- **Trattamento collegato ad un interesse pubblico non viene più inquadrato dal punto di vista soggettivo**, ossia con riferimento all'appartenenza dei Titolari alla categoria di soggetti pubblici, **bensì da quello oggettivo** con riferimento alla finalità del trattamento.

- Una **specifica disciplina** viene introdotta per **il trattamento delle particolari categorie di dati** di cui all'art. 9 del GDPR necessari per motivi di interesse pubblico rilevante

- **Consenso del minore** per l'accesso ai servizi della società dell'informazione fissato a **14 anni**

- **Introduzione del concetto di soggetti designati:** coloro ai quali all'interno dell'amministrazione sono affidati specifici compiti in merito al trattamento dei dati personali (responsabili interni e incaricati secondo la terminologia del previgente Codice).

- **Disciplina sanzionatoria articolata:** sanzioni ammnistrative previste dal Regolamento + sanzioni penali in caso di trattamento illecito di dati.