IL NUOVO REGOLAMENTO PRIVACY

Cosa devono sapere le scuole

A cura del DPO Avv. Stab. Ab.
Giacomo Briga

Una nuova fonte normativa per la privacy

- **Il Regolamento UE 2016/679 del 27 aprile 2016 concerne la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati; è stato pubblicato nella GUCE il 4 maggio 2016, è entrato in vigore il 24 maggio 2016 ed è diventato direttamente applicabile in tutti gli Stati membri a partire dal 25 maggio 2018.**

- **In quanto Regolamento UE non richiede una legge nazionale di recepimento.**

Quale la filosofia?

Un passo avanti rispetto alla normativa precedente…

Il Regolamento promuove la responsabilizzazione (*accoutability*) dei titolari del trattamento e l'adozione di approcci e politiche che tengano conto costantemente del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati.

Il principio chiave è "privacy by design", cioè garantire la protezione dei dati sin dalla fase di ideazione e progettazione di un trattamento o di un sistema e adottare comportamenti che consentano di prevenire rischi per la protezione dei dati.

Cosa non cambia

L'impianto complessivo del Codice attuale rimane invariato, con particolare riferimento a:

- **Presupposti su cui si fonda la legittimità del trattamento**
- **Necessità della informativa (con qualche modifica)**
- **Tipologia di diritti degli interessati**
- **"Attori"o figure di riferimento (titolare, responsabile del trattamento, incaricato, interessato)**

Cosa non cambia…

- **Presupposti su cui si fonda la legittimità del trattamento**

ll Regolamento conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica; **i fondamenti di liceità del trattamento sono indicati all'art. 6 del regolamento e coincidono, in linea di massima, con quelli previsti attualmente dal Codice**(consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, **interesse pubblico o esercizio di pubblici poteri**, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati).

Cosa non cambia…

- **Necessità dell' informativa con queste modifiche (contenuti)**

I contenuti dell'informativa sono elencati **in modo tassativo** negli articoli 13, paragrafo 1, e 14, paragrafo 1, del Regolamento e in parte sono più ampi rispetto al Codice. In particolare, il titolare **DEVE SEMPRE** specificare la **base giuridica** del trattamento, nonché **se trasferisce i dati personali in Paesi terzi** e, in caso affermativo, **attraverso quali strumenti**(esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo); **il periodo di conservazione dei dati** o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di **presentare un reclamo** all'autorità di controllo. Se il trattamento comporta processi decisionali automatizzati (anche la **profilazione**), l'informativa deve specificarlo e deve indicare anche la **logica** di tali processi decisionali e le conseguenze previste per l'interessato.

Cosa non cambia…

- **Necessità dell'informativa con queste modifiche (tempi)**

Nel caso di dati personali non raccolti direttamente presso l'interessato *(art. 14 del Regolamento)*, l'informativa deve essere fornita **entro un termine ragionevole che non può superare 1 mese** dalla raccolta, oppure **al momento della comunicazione** (**NON** della registrazione) dei dati (a terzi o all'interessato) (diversamente da quanto prevede attualmente l'art. 13, comma 4, del Codice).

Cosa non cambia ...

- **Necessità dell'informativa con queste modifiche (modalità)**

Il regolamento specifica molto più in dettaglio rispetto al Codice le caratteristiche dell'informativa, che deve avere forma **concisa, trasparente, intelligibile per l'interessato e facilmente accessibile**; occorre utilizzare un linguaggio **chiaro e semplice.**

Informativa **per i minori** occorre prevedere informative idonee: "dato che i minori meritano una protezione specifica, quando il trattamento dei dati li riguarda, qualsiasi informazione o comunicazione dovrebbe utilizzare un linguaggio semplice e chiaro che un minore possa facilmente capire (considerando 58)

Cosa non cambia …

- **Necessità dell'informativa con queste modifiche (modalità)**

L'informativa è data,**in linea di principio, per iscritto** e **preferibilmente in formato elettronico** anche se sono ammessi "altri mezzi", quindi può essere fornita anche oralmente. Il regolamento ammette, soprattutto, l'utilizzo di **icone** per presentare i contenuti dell'informativa in forma sintetica, **ma solo "in combinazione" con l'informativa estesa** (queste icone dovranno essere identiche in tutta l'Ue e saranno definite prossimamente dalla Commissione europea).

Cosa non cambia …

- **Necessità dell'informativa: Raccomandazioni del Garante**

E' opportuno che i titolari di trattamento (quindi le scuole) **verifichino la rispondenza delle informative** attualmente utilizzate a tutti i criteri sopra delineati, con particolare riguardo ai **contenuti obbligatori** e alle **modalità di redazione** ,in modo da apportare le modifiche o le integrazioni eventualmente necessarie.

