TOSHIBA

# WHAT GDPR MEANS FOR YOUR BUSINESS

TOGETHER INFORMATION

# THE GENERAL DATA PROTECTION REGULATION - WHAT DOES IT MEAN FOR YOUR BUSINESS?

Coming into force on 25th May 2018 the new General Data Protection Regulation (GDPR) will affect business al around the world. Even though it is an EU directive, which most likely will also be adopted by the other European Economic Area (EEA) member states, it applies to all companies doing business with residents of the EU countries and possibly also EEA countries. With this in mind, we've compiled this short guide to help you understand what the legislation is all about and what steps you can take to assist with your plans for compliance.

## What is GDPR and how does it apply to businesses?

According to EUGDPR.org GDPR is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify existing data protection for all individuals within the European Union.

GDPR is designed "to harmonise data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organisations across the region approach data privacy." The regulation thus relates to many aspects of personal data including name, address, photos, email addresses, etc.

Although the GDPR may sound like a completely new regulation, you are probably aware of its predecessor, the Data Protection Directive 95/46/EC. Until now, all businesses and data processors had to comply with this Directive, so it's likely that your organisation has already taken steps to meet its requirements, many of which are similar – but not necessarily identical – to the requirements of GDPR.

One of the biggest changes is the extended jurisdiction of GDPR. The new regulations will apply to all organisations processing the personal data of subjects residing in the EU, regardless of the organisation's location. This means that GDPR will also apply to the processing of personal data of individuals in the EU by a controller or processor that is not established in the EU, but is offering goods or services to EU residents (irrespective of whether payment is required) and is monitoring behaviour that takes place within the EU.

It is vital for all organisations to implement a GDPR strategy – doing nothing is not an option, as failing to comply with the requirements of GDPR can result in fines of up to €20 million or 4% of an organisation's worldwide turnover, whichever is greater!

## Benefits for businesses and individuals

Although many businesses may feel that GDPR is just another regulatory hoop to jump through, there are clear benefits to be had from compliance.

First of all, GDPR will prompt businesses to improve their data collection and management and to consolidate it into a unified platform. The direct benefits will be that data which can contribute to the success of the business will be much easier to locate and access. A desirable knock-on effect will be that businesses will be better equipped to engage with their customers by providing more relevant information relating to products and services. It will also make it easier for them to respond to customers' requirements.

Ultimately, these positive organisational changes will also bestow a 'golden record' status to data processors and improve their standing with insurers. By including stronger security processes companies will find themselves in better standing with business insurance companies. So, achieving compliance with GDPR will be a step forward for many businesses, giving them an incentive to take useful actions they may have been postponing or have been unsure how to approach.

## Legitimate interests

In addition to the well-known condition of consent, there are a number of other lawful conditions which can permit the processing of appropriate personal data. These can include where the parties are negotiating or performing a contract; where the processing is in the vital interests of the data subject; or where it is necessary to satisfy some statutory obligation. A less well-understood condition for processing is the "legitimate interests" of the data controller. Under this condition, personal data can be processed in limited ways which further the business's legitimate interests, provided that by doing so they do not interfere with or impair the data subject's rights or expose the personal data to risk."

### WHAT IS THE DIFFERENCE BETWEEN EU AND EAA ?

**EU member states:**
Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom

**EEA member states:**
All EU member states + Iceland, Lichtenstein and Norway

# THE SIX PRINCIPLES OF DATA PRIVACY

To help organisations achieve successful compliance, GDPR highlights six key principles that need to be followed by all data processors and controllers. We will look at each of these principles and explain what they actually mean for business owners and organisations.

1

**Lawfulness, fairness and transparency -** This principle states that individuals' "personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject". The data controller has to explain to the data subject how his/her data will be processed.

This has to be done in a clear, concise, transparent and easy to understand manner. Furthermore, the concept of fairness implies that what is processed must match-up with how it has been described to the subject. Finally, lawfulness means that processing must meet the requirements described in GDPR [article 5, clause 1(a)]: http://www.privacy-regulation.eu/en/article-5-principles-relating-to-processing-of-personal-data-GDPR.htm.

