General Data Protection Regulation

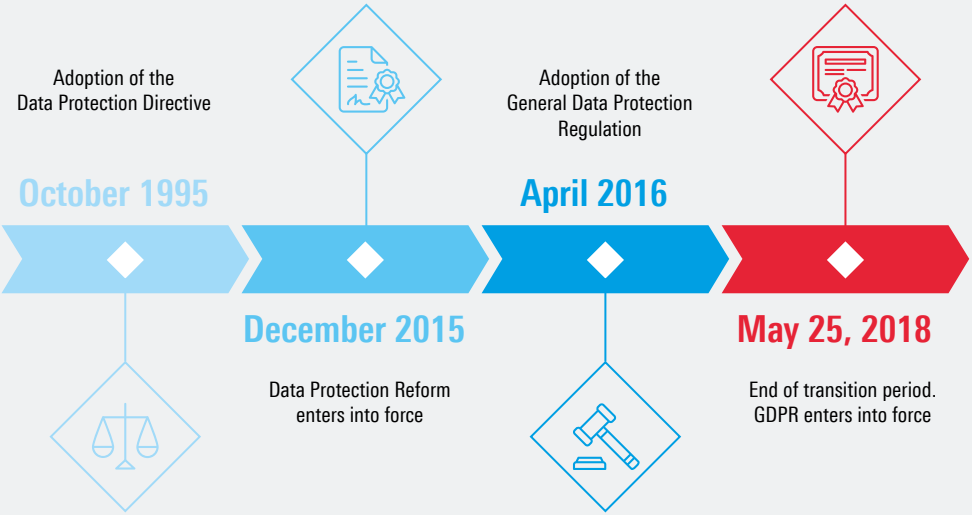
Product and solution portfolio

ROHDE&SCHWARZ
Cybersecurity

GDPR: What companies need to know now

After the transitional period ends on May 25, 2018, the General Data Protection Regulation (GDPR) will become directly applicable law for all companies in the European Union. The primary objective of GDPR is to **harmonize data privacy laws between EU member states and enhance data protection and data security standards**. GDPR replaces the 1995 Data Protection Directive (95/46/EC) and extends the German Federal Data Protection Act, which has been amended to reflect the provisions of GDPR.

Any national data protection and data security regulations stricter than GDPR will remain valid. Consequently, the GDPR complements and expands existing European and national laws. In Germany, these include the Federal Data Protection Act (BDSG), the Telecommunications Act (TGK) and the IT Security Act (ITSG). European regulations include the Directive on Security of Network and Information Systems (NIS) and the ePrivacy Regulation, which will enter into force at the same time as GDPR. There are also sector-specific regulations at the national and international level, such as the E-Health Act for the healthcare sector and the regulations of the Basel Committee on Banking Supervision (Basel III) that apply to financial service providers.



GDPR Principles

GDPR will **increase the rights of individuals and the obligations of companies** with regard to data protection and data security. When processing **personal data**, companies are required to act in accordance with the following principles.[1]

- **Legality:** There has to be a legal basis for processing data. In particular, the consent of the data subject must be obtained.
- **Transparency:** It has to be clear what data the company will collect, use, view or process.
- **Purpose:** Data can be collected and processed only for a specified, explicit and legitimate purpose.
- **Data minimization:** Companies must process data only to the extent required for the intended purpose.
- **Accuracy:** Personal data must be factually correct. Incorrect data must be immediately deleted.
- **Storage limitation:** Data can be stored only as long as required for the intended processing purposes.
- **Integrity and confidentiality:** Data must be processed in a manner that ensures appropriate security of the personal data.

Most previous laws simply required compliance with IT security standards. However, GDPR requires that companies take into account **state-of-the-art** developments concerning data security and apply the principles of data integrity and resilience. GDPR leads to a **paradigm shift in data security** – away from standards and towards technology-based "privacy by design" and "privacy by default".

1 Art. 5 EU GDPR

Increased requirements and sanctions

GDPR results in new data security obligations for companies. When processing personal data, it requires an appropriate level of protection must be ensured for the risk involved. For the principle of **integrity and confidentiality**[2], the regulation requires companies to take the necessary **technical and organizational measures** to ensure that data is protected against unauthorized or unlawful processing, loss, or unintentional destruction or damage. Under technical measures, the regulation explicitly mentions encryption and pseudonymization[3] of personal data as well as processing that takes into account the state of the art in data security technology and the likelihood and severity of risks[4] for the rights of the individuals concerned.

These regulations apply to all companies headquartered in the European Union as well as those that process the personal data of individuals within the EU. Breaches of the GDPR are subject to serious penalties. They may result in per infringement fines of up to **4 % of the total worldwide annual revenue** of the sanctioned company or **EUR 20 million**.

