ARAVO

EU GDPR & THIRD PARTY RISK

Companies have until May 2018 to comply with the EU GDPR. This far-reaching data privacy regulation gives regulatory authorities greater powers to take action against companies that breach the law.

Too often companies' greatest risk exposure lies with third parties, so it is important to be considering and implementing your third party compliance programs now to protect one of your most valuable assets - your clients' private and personal information.

The regulation introduces tough new penalties of fines up to

4% ANNUAL GLOBAL REVENUE

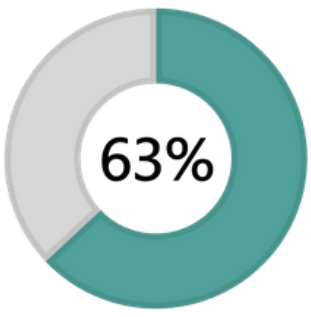
or

20 MILLION EUROS

whichever is greater

Third Parties Are Often Your Weakest Link

Third parties represent your biggest threat to data security - about 63% of all data breaches involve third parties.



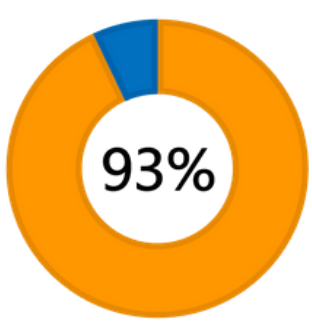
Some of the largest financial sanctions for data control failures have been because of third party actions.

HOME DEPOT

TARGET

AT&T

Look to trends in other regulation. 93% of FCPA sanctions are associated with third party actions.



The Regulation is broad and extra-territorial in scope. Applies to any entity that touches personal data on EU citizens, even if that entity did not collect that data itself.

The definition of personal data is broader, including identifiers such as: social identity, economic, cultural, physical, mental and genetic.
It extends consumer rights across: access, consent, correction, data portability and erasure.

There is a new provision for 'privacy by design' which calls for data protection to be built into products and services, rather than being tackled as an afterthought.

Companies will need to design compliant policies, procedures and systems at the outset of any product or process development.

Data Controller Vs Data Processor

A data controller is a person or organization who decides how data is to be stored and processed.
A data processor is a person or organization who uses that data for business purposes.

E.g. if a retailer collects customer information, which it shares with a third party call center, the retailer is the data controller, and the call center is a data processor.

Data Processor

Data Processors can be held directly liable for the protection of personal data.
If there is a breach, data processors must notify the company they're doing the work for, i.e. the controller, 'without undue delay'.

Data Controller

Data controllers must ensure that there are adequate contracts in place governing data processors. Controllers must report a data beach to the authorities no longer than 72 hours after becoming aware of the breach, unless the breach has a low risk to the data subject's rights.

A data breach is defined as any accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access to personal data.

Data breach → **72 hours** → Data Protection Authorities

notify

describing

- The number of records that have been exposed
- Categories of data breached
- Measures taken to mitigate adverse effect
- Measures taken to address the data breach
- Consequences of the data breach

If the breach is likely to result in a high risk to the rights and freedoms of the data subject

You must notify all data subjects that may be affected

A data breach exposes your company to the risk of significant **reputational damage.**

5 Steps To Take Now

To mitigate third party risk associated with the EU GDPR

1) BY 1H 2017

Partnering with your firm's Data Privacy or Compliance Officer, map your data. Understand where your data is (what third parties have access to it), what data they have (categories of data) and what they are doing with it. Make sure you only collect what is necessary and review legal grounds for processing.

2) BY 1H 2017

Ensure you have budget and resource allocated for completing GDPR assessments with third parties for 2017 and remediation projects in 1H 2018.

3) BY 3Q 2017

Review your contracts. GDPR contains new requirements for contracts with data processors, as well as between data controllers. Third parties should be categorized (as processors or controllers) and contracts should be reviewed for compliance with GDPR.

4) BY 3Q 2017

Complete a Pre-implementation Assessment of all your third parties that have access to, handle or touch your client/personal data to ascertain:

a) their awareness of GDPR;

b) that they have appropriate technical and organizational measures in place to comply.

Having this assessment completed by 3Q2017 will determine any high risk suppliers for further review.

5) BY 1Q 2018

Ensure that third parties are risk-scored according to assessments and other due diligence. For high-risk third parties, identify audit partners for the assessment of processes and to determine if on-site audits are required. Agree with your compliance team on remediation programs and on-going monitoring requirements.

You have until 18 May 2018 to be compliant with the GDPR.

Programs take time, so contact Aravo today to discover how we can support you with our GDPR third party risk management application.

info@aravo.com