Three years of the General Data Protection Regulation in Germany

05/26/2021

After three years of practical work with the General Data Protection Regulation, the Hessian Commissioner for Data Protection and Freedom of Information takes stock.

Fotolia_204144852_S.jpg

© Chris fotolia.com

The General Data Protection Regulation came into force five years ago and has been in force in Germany for three years. It has been received with many expectations and fears. Much of this was exaggerated, for many things a practicable practice has been established, some still await implementation. After the first three years of practical experience with her, a realistic interim balance can be drawn.

The greatest success of the General Data Protection Regulation is that it expresses the values that the member states of the European Union have agreed on as they move into the digital society. Its principles, in order to shape the basic rights to data protection and self-determination, are indispensable conditions for a society worth living in. For example, they demand sufficient transparency in data processing for the data subjects, the linking of data processing to the purpose of legitimate data collection, the minimization of the personal reference of the data to what is necessary to achieve the purpose and the guarantee of data protection through the technical and organizational design of the processing systems. The regulation thus shows a third way of global digitization - between the control of everyday life in China and the data exploitation of Californian digital capitalism. Many countries around the world want to go down this path and are passing data protection laws that are based on the General Data Protection Regulation.

For the first time, the General Data Protection Regulation offers uniform, directly binding regulations for data protection throughout the European Union for the increasing handling of personal data. It has thus promoted the discussion about the necessity and content of data protection and strengthened respect for the fundamental rights of the persons concerned. In particular, with its threats of sanctions based on competition law, but also with its establishment of independent, strong supervisory authorities, it has drawn a lot of attention to data protection.

Despite this strengthening of data protection, fears of inadequate data protection bureaucracy were exaggerated. Practice has shown that the transition to the new data protection regulations was not as costly as their opponents had predicted. The

General Data Protection Regulation largely continues the provisions of the previous data protection directive. Anyone who had already complied with the data protection rules before the General Data Protection Regulation came into force only had to change a little in their practical work. Legislative innovations in the ordinance, such as the enactment of codes of conduct or the certification of processing operations, have hardly been accepted in practice. They could lead to further simplifications.

However, three years of data protection practice have also made weaknesses in the General Data Protection Regulation increasingly clear. On the one hand, it has not led to a uniform data protection practice in the European Union: the abstract nature of many regulations leaves room for different interpretations and the many opening clauses open up scope for divergent laws in the member states. With regard to the coordination of the independent supervisory authorities, it has provided for complicated procedures that require uniform objectives and a cultural change that is (still) missing. On the other hand, it missed the necessary modernization of data protection in view of the challenges posed by the latest information technologies such as big data, the Internet of Things or artificial intelligence: It contains predominantly abstract, technology- and risk-neutral regulations that are difficult and highly controversial to put into concrete terms in practice. Examples of this are the necessary balancing of data-driven business models between the legitimate interests of the person responsible and the interests of the data subject worthy of protection, without the regulation specifying suitable criteria for this. Another example are the countless disputes over the extent of the right to information. The lack of specificity in many of the provisions of the regulation ties up millions of hours of work every day and hinders innovation and investment.

Social power always penetrates into gaps left by the law. Such loopholes are primarily used by global corporations and other powerful data processors to assert their interests – often to the detriment of the data subjects. Compensating for deficits in legislation afterwards causes a lot of work for the supervisory authorities. Advances in data protection practice are particularly evident where the European Data Protection Board, the Conference of Independent Federal and State Supervisory Authorities or individual supervisory authorities have provided legal clarity - but always at the risk that those who disagree will seek legal clarification from the courts call up. This could often have been avoided by a few risk-oriented stipulations by the Union legislature.

European and German legislation should learn from experiences with the General Data Protection Regulation for future digitization projects. At least the European Commission seems to have gotten this message. In its draft regulation on the regulation of artificial intelligence, it has given up strict technology and risk neutrality in the regulation and regulates in a sector-

and application-specific manner how risks to fundamental rights can be averted by artificial intelligence.

Prof. Dr. Alexander Roßnagel, Hessian Commissioner for Data Protection and Freedom of Information

Contact for press representativesPress spokeswoman: Ms. Maria Christina RostPress and public relations: Telephone: +49 611 1408 119The Hessian Commissioner for Data Protection and Freedom of InformationP.O. Box 316365021 Wiesbaden