EU General Data Protection Regulation (EU-GDPR)

Protection of personal data: Understand the key requirements of the harmonized EU standard

White paper

Abstract

Due to technical progress and increasing globalization, a harmonization of data protection regulations in Europe is both meaningful and necessary. The European Union (EU) General Data Protection Regulation, abbreviated to "EU-GDPR", facilitates this harmonization.

Officially published on 25.05.2018, the EU-GDPR is now applicable law in all member-states of the EU and as such replaces previous national data protection law. Nevertheless, the EU-GDPR includes so-called escape clauses in certain areas, on the basis of which the member-states may complement the EU-GDPR with additional national regulations. This whitepaper explains key principles and rules of the EU-GDPR.

TÜV SÜD

Contents

About the TÜV SÜD experts

Doris Kiefer, lawyer

Ms Doris Kiefer is a lawyer and certified data protection officer. Working for TÜV SÜD Sec-IT GmbH in Munich as a technical expert in the field of data protection, she gives advice on matters of data protection law throughout Germany. In addition, Ms Kiefer is an external data protection officer, and the co-publisher of the "Electronic Data Protection Handbook". She regularly publishes specialist articles and gives talks on current topics in the field of data protection.

Markus Säugling, lawyer

Mr Markus Säugling is a lawyer, working for several companies as data protection auditor, ISO/IEC 27001 lead auditor and a certified external data protection officer. He is a founding partner of the consultancy MAGELLAN, which specializes in the provision of consultancy services and is a legal practice in the fields of data protection, information technology and IT security. He advises both small and medium-sized companies, as well as trade associations and other business groups.

1. Key principles and rules

1.1 Transparency and information obligations, article 12 et seqq.

The EU-GDPR increases the obligations to provide information when personal data is collected from data subjects. In addition to the well-known information obligations such as the identity of the controller, as well as the purpose and categories of recipient, the following information is now required

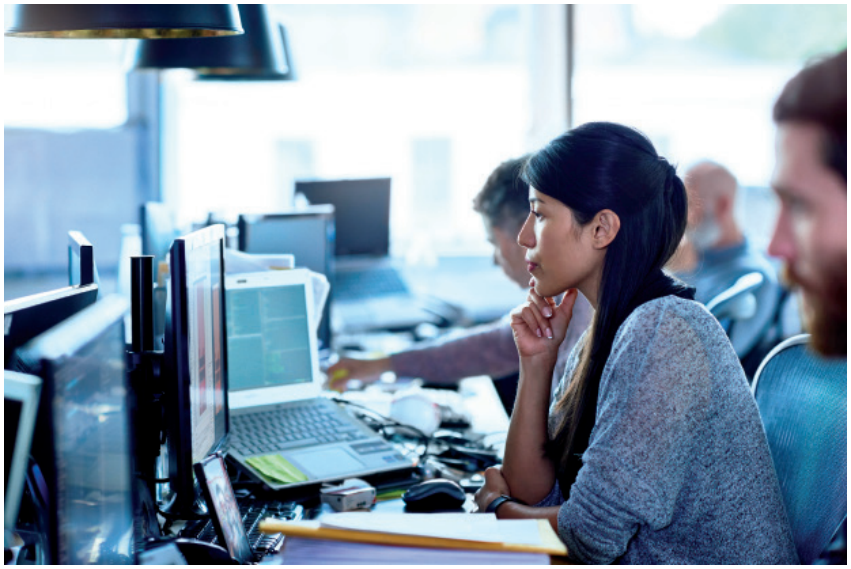
- Contact data of the controller and his deputy
- Contact data of the data protection officer
- The controller's legitimate interests
- The intention to transfer data to a third country or to an international organization (and the Commission's associated adequacy decision)
- How long the data will be stored
- Data subjects' rights to information, erasure, correction, restriction the right to revoke consent, the right to appeal to a supervisory authority etc.
- The reasoning behind, and consequences of, any profiling activities.

Recommended action
Implement processes to ensure that the data subject is informed and kept up-to-date. Revise your data protection declarations!

1.2 Processing of personal data, article 5 et seqq.

Processing of personal data is, inter alia, only lawful provided that at least one of the following criteria has been fulfilled: consent has been obtained for one or more purposes, processing is required on the basis of a contract (or pre-contractual measures), a legal basis is present, or processing personal data is necessitated by a legitimate interest of the controller or of a third party. In this context, data processing may not be based on the law of a third state. Consent is conditional on it being given voluntarily, and must be in an easily comprehensible form, including simple language. Consent in written form is not explicitly required. However, as documentation of the consent must be retained, a written consent is recommended.

