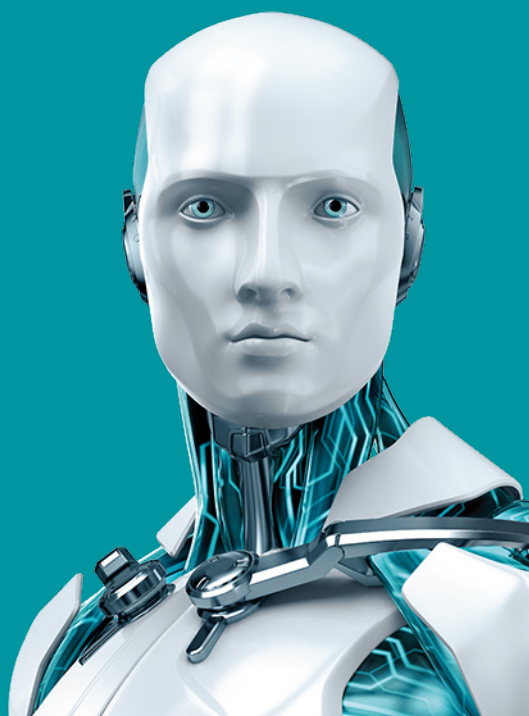
GDPR

IS GDPR GOOD OR BAD NEWS FOR BUSINESS?

Based on:
"A concise guide to the key provisions of the General Data Protection Regulation (GDPR)" by Kemp Jones Solicitors LLP

ESET ENJOY SAFER TECHNOLOGY™



Contents

EXECUTIVE SUMMARY

Recent years have brought major advances in information technology, and fundamental changes to the ways in which individuals and organizations communicate and share information. However, while these developments have led to more frequent data usage, the trend hasn't been equally reflected in all of the legal codes of EU member states.

To achieve harmonization, a new single data protection law – General Data Protection Regulation (GDPR) – has been passed and will come into force on May 25, 2018. The changes it brings will have implications for businesses of all sizes that process the personal data of Europeans, whether in or out of the EU.

Some core concepts existing under the current EU data protection regime (Data Protection Directive or DPD introduced in 1995) will remain broadly similar, such as the concept of personal data, data controllers and data processors. However, **many new concepts and approaches** will come into force that may create compliance difficulties for businesses.

Some of the significant changes include:
- Expanded territorial scope, including EU as well as non-EU companies
- Higher fines and a broader range of powers for national data protection authorities (NDPA)
- Stricter rules for acquiring and retracting an individual's consent
- Stricter breach notification rules

GDPR also expands the rights of individuals, by giving them:
- Right to object to profiling
- Right to obtain a copy of their gathered personal data
- Right to be forgotten

However, GDPR also means good news for the companies working with data. It will remove excessive national variation in the data protection compliance obligations and replace them with one common set of rules, mainly lowering the burden for multinational businesses.

Another benefit is the move to the "one-stop shop" concept which will allow companies to deal with a single data protection authority.

This whitepaper offers a more detailed description of the aforementioned bullet points as well as several other changes brought by GDPR.

GDPR: A MORE CONSISTENT SET OF DATA PROTECTION RULES

GDPR introduces a single legal framework that applies across all EU member states, meaning that businesses will face a more consistent set of data protection compliance obligations from one EU member state to another.

But GDPR doesn't solely concern businesses or entities working with personal data within the EU. Many non-EU companies or organizations that were not required to comply with the former regulation (Data Protection Directive or DPD) will have to follow the new rules.

A company is subject to the GDPR if it either:
- offers goods or services to data subjects in the EU, irrespective of whether payment is received
- monitors its data subjects' behavior within the EU

***Data Subject** - a natural person whose personal data is processed by a controller or processor.*

*For the sake of clarity, throughout this whitepaper the term will also be referred to as **customers or employees**.*

Despite introducing a more streamlined legal framework, the GDPR is still likely to entail significant changes for many businesses, requiring substantial lead-time.

