General Data Protection Regulation

Starting on May 25, 2018 the Regulation of the European Parliament and of the Council (EU) 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, the so-called "GDPR" will be in effect. This groundbreaking legal act unifies data protection across the EU and affects all entities that process personal data.

This new European standard requires a comprehensive approach to the field of information security, although it focuses on personal data only. In connection with this regulation, new obligations arise for the automatic processing of personal data. This leads to better transparency, as well as heightened security.

This can be achieved by adopting appropriate concrete measures, not only in the field of cybernetic security, but also physical security, administrative, organizational and procedural. It is necessary to interconnect all of these areas comprehensively in order to make privacy function as a seamless system.

A synthesis of an appropriate organizational structure, clearly defined processes and procedures, good documentation for management and correctly applied technologies is essential for ensuring the satisfactory protection of personal data.

GDPR - New Obligations

Stated briefly and simply, there is a significant tightening of regulations in processing personal data. New conditions not only require the modification of existing processes related to data processing in the organization, but they also require the compulsory implementation of many additional measures.

Essential news and changes in personal data protection arising from the GDPR

Strengthening the rights of personal data subjects

Broader information obligations towards authorities and data subjects

A significant increase in potential penalties for breaching the regulation

The requirement for explicit consent for all processing

The obligation to report personal data breaches

Pseudonymisation and encryption of personal data

Unification of privacy data protection across the EU

New rules for the relationship among data controllers and processors, including supply chains

Data Protection Impact Assessment (DPIA)

Data Protection Officer (DPO)

Codices and certificates

Increased protection of personal data

AEC Solution

Using more than twenty-five years of experience in information security and information technologies, we offer a wide array of products and services. This makes it possible to meet the majority of the new European legislative standard requirements. There is no need to solve all the required measures using your own internal resources. Our specialists can help you with a number of them. Such outsourcing is also cost-effective in many cases. GDPR complexity requires a comprehensive approach to managing privacy. AEC offers a unique pairing of knowledge in the area of systematic information security management and deployment of appropriate security technologies.

Analysis of Compliance with GDPR Requirements

The foundation for proper implementation of GDPR requirements is a detailed comparison between the current state and data protection requirements as defined in Regulation. That is the only way to ensure the effective implementation of all GDPR requirements. AEC can prepare a detailed analysis and recommend a suitable procedure and scope of implementation.

Design and Implementation of Processes and Methodologies

GDPR is based on the principle of "privacy by design" and a "risk-based approach." This requires not only the introduction of new security processes and methodologies within an organization, but it often has an impact on the context of information systems' architecture and applications. These include procedures for reporting security incidents, information obligations, or the right to erasure. AEC can design and implement processes and a methodology customized to the organization's environment.

Processing Management Documents

An essential part of personal data protection is appropriate organizational management documentation (policies, directives etc.) that demonstrates compliance with GDPR requirements. AEC can prepare governing documents or modify the extent of existing internal policies and processes to be consistent with respect to GDPR requirements.

In order to comply with GDPR, the organization will have to answer a series of elementary questions:

- What data is being processed and in which locations is it being stored in our systems? Can we "erase" personal information if the data subject requires it?
- How is data managed, and how is it protected? Is it secured sufficiently?
- How does internal documentation deal with the protection and processing of personal data, and is it in compliance with GDPR requirements?
- What are the roles involved in the processing of personal data? What are their responsibilities? Are the current obligations sufficient to meet GDPR requirements?
- What are the roles of third parties in data processing and how do we ensure cooperation with them (contractually)? Do we have sufficient collateral in the event of possible problems?
- How do we deal with procedures for the leakage of personal information and the subsequent informing of data subjects and the regulator?
- Do we provide personnel training and education adequately?

