General Data Protection Regulation

May 25, 2018

DON'T PANIC !

→ PLAN !

RADAR SERVICES

Protect the human behind the data record.

On May 25, 2018 the General Data Protection Regulation (GDPR) is entering into force. It requires organizations to put more emphasis on the human behind the data record. This data has to be protected and should hold him accountable. If this does not work out, organizations are facing high penalties.

» Territorial applicability

The EU-GDPR protects a wide range of persons. Organizations that process data of EU citizens in their systems are governed by this regulation. They do not need to be located in the EU or use a server of the EU.

» The affected data

Solely anonymous data, which is data whose personal origin is no more identifiable, shall not fall under the scope of this regulation.

DON'T PANIC!

PLAN!

1. Prioritize your tasks.

Develop a basic concept for fulfilling the requirements based on the status quo of your company. Prioritize your To Dos. Consult legal and IT security experts in the course of planning in order to interpret the individual requirements of the GDPR correctly.

On the one hand your company shall be protected from cyber attacks, on the other hand, the people whose data you are processing, shall be provided with rights and established processes. A third strategically important step is the establishment of security measures in product and process design.

Focus all your measures on improving the trust in you and your IT of clients, employees and stakeholders.

2. Secure your IT.

The central article 32 EU-GDPR states:
"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk."

So it is clear that the legislator has no specific security measures defined but rather recommends appropriate risk-based technical and organizational measures.

Compare your potential risks with actual IT security measures and analyse possible gaps. Develop the ability to detect and react to cyber attacks quickly in order to minimize potential damages. Evaluate the tool Security Information & Event Management (SIEM)[1] for a proactive monitoring of your IT security.

[1] SIEM is allowing the proactive monitoring of the networks and the identification of security threats in real time. SIEM is flexible and scalable and can be easily integrated with Log-sources from various system – from network equipment and storage devices to operating systems and applications. SIEM collects logs and performs quick searches. SIEM offers a comprehensive overview of the activities in the corporate network and documents all transactions carefully. In case of information leakage SIEM is securing logs and allows an overview of the data accessed. Thereby SIEM enables besides others quick information flow to authorities.

3. Focus on detection.

The GDPR stipulates reporting obligations to supervisory authorities in case of security incidents within a maximum of 72 hours after becoming known. Also persons concerned have to be informed in case the incident is expected to have a high risk for personal rights and freedoms. In case an organization is not fulfilling its duties, high fines (up to the higher of 4% of annual worldwide turnover and EUR 20 million) have to be paid. Considerable reputational damages are associated with it.

These scenarios have to be prevented on the one hand and on the other hand documentation measures as well as functioning emergency processes (Best Practices) need to be followed.

The Security Information & Event Management (SIEM) therefore fulfills various tasks. Moreover, the usage of tools such as Network-based Intrusion Detection Systems, a continuous Vulnerability Management and Advanced Threat Detection for Email & Web shall be verified.

The goal of this risk management modules is to establish a comprehensive protection mechanism for the organizational IT, including the parts that process personal data.

4. Map your data.

In future persons have to explicitly agree to the use of data. It must be disclosed to them how and where the data is used. The agreement is always earmarked, meaning for specific processing purposes. Declarations of consent can also be withdrawn. Organizations have to keep up with this sustainably.

Moreover, each person has the right to receive clear and easily comprehensible information with regards to the processing of data. Also the transfer of this data into systems of other service providers has to be possible upon request without a problem.

A complete overview is required of all the IT assets in use and the personal data that is made available by them. Thereupon processes are established that allow persons their rights of insight, data portability and cancellation.

5. Secure by design & default.

THE GDPR requires companies to address data protection proactively. It also requires that technology which it uses in the data processing shall be "designed" in order to be data protection friendly by nature and does not allow for specific data processing or at least does so securely. Data Protection by Default means that automatically the strictest data protection settings are applied if a client purchases a new product or service.

Besides that Data Protection by Design means that services and business processes and personal data shall be treated in the sense of the GDPR. IT departments have to integrate data protection and privacy in the entire system respectively process life cycle in order to have proof in case of doubt.

In the future also your product and process design shall be aligned based on data protection issues. Evaluate the possibilities and requirements for such changes in time and across industries.

How we can support you.

RadarServices is specialized on the real-time detection of IT security risks. This includes a continuous monitoring of all gateways for malware and all communication channels across organizational borders, a continuous analysis and correlation of logs of all systems as well as continuous vulnerability analysis, internally and externally.

All these services are delivered as Managed Services. Data thereby never leaves the company. The services combine (1) the technology developed in Europe, (2) the work of analysis experts in the worldwide Security Operations Centers (SOCs) and (3) established processes and best practices in case of IT security incidents.

The result:

A particularly effective and efficient improvement of IT security and risk management, a continuous IT security monitoring and an overview of all the security relevant information of the entire company on the push of a button. An ideal service package in order to protect your IT continuously and preventatively from attacks. Additionally by using state-of-the-art engineering you fulfill a particularly important part of the requirements that the GDPR demands from organization.

RADAR SERVICES
Publishing

Author: Dr. Isabell Claus

About RadarServices Publishing

RadarServices Publishing is publishing articles, reports, studies and journals with regards to the subject matter of IT security. Our goal is to provide an insight into the experiences of industry experts as well as to pass on knowhow regarding IT security through academic and non-academic research to companies, public institutions and other organizations. We are actively including co-authors from academia and the economy in order to promote knowhow about current developments in the field of IT security in the public and especially for corporate executives as well as in politics. RadarServices Publishing is part of RadarServices.

About this publication

This publication exclusively contains general information. RadarServices and/or its related companies do not render technical consulting services with this publication. This publication does not substitute consulting services and should not be regarded as a basis for business or investment decisions/negotiations. Neither RadarServices nor its related companies are liable for losses that incurred due to persons relying on information provided in this publication.

About RadarServices

RadarServices is the European market leader for proactive IT security monitoring and IT risk detection as managed services. The services uniquely combine automated detection of security relevant issues and risks with the analysis and assessment done by experts. Data never leaves the client's premises. There is no need for training, configuration or maintenance and no requirement for additional capital expenditures or headcount.

RadarServices
Cybersecurity World
Zieglergasse 6
1070 Vienna, Austria

P: +43 (1) 929 12 71-0
F: +43 (1) 929 12 71-710
E: sales@radarservices.com
www.radarservices.com