Data Security Solutions for Compliance with EU General Data Protection Regulation (GDPR)

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

Rapid advancements in technology and mounting cyber-criminal activities serve as catalysts for changes in the current Data Protection Act 1998 (DPA). In addition, numerous variations in the enforcement of data protection by each member state under the current directive led to the need for a uniform and consistent structure to guide, monitor and enforce data protection.

The EU is currently finalizing the new General Data Protection Regulation (GDPR) with expected adoption in late 2015 or early 2016. The GDPR proposes a single law for data protection to cover all 28 EU member states in place of the current DPA.

Solutions statement

Dell can help you gain business assurance, enabling an easier path to data protection, compliance and business continuity for both Dell and non-Dell systems.

Dell Data Protection | Encyption (DDP | E) is a flexible suite of enhanced security solutions that can help you comply with the evolving EU data security regulations. The comprehensive suite can help EU states meet the GDPR data security compliance mandates.

DDP | E delivers data security across the broadest range of devices and platforms, from iOS and Android mobile devices, cloud, external media, self-encrypting drives, Microsoft BitLocker™, to Dell and non-Dell Windows PCs and Mac.

Being compliant with global regulatory mandates is easier with DDP | E.

- Encrypt and secure data across multiple endpoints from a common management platform.
- Easy generation of automatic audit trails that offer 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 organization 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.

Who does GDPR impact?

GDPR mandates should be of global interest, since it extends to organisations operating in Europe regardless of whether the data they handle is stored within the boundaries of the EU or not. The GDPR will affect any organisation that gathers, processes, or stores personal data, and defines personal data as any information about an individual, whether it relates to his or her private, professional or public life.

"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

This is very similar to many US data protection laws. For example, a company based in France doing business with American customers in California must comply with California's data protection law. If that same company also does business with customers in Massachusetts, then it must also comply with Massachusetts' data protection law, and so on.

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 by approximately the end of 2017. 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:

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

The proposed legislation will require everyone who holds data on European citizens to implement appropriate security measures to protect the data, and have a clear data protection policy. That data may include names, photos, email addresses, bank details, posts on social networks, medical information or a computer's IP address.

Although regulation beyond EU borders will be a challenge given the huge proposed fines, those providing products or services to EU customers or processing their data may have to face the long arm of the law if an incident is reported.

Fines for non-compliance could cost millions

When finalized the Regulation will enforce tough penalties, a step welcomed by privacy advocates. The previous DPA Directive's penalty measures were open to interpretation and applied at the discretion of the individual member states. The new Regulation lays out a strict regime of sanctions. Under the proposed legislation, organisations can incur fines of up to €100 million or 2% of global annual turnover, if they suffer a breach of personal data.

In addition, they will have to notify affected customers of the breach, with all the associated costs and loss of reputation.

However, if companies can show that the personal data was subject to technological protection measures rendering it unintelligible to unauthorized people (e.g. encryption), they don't need to notify affected data subjects of the breach;and the likelihood of being fined as a result of a breach should be very greatly reduced.

The "appropriate" nature of security is loosely defined

The Act does not define "appropriate." However, it does say that an assessment of the appropriate security measures in a particular case should consider technological developments and the costs involved. The Act does not require having state-of-the-art security technology to protect the personal data held, but recommends the level of security adequately support the risk management strategies of an organisation.

Encryption is widely agreed to be the best data security measure available as it renders the data unintelligible to unauthorized parties in cases of data loss. Due to the increase number of reports of stolen laptops containing personal information from vehicles, dwellings or forgotten in public places without being protected adequately, the ICO has formed the view that in future, where such losses occur and where encryption software has not been used to protect the data, regulatory action may be pursued.

The ICO further recommends that portable and mobile devices including magnetic media used to store and transmit personal information, the loss of which could cause damage or distress to individuals, should be protected using approved encryption software designed to guard against the compromise of information.

The worst data breach incidents are costing UK businesses between £1.5–£3 million on average through business disruption, lost sales & assets and damage to reputation, according to new research by the UK government and consultancy PwC. (June 3, 2015)

Encryption provides 'safe harbour'

DDP | E's comprehensive solution offers the most comprehensive and complete protection of data at rest for all Dell and non-Dell clients, and Full Volume Encryption on Dell Latitude, OptiPlex and Precision systems.

DDP | E provides pre-defined templates designed to address specific security goals, or customers can create their own templates to help them meet with regulatory compliances. Having out of the box, pre-set templates helps kick-start organisations on the road to compliance and creates the functional equivalent of a 'safe harbour' in the event of a breach.

Next steps for organizations

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.

Develop processes now to deal with data breaches. Every organization must address compliance requirements in terms of their unique business goals and technical environment. As next steps, organisations should re-evaluate existing IT security to ensure measures are in place to prevent privacy breaches. How you store, manage and secure data is going to be trickier to manage, including data stored in the cloud.

This is especially important for small businesses that often times lack robust IT resources. Determine whether an endpoint data protection—including encryption—enables the organisation to avoid breach notification requirements of GDPR including information transferred overseas to other parties.

Cross-border data transfers

As with intra-group international data transfers, it will be important to ensure that there is a legitimate basis for transferring personal data to jurisdictions that are not recognised as having adequate data protection regulation.

Failure to comply with the proposed regulation's requirements in cross border data transfers could attract a fine of up to 2% of annual worldwide turnover; the consequences of non-compliance could be severe.

In sum, 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.

Data breach planning should be at the same level organisations would consider any other major business risk. It requires the same level of planning, the same level of rehearsal and the same level of practice.

About Dell

Dell Inc. listens to our customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.dell.com.

Learn more at dell.com/dataprotection