TOSHIBA
Leading Innovation

GDPR

Information Guide

- The EU General Data Protection Regulation (GDPR) will come into force on 25th May 2018.
- It is binding for all organisations, companies and institutions which offer their products and services to people living in the the European Union.
- It regulates the data collecting and processing of personal data and information about EU residents.

TOGETHER INFORMATION

ABOUT GDPR

GDPR is not really new. It is an expansion of the already existing Data Protection Directive. But the GDPR has defined new categories, such as genetic and biometric data, which previously did not exist. Also, the definition of what should be considered personal data has been revised, e.g. medical data, is now also protected under the new regulation. The GDPR also gives people more control over their personal data as they now have the right to ask which personal data a business has collected about them and can even request that all data is deleted if there are no legitimate grounds for retaining it.

In case of a personal data breach which is a likely to result in a risk to the rights and freedoms of individuals, companies need to inform their national data protection regulator within 72 hours.

What does it mean for your business?

Personal data is needed to do business: Without an address, goods cannot be delivered, without telephone numbers and e-mail addresses suppliers cannot be contacted and without storing bank details, employees cannot be paid. All of this will not change. But with GDPR in force companies need to ensure that all the data they collect and process is safe. By documenting what, how and where personal data is stored, companies can easily provide this information if requested to do so by the authorities.

WHAT IS PERSONAL DATA?

Personal identifiable information (PII) or personal data is any information that can identify a person. Below we have listed some of the information to which GDPR applies. This list is not intended to be exhaustive. It includes, but is not limited to:

- Contact details
  - name, postal address, telephone number, e-mail address, user IDs etc.
- Birthday
  - date and/or place of birth
- Verification data
  - password, answers to security questions (e.g. mother's maiden name)
- Medical information
  - medical records, prescriptions
- Account details
  - bank accounts, insurances
- ID details
  - passport or ID card number, driver licence number

Why is it so important?

Just as a private person doesn't want personal data to be stolen, misused or tampered with in any way, business partners and customers expect the same. Now with GDPR in force, not complying with the regulation has more severe consequences: it can result in fines of up to 4% of a company's revenue. This is something which can be avoided by taking the necessary steps. Plus, if a company is known to take all necessary measures to protect personal data, it will be good for its reputation.

Which measures should be taken?

Following some, but not limited to, things which need to be considered. It is recommended that companies consult with legal advisors for a detailed list of individual measures which need to be taken.

- Listing personal data being collected
  - Different departments collect and process data. It therefore is recommended to involve all departments (HR, Legal, IT, Finance, Marketing etc.) to get a comprehensive overview of who collects what.
- Documenting access to personal data
  - The GDPR requires to document how access to personal data is restricted, where the data is stored, for how long it is stored, for what it is used and who has access to it.
- Control over personal data
  - The new regulation reinforces the right of individuals to know which data about them is being collected and demand the deletion of this data if there aren't compelling reasons to store it.
- External partners
  - Suppliers, business partners or sub-contractors who work with the personal data collected by a company should be contacted to ensure the way they process this data is GDPR compliant.
- Management of data breaches
  - An action plan needs to be in place in the event that a data breach needs to be reported to the authorities.

WHAT IS GDPR?

The **General Data Protection Regulation** (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU. The GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

HOW CAN TOSHIBA HELP?

Why is GDPR relevant for MFPs?

Each day millions of pages with confidential and/or personal data are being used. Having full control over who can access the data and making sure that it is handled securely is vital. With multifunction products (MFPs) and printers being able to store large amounts of data on their hard disk drive and being an integral part of business networks, the systems therefore need to be protected from unauthorised access just like any other IT device.

How can Toshiba help protect personal data?

Toshiba is a leading provider of information technology and protecting data has always had utmost priority for us. Toshiba e-BRIDGE Next products comply with the Common Criteria Evaluated Assurance Level 3 (EAL 3), conform to ISO/IEC15408 and meet the IEEE 2600.1 standards. But what does that mean? It means our systems were designed to easily integrate into secure IT environments and help protect document workflow processes.

As early as 2012 Toshiba started equipping all new e-BRIDGE systems with a secure hard disk drive. This HDD not only works with state-of-the-art encryption, it also features a sophisticated authentication system, which ensures, that even if the HDD falls into the wrong hands, the data is still protected.

For ultimate security the optional Data Overwrite feature automatically overwrites all data up to five times, erasing it entirely after you have printed, scanned, copied or faxed a document. This way nothing is permanently saved on the HDD and there is no data left to be compromised.

But Toshiba also offers other possibilities to protect confidential data from unauthorised access. These can be categorised as follows:

- Access security
  - Restricting access helps prevent data from leaking. Using role-based access ensures full control over which device features can be utilised by which user. Moreover, Toshiba offers a number of advanced authentication and output management solutions to make access control easy to use and easy to configure.
- Document security
  - To make sure confidential information is protected from unauthorised access, Toshiba offers several solutions to give you advanced control over your documents. Whether you create secure PDFs, store files in protected folders or use the private print function, you can be sure your data will always be safe.
- Device security
  - Toshiba e-BRIDGE systems can be shielded from cyber attacks just like any other device within an IT network. The SSL protocol employs encryption technology to protect all data travelling to and from the MFP, while IP Filtering acts like a firewall to protect your internal network from intruders. Also, SMB Signing adds a digital signature to verify that data is received from authenticated sources and ensures the integrity of all communications.

For a detailed list of safety and security features and to learn how you can utilise our software solutions to protect your data, please contact your local Toshiba partner.

PROTECT PERSONAL DATA

Toshiba systems offer various methods to ensure personal data is safe. By making full use of these possibilities any information processed on your MFP is protectedn to the highest possible extent from unauthorised access.

About Toshiba Tec

Toshiba Tec Germany Imaging Systems GmbH is part of the globally operating Toshiba Tec Corporation, active in various high-tech industrial sectors.

Toshiba Tec Corporation is a leading provider of information technology, operating across multiple industries - ranging from retail, education and business services to hospitality and manufacturing. With headquarters in Japan and over 80 subsidiaries worldwide, Toshiba Tec Corporation helps organisations transform the way they create, record, share, manage and display information.

For more information please contact us:

Toshiba Tec Germany Imaging Systems GmbH
Carl-Schurz-Str. 7
41460 Neuss
Germany

Telephone
+49 2131-1245-0

Website
www.toshibatec.eu

Together Information is Toshiba's vision for how people and organisations create, record, share, manage and display ideas and data.

It is based on our belief that the most successful organisations are those that communicate information in the most efficient way.

We make that possible through an integrated portfolio of industry-specific solutions, all of which reflect Toshiba's commitment to the future of the planet.

Technical data is subject to change without prior notice. All company and/or product names are trademarks and/or registered trademarks of their respective manufacturers in their markets and/or countries. All rights reserved. Copyright ©2018 TOSHIBA TEC. BR_GDPR_201802145