InfosecPartners
CYBERSECURITY

#SECURITYMANAGED

European Data Protection gets an overhaul

The General Data Protection Regulation (GDPR) was finally approved by the European Union (EU) Parliament on 14 April 2016. The culmination of four years' work towards a complete overhaul of EU data protection laws, the GDPR will come into force 20 days after its publication in the EU Official Journal and its provisions will be directly applicable in all member states two years after this date, likely to be around May 2018.

The primary objective of the GDPR is to give citizens back control of their personal data - strengthening and unifying data protection for individuals within the EU, whilst addressing the export of personal data outside the EU.

Compliance requirements

GDPR will have a far reaching impact for organizations throughout the world. With the demise of Safe Harbour, companies that export and handle the personal data of European citizens will also need to comply with the new requirements put forth or be subject to consequences.

You could be fined €20 Million EUR for a security breach or 4% of global turnover, whichever is higher

If your organization suffers a data breach, under the new EU compliance standard, the following may apply depending on the severity of the breach.

- Your organization must notify the local data protection authority and potentially the owners of the breached records.
- The Data Protection Controller can order you to stop processing data or to delete it.

What is GDPR?

- The EU General Data Protection Regulation (GDPR) replaces the EU Data Protection Directive (DPD).
- A unified set of data protection rules across the EU, the GDPR has direct effect and does not require domestic legislation to be passed.
- The maximum penalty for a breach of the data protection legislation is €20M or 4% of global turnover whichever is higher.
- The GDPR catches data controllers and processors outside the EU whose processing activities relate to the offering of goods or services (even if for free) to, or monitoring the behaviour (within the EU) of, EU data subjects
- Data protection impact assessments such as those offered by Infosec Partners, are essential for demonstrating compliance to GDPR.

- The data subjects can sue you where their data privacy rights have been infringed.

Lower category penalty

- Penalties are broken out into two main categories, the lower category attracting a maximum penalty of 2pc of turnover, or €10m.
- This lower penalty is reserved for 'operational' breaches relating to the mechanisms of governance and control over personal data in the organisation.
- Examples include: not conducting data protection impact assessments during design of processing, not ensuring security controls are implemented, or not keeping a record of your processing activities or taking appropriate organisational and technical measures regarding security.

Higher category penalty

- Alternatively, your organization could be fined the higher penalty of up to €20 million or 4% of global turnover, whichever is higher.
- This higher penalty is reserved for fundamental breaches of core principles relating to obtaining and processing of data and the handling of requests from data subjects relating to their rights under the Regulation.

Get ready for GDPR: Eight immediate actions

1. Prepare for security breaches – be able to demonstrate you can react quickly to a breach.
2. Establish a framework for accountability.
3. Ensure Privacy by Design is embedded into processes and products.
4. Consider your data processing and how much personally identifiable information (PII) you process.
5. Ensure your privacy notices and policies are clear and easy to understand.
6. Consider the rights of data subjects.
7. If you are a supplier, consider whether you have new obligations. If you use suppliers, consider how they manage your client data.
8. Review the need for cross-border international data transfers.

GDPR COMPLIANCE ASSESSMENT

Evaluates an organisation's compliance to GDPR. The GDPR Compliance Assessment reviews the security policies and infrastructure in place, as well as agreements with 3rd party suppliers which may process data on their behalf.

Contact Infosec Partners today for more information on GDPR, the 'GDPR Compliance Assessment' and other security testing and managed security services designed to protect your organisation and manage risk.

There is no Safe Harbor

On 6th October 2015, the European Court of Justice (ECJ) – Europe's highest court – ruled that the US-EU Safe Harbour agreement between the European Commission and the US Department of Commerce was invalid.

Safe Harbor was an agreement set in 2000 which allowed US companies to self-certify they had appropriate security measures in place, streamlining data transfers between the two regions. The ECJ rules that the 15-year-old agreement invalid on grounds that EU citizens' privacy was endangered by government surveillance in the United States.

Companies which previously signed up to Safe Harbor, will now have to meet GDPR compliance or else they will face significant penalties.

InfosecPartners
CYBERSECURITY

A trusted advisor to significant organisations, Infosec Partners provides full-spectrum information security expertise and managed services to some of the world's largest and most sensitive businesses, high-profile individuals and families.

www.infosecpartners.com

Speak with a trusted advisor today:

+44 845 257 5903

secure@infosecpartners.com