2 Article 5(1)(f) EU GDPR
3 Articles 6(4)(e), 31(1)(a), 32(1)(a) EU GDPR
4 Article 32 EU GDPR

New organizational and technical measures

In addition to the massive increase in the maximum fines, GDPR imposes major challenges on companies with regard to the implementation of the new technical and organizational measures needed for compliance.

These include measures to ensure the confidentiality, integrity, availability and resilience of the processing systems and services. Companies must also ensure the availability and accessibility of personal data in the event of a physical or technical incident, i.e. they must ensure that data can be **restored**. In addition, they must implement **processes to regularly monitor, assess and evaluate** the effectiveness of technical and organizational measures for ensuring the security of data processing.

Consequently, GDPR results in more stringent requirements for companies.
These include:

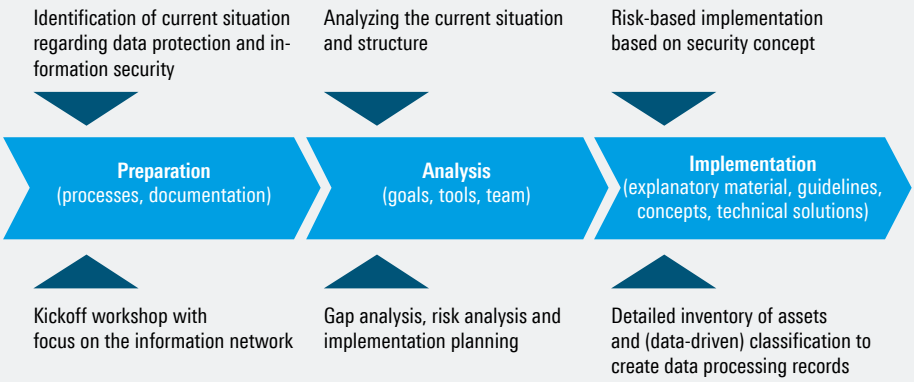
- Increased requirements for **data processing records**
- Mandatory **data protection impact assessment (DPIA)** for the processing of personal data
- Increased obligation to provide **information and access** to data subjects
- More **technical and organizational data protection requirements**
- **Obligation to report data breaches** within 72 hours

Consulting services offered by Rohde & Schwarz Cybersecurity on GDPR compliance

To help companies implement GDPR, experts at Rohde & Schwarz Cybersecurity offer support for creating data processing records[5], for the DPIA[6] and with risk assessment and risk mitigation measures. Together with the introduction of an Information Security Management System (ISMS) and the deployment of innovative security solutions, this will ensure ongoing data protection compliance.

For the concrete implementation, the results of an analysis of the current situation will be used as the basis of project phases to comply with the GDPR:

Project phases to comply with GDPR



5 Article 30 EU GDPR
6 Article 35 EU GDPR

Successfully establish data security: Security concept and data protection management system

To implement GDPR and a company-wide security strategy, it is advisable to create a **security concept** to map out the necessary steps and achieve the defined security objectives. The security concept becomes the **central document in the security process** and also serves to document the results.

The project phases are based on the following structure:

1. Analysis of IT structure
2. Identification of protection requirements
3. Modelling in accordance with the IT baseline protection approach
4. Basic security check
5. Supplementary security analysis
6. Risk analysis
7. Comprehensive documentation

Back to basics: creating a data protection management system

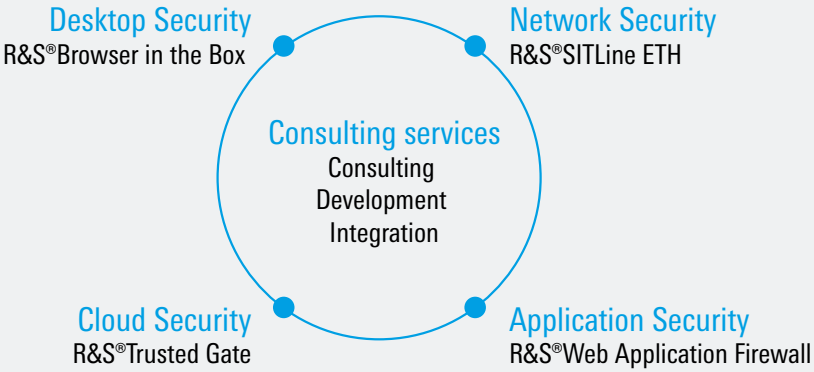
GDPR establishes an **obligation to demonstrate compliance in accordance with the accountability principle**. This means that companies must be able to prove that they are in compliance with the data protection regulations. This also applies to data security, which means companies need to implement a **data protection management system**.