National data protection authorities will gain more power

Currently, fines under national law vary, and are comparatively low, reaching into the hundreds of thousands in some countries. GDPR will increase the maximum fines significantly, making non-compliance a very-high risk issue. Penalties are to be divided into two groups:

1. **Up to 2% of annual worldwide turnover of the preceding financial year** or **10 million euros** (whichever is the greater) for violations relating to internal record keeping, data processor contracts, data security and breach notification, data protection officers, and data protection by design and default.

> ***Data Processor*** *- the entity that processes data on behalf of the Data Controller.*
>
> *For the sake of clarity, throughout this whitepaper the term will be referred to as* ***processing company****.*

2. **Up to 4% of annual worldwide turnover of the preceding financial year** or **20 million euros** (whichever is the greater) for violations relating to breaches of the data protection principles, conditions for consent, data subjects' rights and international data transfers.

Powers of National data protection authorities (NDPAs) will increase as well, enabling them to:

- Impose the aforementioned fines
- Carry out audits
- Require business to provide information
- Obtain access to company premises

Obtaining consent becomes more difficult

Prior to GDPR, **ordinary consent** was necessary for non-sensitive personal data and **explicit consent** for sensitive personal data.

After May 2018, data subjects must give consent in all cases *"by a clear affirmative action establishing a freely given, specific, informed and unambiguous indication of the individual's agreement to their personal data being processed, such as by a written statement."*

Businesses will bear the burden of proof that customers or employees have given their consent to the processing of their data and that it was obtained in a valid manner. In case the processing has multiple purposes, consent is necessary for each of them separately.

In addition to that, end-users, customers and employees must be able to withdraw their consent at any time, given that such procedures will be equally simple as providing consent. Additionally, businesses can **no longer require** consent in exchange for their services, or "execution of the contract", nor use data unnecessary for these activities.

Risk-based approach to compliance

Under the new GDPR rules, businesses will bear responsibility for assessing the degree of risk that their processing activities pose to data subjects – such as end-users, customers or employees.

This can be seen in several of the provisions, for example, the new accountability principle and requirement for data controllers to maintain documentation, privacy by design and default, privacy impact assessments, data security requirements and the appointment of a data protection officer.

Low-risk processing activities may face a reduced compliance burden.

> ***Data Controller*** *- the entity that determines the purposes, conditions and means of the processing of personal data.*
>
> *For the sake of clarity, throughout this whitepaper the term will be referred to as* ***controlling company or company in control****.*

The "one-stop shop"

For multinational businesses, present in more than one EU market, GDPR will represent a substantial change in communications with the data protection authorities. It allows businesses to communicate and predominantly, deal with a single NDPA.

This is also described as a "lead supervisory authority", usually responsible for the main establishment of the business within the EU.

The lead NDPA will be responsible for all regulation of cross-border processing activities carried out by that controlling or processing company. It must also work with all the other concerned NDPAs, as they all have a say in decisions on enforcement relating to cross-border processing activities.

If these NDPAs cannot agree on a decision, the matter is referred to the **European Data Protection Board (EDPB)**. This has a range of powers to ensure the consistent application of the GDPR across the EU – including the authority to make the final decision in enforcement cases. Purely local cases will continue to be handled by the NDPA for the local jurisdiction.

NEW OBLIGATIONS OF COMPANIES UNDER GDPR

Privacy by design and by default

In particular, the GDPR will require businesses to implement technical and organizational measures to ensure that the requirements of the GDPR – "privacy by design" as well as "privacy by default" – are met.

Businesses must take data protection requirements into account from the inception of any new technology, product or service that involves the processing of personal data (privacy by design) and by implementing appropriate measures to the processing of personal data (privacy by default).

GDPR names several measures that can help companies achieve these goals - mentioning minimization of personal data processing, encrypting or pseudonymising personal data, transparency with regard to the functions and processing of personal data, enabling data subjects to monitor how their data is being handled. These measures are also to be kept up-to-date in the future.

Mandatory privacy impact assessments

If any newly developed technologies are likely to result in a high risk to end-users, customers or employees, businesses will be required to perform data **protection impact assessment** (PIAs) before carrying out any processing.

