1&1 IONOS

White Paper

Overview of the new EU General Data Protection Regulation

Practical suggestions for implementation for German SMEs

Internet made in Germany

1. Table of contents

1. **Table of contents** 2
2. **Summary/checklist** 3
3. **Introduction** 4
4. **Scope** 4
5. **Admissibility of data processing** 5
   - a) Prohibition without prejudice to permission 5
   - b) Statutory authorization 5
   - c) Special processing situation: sensitive data 6
   - d) Special processing situation: employee data 6
   - e) Special processing situation: video surveillance 7
   - f) Special processing situation: scoring 7
   - g) Special processing situation: advertising 7
   - h) Special processing situation: big data 8
6. **Contract data processing** 8
   - a) General 8
   - b) Obligations 9
   - c) Transfer of data to third countries 10
7. **Organizational measures** 11
   - a) Documentation obligations 11
   - b) Information requirements 11
   - c) Impact assessment 12
   - d) Reporting requirements for data breaches 12
8. **Technical measures** 13
   - a) Technical requirements 13
   - b) Certification 13
   - c) Data portability 14
   - d) Privacy by design, privacy by default 14
9. **Rights of the data subjects** 15
10. **Data protection officer** 15
11. **Sanctions** 16
12. **Outlook** 17

2. Summary/Check List

Summary

The new EU Basic Data Privacy Regulation applies to all companies in the European Union as of May 25, 2018 and establishes a number of new obligations under the data protection law. It does not just apply to EU companies, but also to companies headquartered in third countries that offer goods/services to EU citizens. New additions to the law include, initially, the direct liability of data processors (IT service providers), significantly higher administrative fines (up to 4% of the group global sales or EUR 20 million) and a single supervisory authority for group companies (one-stop shop). The following important provisions have been added: expanded obligations to provide documentation, supporting evidence and information, privacy impact assessments, the right to be forgotten, maintaining a record of the processing activities, expanded obligations in the event of data breaches, privacy by design/default, the right of data portability and expanded rights for the data subjects. The basic principles of the right of information self-determination, prohibition without prejudice to permission, data avoidance and minimization, earmarking and transparency shall continue to apply.

Check list

The following points must be implemented by May 25, 2018:

- Documenting all business processes (accountability)
- Reviewing the business processes with regard to the existence of permission
- Documenting the weighing of interests during processing based on legitimate interests
- Creating and revising a record of processing activities
- Establishing a procedure for a privacy impact assessment
- Revising declarations of consent and, if necessary, obtaining new ones from the data subjects
- Redesigning the instructions for the data subjects (data privacy statement, etc.)
- Implementing reporting procedures in the event of data breaches
- Reviewing the legal compliance of data transfers within the company and to third party companies
- Amending existing contract data processing contracts and signing new ones with service providers
- Developing/revising a plan for deletion of the data and setting up procedures for deleting the data upon request
- Making the right to data portability technically possible

- Integrating privacy by design/default as fundamental principles in the development process
- Revising data protection guidelines for employees

3. Introduction

The new EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation or „GDPR") entered into force on May 24, 2016 and comes into effect on **May 25, 2018**. The German law on implementing the GDPR, the new Federal Data Protection Act (Bundesdatenschutzgesetz or „BDSG-new" for short), was announced in the German Federal Gazette on July 5, 2017; it also enters into force on May 25, 2018. Therefore, the legal foundations for the new data protection law do exist.

Many companies, particularly SMEs, have not yet looked into the issue. They assume that the beginning of 2018 is early enough to start **implementing** the law. In view of the fact that all of the business processes and data transfers have to be analyzed, all of the documents related to data protection have to be revised and new technical procedures need to be implemented, companies should not wait to start implementing the new provisions. This guideline provides a 17-page overview of the most important contents of the GDPR and practical suggestions on how to implement it within the company.

