

GDPR

with SIMAC solutions



The General Data Protection Regulation (EU) 2016/679 (GDPR) enters into validity on the day of 25.5.2018. The new rights are also linked to obligations which must be met by all public subjects providing goods and services within the territory of the European Union. The changes are projected most into internal processes, client – customer documentation and information systems. Sanctions for failure to abide by obligations may reach up to €20 million or 4% of the total annual turnover of the administrator or processor. **For this reason it is necessary to start now.**

How can we help you?

We will guide you safely through the entire GDPR process (see the methodology of Simac Technik ČR on the other side of the product list), from the introductory – brief initial analysis to the actual implementation of the proposed procedural and legal solutions, including any applicable changes in the field of information technologies (IT). As a leading systems integrator we co-operate only with verified and renowned technological manufactures operating on the worldwide IT market.

In co-operation with you we will ensure in particular the following:



mapping of data architecture and proposal of optimal solutions in the field of IT, including applicable investments and your own choice of an appropriate solution, all taking into account the financial and time demands,



assistance with implementation of essential IT solutions, including any applicable supply of recommended and suitable SW and HW,



creation of a complex set of sample contracts relating to the entire issue of GDPR, including the necessary internal directives, consent of the affected subjects and processing clauses,



performance of an assessment of all internal and external processes within your organisation from the perspective of personal data protection (Data Protection Impact Assessment)



assistance with communication with supervisory bodies,



advice with applicable appointment of a Data Protection Officer or with outsourcing of this new position of employment,



assistance in continuous evaluation of the compliance of all your existing and prepared activities so as to ensure that compatibility with GDPR is guaranteed at every moment (Protection by Design principle).



analysis of data in processing from the perspective of personal data protection,



complex procedural, data and legal audit for the purpose of determining the impacts of GDPR on your organisation,

Throughout the entire GDPR implementation process we co-operate and form a joint team together with the international legal office UEPA, whose lawyers have extensive experience with personal data protection.



Preliminary analysis

- Reconnaissance of organizational structure and identification of personal data in processing
- Determination of state of documentation of processes and ICT environment
- Determination of responsible employees
- Interview with owners of relevant processes and services
- Analysis and evaluation of determined data

Main outputs:
Final report including estimate of degree of preparedness for GDPR



Detailed analysis

- Identification of personal data
- Review of processes with the aim of identifying movement of personal data
- Mapping of data movement
- Mapping of safeguarding of environment
- Evaluation of compliance of personal data processing with GDPR

Main outputs:
Document evaluating compliance of current state of personal data processing with requirements of GDPR



Proposed measure

- Measure for meeting requirements
- Proposal for configuration adjustments
- Proposal for adjustment of processes
- New tools and processes
- Adjustments to input/output interfaces
- Recommendations for adjustments to applications

Main outputs:
Definition of GDPR implementation, measures and decomposition into individual implementation projects.



Implementation

- Realization of GDPR implementation measure, i.e. according to set priorities for realization of individual implementation projects

Main outputs:
Status reports on course of GDPR implementation



Audit

- Testing of incidence of unsecured or unidentified data
- Testing of data securing
- Testing of procedures, processes and knowledge

Main outputs:
Results of audit tests and recommendations for correction