Meet EU General Data Protection Regulation Compliance Seamlessly with Dell Data Security Solutions

If you do business with customers in Europe you need to comply before May 2018!

The European Parliament officially adopted the General Data Protection Regulation (GDPR) on 14 April 2016. This is the most comprehensive reform to the EU's data protection law in 20 years. Companies have until May 2018 to review their policies and ensure they are proactive and compliant with cyber security before the Regulation becomes a legal legislation.

Data protection has up until now mainly been regulated in the EU under a 1995 Directive that controls the processing of personal data. The 28 EU Member States had to adopt their own national legislation to implement this Directive.

In 2012, the European Commission officially began the legislative reform process with the overall objective of significantly overhauling the 1995 rules in order to catch up with the huge advances of the digital age.

The new Data Protection Regulation will apply one consistent set of requirements for all organizations that hold data on European citizens. It will be directly applicable in all Member States without the need for implementing national legislation.

Dell Data Security Solutions ensures encryption is embedded into all endpoints, so organisations can quickly and easily gain business assurance, enabling an easier path to data protection, demonstrate compliance and business continuity for both Dell and non-Dell systems.

Dell Data Protection | Encryption (DDP | E) provides you with the confidence that your data and your customers' data is secure, with a solution designed for simple, comprehensive and flexible protection. It is a policy-based solution that protects data stored on the system drive and/or external media.

Designed for easy deployment, end-user transparency, and hassle-free compliance, the DDP | E portfolio of products delivers a high level of protection and fills critical security gaps.

- Encrypt and secure data across multiple endpoints from a common management platform.
- Easy generation of automatic audit trails that offers proof of end-to-end data security.
- Customizable reporting on all endpoints including multi-vendor IT landscapes.
- Protection of unprotected personal data from leaving the organisations on USB flash drives or other forms of removable media.
- Provide a transparent end-user interface that supports user productivity and keeps data safe.
- Protection of data from unwarranted access, thus reducing risk of internal breaches.

Learn more at dell.com/datasecurity

Who does GDPR impact?

The Regulation applies to organizations within the EU and to those organizations outside of the EU that offer goods and services to, or monitor the behaviour of EU citizens. In terms of personal data security, this means implementing appropriate security measures to protect the data.

> "The Information Commissioner's Office (ICO) guidance is clear: all personal information–the loss of which is liable to cause individuals damage and distress–must be encrypted. Encryption is one of the most basic security measures and is not expensive to put in place–yet we continue to see incidents reported to us. This type of breach is inexcusable and is putting people's personal information at risk unnecessarily."
>
> Sally Anne Poole
> Enforcement Group Manager, ICO

As a regulation and not a directive, the GDPR will have immediate effect on all 28 EU Member States after the two-year transition period and does not require any national changes in legislation. Companies will be required to adapt to the new regulation, begin preparing for compliance, and complete implementation before May 2018. Although it sounds like a lot of time, a great deal of preparation will be necessary to bring an organisation into line with the requirements.

Primary elements of GDPR around protecting personal data

The GDPR legislation is very broad and covers many aspects of personal data. The following are elements of GDPR that govern data security:

Data Breach Notification

Breaches will have to be reported, including what action has been done to mitigate them, to the Data Protection Authorities (DPA) not later than 72 hours after a data controller has become aware of the breach.

A reasoned justification must be provided if this time frame is not met. In most cases, the data controller must also notify the affected data subjects without undue delay.

Removal of notification requirement

The text also contains a welcome threshold. Notification does not need to be made to the DPA if the breach is unlikely to result in a risk to the rights and freedoms of individuals. Instead of notification, the policy now requires data controllers to put in place effective procedures and technologies.

Encryption is widely agreed to be the best security measure available as it renders the data unintelligible to unauthorized parties in cases of data loss. The law specifically encourages data controllers to implement technologies such as encryption to safeguard data.

Sanctions

The approach to penalties under the GDPR has propelled data protection into the boardroom.

The Data Protection Authorities are now endowed with a number of powers including issuaance of non-compliance warnings, carry out audits, requiring specific remediation within a specified time frame, order erasure of data and suspend data transfers to a third country. Crucially, they are also empowered to issue substantial administrative fines.

The authorities can impose fines up to €20 million or 4% of annual worldwide turnover. Less serious violations would incur fines up to €10 million or 2% of annual worldwide turnover.

However, if the data controller has "implemented appropriate technological protection measures that render the data unintelligible to any person who is not authorized to access it, such as encryption"; the likelihood of being fined as a result of a breach should be very greatly reduced & organizations don't need to notify affected data subjects of the breach.

How can Dell help?

Data security is increasingly becoming a bigger problem for organisations of every industry and geography. Security breaches have quickly escalated into a major source of reputational damage, business interruption, erosion of customer confidence and economic loss.

Encryption helps protect both against the **likelihood** of a security breach arising in the first place and the adverse **consequences** of the breach – both for the individuals whose data are compromised and also for the business in terms of mitigating its liabilities following the breach.

According to a survey carried out by Vanson Bourne* , 69% of respondents state that they will need to make investments in technology to reduce the impact of the new data protection regulation, with encryption being the technology most likely to be invested in.

http://www.vansonbourne.com/research-insights/

Dell Data Protection | Encryption solution offers the most comprehensive and complete protection of data at rest for all Dell and non-Dell clients. .

Dell Data Protection | Encryption provides policies designed to address security goals, or customers can create their own policies to help them meet with regulatory compliances. Having out of the box, policies helps kick start organisations on the road to compliance and creates the functional equivalent of a 'safe harbour' in the event of a breach.

Deploy endpoint encryption as part of a standard refresh cycle

Dell Data Protection | Encryption can be pre-installed at factory for a small nominal extra fee. In essence, the sofware just becomes a line item in the standard PC configuration. It can be pre-installed on any and every Dell PC.

This has significant advantages:

- Eliminates the need for extra budget approvals.
- Spreads the budget over the course of your refresh cycle.
- Factory pre-installation allows for a faster and easier deployment.
- The encryption server console automatically detects new "GDPR ready" machines when they are connected to the network and applies the security strategies and policies

Depending on your refresh cycle, by the time the regulation becomes law; you will already have the majority of your endpoints "GDPR ready".