GDPR

Quick guide to the EU General Data Protection Regulation

ENJOY SAFER TECHNOLOGY®

The General Data Protection Regulation (GDPR) replaces the EU's 1995 Data Protection Directive 95/46/EC. The GDPR has been 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.

On 8 April 2016 the Council adopted the GDPR and an associated Directive. And on 14 April 2016 the Regulation and the Directive were adopted by the European Parliament.

On 4 May 2016, the official texts of the Regulation and the Directive were published in the Official Journal of the European Union. The Regulation will apply from May 25, 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 considerable 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 that 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 that do not comply with EU rules up to 4% of their global annual turnover. Administrative fines are not mandatory and if imposed must be decided in each individual case and must be effective, proportionate and dissuasive.
- 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 their goods and services (including free goods and services) to EU citizens, or if these organizations monitor the behavior of individuals in the EU.
- 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.

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

By strengthening data protection 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 that relate, even indirectly, to customers, clients, staff, pupils and any other record relating to an individual.

What does the Regulation say about protecting data?

Article 32, Security of processing states:[3]

> 1. *Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, 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 processing systems and services;*
> c) *the ability to restore the availability and access to personal 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.*

Encryption is the easiest and safest way to secure data as required by Article 32 of the GDPR. The technology is an established means of protecting information that is vulnerable to theft or loss. The GDPR also makes the case for effective disaster recovery plans, password recovery and key management systems.

Article 30 of Regulation 3 requires that records must be kept, including a general description of the technical and organizational security measures taken, as referred to in Article 32, meaning that organisations need records and proof that systems are secure and that encrypted data is recoverable after a technical incident.

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

3 Text of the Regulation: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

What are the data breach-notification rules?

Article 33[3] requires notification of a personal data breach to the supervisory authority and states that in the case of a personal data breach, the supervisory authority must be notified, where feasible, not later than 72 hours after the organization in question becomes aware of the breach. Any notification beyond 72 hours must be accompanied by a reasoned justification for the delay.

Article 34[3] refers to the communication of a personal data breach to the data subject and states that:

> 1. *When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.*

However, it goes on to state that:

> 3. *The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:*
>
> *a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;*
>
> *b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;*
>
> *c) it would involve disproportionate effort. In such a 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 later 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?

Article 83, General conditions for imposing administrative fines—point 4:[4]

> 4. *Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher:*
>
> *a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43; Thus covering articles regarding breach notification rules – Article 33 and Article 34, and point five of Article 83 further states:*
>
> 5. *Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher:*
>
> *a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;*

4 Text of the Regulation: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

> *Where Article 5, Principles relating to processing of personal data, states:*
>
> *1. Personal data shall be:*
>
> *f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').*

This clear intent to penalise and discourage offenders will come into force in less than 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 having one of Europe's weakest enforcement regimes to having one of its strongest. The regulation will be enforced throughout all 28 member states from May 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 principles of the GDPR, as stated in Article 5, is ensuring appropriate security for personal data. And as stated in Article 32, Security of processing, encryption is an appropriate technical measure to achieve this. 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 Encryption by ESET is designed to tackle these requirements in a simple and effective manner.

Objective	DESlock Encryption by ESET
Secure data at rest within the organisation	All commercial versions of DESlock Encryption 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 Encryption 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 Encryption 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 makes 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 Encryption 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

How ESET can help with GDPR

https://encryption.eset.com/

Reform of EU data protection rules

http://ec.europa.eu/justice/data-protection/reform/

Regulation (EU) 2016/679 of the European Parliament and of the Council

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

TRY DESLOCK ENCRYPTION FOR FREE

Learn more at **encryption.eset.com**

eset ENJOY SAFER TECHNOLOGY®