Cosa non cambia …

- **Diritti degli interessati**

- Diritto di accesso
- Diritto di cancellazione (diritto all'oblio)
- Diritto di limitazione del trattamento
- Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), 1 mese, estendibili fino a 3 mesi in casi di particolare complessità; il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.

Cosa non cambia…

- **Attori o figure di riferimento**

Il regolamento definisce **caratteristiche soggettive e responsabilità di titolare e responsabile del trattamento** negli stessi termini di cui alla direttiva 95/46/CE (e, quindi, al Codice italiano).

Pur non prevedendo espressamente la **figura dell' "incaricato" del trattamento** (ex art. 30 Codice), il regolamento **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"*(si veda, in particolare, art. 4, n. 10, del regolamento)*.

Cosa non cambia …

- **Attori o figure di riferimento**

Il regolamento:

disciplina la **contitolarità del trattamento***(art. 26)* e impone ai titolari di definire specificamente (con un atto giuridicamente valido ai sensi del diritto nazionale) il rispettivo ambito di responsabilità e i compiti **con particolare riguardo all'esercizio dei diritti degli interessati**, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari operanti congiuntamente (es. la gestione dell'organico attua una contitolarità di trattamento tra IISS e AT-USR-MIUR?)

Cosa non cambia…

- **Attori o figure di riferimento**

Il regolamento:

Fissa più dettagliatamente *(rispetto all'art.29 delCodice)* le **caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento** attribuendogli specifici compiti:deve trattarsi,infatti, di un **contratto**(o altro **atto giuridico** conforme al diritto nazionale) e deve **disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell'art.28** al fine di dimostrare che il responsabile fornisce"garanzie sufficienti“ quali, in particolare, la natura, durata e finalità del trattamento o dei trattamenti assegnati, le categorie di dati oggetto di trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel regolamento;

Cosa non cambia …

- **Attori o figure di riferimento**

Il regolamento:

Consente la **nomina di sub responsabili del trattamento** da parte di un responsabile *(si veda art.28, paragrafo 4)*,per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario; quest'ultimo **risponde dinanzi al titolare dell'inadempimento dell'eventualesub-responsabil**e ,anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso"non gli è in alcun modo imputabile"*(si veda art.82, paragrafo 1 e paragrafo 3);*

Cosa cambia ?

APPROCCIO BASATO SUL RISCHIO E MISURE DI ACCOUNTABILITY(RESPONSABILIZZAZIONE) DI TITOLARI E RESPONSABILI

Cosa cambia

Il regolamento pone con forza l'accento sulla"responsabilizzazione" (accountability nell'accezione inglese) di titolari e responsabili – ossia, **sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento***(artt. 23-25, in particolare, e l'intero Capo IV del regolamento)*.

Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali – nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

Ovviamente per gli enti pubblici questa “autonomia” decisionale è limitata dai pertinenti vincoli normativi

Cosa cambia

Il primo fra tali criteri è sintetizzato dall'espressione inglese **"data protection by default and by design"***(art. 25)*, ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. **Tutto questo deve avvenire a monte**, prima di procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto afferma l'art. 25 del regolamento) e richiede, pertanto, **un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili.**

Si tratta della mappatura privacy dei processi

Cosa cambia

Il primo fra tali criteri è sintetizzato dall'espressione inglese **"data protection by default and by design"***(art. 25)*, ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. **Tutto questo deve avvenire a monte**, prima di procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto afferma l'art. 25 del regolamento) e richiede, pertanto, **un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili.**

Si tratta della mappatura privacy dei processi

Cosa cambia

Fondamentali fra tali attività sono quelle connesse al secondo criterio individuato nel regolamento rispetto alla gestione degli obblighi dei titolari, ossia **il rischio inerente al trattamento**. Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati *(considerando 75-77)*; tali impatti dovranno essere analizzati attraverso un apposito **processo di valutazione***(artt. 35-36)*tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi. All'esito di questa valutazione di impatto il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare.

Cosa cambia

Registro dei trattamenti

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio*(art. 30, paragrafo 5)*, devono tenere un registro delle

operazioni di trattamento i cui contenuti sono indicati all'art. 30.

Si tratta di uno **strumento fondamentale** allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico **–indispensabile per ogni valutazione e analisi del rischio**. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

Quid iuris per le scuole?

Cosa cambia

- La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì **parte integrante di un sistema di corretta gestione dei dati personali**.

