Data Security and the General Data Protection Regulation (GDPR)

This document is purely for general guidance purposes and does not constitute legal advice or legal analysis.

Executive summary

Cyber-attacks and data security breaches have become an everyday occurrence and any organisation, whatever its size or type of business, can be a target. Every organisation has some form of personal data, such as customer details and employee information, that is highly prized by criminals.

IT professionals often ask what specific privacy and data security requirements they should implement in their organisation.

To answer the question, consider the following:

1. Carry out a detailed and objective privacy impact assessment setting out the personal data being processed and the processing operations and evaluate the risks. It is important to emphasise that this exercise is aimed at personal data rather than data in general.

2. Based on your evaluation of the risks, select the appropriate state-of-the-art technical and organisational measures that all stakeholders agree will be effective and capable of being implemented within the organisation. When considering these data security measures, the organisation should bear in mind that cyber-risk has to be managed in the same way as anything else that can damage the business. According to GDPR, the measures may include, pseudonymisation, encryption, measures ensuring on-going confidentiality, integrity, availability and the resilience of systems and services.

The GDPR – aims and penalties*

The General Data Protection Regulation (GDPR) aims to change the current EU data protection framework. GDPR was published on 27th April 2016 and provides a two-year transition period to allow organisations to adjust to the new requirements and procedures.

Following the end of this transition period, GDPR will be directly applicable throughout the EU from 25th May 2018, without requiring implementation through national law by EU member states. The goal of European regulators was to harmonise the current legal framework and to increase legal certainty. GDPR applies to the processing of personal data of an EU data subject and will include the activities of many overseas organisations. GDPR also introduces significant fines for non-compliance, including revenue-based fines of up to 4% of total annual worldwide turnover.

This is bad news for multinational organisations as it means that in many cases group revenues will be taken into account when calculating fines, even where some of those group companies, provided they are deemed to be part of the same undertaking, have nothing to do with the processing of data to which the fine relates.

GDPR makes it considerably easier for individuals to bring private claims against an organisation that is a data controller or processor.

The GDPR and data security measures*

Protecting personal data is a complex challenge. Many organisations are storing far more personal data than they actually need, including duplicates or out-of-date personal data, all of which adds unnecessarily to the burden of privacy compliance. The new data security requirements under the GDPR takes into account the data protection authorities' past experience and the new digital environment in which cyber-criminals operate as businesses and trade personal data in underground data markets.

Given the large potential fines, there may be a number of changes associated with the GDPR. One of the areas where significant change may occur in the next few years is data security, particularly the increased adoption of data pseudonymisation and data encryption best practices. GDPR requires organisations to implement technical and organisational security measures to provide appropriate protection to the personal data they hold. When determining the appropriate security measures, organisations must take into account the nature, scope, context and purposes of their use of personal data.

GDPR expressly states that data security measures include:

- The pseudonymisation and encryption of personal data
- Measures to ensure the resilience of the systems and services processing data
- Frequent testing of the effectiveness of the data security measures.

In summary, with the introduction of the GDPR, encryption and other security measures are established as data protection standards that an organisation may want to consider adopting or risk facing the consequences of non-compliance.

> “The GDPR gives regulators greater enforcement powers. If an organisation can't demonstrate that good data protection is a cornerstone of their business policy and practices, they're leaving themselves open to enforcement action that can damage their public reputation and possibly their bank balance. That makes data protection a boardroom issue.”

Elizabeth Denham
UK Information Commissioner

Source:
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/03/data-protection-practitioners-conference-2017/

*Most recent European Commission publication.
http://ec.europa.eu/justice/data-protection/reform/index_en.htm

How can Dell help?

Data-centric encryption

Dell Encryption Enterprise delivers a layered, multi-key approach to encryption that is unlike any other encryption solution available today. It automatically applies different encryption keys for different users and different types of data, ensuring that only the rightful owner can access sensitive information, even on multi-user systems. The solution also enables automated patch management and other system maintenance without requiring a separate process for encrypted systems. End-users can work just as they always have, while the data stays secure, from the device to the cloud. Encryption keys always remain within the enterprise network, so that IT and executives know that their corporate data is protected.