2

**Purpose limitations -** According to this principle, data collectors and data processors are required to collect personal information only "for specified, explicit and legitimate purposes and not further process it in a manner that is incompatible with those purposes".

This means that processing personal data is limited to the original purpose for which data was collected. Processing "for another purpose" or at a later stage is not permissible without further legal permission from the subject.

3

**Data minimisation** - Only personal data that is "adequate and relevant" should be processed. Its collection has to be limited to what is necessary in relation to the purposes for which data is being processed. Therefore, data processors should not gather lots of details for possible future use or for creating a detailed customer profile unless it serves some lawful purpose.

Data minimisation follows from the purpose limitation principle and makes it clear that companies have to gather enough data to achieve their purpose from the very beginning, but not more than needed.

4

**Accuracy** - As was the case with the Data Protection Act, the forerunner of GDPR, the principle of accuracy aims to maintain high standards of data quality. This means that personal data has to be accurate and periodically revised so that it is kept up to date.

5

**Storage limitations** - One of the most important principles enshrined in GDPR is that personal information has to be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed".

Business owners have to periodically review and evaluate the data they hold. They must also undertake methodical cleansing because once they no longer need personal data for the purpose for which it was collected the data has to be discarded.

6

**Integrity and confidentiality** – This principle is particularly important for processors, and failing to observe it can attract punitive fines. It states that "personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".

The application of this principle to processors is one of the key changes introduced by GDPR and, in the wake of high profile data breaches and ever-growing data security risks, data processors need to give it particular attention.

This means that data controllers and processors must conduct risk assessments and implement a robust data security policy, as well as observing GDPR's strict breach reporting provisions. This principle needs to be followed carefully and effectively, as high-profile data breaches can cause significant embarrassment and expense for businesses.

# MYTHS ABOUT GDPR

In the months and years running up to the implementation of GDPR there has been a great deal of speculation about its implications, and this has given rise to a large number of myths about what GDPR does and does not mean. This is leading to confusion and concern. In this section, we look at some of the most common myths about GDPR and hopefully bring some much-needed clarity.

## #1: GDPR is just an IT problem

### Our verdict: FALSE

Because the conversation has revolved around data security and safeguarding companies' systems from malicious attacks, many people presume that it is the responsibility of IT departments to prepare for GDPR compliance.

In reality, GDPR involves much more than that. If a company has invested in data protection systems to meet the requirements of the 1998 Data Protection Act, these will provide a very good foundation for compliance with GDPR. However, internal policies and procedures will also have to be assessed and revised in order to demonstrate compliance. The focus should rest on overall risk assessment, improved data privacy standards and robust data loss and data breach notification procedures. Although physical security and integrity remain a priority under GDPR, new concepts such as 'right to be forgotten' and the 'right to data portability' will need to be considered by all areas of the business.

## #2: You must have consent if you want to process personal data

### Our verdict: FALSE

For a company to store and process an individual's personal information, it has to have a lawful basis before any data processing takes place. Consent is one such basis, but not the only one. GDPR raises the bar in what is considered to be 'consent' for data processing. Individuals must provide consent by ticking the relevant opt-in boxes, while organisations must be able show how and when this consent was provided.

Preference centres (also known as privacy dashboards) can be set up in order to provide individuals with "ongoing choice and control" over the ways in which they give their consent. So, when a person wishes to withdraw consent for their data to be processed, withdrawal should be made possible by the same method as the opting-in method.

## #3: Failure to report a breach in time may carry heavy penalties

### Our verdict: TRUE

The supervisory authorities in each state will have the right to issue fines to those companies failing to admit to a data breach and not providing notification of it within 72 hours. But fines can be avoided if organisations are open, honest and report without undue delay. This works alongside the basic transparency principles of GDPR. It all comes down to adopting best practice and being as honest as possible if things do go wrong. The authority will offer support and advice to help businesses stay on the right side of the law and avoid penalties.