4. Scope

The new GDPR applies, on the one hand, to companies that process personal data in the context of the activities of an establishment in the European Union (the **establishment principle**). On the other hand, it also applies to companies that do not have an establishment in the EU, but offer their goods and services to people residing there (**law of the place where relevant performance occurs**) or monitors them there, according to Article 3 of the GDPR[1] . Companies like Google or Facebook would therefore also fall under the GDPR even though they do not have an establishment in the EU, since they offer their goods or services to EU citizens. According to Article 27, companies like these must designate a representative in the EU to act as contact person to data subjects and supervisory authorities.

[1] All of the following Articles that do not cite the legal basis are Articles of the GDPR.

5. Admissibility of data processing

a) Prohibition subject to authority approval

The GDPR, just like the previous EU Data Protection Directive 95/46/EC and German Data Protection Act, stipulates that personal data may only be processed if the data subject has given its consent (prohibition subject to authority approval). Companies must therefore ensure that the data subject has given consent for the respective processing of the personal data or there is an EU or member state law that deems it necessary. According to Article 6, processing shall be only **lawful** if it is necessary for the performance of a contract or necessary in order to protect a vital interest.
Article 7 governs the conditions for **consent**, which requires the company to provide proof of the consent. However, unlike with the old GDPR, that consent is no longer required to be in writing. In the future, companies can therefore also obtain consent **electronically** or otherwise, but it should be noted that the burden of proof is on the company. Companies are prohibited from making performance of a contract dependent on consent, provided that the data are not required for actual performance of the contract (**prohibition of coupling**).

Practical tip: *According to Recital 171, any already existing consent shall remain valid if the manner in which the consent has been given is in line with the conditions of this regulation. However, since Article 13 mandates much more comprehensive information requirements, all of your consent templates should be revised accordingly.*

b) Statutory authorization

The processing of personal data without a data subject's consent is only permitted in the exercise of official authority (Art. 6). In addition to the necessity for the performance of a contract (question: is processing the personal data in question necessary for the performance of the contract?) and for the **purposes of legitimate interests**, and are there exceptional cases for this, such as for compliance with a legal obligation, to protect vital interests or to perform tasks in the public interest. It is important that the processing is carried out for the purposes of legitimate interests. This option will most likely play the biggest role in data protection in the future. In the weighing of interests companies will have to determine whether there are interests of the data subjects not worthy of protection that are more important than their own legitimate interests in using the data. The data in question may be processed only if this is not the case. The weighing of interests must be documented, because the data protection authorities will ask for this documentation during the next audit. The (new) right to object, which allows the data subject to object to the processing of their data based on legitimate interests in accordance with Article 21 of the GDPR is also important, although here the exception in Article 36 of the new GDPR should be taken into consideration in cases of public interest.

Practical tip: *Documenting the balance of interests was advisable until now, but was not mandatory. This is therefore a tedious yet important new task in the implementation of the GDPR in all cases in which the processing of personal data cannot be based on performance of the contract or consent.*

c) Special processing situation: sensitive data

Article 9 includes special provisions in the event of processing extremely sensitive data. According to Article 9, the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation is only permitted if certain conditions are met. For example, this is the case when there is consent or the necessity of medical treatment. The German law includes additional provisions concerning permission in Section 22 of BDSG-new, for example when the processing is required in accordance with the Social Insurance Code (Sozialgesetzbuch, SGB). While citing examples of particular cases, paragraph 2 of this provision also stipulates that appropriate technical and organizational measures be taken while taking into account the state of the art to safeguard sensitive personal data; Sections 27 and 28 of BDSG-new must also be noted.

Practical tip: *Avoid processing sensitive data to the extent that it is operationally feasible. The supervisory authorities pay special attention to this and require extremely accurate documentation. However, if you must process sensitive data, always base the processing of that data on the data subject's consent, which must be worded very clearly.*

d) Special processing situation: employee data

There is no special consideration given to the protection of employee data in the GDPR. However, German lawmakers included provisions in Section 26 of BDSG-new that expand on Section 32 in the previous version. Personal data can continue to be processed where necessary for performance of a contract or to detect crimes. What is new is the admissibility if it is necessary to comply with legal obligations to fulfill work agreements or collective agreements. The basis of consent in the employment relationship is also covered for the first time in Section 26(2) BDSG-new. According to this, the employee's consent may only be considered to have been freely given if it is associated with a legal or economic advantage for the employee or if the employer and employee are pursuing the same interests. Consent must always be given in written form.