In addition, GDPR greatly increases the obligations of companies and controllers with regard to providing information to the data subjects and the reporting obligations in case of breaches and security incidents. A data protection management system enables a company to respond quickly if such events occur.

Security solutions from Rohde&Schwarz Cybersecurity for implementing GDPR

Offering a broad portfolio of IT security solutions from a single source and extensive expertise in IT security consulting, Rohde&Schwarz Cybersecurity is your reliable partner for the organizational and technical implementation of GDPR in your company.

Solution portfolio for the challenges of GDPR



Solutions for network and application security

Network Security: R&S®SITLine ETH

Secure data transmission with Ethernet encryption

The R&S®SITLine ETH range of Ethernet encryptors protect organizations against espionage and the manipulation of data transported via landline, radio relay and satellite links. The encrypted throughput can be increased up to 40 Gbit/s per device by means of a firmware update with no need to upgrade hardware. The devices combine easy administration (including separated network and security management) with a compact form factor and low system costs. They are BSI-approved for classified communications at German and NATO RESTRICTED security levels.

Application Security: R&S®Web Application Firewall

Protecting web-based business processes

The R&S®Web Application Firewall is a comprehensive security suite for web apps, web services and databases. It protects your data in business applications such as SAP, Oracle and Microsoft® Dynamics 365™, in internet and intranet websites, in extranet apps (e.g. Outlook Web Access™, Microsoft® SharePoint™), in web services for machine-to-machine communications, in IoT architectures and in backends for mobile apps. For an even higher level of security, a vulnerability scanner, IP libraries and access management systems are available for integration.

Solutions for cloud and desktop security

Cloud Security: R&S®Trusted Gate

Security and data protection compliance for cloud environments and collaboration tools

The R&S®Trusted Gate product range uses innovative encryption technology and fragmentation of sensitive documents to enable companies to protect data and work securely in data clouds (e.g. Google Drive, Magenta, Box.com) and with collaboration tools (e.g. Microsoft® SharePoint™, Microsoft® Office 365™). With R&S®Trusted Gate, you decide where your data is stored and can ensure that it will not leave a given region. Through document-centered encryption and role-based access control, your business-critical information is protected against cyberattacks and espionage.

Desktop Security: R&S®Browser in the Box

The virtual environment for secure and comfortable browsing

R&S®Browser in the Box offers proactive protection against cyberattacks. Thanks to the secure separation of the browser from the rest of the PC, you and your corporate network are protected against Trojan horses, ransomware, ATPs and zero-day exploits. Active content such as Java, JavaScript or Flash and dangerous links are no longer a threat. The management tool lets you easily configure security policies from one central interface. User rights are assigned in the browser with just a few clicks, e.g. for printing, uploads/downloads and copy/paste. R&S®Browser in the Box fulfills compliance guidelines in line with applicable data protection laws.

Rohde&Schwarz Cybersecurity

Rohde&Schwarz Cybersecurity is a leading IT security company that protects companies and public institutions around the world against cyberattacks. The company develops and produces technologically leading solutions for information and network security, including highly secure encryption solutions, next-generation firewalls and firewalls for business-critical web applications, innovative approaches for working in the cloud securely as well as endpoint security. The award-winning and certified IT security solutions range from compact, all-in-one products to customized solutions for critical infrastructures. To prevent cyberattacks proactively, rather than reactively, the trusted IT solutions are developed following the security-by-design approach. More than 500 people are employed at locations in Germany, France, Spain and the Netherlands.

Rohde&Schwarz

The Rohde&Schwarz technology group develops, produces and markets innovative test and measurement, information and communications technology products for professional users. Rohde&Schwarz focuses on test and measurement, broadcast and media, cybersecurity, secure communications and monitoring and network testing, areas that address many different industry and government-sector market segments. Founded more than 80 years ago, the independent company has an extensive sales and service network in more than 70 countries. On June 30, 2017, Rohde&Schwarz had approximately 10,500 employees. The group achieved a net revenue of approximately EUR 1.9 billion in the 2016/2017 fiscal year (July to June). The company is headquartered in Munich, Germany, and also has regional hubs in Asia and the USA.

Rohde & Schwarz Cybersecurity GmbH
Muehldorfstrasse 15 | 81671 Munich
Info: +49 30 65884-222
Email: cybersecurity@rohde-schwarz.com
www.cybersecurity.rohde-schwarz.com

Rohde & Schwarz GmbH & Co. KG
www.rohde-schwarz.com

Printed in Germany | May 2018 (sch)
PD 3607.8647.62 V 01.00

3607864762