Software development with data protection by design and by default

Article by Dr. Carlo Piltz and Olga Kasner

Whenever personal data are processed in or by software, it must be ensured at an early stage that the software solution and the processes which the software supports meet the requirements of the General Data Protection Regulation (GDPR).

Personal data are an indispensable basis of product development for both software companies and the customers who purchase the software, and form an essential part of the software used in both the B2B and B2C markets. However, the principle of data minimization dictates that processing of data should be kept to an absolute minimum.

So what changes can be made to software development so as to ensure that GDPR requirements do not emerge as a compliance problem later on?

Software development should follow a methodology with key activities which incorporate and consider data protection issues along with "security by design." Article 25 of the GDPR states that the controller is responsible for effectively implementing data protection principles and for protecting the rights and freedoms of data subjects. To do so, the controller is first required to take appropriate technical and organizational measures and necessary safeguards.

Ensuring effective data protection at the time of processing necessarily means that data protection must be taken into account when designing the system, and that the default settings used must be ensure the greatest possible level of data protection. This is required by the principles of "data protection by design" and "data protection by default," which are defined in Article 25 and Recital 78 of the GDPR.

In its new Guidelines 4/2019 on Article 25 of the GDPR: "Data Protection by Design und by Default (DPbDD)," the European Data Protection Board (EDPB) requires controllers to consider DPbDD when planning new processing activities. The Guidelines, which cover key aspects which are to be taken into account by controllers
when designing processing activities, refer in turn to the guidelines issued by the Norwegian Data Protection Authority, "Software development with Data Protection by Design and by Default."

These guidelines, which were developed partially in collaboration with security experts and software developers in the public and private sectors, provide a methodology with key activities which details for developers, software architects, project managers, testers, data protection officers and security consultants how data protection principles, the rights of data subjects and the requirements of the GDPR are to be incorporated in each stage of the development process.

These guidelines from the Norwegian Data Protection Authority cover all aspects of the software development process, along with recommendations for how to implement these measures so as to enable software developers to integrate data protection requirements in the development process.

About us:
reuschlaw Legal Consultants advise companies active on a national and international scale in more than 30 countries in the areas of product liability, product safety law, recall management, insurance law, cybersecurity and data protection, compliance management and contract law.

Company contact: Melanie Schaumann | Head of Marketing & Communications | T > +49 30 / 2332895 | E > melanie.schaumann@reuschlaw.de