Practical tip: *Avoid employee consent in the employment relationship. It can be withdrawn at any time unless it is specifically given in a works agreement. Instead, you should base the processing of employees' personal data (when possible) on the necessity of performance of a contract or ensure effective anonymization of the employee data, which cancels the need for data protection.*

e) Special processing situation: video surveillance

Video surveillance is not expressly regulated in the GDPR. As for the lawfulness of processing without consent, the general provision of Article 6 (1) (f), i.e. processing based on legitimate interests, therefore applies. As such, before installing a video surveillance system you must perform a documented weighing of interests and, if there are risks for the data subjects, as well as a (well-documented) data protection impact assessment in accordance with Article 35 (see number 5c below). The individual video cameras must be listed in the record of processing activities. From a data protection standpoint, video surveillance involves significant costs for its implementation, so the supervisory authorities have high requirements for it. When monitoring publicly accessible areas, Section 4 of BDSG-new, which states that a company's video surveillance is only permitted when necessary to exercise the right to determine who shall be allowed or denied access or to pursue legitimate interests, must be observed; the latter is only permitted when the weighing of interests is positive (see item 3 (c) above in this regard). Other new provisions include the expanded obligation to provide information: the fact that the area is being monitored and the controller's name and contact details must be identifiable in an appropriate location as early as possible.

Practical tip: *Video surveillance requires „Advanced data protection." Let the professionals handle it and make sure that the data protection impact assessment is adequately documented.*

f) Special processing situation: scoring

Scoring (determining the probability of defaulting on a loan, for example) is not expressly regulated in the GDPR. However, Section 31 BDSG-new contains national special rules that are understood as ascertaining the probability for the weighing of interests (see item 3 (c) above). In particular, it defines negative traits that make scoring inadmissible, such as only using address data, for example.

g) Special processing situation: advertising

Processing personal data for advertising purposes is also not expressly regulated in the GDPR. You must therefore once again weigh the interests – provided

no consent has been given. Recital 47 of the GDPR expressly recognizes that a „legitimate interest" exists in the case of direct advertising, so the legitimate interests of the data subject should be carefully assessed when documenting the weighing of interest. The data subject's right to object should once again be noted in accordance with Article 21 (here paragraph 2), this also applies to the required obligations to provide information pursuant to Articles 13 and 14 (see item 5 (b) below).

Practical tip: *Section 7 of the Act against Unfair Competition (UWG) should also be observed when processing data for advertising purposes. It contains the concrete specifications for marketing measures in Germany.*

h) Special processing situation: big data

The processing of personal data based on legitimate interests must also serve the subject of „big data," because personal data that are collected based on consent or a contractual requirement are subject to earmarking for specified, explicit and legitimate purposes (Article 5 (1) (b)). They may not be processed for „other purposes" if consent for this has not been granted. The use of big data therefore requires a comprehensive, documented weighing of interests; anonymization or pseudonymization of the data in question would be even better. The prohibition of coupling as per Article 5 (4) and the ePrivacy Regulation on the collection via the Internet (tracking only when the data subject has opted in) apply here.

Practical tip: *The parties interested in big data assessments cannot try to justify themselves using the law, not even if based on legitimate interests. You should therefore ensure that the big data systems only process (previously effective) anonymized data.*

6. Contract data processing with regard to cloud computing

a) General

With regard to contract data processing, the GDPR is based on the same principles as the old BDSG. Typical cases of contract data processing are cloud computing, IT outsourcing, removing data for the purpose of destroying files or remote maintenance by IT service providers with access to internal personal data. However, newly added provisions include, among other things, increasing the technical/organizational requirements to the state of the art as well as obli-

gations of cooperation for reporting requirements and data protection impact assessments.

