



IS YOUR BUSINESS READY FOR GDPR?

IMPLICATIONS OF THE EU'S GENERAL DATA PROTECTION REGULATION FOR COMPANIES WORLDWIDE.



WHAT IS GDPR?

GDPR is a new framework for data protection laws, designed to strengthen and unify personal data protection and data handling across the EU.

Brexit impact:
UK will fully commit to GDPR regulations (through the Data Protection Bill)

GDPR WILL INTRODUCE NEW:

- data management obligations
- regime of potential fines in case of non-compliance
- enhanced rights for people to access the information companies hold about them (SARs)

Under GDPR, organizations only have

1 MONTH

to reply to **Subject Access Requests**

WHO NEEDS TO PREPARE?

Organizations that process personal data or provide or sell services to EU residents, **irrespective** of where the processing takes place.



If you are based:

- ✓ in the EU and collect or process EU resident personal data
- ✓ outside the EU and process personal data, monitor behavior or offer goods or services to EU residents

MANAGE THIRD-PARTY RISKS

Any third-party entity that processes personally identifiable information on behalf of your business is legally obligated to be in compliance with GDPR.

WHAT ARE THE CONSEQUENCES OF NON-COMPLIANCE?

Fines are only the tip of the iceberg.

Minor Offenses

e.g. administrative offense

up to **€10 million** or **2%** of a firm's global turnover*

Major Offenses

e.g. that have a legal effect on the rights and freedoms of the EU individual

up to **€20 million** or **4%** of a firm's global turnover*

*whichever is greater



Exclusion from business opportunities

Reputational damage and loss of client trust

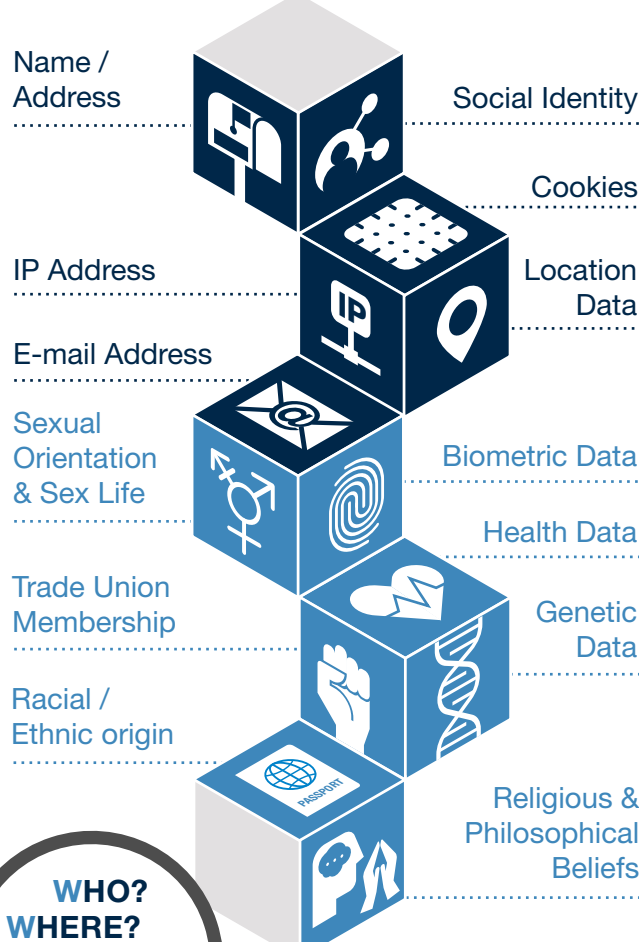


Legal redress open to class action

DATA BREAKDOWN

Categories of information that fall within the definition of "personal data" are subject to GDPR.

- Personal data
- Personal data classified as sensitive

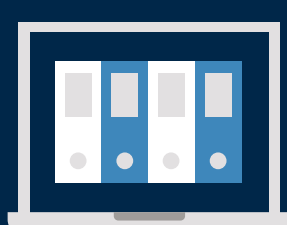


WHO? WHERE? WHAT? WHEN? WHY?

Data mapping identifies the **'5 Ws'** of personal data under your control

WHAT ARE THE ORGANIZATIONAL OBLIGATIONS RELATED TO GDPR?

Be accountable and demonstrate compliance ...



... by maintaining a record of all data processing activities.

Data Protection Impact Assessment is mandatory ...



... if the processing is likely to result in high risk to the rights and freedoms of the data subject.

Privacy and security by design and default ...



... through appropriate technical and organizational controls.

Data breaches need to be ...



... reported to the supervisory body / regulator within 72 hours.

A data protection officer ...



... needs to be in place if you are a public body, process personal data on a large scale or process sensitive data.

Transfer of personal data outside the EU ...



... is allowed only if appropriate safeguards are in place.

Under audits, the fulfilment of obligations needs to be demonstrated to the Data Protection Authority.

71%

of non-EU organizations struggle with assessing whether their GDPR preparations will be sufficient.**

**based on a "Privacy and the EU GDPR" survey conducted by TrustArc

60%

of companies are unprepared for GDPR.***

***based on a study by Senzing

ARE YOU FULLY INFORMED AND PREPARED FOR GDPR?

As a global consulting firm, Alvarez & Marsal can help you mitigate risk and limit your non-compliance fees. Contact us today to schedule a meeting with one of our GDPR consultants.

Phil Beckett
Managing Director
+44 207 663 0778
pbeckett@alvarezandmarsal.com

Mark Kindy
Managing Director
+1 212 763 9645
mkindy@alvarezandmarsal.com

Produced by A&M's Insight Center and Corporate Marketing

alvarezandmarsal.com



ALVAREZ & MARSAL