The data subject is entitled to revoke their consent at any time. This process must be as simple as granting consent. The awarding of a contract,



or provision of a service, may not be made dependent on the data subject's consent, unless the data processing to which the data subject is to give his consent is required in order to fulfil the contract.

There are special rules for consent by a child (see section 1.3). The processing of sensitive data is forbidden as a matter of principle unless the data subject's consent has been obtained.

Recommended action
Ensure by both technical and organizational means that documentation of the consent can be retained.

1.3 Child's consent, article 8

In accordance with EU-GDPR, a child's consent is only lawful when the child is sixteen years of age or the parents have given their consent to the data processing.

Recommended action
Develop technical and organizational means required to prove that the parents have given their consent.

1.4 Profiling, article 22

The EU-GDPR introduces the concept of "profiling". Profiling is to be understood as any kind of automated processing with the aim of using the data to evaluate, analyse or predict certain personal aspects of the data subject.
The EU-GDPR gives every data subject the right not to be subject to such (based on an automated processing) a decision, should this decision entail legal consequences, or be capable of having considerable consequences for the data subject in some other way. For that reason, controllers are required to take appropriate measures in order to safeguard the data subjects' rights, liberties and legitimate interests. The minimum requirement includes the right of an individual to intervene in order to present his/her own point of view and to appeal the decision.

Recommended action
Assess the compliance of existing automated processes and implement any measure required to ensure the rights of the data subjects as described above.

1.5 Advertising and direct marketing, article 6 para 1 letter f.

The EU-GDPR provides for a general balancing of interests between the legitimate interests of the company and the interests and basic rights of the data subject (advertising target). As evidenced by the recitals in the EU-GDPR, the processing of personal data for the purpose of direct marketing is to be regarded as a legitimate interest of a company.

Recommended action
You should verify the legality of existing automated processing structures and take measures to safeguard the data subjects' essential rights referred to in conformity with the law.

1.6 Further processing, article 6

The EU-GDPR has introduced the concept of purpose limitation. The Regulation makes a distinction between initial processing and further processing. According to this distinction, further processing is only permitted provided it is consistent with the unambiguous and lawful purpose originally established as the purpose behind the collection of the data. This is referred to as "compatibility verification", since it must be determined whether the original purpose of the initial processing is also compatible with the purpose of further processing.

Recommended action
Ensure that there is a clearly defined and lawful purpose for both the initial processing as well as for further processing of personal data.

1.7 Right to erasure ("right to be forgotten"), article 17

Personal data must be erased should the purpose for it having been recorded no longer apply, provided that no other legal grounds exist to justify further processing.

There is also a special obligation stipulating that personal data relating to children (up to the age of sixteen) must be erased. Moreover, companies are required to take particular action in cases in which personal data is to be made "public". Subject to available technologies and the costs of implementing adequate measures, companies are required to notify other companies that the data subject demands the erasure of all links, copies and replications of data.

Recommended action
Assess erasure and blocking concepts of existing IT systems, as well as the selection criteria for any new systems. The precautions for the protection of children require that children's personal data should be identifiable as such. You must establish appropriate information processes or – if possible – design internal processes in such a way that no data of this kind can be published.

1.8 Right to data portability, article 20

The EU-GDPR requires that companies are able to return information that a data subject has provided to the company in a structured, commonly used and machine-readable format. At the data subject's request, this data must be transferred directly to another company, provided that this is technically feasible. This marks the end of heterogeneous, company-specific data formats in European companies, at least on paper.

Recommended action
Take precautions, both in your processes as well as technically, to ensure that data within your IT systems is stored in a form that is transferrable. In this context, the way in which data is recorded should be examined since the obligation to transfer data covers all the subject's data.

1.9 Responsibility of the controller responsible for processing, article 24

The controller responsible for processing is required to take appropriate technical and organizational measures in order to ensure that personal data is processed in conformity with the EU-GDPR. In this context, technical and organizational measures must be examined and, where applicable, updated. The controller responsible for processing must determine beforehand the likelihood and severity of the risks for individual rights and liberties. Moreover, they must provide evidence that personal data is processed in conformity with the Regulation. Accordingly, a (documented) risk assessment is required, which assesses on the basis of an objective evaluation the risks to which the data processing is subject and how high the relevant risk is considered to be. As part of this evaluation, the cause, likelihood and severity may be applied as criteria.

