Infopaper

brainloop

Preparing your organisation for the EU data protection reform

Whether you are part of a European company or a non-European company that trades or stores data inside Europe, it is likely that the new European data protection regulations coming into play will affect the way you handle employee and customer data. So how do you prepare for the upcoming reform?

The General Data Protection Regulation (GDPR) is set to be fully implemented in 2017 and will unite the data protection regulations of each European country. GDPR has been designed to address the changing way businesses operate in the modern world, tackling issues surrounding the protection of personal data on social networking sites and data stored and transferred in the globally-accessible Cloud. But how will these changes affect those of us on the ground?

The introduction of penalties of up to 5% of global annual turnover and the obligation to report data leaks are sure to have a significant impact on the way companies approach data protection. In the absence of a crystal ball, here is a view of what companies can do to ensure that they are protecting the sensitive information they hold about their employees and customers and avoid being hit by new data protection penalties.

Think about how you work with other countries

Increased globalisation has led to a borderless business culture where data can travel between countries and devices instantaneously. The way we store and share data has changed rapidly in the past decade and it is necessary that the regulations surrounding data protection are reviewed and adapted to reflect this; an organisation's firewall cannot protect confidential documents or information when it is shared externally or to another country.

One of the major changes in the GDPR is expanding the territorial scope of the laws to not only include companies that are established in the EU, but also those that are based elsewhere but processing personal data of people residing in the EU. Now, many organisations that were outside the scope of application will now be directly subject to the requirements.

ICO Fines

5%

Up to 5% of Global Annual Turnover for data breaches. This puts Data Protection on a par with Anti-Bribery and Anti-Trust making compliance prohibitively expensive.

Data Protection Officers

The appointment of a data Protection Officer (DPO) may be mandatory.

Security Breach Notification

It will be mandated for organisations to report data breaches.

This development brings the important question of data residency squarely into the limelight for GDPR. Now more than ever, EU-based businesses and individuals are questioning if their data is being handled and stored in European-based data centres. Under GDPR, businesses will have to ensure that the information stored in their data centres never leaves the country-specific legal area without authorisation.

The recently repealed Safe Harbour Agreement between Europe and the United States shows that even the European Court of Justice (ECJ) believes that data from Europe is not always safe when stored overseas. New procedures will no doubt follow the repeal announcement, in which customers will likely be able to approve the transmission and processing of their data on both sides of the Atlantic. Despite this, businesses still run the risk of violating European privacy laws and allowing business-critical information to fall into the wrong hands if they store data outside the EU.

Review how you currently handle personal data

Whether you work in a small or large organisation, it is likely that you process a significant amount of personal data relating to employees and customers, be that in the form of contact details, social networking activity or professional and personal history. Given the uptake of Cloud services in recent years, this personal data is now unlikely to be stored solely within the organisation. In anticipation of GDPR, companies must review the way they collect, classify, store, share and protect the data they possess.

Under the new regime, the definition of 'personal data' is expected to broaden, bringing many more types of information into the regulated perimeter. Businesses will also have to make sure that this far wider scope of relevant data is secured by adopting modern encryption methods and other technical safeguards such as rights management, two factor authentication, operator shielding and full audit trails. While this may sound like a significant burden to businesses, many data-handling solution providers are already offering data protection by "default", meaning that products and services are automatically provisioned with the highest level of privacy.

While information is a valuable asset to businesses and one that needs to be effectively guarded to protect customer information and trade secrets, it also needs to be communicated and shared with third parties. There is a fine balance between enabling a business to continue to operate effectively with the right access to the data it requires, while also protecting the privacy of the data subjects and complying with regulations. Simple and secure technical measures need to be put in place to ensure this balance is possible.

«The European Court of Justice believes that data from Europe is not always safe when stored overseas.»

81%

of large organisations had an information security breach in 2014

58%

of large organisations suffered staff-related information security breaches

31%

Of the worst information security breaches were caused by inadvertent human

Sources:
2014 Information Security Breaches Survey by Department for Business Innovation & Skills

Collaboration has to be as simple as it is secure

In today's world, many companies need to collaborate with third parties to remain innovative but they also need to adhere to data protection regulations like GDPR in order to protect their customers' information and their own reputation. Using simple and secure data storage and sharing technologies will make it easier to fulfill both requirements of modern business.

When sharing data with third parties, wherever they are located, businesses should use a collaboration platform that is simple for employees to adopt and use and supports them in their everyday work, so it is perceived as a helpful tool rather than a hindrance.

To make it easier for your business to protect customers' data and comply with GDPR, you should opt for a collaboration platform that:

- Protects data transmission and storage by cryptographic means
- Has strong authentication measures to ensure only authorised users can access data
- Allows you to tailor users' access rights and modify what they can do with a document
- Provides a tamperproof audit trail, enabling traceable and transparent insight into how documents are being used and edited
- Is accessible securely when employees are travelling abroad or are out of the office

If you haven't already done so, now is the best time to start preparing your business for the full implementation of GDPR in 2017. By reviewing the way your company collects, stores and shares data with thes new data protection regulations in mind, you will be able to ensure your ongoing compliance and avoid devastating fines and reputational damage in the future.

Please get in touch to discuss how we can protect your business's valuable information london@brainloop.com

Brainloop. simply secure.

Brainloop is a leading provider of solutions for enterprise-wide collaboration on confidential information and documents, both within the company and beyond. Brainloop, which is headquartered in Munich, Germany and has subsidiaries in Austria, Switzerland, France, and the UK, was founded in 2000. The company counts a large number of midsized, Fortune and FTSE companies among its customers, as well as most of Germany's DAX 30 blue-chip groups.

«Brainloop Secure Dataroom resolves the challenge of protecting confidential information and delivers business solutions for Board Communications, Secure Collaboration, M&A and Due Diligence, Real Estate Portfolio Management, and more.»