- I contenuti del registro sono indicati nell'art. 30 (vi è sostanziale **coincidenza fra i contenuti della notifica dei trattamenti di cui all'art. 38 del Codice e quelli che devono costituire il registro dei trattamenti ex art. 30 regolament**o.

- Il Garante invita tutti i titolari di trattamento a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche.

Cosa cambia

Misure di sicurezza

Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio "del trattamento (art.32, paragrafo1); in questo senso, **la lista di cui al paragrafo 1 dell'art.32 è una lista aperta e non esaustiva** ("tra le altre, se del caso").

Per lo stesso motivo, **non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure“ minime“ di sicurezza** *(ex art.33 Codice)* poiché tale valutazione sarà rimessa ,caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art.32 del regolamento.

Cosa cambia

Misure di sicurezza

Facendo riferimento alle prescrizioni contenute, in particolare, nell'Allegato"B“ al Codice, il Garante potrà valutare la definizione di linee-guida o buone prassi sulla base dei risultati positivi conseguiti in questi anni.

Inoltre,per alcune tipologie di trattamenti (ad es. quelli in ambito pubblico)potranno restare in vigore (in base all'art.6, paragrafo 2,del regolamento)le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili:è il caso,in particolare,dei trattamenti di dati sensibili svolti dai soggetti pubblici per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex. artt.20 e 22 Codice), **ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti**.

Cosa cambia

- **OBBLIGO DI DOCUMENTAZIONE DELLE VIOLAZIONI (data breach)**

Tutti i titolari di trattamento dovranno **documentare le violazioni** di dati personali subite e in alcuni casi notificarle all'autorità di controllo indicando le relative circostanze e conseguenze e i provvedimenti adottati *(art.33,paragrafo5)*.

Tale obbligo è sostanzialmente simile a quello attualmente previsto dall'art. 32-bis, comma7, delCodice.

I titolari di trattamento devono quindi adottare le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

Cosa cambia

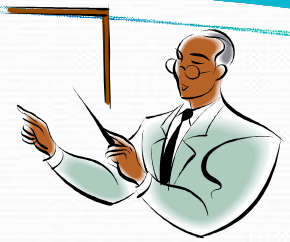
RESPONSABILE DELLA PROTEZIONE DEI DATI
(RDP o DPO)

- Viene introdotta una nuova figura: il "responsabile della protezione dati“ (RPD) o Data Protection Office r(DPO) - *art.39.*
- Si tratta di una figura finalizzata a facilitare l'attuazione del regolamento da parte del titolare/del responsabile.
- Fra i compiti del RPD vi è "la sensibilizzazione e la formazione del personale“ e la sorveglianza sullo svolgimento della valutazione di impatto di cui all'art. 35.
- La sua designazione è obbligatoria per gli enti pubblici *(art.37)*

La Scuola

Organigramma e dati personali

DIRIGENTE SCOLASTICO



Docenti
Collaboratori

Consiglio d’istituto

Direttore amministrativo

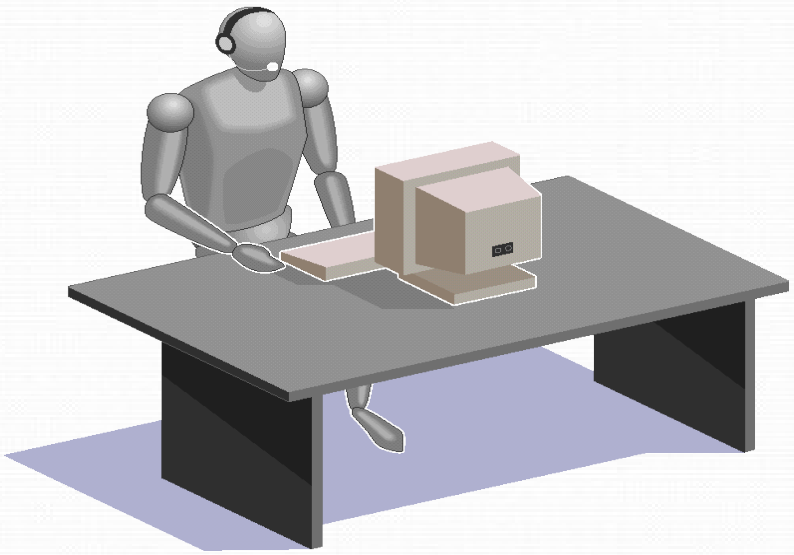
Docenti – Assistenti Amministrativi – Collaboratori Scolastici

Direttore amministrativo

- Contabilità
- Area personale
- Area didattica
- Area affari generali

Le aree di trattamento

- Didattica
  - Dati relativi agli alunni
- Personale
  - Gestione del personale
- Contabilità
  - Stipendi
  - Archivi relativi ai fornitori
- Affari generali
  - Protocollo
  - Archivio
  - Rapporti con enti e imprese



