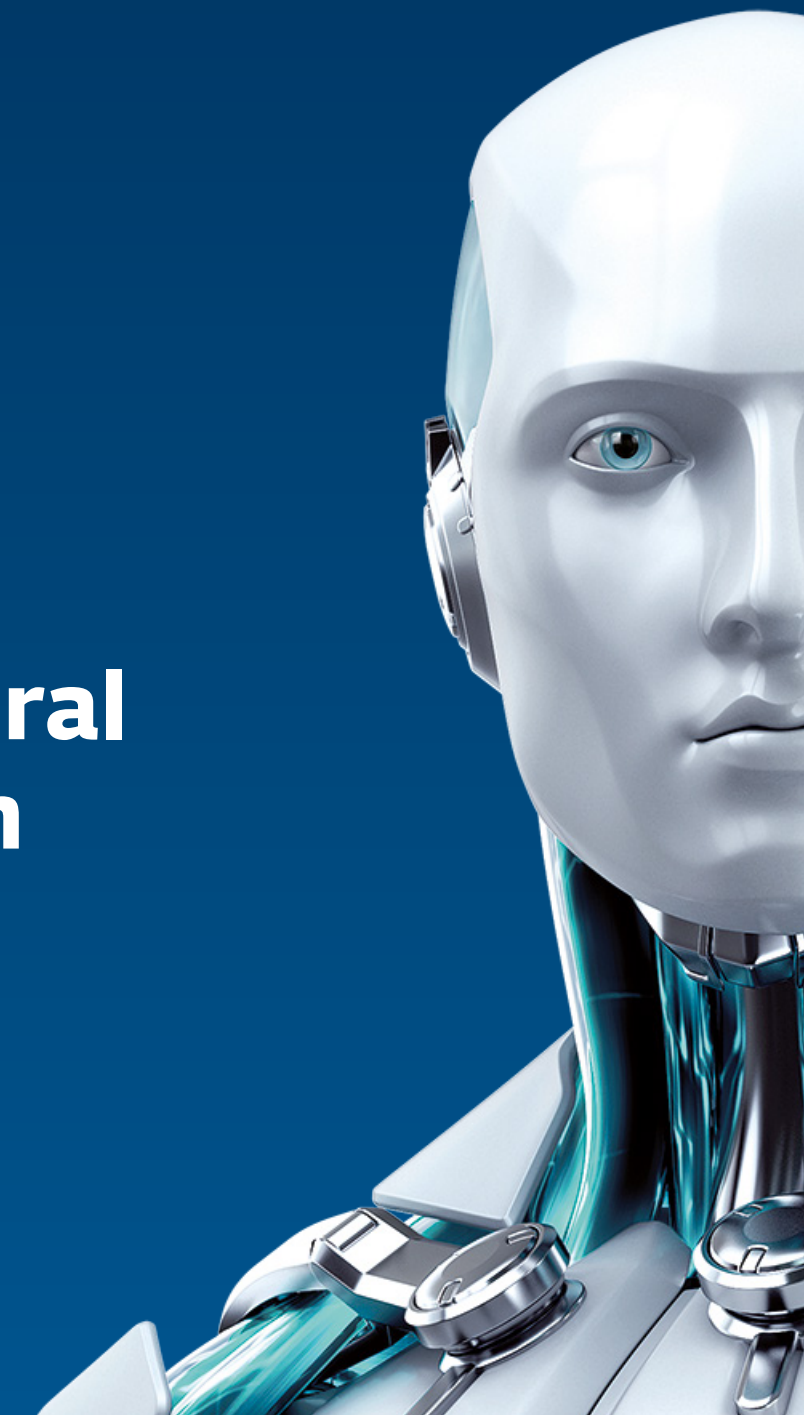
ESET TECHNOLOGY ALLIANCE

DESlock+
protect your data.