b) Obligations

The admissibility of contract data processing is now regulated in Article 28, according to which the company has to evaluate the appropriateness of a processor to see whether it offers sufficient guarantees that it has implemented appropriate technical and organizational measures to ensure sufficient data protection. An approved code of conduct as per Article 40 or certification as per Article 42 are acceptable proof of this. In addition, a contract must be concluded with the contract data processor in written or (and this is new) in electronic form about the job, which is bound by instructions. The contents of the contract are stipulated in Article 28 (3). The processor may only engage another processor with the prior specific authorization of the controller. The processor shall initially be fully liable for any data protection infringements, as governed in Article 28 (10); this also applies to administrative fines (Article 82). In addition, the processor now also must maintain a record of processing activities for all of the categories under its responsibility, which must be made available to the supervisory authorities on request (Article 30 (2)). The processor has its own reporting requirements to the controller in the event of data breaches, which could result in administrative fines (Article 83 (4) et seq.).

Practical tip: *There are still many (even large) companies that are still at square one when it comes to contract data processing and do not even have written contract data processing contracts with their service providers and freelance employees even though they have system access. Remember that the supervisory authorities frequently audit with regard to contract data processing and very frequently find things. This should be your number one priority. Note that contract data processing does not just mean that data are actively sent outside the company (like with cloud computing), but rather passive data access from outside the company (e.g. remote maintenance by a software manufacturer, remote access for freelance employees) is also a data transfer that must be performed in conformity with the law. Global companies in particular should pay attention to their due diligence obligations with international data transfers (see item 6 (c) below).*

Many German companies consider the exchange of personal data in a company to be privileged („company privilege"), in other words, they do not feel it requires special arrangements. This assumption is incorrect. The old BDSG as well as the new GDPR do not grant company privilege. The same legal provisions as the ones for the exchange of data between any companies of a group company also apply to the exchange of data between any unrelated companies. If a French parent company wants to access its German subsidiary's data, then this is a transfer of personal data from German to French servers and requires the data subject's consent or legal permission (see item 3 (c) above). However, if the processing is based on legitimate interests, Recital 48 may help, which stipulates

that the transmitting of personal data within the group is recognized as a „legitimate interest."

Practical tip: *Up to now there have been very few groups (especially international groups) that have achieved compliance when it comes to the subject of data transfers. You should therefore review all of the data transfers within the group and establish the legal basis for the transmitting of data (e.g. through standard contractual clauses, see the following section).*

c) Transfer of data to third countries

Even the new GDPR requires an existing and sufficient level of data protection for the transfer of personal data to locations outside the EU (Article 44 et seq.). Companies cannot therefore hire cloud providers with servers located outside the EU unless special prerequisites are met. On the one hand, an **adequacy decision** by the EU Commission may be considered, which currently applies to the countries of Andorra, Argentina, Canada, Switzerland, the Faroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand and Uruguay. A data transfer can therefore be carried out into these countries without any further safeguarding, provided the prohibition subject to authority approval is observed (see item 3 (a) above). Furthermore, an appropriate level of data protection can be achieved outside the EU using so-called **standard contractual clauses**, which are adopted by the Commission (or by supervisory authorities) and signed by the recipient of the data. It is also possible to achieve an adequate level of data protection through internal data protection regulations (Article 47) or „binding corporate rules." In doing so, all of the group companies are brought into compliance with the GDPR data protection principles and the entire set of guidelines is then reviewed by the relevant supervisory authority. If the supervisory authority feels that they meet the requirements, it will approve the set of guidelines, which ensures the required, appropriate level of data protection in group companies in third countries. The newest additions, however, are the **codes of conduct** and **certifications** (Article 46 (2) (e/f)), which the supervisory authorities can approve and which are then used as the legal basis for creating the required, appropriate level of data protection.