Area didattica / Dati relativi agli alunni

Cartaceo

❑ DATI PERSONALI

- Fascicolo personale
  - ✓Curriculum studi
  - ✓Dati personali
  - ✓Dati dei genitori
  - ✓Fotografia
- Registro iscrizioni
- Registro tasse scolastiche
- Registro certificati
- Registro diplomi

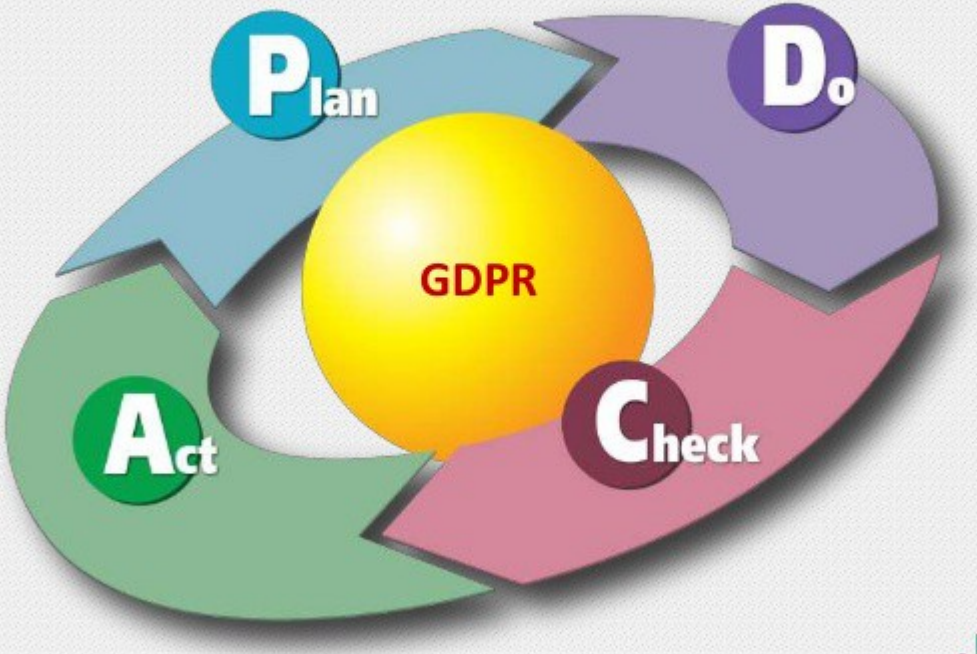
Area personale / Gestione del personale

Cartaceo

- COMUNICAZIONE dati personali

- ✓Elenchi del personale
- ✓Elenchi elettorali
- ✓Registro dei consigli di classe
- ✓Registro dei voti
- ✓Registro esiti esami e idoneità
- ✓Pratiche viaggi istruzione
- ✓Invio dati al CSA
- ✓INPS
- ✓INPDAP
- ✓Servizi Vari (MEF)
- ✓Ragioneria (MEF)
- ✓Altre scuole

GDPR – cosa fare per adeguarsi



CONSULENTI
PRIVACY TORINO

GDPR – cosa fare per adeguarsi

Raccolta di informazioni – sullo stato di adeguamento rif. Al Codice e al Regolamento Privacy, tipo di attività, strumenti aziendali, sistema informatico…

Stesura del piano privacy – obiettivi, fasi, tempi, responsabilità, budget e approvazione delle funzioni deputate

Interviste approfondite e analisi dei documenti – per poter svolgere le fasi successive di adeguamento al Regolamento e implementazione del sistema privacy

Analisi del contesto, delle esigenze , dei rischi e delle misure in essere o da implementare

CONSULENTI PRIVACY TORINO

GDPR – cosa fare per adeguarsi

Adeguamento al GDPR e implementazione del sistema di gestione della privacy – stesura di documenti, modelli, regolamenti e procedure; condivisione con le risorse aziendali e successiva applicazione

Adeguamento del sistema informatico – implementazione dei sistemi per arginare i rischi

Formazione del personale – corsi collettivi o specialistici anche in base alle attività da gestire