Quick guide to the EU General Data Protection Regulation

2016 sees the 1995 Data Protection Directive brought up to date with new EU-wide Regulation



ENJOY SAFER TECHNOLOGY™

The General Data Protection Regulation (GDPR) is a comprehensive reform of the EU's 1995 data protection regulation, being developed to strengthen and unify online privacy rights and data protection for individuals within the European Union (EU) while streamlining the data protection obligations of businesses serving EU citizens through a single Regulation instead of 28 different National laws.

The initial proposal for GDPR was released on 25 January 2012 with the aim of formal adoption in early 2016.

The European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) voted positively on the outcome of the negotiations between the European Parliament, the European Commission and the European Council with adoption expected in Spring 2016. Unlike a Directive, a Regulation does not require any additional legislation from National Governments and enforcement of the GDPR is timetabled to start in the first half of 2018.

The 28 EU Member States have implemented the 1995 rules differently, making it difficult and costly for EU businesses to operate across internal borders and with gross differences in enforcement. It is estimated that the elimination of this fragmentation will lead to savings for businesses of around €2.3 billion a year across the European Union.

WHAT ARE THE CHANGES?

Key changes in the reform include[1]:

- The right to know when one's data has been hacked: Companies and organisations must notify the national supervisory authority of data breaches which put individuals at risk and communicate to the data subject all high risk breaches as soon as possible so that users can take appropriate measures.
- Stronger enforcement of the rules: data protection authorities will be able to fine companies who do not comply with EU rules up to 4% of their global annual turnover.
- One continent, one law: a single, Pan-European law for data protection, replacing the current patchwork of national laws. Companies will deal with one law, not 28. The benefits are estimated at €2.3 billion per year.
- Organisations must notify the national authority of serious data breaches as soon as possible (if feasible within 24 hours).
- EU rules must apply if personal data is handled abroad by companies that are active in the EU market and offer their services to EU citizens.
- Data protection by design and by default: 'Data protection by design' and 'Data protection by default' are now essential elements in EU data protection rules. Data protection safeguards will be built into products and services from the earliest stage of development, and privacy-friendly default settings will be the norm.

By making Data Protection an essential, key element of the regulation The EU is making it mandatory for businesses to adequately protect sensitive personal data, defined as:

"any information relating to an identified or identifiable natural person hereinafter referred to as 'data subject'; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity;"[2]

This broad definition of personal data easily covers the simplest records relating, even indirectly, to customers, clients, staff, pupils and any other record relating to an individual.

1 Press Release Summary: http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm

2 REGULATION (EC) No 45/2001: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2001.008.01.0001.01.ENG

WHAT DOES THE REGULATION SAY ABOUT PROTECTING DATA?

Section 2, Data Security, Article 30: Security of Processing states[3]:

1. Having regard to the state of the art and the costs of implementation and taking into account the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, the controller and the processor shall implement appropriate technical and organisational measures, to ensure a level of security appropriate to the risk, including inter alia, as appropriate:

a) the pseudonymisation and encryption of personal data;

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data;

c) the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

Article 30 removes any doubt as to whether systems and storage which leave secure premises should be encrypted. The technology is an established well-known means of protecting information which is vulnerable to theft or loss. It also makes the case for effective disaster recovery plans, password recovery and key management systems.

Article 28 of the Regulation[3] requires that records must be kept including a general description of the technical and organisational security measures taken, as referred to in Article 30, meaning that organisations need records and proof that systems are secure and that encrypted data is recoverable after a technical incident.

3 Text of the Regulation: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

WHAT ARE THE DATA BREACH-NOTIFICATION RULES?

Article 31[3] details Notification of a personal data breach to the supervisory authority and requires that in the case of a personal data breach, notify the Supervisory Authority where feasible, not later than 72 hours after having become aware of it. Any notification beyond 72 hours must be accompanied by a reasoned justification for the delay.

Article 32[3] refers to the communication of a personal data breach to the data subject and states that:

When the personal data breach is likely to result in a high risk the rights and freedoms of individuals the controller shall communicate the personal data breach to the data subject without undue delay.