Practical tip: *This also includes the EU-US Privacy Shield. The EU Commission has thus equipped all of the member US companies with an adequate level of data protection. However, please remember that (as of August 2017) the Privacy Shield as well as the standard contractual clauses are currently being challenged in court and the latter in particular may possibly be declared invalid in 2017 or 2018, which would then create an acute need for action if you store personal data in the United States or other third countries.*

7. Organizational measures

a) Documentation obligations

Companies have had extensive documentation obligations imposed on them by the new GDPR. For example, according to Article 30, they must maintain a (at least electronic) **record of their data processing activities** that includes, among other things, the company's contact details, the purposes of the respective processing, a description of the categories of data subjects and data, transfers of personal data to third countries or international organizations, time limits for erasure of the data and a description of the technical and organizational measures. In the case of video surveillance this must be performed in each case (Section 4 BDSG-new). However, companies that do not regularly process personal data and employ fewer than 250 employees are exempt from the obligation to maintain a record in accordance with Article 30 (5). This exception only applies to a few German companies, though, since regularly processing personal data has become standard these days (e.g. maintaining a company's own customer or employee database). In addition, according to Article 5 (2), companies are responsible for their compliance („**accountability**"). In contrast to the previous provisions in the BDSG companies are now obligated to prove their compliance with the GDPR principles in Article 5 (1) to the supervisory authorities, especially the „lawfulness of the processing," which is a de facto reversal of the burden of proof.

Practical tip: *This also includes the EU-US Privacy Shield. The EU Commission has thus equipped all of the member US companies with an adequate level of data protection. However, please remember that (as of August 2017) the Privacy Shield as well as the standard contractual clauses are currently being challenged in court and the latter in particular may possibly be declared invalid in 2017 or 2018, which would then create an acute need for action if you store personal data in the United States or other third countries.*

b) Obligation to provide information

According to Article 13, before their personal data are collected the data subjects must be thoroughly **informed** about the planned use, including the contact details of the company, the purposes and the legal basis for the processing, if necessary disclosing the „legitimate interest," the fact that the data may be transferred to third countries and the legal basis for the transfer, the period for which the personal data will be stored and/or the criteria used to determine that period or the existence of data subject rights. If the data are not obtained directly from the data subject, then, in accordance with Article 14, the controller must also provide the data subject with the source from which the data originates and what categories of personal data are affected. The above obligations to provide information shall not apply if the data subject already

has that information or if the direct provision of such information would prove impossible or would involve a disproportionate effort. Further exceptions are listed in Sections 32 and 33 BDSG-new. **Formally**, with the obligations to provide information it must be noted that the information be precise, readily available and provided in clear and simple language (see Article 12). If the target group is children, the information must be provided in language that they can easily understand. The information should be in written form, but electronic form is also permitted on the Internet; it may only be in verbal form in exceptional cases. However, in accordance with Article 21 (4), instructions on the rights to object shall be presented separately from any other information. In accordance with Article 14 (3), if possible, the information must be provided at the time it is obtained, but at the latest within a reasonable period (no more than 1 month) after obtaining the personal data.

Practical tip: *All of the texts about the rights and obligations under the data protection law must be revised, because of the new changes stipulated in the new Articles 13 and 14. Please remember that, as per Article 39, the data protection officer is only obligated to „monitor, inform and advise," and not to draw up the documents related to data protection. This is the job of the executives who, if needed, can delegate it to the legal department.*

c) Data protection impact assessment

Article 35 of the GDPR introduces a duty to provide a data protection impact assessment in the event that a concrete type of processing is likely to result in a high risk to the rights and freedoms of the data subjects. According to Recital 75, a high risk like this is one where the processing may give rise to discrimination, identity theft, financial loss, damage to reputations or profile building using location information. Controllers must give the supervisory authorities a list of the processing activities in which an impact assessment is normally carried out (black list). In addition to a systematic description of the processing operations, a data protection impact statement (previously called „prior vetting") must also contain the purposes of the processing. Based on this, the interests of the company in said processing (e.g. introducing video surveillance) must be weighed against the interests of the data subjects in refraining from processing the data. This weighing of interests must be documented.