Recommended action
A documented description of the likelihood and severity of the risks to the data subject's individual rights involves considerable effort. Take steps to ensure sufficient resources.

1.10 Data protection by default, article 25

Companies are required to implement data protection by default. Both at the conceptual stage as well as during data processing itself, they must provide for technical and organizational measures so that, by means of appropriate pre-settings, as a matter of principle, only the data which is required for processing can actually be processed. This obligation applies to both the quantity of personal data recorded as well as to the extent of its processing, the length of time it is stored and its accessibility.

Recommended action
Take appropriate technical and organizational measures. Moreover, existing IT systems (particularly own software and apps) should be reviewed with regard to data processing requirements.

1.11 Processor, article 28 and joint controllers, article 26

Specific requirements apply where processing is to be carried out on behalf of a controller. Moreover, the EU-GDPR provides a "new form" of cooperation with regards to the functions of joint controllers. According to the EU-GDPR, controllers can collaborate jointly provided that the joint purposes and means of processing have been agreed on. The agreement must be in a transparent form and provide clear information on the responsibility for different functions. Importantly, this requirement includes the volume of the data, extent of processing, duration of storage and accessibility.

Recommended action
Review existing processors and adapt the contractual basis to meet the requirements. You should also assess existing collaborations to see if a joint cooperation model could be a better alternative for both sides.

1.12 Obligations to notify infringements of data protection, article 33

There is an obligation to notify the data subject should their personal data be infringed, and there is a probability of this entailing a high risk for the data subject's rights and liberties. The data subject must be informed without undue delay and in clear and simple language:

- of the nature of the infringement,
- the data protection officer's name and contact data, or some other person to contact for further information,
- a description of the probable consequences of the infringement of the protection of personal data, as well as a description of measures taken or proposed to remedy the infringement and, if applicable, to limit their possible negative consequences.

The controller must submit a report on the infringement to the responsible regulatory authority, which must also fulfil certain conditions, within 72 of hours of becoming aware of the infringement.

Recommended action
Develop processes so that data protection infringements can be reported within the stipulated deadline and with the required details. Document all infringements and the measures that must be taken to remedy them. Train your employees so that data protection infringements can be identified and reported in time. Develop measures to optimise processes from past infringements.

1.13 Security of processing, article 32

The risk-based approach of EU-GDPR requires companies to implement suitable technical and organizational measures with which a level of protection adequate to the risk is assured. In this case, not only the state of technology; the costs of implementation; the nature, extent, circumstances and the purpose of processing, must be considered, but also the likelihood of the risk and the severity of such a risk for the data subject's rights.

The EU-GDPR explicitly demands the technical use of pseudonymisation and encryption. Moreover, measures must be taken with respect to the confidentiality, integrity, accessibility and resilience of the systems. Companies are not only required to ensure the rapid recovery of access to the data in the event of physical or technical incident, but also to establish regular processes in order to appraise and evaluate the effectiveness of existing technical and organizational measures on a regular basis.

Recommended action
Assess your measures for compliance against the requirements of EU-GDPR. Precautions should be taken to ensure that you carry out a regular review and obtain the accompanying documentation.

1.14 Data protection impact assessment, article 35

The obligation to carry out a data protection impact assessment applies to all data processing and the whole life-cycle of data processing. This applies particularly when new technologies are used, which, due to the nature, extent, circumstances and the purpose of the processing, probably entail a high risk to the data subject's individual rights and liberties.

The data protection impact assessment requires a systematic description of the planned processing steps and processing purposes including, where applicable, the legitimate interests pursued by the company, an evaluation of the necessity and proportionality of the processing steps with regard to the purpose, as well as an assessment of the risk to the data subjects' rights and liberties.

Recommended action
Adapt processes for impact assessment and implement them in the broad spectrum of requirements that is now stipulated. In addition, you should review the contents of existing impact assessments, checklists and documentation.

1.15 Functions and obligations of the data protection officer, article 37 et seqq.

Apart from a few exceptions, the EU-GDPR allows the member-states to choose whether companies in the private sector are required to appoint a data protection officer.