However, it goes on to state that:

The communication to the data subject referred to in paragraph 1 shall not be required if:

a) the controller has implemented appropriate technical and organisational protection measures, and that those measures were applied to the data affected by the personal data breach, in particular those that render the data unintelligible to any person who is not authorised to access it, such as encryption; or

b) the controller has taken subsequent measures which ensure that the high risk for the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; or

c) it would involve disproportionate effort. In such case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Studies have shown that the earlier a data breach is reported the more damaging are the consequences to the organisation in question. Again, it is clear that encryption is considered a sufficient safeguard to preclude this and the consequences for corporate reputation.

HOW DOES THE REGULATION DISCOURAGE OFFENDERS?

Point six of Article 79[4], Administrative sanctions states:

The supervisory authority shall impose a fine up to 1,000,000 EUR or, in case of an enterprise, up to 2% of its annual worldwide turnover, to anyone who, intentionally or negligently:

> Note (e) does not adopt internal policies or does not implement appropriate measures for ensuring and demonstrating compliance pursuant to Articles 22, 23 and 30;
>
> Note (h) does not alert on or notify a personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the data subject pursuant to Articles 31 and 32;

This clear intent to penalise and discourage offenders will come into force over the next two years so it's time to act now.

Some countries have already started work; The Dutch senate passed a bill in May 2015 to amend their Data Protection Act in anticipation of and pre-empting the GDPR, moving the Netherlands from one of the most weakly enforced of Europe's nations to one of the strongest. The regulation will be enforced throughout all 28 member states by mid 2018.

WHAT MEASURES SHOULD BE TAKEN NOW?

The Regulation requires organisations of all sizes to adopt a new set of processes and policies aimed at giving Individuals greater control over their personal records. Much of this will involve writing new processes and manuals, retraining staff and updating systems to accommodate these new procedures. Other steps involve practical measures, such as employing encryption where data is exposed to risk.

A lost or stolen laptop or USB stick need not lead to a penalty if it has been encrypted with a validated product. DESlock software has been helping organisations of all sizes to encrypt laptops, removable media, email and files for many years. Our products cover all Windows platforms from XP to Windows 10 and iOS from Version 7 and up. Our software is built upon a FIPS 140-2 level 1 validated cryptographic subsystem and our key management system and unique management server are the subject of worldwide patents.

Contact ESET in your region or your ESET Reseller for more information, to arrange a product demo or for trial software.

One of the key requirements of the EU GDPR is that Personal Data is encrypted; where encryption is used as a technical measure it must be possible to restore it promptly after an incident and records must be kept to prove that systems are both secure and recoverable.

DESlock is designed to tackle these requirements in a simple and effective manner.

4 Text of the Regulation: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

Objective	DESlock+
Secure data at rest within the organisation	All commercial versions of DESlock+ include file, folder and removable media encryption as standard to secure data at the endpoint.
Secure data in transit	DESlock+ Pro includes full-disk and removable media encryption for USB drives and optical media to secure data on the move
Secure data for mobile / home working practices	Commercial DESlock+ licences extend to a second installation on a privately-owned PC. Beyond this, DESlock+ Go adds portable encryption to any USB storage device.
Secure transfer of data between locations	All versions of DESlock+ include an Outlook plug-in, clipboard encryption compatible with all mail clients including webmail, and attachment encryption for any system. optical media encryption allows the safe transfer of data stored on CD or DVD.
Block / Limit access to certain data	Unique, patented key-sharing technology make it simple to deploy and manage complex, multi-layered teams and workgroups.
Allow access to secure data when requested.	The DESlock+ Enterprise Server is designed for remote user management via a secure internet connection. Keys may be centrally distributed and withdrawn rapidly.
Secure safe storage of personal data	DESlock+ is FIPS-140-2 validated and uses reliable, approved and secure industry standard encryption algorithms and methods.
Secure destruction of redundant data	The DESlock+ Desktop Shredder tool securely deletes data to the DoD-5220.22-M standard ensuring that it is completely unrecoverable.

Further Information

General Information
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2015/15-12-08_Truste_speech_EN.pdf

Details of the Regulation
http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf

Draft Compromise
http://www.statewatch.org/news/2015/dec/eu-council-dp-dir-leas-draft-final-compromise-15174-15.pdf