Our Services in the Field of GDPR

- Analysis of compliance with the GDPR requirements
- Consultation, design and the implementation of related processes / activities / practices into the organizational structure
- The preparation of management documents (policies, directives, other documents)
- The implementation of the technical tools SIEM, DLP, FW / WAF / IPS, NBA, document classification
- A Data Protection Impact Assessment
- Outsourcing the role of the Data Protection Officer (DPO)
- GRC implementations for the effective management of personal data and related processes

Implementation of Technical Measures

The basic GDPR requirement to ensure the protection of personal data is to guarantee their confidentiality, availability and integrity. This implies the deployment of adequate technical measures to ensure proper security and to identify a security breach (Data Loss Prevention, Network Behavior Analysis, SandBox, cryptographic tools etc.). AEC can design and implement appropriate technical solutions according to the individual needs of organizations.

Data Protection Impact Assessment

Data Protection Impact Assessment is an essential tool to ensure high security of personal data while handling any personal information, such as profiling, processing sensitive data or carrying out public area monitoring (CCTV), etc. AEC can assess the obligation of the organization to implement DPIA and if such obligation arises, it can propose the appropriate method of implementing DPIA in existing (e.g. project) methodologies. In addition, AEC can also provide the processing of specific DPIA analysis, including any consultation with the Supervisory Authority.

Data Protection Officer – DPO

One of the new GDPR requirements for compulsory subjects is to appoint a Data Protection Officer. This role requires a person with sufficient experience and expertise in the area of personal data protection. There is an expectation that there will be a shortage of suitable candidates for the DPO position in the job market. However, this role can also be outsourced. This service can be provided by AEC with their experienced and certified consultants to ensure the fulfillment of all the obligations of the DPO.

Implementation of GRC Solutions

GDPR creates many partial duties, particularly for large organizations processing a large volume of personal data. GRC solutions (Governance, Risk and Compliance) can be an essential element that enables the effective management of personal data protection and compliance to GDPR requirements, including monitoring the extent of compliance. AEC can provide optimal design and implementation of appropriate GRC solutions, with their team of experienced consultants for this purpose.

Governance - Risk – Compliance (GRC)

GRC solutions help to implement processes in the areas of process management (IT processes, security processes, business processes), enterprise risk management (ERM, the risk of information security, IT risk, supply risk), and compliance with applicable laws and regulations. GRC aims to achieve automated and efficient information sharing, implementation of activities and limiting the uneconomical waste of resources.

GRC tools are increasingly finding their way into all types of organizations. The reason for their acquisition are often due to various external pressures, e.g. the need to meet the requirements of the law on cyber security (181/2014 Coll., and related regulations in Czech Republic) or other regulatory requirements. These requirements are constantly growing; we can also expect more of them in the context of GDPR. However, GRC tools are not only for the fulfillment of regulations, they are also capable of automating processes and activities to reduce internal costs considerably.

The deployment of GRC tools does not consist of the installation of the tool itself. Greater emphasis should be placed on the implementation, which consists of:

- The definition of the scope of the implementation of GRC tools – selection of processes for implementation and detailed analysis, including the definition of the organization's requirements, identification of data sources and the like.
- Selecting the most appropriate tool that covers the defined needs of the organization.
- Installing the tool and its integration into the IS infrastructure of the organization (including connection to other systems and applications).
- The implementation of existing and optimized processes into the GRC tool (customization of the solution).
- Subsequent continuous support of the solution.

GRC specialists from AEC will guide you through the implementation of GRC solutions. Our main contribution is that we are not just integrators and implementers, but we have extensive experience with information security and ICT.

www.aec.cz

Why Address This Issue?

- The deteriorating security situation is placing ever-greater demands on the identification, evaluation and continuous monitoring of risks in organizations and their information systems.
- New regulations, such as GDPR, force organizations to adapt their information systems and processes, and constantly monitor the rate of implementation of the various legal requirements (compliance).
- All internal and external requirements meshed with security policies need to be periodically reviewed and monitored to review the success of their enforcement in everyday practice.
- The workflow of key operational processes should be standardized and automated, the data of these processes should be available, and metrics should be continuously evaluated.

AEC a.s.
Veveří 102
616 00 Brno, Czech Republic
Phone: +420 541 235 466

AEC a.s.
European Business Center
Dukelských hrdinů 34
170 00 Praha 7, Czech Republic
Phone: +420 267 311 402
Fax: +420 266 177 155

AEC
DATA SECURITY