## #4: All organisations will have to appoint a data protection officer

### Our verdict: FALSE

The GDPR does not require everyone to appoint a data protection officer, but for bigger organisations establishing such a role is advisable. Recent surveys in the UK show that 70 per cent of businesses with more than 100 employees have already appointed a data protection officer, which is a great step towards consistent and lawful data processing activities.

**#5: All personal data breaches will need to be reported to the authorities**

**Our verdict: FALSE**

If a data breach is likely to hurt individuals' rights and personal freedom, reporting the data breach to the national data protection authorities is mandatory and failure to do so within 72 hours will result in heavy fines. However, if it is unlikely that there's a risk to people's rights and freedoms from the breach, companies do not need to file a report.

The difficulty here arises from deciding on the threshold to determine whether or not an incident needs to be reported to the authorities. A pragmatic approach is to report all data breaches where there is uncertainty and askthe authorities for advise on the best course of action.

## GDPR-compliant products

The imminent arrival of GDPR has led to many companies trying to gain a competitive advantage by promising to provide GDPR-compliant products and services. In reality, very few organisations are in a position to counsel other businesses and authorities have been cautioning people to be extremely vigilant when entrusting the safety of their data to companies claiming GDPR compliance.

While it may be a stretch to assume compliance is possible 'out of the box', it is certainly true that some products will help organisations achieve compliance, whether through encrypting data they handle or automating data driven business processes, for example. Here are a few failsafe ways of choosing the right solutions to support your GDPR activities and the good news is that these solutions are relatively easy to implement.

The first and most important step is to put in place a clear and reliable data assessment procedure. To do so, organisations should choose to work with a recognised partner that will help them assess the methods they employ for handling documents and data within their business. If deficiencies are detected, an experienced and well-informed partner will be able to recommend hardware and software tools that can help support procedures that comply with the new rules.

This could involve, for example, enhancing data security through end-to-end encryption with SSL and IPSec protocol support, data overwrite functionality and secure hard drives on printing devices. A good data partner will also be able to help with requested or unrequested source data from the large number of intrinsic back-end applications and ERP systems being operated across the whole enterprise.

Crucially, storing all documents in a central repository that can be audited and put under restricted access will offer an extra level of data security, as no unauthorised personnel within the company will be able to access sensitive information.

Data management support can also help implement a uniform capture process for all documents or data entering the business so that all personal data is handled consistently and classified, indexed and archived for easy and rapid retrieval.

This is important, because GDPR enshrines the 'right of access' and 'right to be forgotten' where data subjects can ask for copies of all their personal data, or ask for all old or non-essential data to be deleted. Data management systems can make the heavy tasks of data deletion when it is no longer needed, or retrieval in response to customer requests - simple and seamless.

# IN SUMMARY

Data security and individuals' rights to control the use of their personal details have long been an important issue for the European Union. High profile data breaches have proven time and again and the need for better data management and security in SMEs and multinational enterprises alike. GDPR is set to raise the bar and give all data controllers and processors a strong incentive to improve their systems and procedures. And no one can afford to get left behind!

# GLOSSARY

**Data processor** — In relation to personal data, it means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

**Data controller** — A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed.

**Data processing** — In relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including—
a) organisation, adaptation or alteration of the information or data,
b) retrieval, consultation or use of the information or data,
c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
d) alignment, combination, blocking, erasure or destruction of the information or data

**SSL** — **Secure Sockets Layer** represents a protocol that enables a secure connection between a client and the server over which to send information.

**IPsec** — **Internet Protocol Security** is a framework for a set of security protocols at the network-processing layer of communication

## Useful links

**General Information:**
http://www.eugdpr.org

**The complete text of the GDPR:**
http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679

**Toshiba Tec Belgium Imaging Systems**
Z.1 Researchpark 160 | 1731 Asse-Zellik | Belgium
be.toshibatec.eu