Organisations with limited in-house security expertise can quickly and easily configure their security using the smart policy settings that come as standard.

Protect, control, and monitor data

Dell Data Guardian can help your organisation to protect data, control data access and gain visibility into data usage while reducing infrastructure complexity. The solution combines encryption, data loss prevention (DLP) and digital rights management (DRM) with file activity monitoring, data visualisation and reporting - all in one integrated package from a single vendor.

Dell Data Guardian provides persistent encryption that protects files from the moment they are created and maintains that protection no matter where they travel or reside. Plug-ins for Microsoft Office automatically encrypt new Word, Excel and PowerPoint files. It can also conduct a sweep of a device to encrypt any unencrypted Word, Excel and PowerPoint files. Each file remains encrypted whether an employee sends it to a colleague by email, moves a file to a network file share, transfers it to an external drive or shares it with colleagues through cloud services like Box, Dropbox, Google or Microsoft.

Advanced threat prevention solutions

Dell Endpoint Security Suite Enterprise and **Dell Threat Defense** are leading-edge, advanced threat prevention solutions using artificial intelligence and machine learning technology that prevents malware from executing before it can do any damage. The solutions are lightweight and sparing on system resources, typically using 1%-3% when malware is detected. The mathematical analysis of files for over 600 mathematical attributes and characteristics allows the technology to detect known and unknown malware (zero-day threats) with an efficacy rating of in excess of 99%.

Dell Endpoint Security Suite Enterprise is targeted at businesses that require encryption and advanced threat protection on the endpoint. The on-premises management server allows businesses to manage both technologies from one management console, enabling policy distribution to clients and integrated compliance reporting.

> “If a business can’t show that good data protection is a cornerstone of their practices, they’re leaving themselves open to a fine or other enforcement action that could damage bank balance or business reputation.”

Elizabeth Denham
UK Information Commissioner

Source:
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/01/gdpr-and-accountability/

Dell Threat Defense is targeted at small and medium businesses that require an effective advanced threat prevention solution. It is easy to set-up for businesses that do not have a dedicated IT department, is easy to deploy and can be centrally managed via a cloud-based console while offering subscription-based pricing.

Cloud-based backup and recovery

Dell Mozy Pro allows you to seamlessly manage backup, sync and mobile access for multi-user environments from a single web-based console. As one of the industry's leading cloud backup service providers, Mozy takes seriously the protection of your data in the cloud by utilising the most comprehensive security and privacy measures. Mozy encrypts your data before it ever leaves your machine, during the transfer process across the wire and while at rest in our data centres, which employ state-of-the-art physical and technical security practices. Mozy also takes proactive steps to protect against attacks, hazards or unauthorised access that could threaten the security, privacy and integrity of your data. In the business of protecting your data and your business, Mozy's strict security policies, industry-standard encryption and world-class data centres deliver the availability, security and privacy needed for the optimal protection of your business data.

Conclusion

As security of personal data becomes ever more central to economic growth and for society at large, the organisational costs of losing or misusing it are increasing and can be devastating from reputational and financial perspectives. The GDPR will drive fundamental changes in the way many organisations process and secure personal data. Given the increasing risk of cybersecurity threats, it is highly likely that a breach is a 'when' not an 'if' event. This means that organisations will need to focus on technical and organisational security measures in their processing activities to comply with GDPR security processing requirements.

At Dell we are committed to helping organisations to successfully comply with the GDPR security processing requirements with our security solutions and innovative technology. Dell offers organisations with the flexibility of deploying hardware-agnostic endpoint solutions as stand-alone security software on our customer's choice of hardware, or for a more integrated approach, customers can purchase them pre-installed on commercial Dell Latitude, OptiPlex, Precision and select XPS systems.

Learn more about the revolutionary Dell Data security solutions at **Dell.com/datasecurity**

This document is for informational purposes only, and may contain typographical errors and technical inaccuracies. The content is provided as is, without express or implied warranties of any kind. The contents are not intended – and under no circumstances may be used or relied upon – as legal advice. If you have any questions about your organisation's legal or regulatory requirements, please consult with an attorney.