The data protection officer is not subject to instructions, may not be recalled or subjected to disadvantages and must report directly to the highest level of management. Their functions include training and advice within the company.

There is an obligation to monitor compliance with the EU-GDPR, other data protection regulations and the company's strategy, including the allocation of responsibilities.

Recommended action
As data protection officer, you need to stay on top of regulatory developments. The EU-GDPR represents an increase in the extent of liability, which the data protection officer must observe in their day-to-day work.

1.16 Certifications, article 42

Certification processes and seals gain importance through the introduction of EU-GDPR, as they demonstrate compliance with the relevant regulations. Certification by accredited certification agencies, or the responsible supervisory body, will be granted on the basis of approved criteria.

Recommended action
Secure sufficient resources in terms of time and finance in order to be able to carry out and maintain relevant certifications. Compliant processes need to be implemented before the certification audits take place.

1.17 International data transmission, article 44 et seqq.

The following applies to a transmission of personal data to a third country or an international organization. Should the EU Commission have established that an adequate level of protection is provided, data may be transferred without any special permission. Should an adequate level of protection not exist, the well-known instruments, such as standard contractual clauses, binding corporate rules or the data subject's consent, may be applied. Particularly with regard to the binding corporate rules, it is to be welcomed that the relevant pre-conditions are now listed in the EU-GDPR. Overall, the principles of the decision in the Safe Harbour judgement of October 2015 have been included in the EU-GDPR.

Recommended action
Compile an overview that links data transmissions to other countries to the relevant jurisdiction. Review any relevant pre-condition and other data protection tools. In any event, review the contractual documents that currently apply.

1.18 Liability and right to compensation, article 82

The EU-GDPR stipulates the responsibility for liability in every company and, in addition, stipulates an obligation to provide compensation even in the event of immaterial damage. In addition to the examination of the actual damage caused, the compliance of the data processing itself might be investigated. With this, the potential liability risk to every company increases.

Recommended action
Review existing data processing practices with regard to their continued lawfulness on the basis of the EU-GDPR's permissions status. You should also carry out a new evaluation of existing liability risks and include any increased extent of liability in existing business processes, as well as in future project planning.

1.19 Extension of liability to foreign companies, article 3

Liability in the EU-GDPR also applies to foreign companies, even if they do not have a subsidiary in a member-state of the EU (so-called lex loci solutionis or law of the place of performance). This extension of liability requires solely that the data processing serves to offer EU citizens goods or services, or to observe their behaviour should this behaviour take place within the EU. Accordingly, not only Facebook and Google etc are liable, but every supplier of goods and services, provided its offer is addressed to EU citizens, for instance by applying a language of the EU, or by facilitating payment in Euro.

Recommended action
If you address or observe citizens within the EU, you will need to become familiar with the EU-GDPR requirements, even if your company does not have a subsidiary in Europe.

1.20 Administrative fines and sanctions, article 83 et seqq.

Depending on the gravity of the offence, the scale of financial penalties outlined by the EU-GDPR range from 10,000,000 Euro to 20,000,000 Euro or, in the event of a company, to up 2 % or 4 % of total sales achieved worldwide in the previous financial year.

Recommended action
Review the lawfulness and compliance of existing data processing processes. We also strongly recommend that you to re-evaluate existing liability risks, to include the increased extent of liability in existing business processes, as well as in future project planning.

2. Conclusion

The introduction of the EU-GDPR requires that all companies review existing data processes and create numerous new processes. Even existing data protection organizations must be thoroughly reviewed and adapted to new requirements. In addition, existing models, checklists and contractual documents must be revised. Data protection principles such as “data protection by design” and “data protection by default” are achieving greater prominence in addition to the added requirements of “data protection impact assessment”. Consequently, technical and organizational measures must be adapted.

Demonstrate compliance to the European data protection regulation.

www.tuv-sud.com/cybersecurity

cybersecurity@tuv-sud.com

Add value. Inspire trust.

TÜV SÜD is a premium quality, safety and sustainability solutions provider that specializes in testing, inspection, auditing, certification, training and knowledge services. Represented in over 1,000 locations worldwide, we hold accreditations in the Americas, Europe, the Middle East and Asia. By delivering objective solutions to our customers, we add tangible value to businesses, consumers and the environment.

TÜV SÜD America
10 Centennial Drive
Peabody, MA 01960
(800) TUV-0123
www.tuv-sud-america.com