In particular, PIAs will be required for:

- A systematic and extensive evaluation of personal aspects by automated processing, which create basis for decisions that produce legal effects concerning the data subjects, or significantly affect them. This includes profiling.
- Processing of special categories of personal data or data relating to criminal convictions and offences on a large scale.
- A systematic monitoring of a publicly accessible area on a large scale.
- Other kinds of processing operations that require a PIA, published by the NDPA.

Controlling companies can carry out a single assessment to address a set of similar processing operations that present similarly high risks.

Where a PIA indicates that the processing would result in a high risk to individuals, prior to any processing taking place, the business must consult with their NDPA.

Standardized icons to indicate important features of the relevant data processing activities in a simplified format may be prescribed by delegated acts.

No more registrations

Instead of registering with an NDPA, controlling companies will have to maintain detailed documentation recording their processing activities.

Similarly, processing companies must keep a record of the categories of processing activities they carry out on behalf of a company in control. GDPR specifies the information each record must contain in each of the aforementioned instances.

This does not apply to businesses employing fewer than 250 people, unless: 1.) the processing is likely to result in high risk to individuals, 2.) the processing is not occasional or 3.) the processing includes sensitive personal data.

Only in certain circumstances, can controlling or processing companies be required to appoint a data protection officer, with expert knowledge of data protection. An employee in such a position may have protected employment status.

New obligations of data processors

Whereas, under former regulations, processing companies were generally not subject to fines or other penalties, GDPR will change that. Processors may be liable to pay fines of up to 4% of annual worldwide turnover from the preceding financial year or 20 million euros, whichever is greater.

The increase in compliance obligations will probably lead to an increase in the cost of data processing services. It may also make negotiation of data processing agreements more difficult, as the processors will have a greater interest in ensuring that the scope of the controller's instructions is clear.

This may also lead to a review of the existing agreements to ensure that the processing companies have met their own obligations under the GDPR. Companies in control should therefore identify agreements that might require review and amend them as necessary.

Strict data breach notification rules

GDPR requires businesses to notify the NDPA of all data breaches without undue delay, within a maximum of 72 hours, unless the data breach is unlikely to result in a risk to individual data subjects. If this is not possible, the business will have to justify the delay to the NDPA via a "reasoned justification".

In cases where the breach is likely to result in high risk to the individuals, GDPR requires businesses to inform data subjects "without undue delay", unless an exception applies. Data processors must notify the data controller.

Based on these new rules, businesses will need to create a data breach response plan, enabling them to react promptly in the event of a data breach. This will also require designation of specific roles and responsibilities within the company, as well as employee training and preparation of notification templates.

Compliance with the new GDPR rules for breach reporting will entail a significant administrative burden, one which may increase costs for businesses.

> ***Encryption*** *- is the process of encoding information in a way that prevents unauthorized parties from being able to read it.*

Encryption

The communication of the data breach to data subjects will not be required if the controller has implemented appropriate protection measures. This applies in particular to means that render personal data unintelligible to any person who is not authorized to access it.

Encryption fulfills this goal, being explicitly named by the GDPR as one of the appropriate technical and organizational measures that businesses shall implement to ensure a level of security adequate to the risk.

Binding Corporate Rules (BCRs)

GDPR introduces a slightly broader range of mechanisms to transfer personal data out of the European Economic Area (EEA).

It formally recognizes the binding corporate rules (BCRs) – agreements used for these purposes in the past – as a lawful data transfer mechanism (whereas some GDPR predecessors did not).

Under the new regulation, BCRs will still require NDPA approval, but the process should become less burdensome than the current system. BCRs are available to both controlling and processing companies.

Businesses should review their procedures and legal basis for transferring personal data outside of the EEA and keep this under review, particularly as the validity of transfer mechanisms continues to be examined by the ECJ amid ongoing cases.

The fines for breach of the data transfer restrictions under GDPR fall into the higher tier for failure to comply with the requirements.

NEW RIGHTS OF DATA SUBJECTS

In general, the rights of customers or employees (data subjects) are expanded under GDPR. The list of new individual rights includes:

The right to be forgotten

Individuals will have the right to request that businesses delete their personal data in certain circumstances. For example, if the information is no longer necessary for the purpose for which it was collected, or the data subject withdraws their consent.