Gestione operativa – il sistema viene avviato

CONSULENTI PRIVACY TORINO

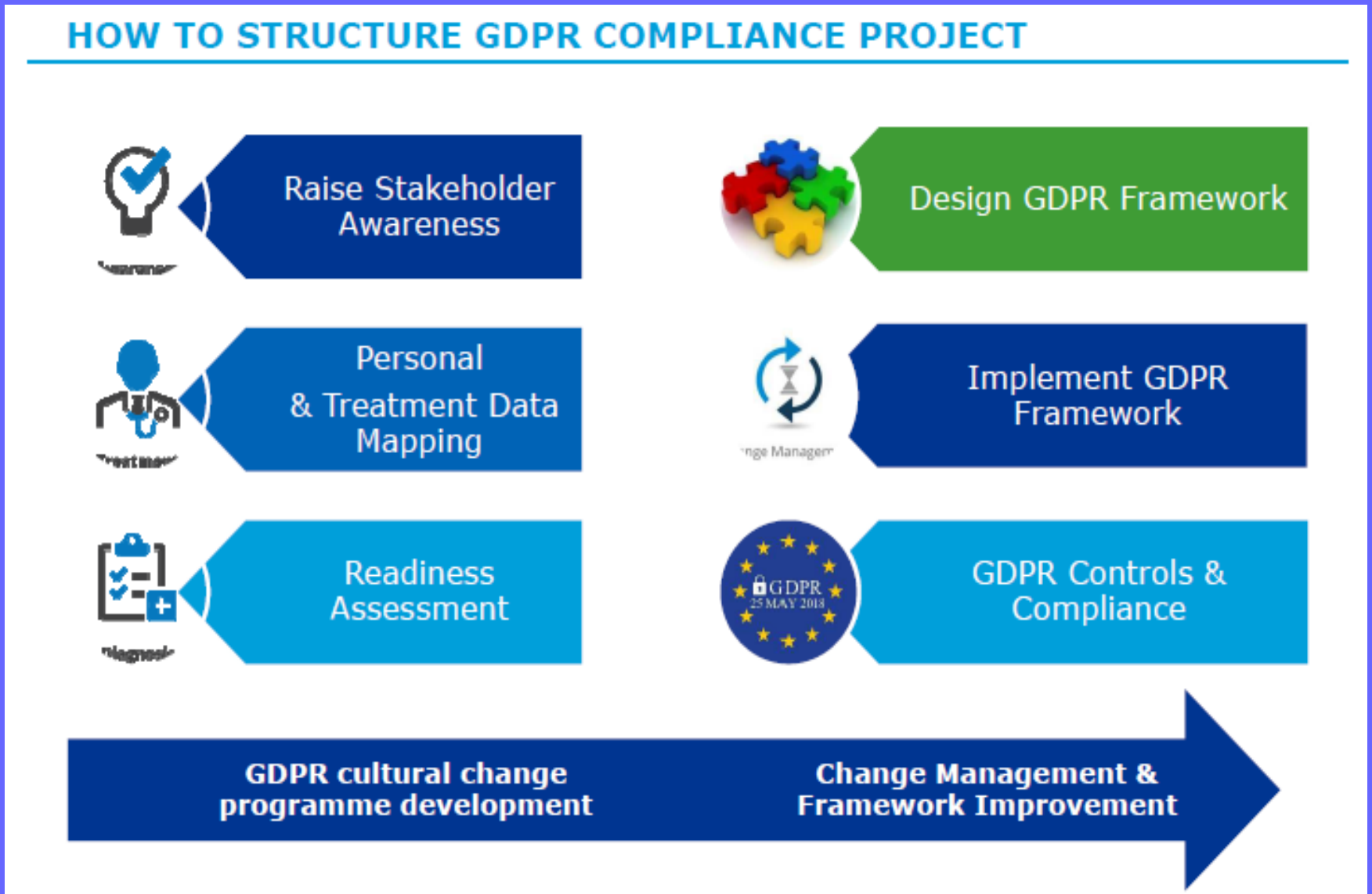
Le sanzioni amministrative pecunarie

Le violazioni agli obblighi in capo alle imprese (20 articoli su 49)
sono punite **fino a 10 milioni di euro o fino al 2% del fatturato mondiale annuo**.
Ad esempio:
> la violazione dell'obbligo di tenuta del registro dei trattamenti;
> la mancata valutazione d'impatto DPIA;
> l'omessa consultazione preventiva dell'Autorità;
> l'omessa notifica di data breach;
> l'omessa nomina del DPO;
> l'omessa adozione di misure di sicurezza adeguate.

Gli altri 29 articoli puniscono **fino a 20 milioni di euro o fino al 4 % del fatturato mondiale annuo** la violazione dei principi del regolamento e dei diritti degli interessati.
Ad esempio:

> i principi di base del trattamento, comprese le condizioni relative al consenso;
> i diritti degli interessati;
> i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale;
> l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo.

Cosa ci suggerisce l'Europa?



FINE DELLA PRESENTAZIONE

GRAZIE PER L'ATTENZIONE!