GDPR quick help: Seven essential data protection measures for startups and companies

June 16, 2020 – Munich: The digital transformation of the economy has opened up many new doors for cybercriminals. Companies must take appropriate measures to protect themselves and the data of their employees, customers and partners. But what do they need to consider?

Most of the provisions of the German Federal Data Protection Act (BDSG) and the General Data Protection Regulation (GDPR) boil down to a simple requirement: those responsible must guarantee the security of sensitive data. Violations can quickly become expensive: In the case of particularly serious data protection violations, the GDPR provides for fines of up to €20 million or up to 4% of the total annual turnover achieved worldwide (see Art. 83 GDPR). Following we present seven essential data protection measures for companies.

1. Compliance assessment

Compliance—this is, the observance of laws and regulatory requirements—affects all companies, but to different degrees. Depending on the industry, additional guidelines may apply in addition to GDPR and BDSG, for example, in the field of competition or financial law.

2. Risk assessment

As a next step, companies should carry out a risk assessment. After all, the more sensitive the data that is to be collected and/or processed, the more elaborated the measures to protect it must be. Assessments of this kind often require the support of a data protection officer.

3. Encryption

It goes without saying that sensitive data must be encrypted both during transmission and storage[1]. Sufficiently encrypted data is considered secure per se; even if data is lost, it cannot be read or recovered by attackers without the appropriate key.

4. Pseudonymization

All information that would help identify the user is removed. For example, the names of persons are replaced by randomly generated character strings. This way, the useful data remains but it no longer contains sensitive information.

5. Access controls

Introducing access controls into your company's workflow is also an efficient method of minimizing the risk. The fewer people have access to the data, the lower the risk of accidental or deliberate data damage or loss.

---

[1] *During processing, data must be available in unencrypted form, but can be protected by appropriate infrastructures as if it was still encrypted. With confidential computing or sealed computing, for example, processing takes place in specially sealed hardware environments that reliably prevent unauthorized access to unencrypted data.*

6. Backups

Backups can help to prevent data loss due to user error or technical failure. They should be created and updated regularly. While regular backups add costs to your business, potential business disruptions are usually far more costly.

7. Deletion

Under the GDPR, companies are obliged to delete the data that they do not need (see art. 5 and art. 17). Consequently, companies need to draw up an appropriate deletion concept. Depending on the type of data, this concept should also specify deletion periods and durations.

"Ultimately, companies must decide, whether they take appropriate measures themselves or use the services of third-party providers specializing in data protection and data security", says Ulrich Ganz, Director Software Engineering at TÜV SÜD's subsidiary uniscon. "Depending on the industry, the size of the company and the type of data collected and/or processed, this can save costs and simplify processes. For example, if companies use certified services, they can prove that they already fulfill their control and due diligence obligations as required by law". This allows companies to concentrate on their core business—and leave data protection to the experts.

For further information contact us at presse@uniscon.de

uniscon — a company of the TÜV SÜD Group

uniscon GmbH is a company of the TÜV SÜD Group. As part of TÜV SÜD's digitalization strategy, uniscon offers high-security cloud applications and solutions for secure, legally compliant data traffic. TÜV SÜD is one of the world's leading technical service providers with over 150 years of industry-specific experience and more than 24,000 employees at around 1,000 locations in 54 countries. Within this strong network, uniscon is able to reliably implement large-scale international projects in the IoT and Industry 4.0 sectors with the Sealed Cloud and its products.

Further information on the company and its solutions at www.uniscon.com

Press contact

uniscon GmbH, Wilhelm Würmseer (Corporate Communications)
Ridlerstr. 57
80339 Munich (Germany)
email: press@uniscon.com
Phone: +49 (0)89 / 41 615 988 104

Kafka Kommunikation GmbH & Co KG, Markus Reck
Auf der Eierwiese 1
82031 Grünwald (Germany)
Tel. +49 (0) 89 74747058-0
Fax + 49 (0) 89 74747058-20