As a result of the court's decision[1], many businesses may already be doing this. However, it remains unclear precisely how this will work in practice and businesses should consider ways how they will give effect to this right, as deletion of personal data is not always straightforward.

The right to object to profiling

In certain circumstances, individuals will have the right to object to their personal data being processed (which includes profiling).

> ***Profiling*** *- is defined broadly and includes most forms of online tracking and behavioral advertising, making it harder for businesses to use data for these activities. The fact of profiling must be disclosed to the data subject, and a PIA is required.*

For businesses which use profiling only on rare occasions, it may be easier to conclude such activities than to comply with GDPR. Companies that regularly engage in profiling need to consider how best to implement appropriate consent mechanisms.

The European Data Protection Board is expected to provide further guidance on profiling.

The right to data portability

Data subjects have a new right to obtain a copy of their personal data from the controlling company in a commonly used and machine-readable format. They will also have the right to transmit those data to another controller - for example, another online service provider.

In exercising their right, data subjects can request the information be transmitted directly from one controller to another, if it is technically feasible.

Businesses that process large quantities of personal data (such as social media businesses, insurance companies or banks) should consider how they make these rights accessible.

While new-to-market online companies might see this as a way to improve competition, the established providers will probably view it in less beneficial terms.

Data subject access requests

Business must reply within one month from the date of receipt of the request and provide more information than was required by the regulations previous to GDPR.

HOW CAN ESET HELP?

As we already mentioned, GDPR is not just introducing stricter rules for the protection of personal data belonging to individuals, it also names measures deemed appropriate for the job – naming encryption as one of them.

Generally, the main benefits of the encryption technology are its strength – thanks to powerful algorithms and growing key length (bits) – wide availability and relatively low cost of implementation, embraced even by some national authorities.

1) In May 2014 in Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12, 13 May 2014, on a referral from a Spanish court, the ECJ explored the existence and scope of the right to be forgotten and ruled that an individual has a right to rectification, erasure or blocking of that information, and a right to object to the processing of the information in certain circumstances.

One example, DESlock Encryption by ESET, offers more than just the basics. It also offers business clients a solution that is simple to deploy, easy to use for even non-technical users and, one that allows for the remote management of keys, settings and security policy. It also allows users to safely encrypt hard drives, removable media, files and email.

In addition, DESlock Encryption allows companies to meet the data security obligations required by GDPR by easily enforcing encryption policies, while keeping productivity high. Apart from all that, DESlock Encryption by ESET solves one of the biggest usability challenges: How can users share encrypted information?

Common passwords are a potential security risk and public-key encryption cause problems, mainly in larger teams with higher staff turnover. Centrally-managed, shared encryption keys avoid these hindrances, mirroring a more natural way – resembling the use of physical keys to lock houses or cars.

More about GDPR and DESlock Encryption can be found on ESET's webpage dedicated to GDPR.

CONCLUSION: PROS AND CONS OF GDPR

GDPR has the potential to introduce positive changes for many businesses. It is designed to increase the harmonization of national data protection laws across the EU while, at the same time, addressing new technological developments. GDPR will be directly applicable across the EU, without the need for national implementation, thanks to which, businesses are likely to face fewer national variations in data protection rules.

Businesses may also benefit from the "one-stop shop" approach, which will permit them to deal primarily with a single DPA. However, there remain areas in which material differences will continue from one member state to another, affecting data protection compliance requirements (including issues of national security, journalism, freedom of speech, employment law, professional secrecy laws and laws on the interception of communications).

On the other hand, GDPR is likely to require organization-wide changes for many companies across the EU, as business will have to ensure that personal data are processed in compliance within the newly set requirements.

Such changes may include redesigning systems that process personal data, renegotiating contracts with third party data processors and restructuring cross-border data transfer arrangements. It may also lead to adapting new organizational and technical measures such as encryption.

Businesses should therefore consider that these changes may require a significant amount of time to implement, and plan ahead. Failure to do so could mean that businesses are left with new requirements to implement, without having set aside appropriate resources necessary to achieve compliance.

TRY DESLOCK ENCRYPTION FOR FREE

Learn more at:
encryption.eset.com

eset
ENJOY SAFER
TECHNOLOGY™