FORTRA

FACT SHEET (Boldon James)

EU General Data Protection Regulation

Protect Sensitive Data on EU Citizens

The EU General Data Protection Regulation (GDPR) came into force on 25th May 2018, yet many organisations are still not fully prepared and compliant. This new regulation replaces the 1995 EU Data Protection Directive, and is intended to plug the trust gap, by modernising the legislation that safeguards personal data within the EU. It makes protection levels more stringent and consistent across member states, superseding fragmented national laws and standardising the way regulations are implemented, audited and enforced. The GDPR is not simply restricted to EU nations, but has an impact around the world, requiring compliance from any organisation in any sector that collects, processes, controls, hosts or shares EU citizens' personal data.

With the regulation having been enforced since 25th May 2018, it is important for organisations to get things in order now – determining the risks to be managed, understanding what data needs to be protected and starting to secure it now, and putting resources and policies in place. The best place to start is with data classification – the first step to a truly data-centric approach to protecting personal information.

Violating the regulation carries a maximum fine of **€20million, or 4% of annual global turnover (whichever is the higher amount)**; escalating data protection to a regular boardroom issue. Cost of non-compliance will also be assessed in terms of reputation loss and damage to the brand, while the regular and periodic data protection audits recommended in the regulation will make it more likely that incidences of non-compliance get picked up.

Secure Your Sensitive Data

The first step in using a data classification approach to ensuring compliance is to understand all of the personal or sensitive data you hold, and the potential risks to its security. You will need to ask:

- What data you already hold on EU residents?
- What data is being collected, and where from?
- Where is it being stored and processed?

Key Changes With The GDPR

- Violation of the GDPR exposes organisations to fines of up to €20million, or 4% of their annual global turnover (whichever is higher)
- All EU citizens have "The Right to be Forgotten"
- Organisations with over 250 employees must appoint a Data Protection Officer (DPO)
- Data processors and data controllers have equal legal obligations and responsibilities, and share joint liability for privacy violations
- Disclosure of a breach must be given to an organisation's national data protection authority (DPA), as well as affected individuals, within 72 hours of a breach occurring
- All organisations, regardless of size or location, must comply with the GDPR if they hold any personal data on EU citizens

- Why you have it?
- How sensitive it is?
- How it is accessed, used or shared - including externally?

The data should then be classified or tagged according to its sensitivity. Once you have singled out the most confidential information you can determine what higher grade controls should be applied to ensure it is adequately protected.

Don't Delay Your Preparations

The sheer volume of unstructured data within organisations, combined with the ever increasing technical abilities of hackers are finding to breach perimeters, make it impossible to rely on people and processes alone to ensure that sensitive personal data is handled appropriately.

Data classification embeds a culture of compliance by involving users in identifying, managing and controlling regulated data, while automating parts of the protection process to enforce rules and policies consistently.

As you prepare for the introduction of the amendment, classifying data as a first step will enable the protection strategy and solutions you implement to be built around the types of data you have, and the levels of security they require.

Visit boldonjames.com/gdpr for more information on how data classification can protect your sensitive data.

How Can Boldon James Help?

Boldon James Classifier, the market leading data classification product, supports compliance with the EU GDPR by:

- Ensuring appropriate control of confidential or sensitive information (as per Article 5)
- Classifying or labelling data with visual (and metadata) labels to highlight any special handling requirements
- Alerting users when personal data is leaving the organisation to warn or prevent them from sending messages that contain sensitive information
- Educating users about the sensitivity of data whilst ensuring adherence to corporate policy
- Providing critical audit information on classification events to enable remediation activity and demonstrate compliance position to regulatory authorities
- Enabling rapid search and data retrieval based on classification labels to support subject access requests
- Utilising metadata labels to drive additional security controls and solutions, such as DLP, encryption and rights management
- Orchestrating data management solutions, such as data retention and archiving, to ensure adherence to data storage requirements

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.