What the new EU GDPR means in 1 minute

The EU GDPR will increase privacy for individuals and give regulatory authorities greater powers to take action against businesses that breach the new laws. Here's what it means for your business:

Tough penalties: fines of up to

4% of annual global revenue

or

€20 million, whichever is greater.

The regulation also applies to **non-EU companies** that process personal data of individuals in the EU.

The **international transfer of data** will continue to be governed under EU GDPR rules.

The **definition of personal data** is now broader and includes identifiers such as

genetic

mental

cultural

economic

social identity.

Obtaining consent for processing personal data must be clear, and must seek an affirmative response.

Parental consent is required for the processing of **personal data of children** under age 16.

Data subjects have the **right to be forgotten** and erased from records.

Users may request a copy of personal **data in a portable format**.

The appointment of a **data protection officer** (DPO) will be mandatory for companies processing high volumes of personal data and good practice for others.

Privacy risk impact assessments will be required for projects where privacy risks are high.

Controllers must **report a data breach** no later than

72 hours

after becoming aware of the breach, unless the breach has a low risk to the individual's rights.

Products, systems and processes must consider **privacy-by-design** concepts during development.

Data controllers must ensure adequate contracts are in place to **govern data processors**.

Data processors can be held **directly liable** for the security of personal data.

Controllers must have a **legal basis for processing** and collecting personal data.

One-stop shop: international companies will only have to deal with one supervisory data protection authority.

ISO 27001 and other certifications will help demonstrate "**adequate technical and organisational measures**" to protect persons' data and systems.

You have to comply with EU GDPR by MAY 2018

Find out more

Read more about the implications of the regulation here.

How IT Governance can help you achieve compliance

IT Governance can help your business adequately prepare for the EU GDPR.
Our specialist and experienced privacy consultancy team are available to assist you with initial readiness assessments, gap analyses and data protection audits.

Contact us today for a EU GDPR gap analysis and audit

servicecentre@itgovernance.co.uk

+44 (0) 845 070 1750

Gli step (e gli aspetti) internazionali del GDPR

Prof. Avv. Giovanni Ziccardi
Università degli Studi di Milano
http://www.ziccardi.org

1. La scelta del Regolamento

- Si è voluto manifestare un momento di **rottura**, dopo oltre vent'anni di **Direttiva** e norme derivate.
- È una posizione normativamente **forte**: provvedimento contro le **piattaforme**, contro gli **over the top**, contro chi **profila**, contro chi **tace**, contro i **grandi**.
- Ci saranno possibilità **concrete** per intervenire contro questi soggetti?

1. La scelta del Regolamento

Un complicatissimo coordinamento tra le **fonti** (che già sta iniziando a manifestarsi)

1. Il Regolamento (Considerando + Articoli).
2. Norme **statali** per ciò che non è esplicitamente previsto dal Regolamento (e rimangono **escluse** aree importanti).
3. Gruppo di lavoro ex art. 29.

1. La scelta del regolamento

4. Singole **autorità di controllo** (quanto è importante conoscerle?).
5. Gruppo di lavoro italiano per **decreti** attuativi e di transizione.
6. **Codici** di condotta/interpretazioni di gruppi.
7. Policy **interne**, spesso provenienti da altri Stati e **tradotte**.

2. Gli Stati alla stessa velocità?

NO

- Italia con i suoi problemi (elezioni, la figura dell'incaricato, i dati trattati da autorità giurisdizionali, il quadro-sanzioni da coordinare).
- **Francia** che "spinge", **Germania** che già aveva un quadro definito e anticipatorio.
- USA: che stanno manifestando un rinnovato interesse, partendo da questa strana cosa (per loro) della efficacia "**universale**" del Regolamento.

2. Gli Stati alla stessa velocità

<u>Non si parla la stessa lingua</u>

Esempio di attività **formativa** a livello mondiale, e problemi di **comprensione** a volte insormontabili.

3. Il DPO come “collante” tra Stati?

- È la figura più “internazionale”, dovrebbe unire, dovrebbe essere un **presidio** in ogni realtà e in ogni Stato nei casi più importanti.
- La gestione del DPO nelle multinazionali, con un DPO **centrale** e, nel singolo Stato, o outsourcing di controllo/audit/revisione o officials, sta generando crisi.
- Figura **delicatissima** che può dare vita a esigenze di riorganizzazione.

4. I data breach: la minaccia condivisa

- La gestione del data breach, sia nel pubblico sia nel privato, come nuova **emergenza**.
- Un senso di assoluta impotenza.
- Problema realmente **internazionale**: saltano i confini
- Anticipato in Itala nel settore **pubblico**.

5. Una nuova geopolitica del dato

- I **registri** dei trattamenti e le **informative** che diventano mappe.
- Una volta le mappe si disegnavano sui tragitti dei viaggiatori e degli esploratori, oggi bisogna ridisegnare il **tracking** dei dati oltre i confini.

Conclusioni

- Impensabile non affrontare i temi in un’ottica **internazionale**.
- Ci sono Paesi più avanti di noi, con cui è utile il confronto ma anche il “furto” di documenti, linee guida e software.

Conclusioni

- Il dato **viaggia** anche se l'impresa o la realtà appare "locale" (si pensi al **cloud** o all'offerta di servizi dal web).
- Moli dubbi sull'idea di un quadro realmente **uniforme** (problema **dell'aggressività** del Legislatore statale, che non rinuncia).

Conclusioni

Da dove iniziare:

1. **Comprendere** il ruolo del DPO.
2. **Geopolitica** dei dati (registro dei trattamenti + tracking costante + attività ricognitive e di previsione varie, anche su rischi e impatto).
3. **Previsione** e **corretta** gestione di data breach.