Practical tip: *For a specific approach to the data protection impact assessment read the practical information from the supervisory authorities in Bavaria or Baden-Wuerttemberg. They frequently contain good practical tips.*

d) Reporting requirements for data breaches

Data breaches can happen at any time. Security flaws in web applications are exploited to gain full access to company systems or hard drives are stolen from

the server room. While only sensitive data are affected by the reporting requirement today in accordance with Section 42a BDSG, companies must also note the reporting requirements for normal personal data in accordance with Articles 33 and 34. As such, a report must be submitted to the responsible supervisory authority after **each data protection violation** unless the data breach is not likely to result in a risk for the data subjects. However, if there is a „high risk" to their rights and freedoms then the data subject must also be informed. This shall not apply if appropriate technical and organizational measures were taken to prevent similar data protection breaches in the future or effective measures to limit the damage were taken and that eliminated the high risk. According to the new principle of the **one stop shop** (Article 56), the **lead supervisory authority** is the one at the location of the „main establishment" and is then considered the contact partner for all of the group's questions concerning data protection law. The report must be submitted immediately, but no later than within 72 hours, and must contain certain information such as the type of data breach, the categories of personal data are affected, the number of data subjects and data sets.

Practical tip: *Create a data sheet with a description of the process for your employees so that they immediately know what to do when there is a data breach.*

8. Technical measures

a) Technical requirements

Technical data protection is regulated in Article 32. It is primarily about IT's classic protection objectives like confidentiality, integrity and availability, which was already taken into consideration in the old BDSG. It now includes the objective of „resilience of the systems"; these systems must be so resilient that their functioning is ensured even during heavy access or use as well as external cyber attacks. Appropriate technical and organizational measures shall be implemented in accordance with Article 32 to fulfill the requirements in accordance with data protection law while keeping in mind the state of technology and implementation costs.

Practical tip: *Until the supervisory authorities have published concrete specifications on the practical implementation of Article 32, companies can use the VDS Guideline VdS 3473, which has a good 38-page overview of the required measures, to orient themselves.*

b) Certification

With the technical requirements the question of how companies can prove their compliance arises, especially when taking accountability into account in

accordance with Article 5 (2). Article 32 (3) offers assistance here, which states that approved codes of conduct or certification procedures can be used as a factor to demonstrate compliance. Codes of conduct or certification procedures like these do not exist yet (as of August 2017). However, it can be assumed that once the GDPR goes into effect they will soon be developed and approved by the supervisory authorities so that in the future a construct will be available to demonstrate compliance with the requirements set out in Article 32. The approval requirements for certification bodies are governed in Section 39 BDSG-new.

Practical tip: *Keep an eye out on what happens in the coming months. It can be assumed that the initial certification procedures for the GDPR may still be offered in 2017. You can find a current overview of GDPR certifications on the Stiftung Datenschutz (data protection foundation) website.*

c) Data portability

Data subjects have a new right to data portability in accordance with Article 20. They can therefore receive the personal data concerning them from the company in a structured, commonly used and machine-readable format. They also have the right to transmit that data directly to a new provider. The technical requirements for this format are not yet clearly defined, but it is expected that the supervisory authorities will publish the corresponding specifications prior to May 2018.

Practical tip: *You will have to adapt your IT systems at this point. Starting in May 2018, personal customer or employee profiles will have to be designed in such a way in terms of technology that they will be able to be published very quickly. If you use providers, you should avoid lock-in effects and expressly include the right to data portability in the contracts.*

d) Privacy by design, privacy by default

In the future, companies will have to comply with data protection requirements at the product development stage. Article 25 states that the appropriate technical and organizational measures must be implemented „at the time of the determination of the means for processing“ (i.e. in the development stage) to ensure compliance with data protection („privacy by design“). If there are configuration options in the product, then you should choose the default setting that is required to fulfill the purpose of the processing („privacy by default“). The principle of data minimization should be taken into consideration here. Both privacy by design and privacy by default were developed with administrative fines in mind in the GDPR (and that is new), which underscores their importance in the eyes of the EU Commission.

Practical tip: *Train your development department and make a close connection with the data protection department available. The supervisory authorities will be looking closely to see whether or not you have already implemented the basic principles of data protection law in the development and production process.*

9. Rights of the data subjects

Data subject rights are being strengthened by the GDPR. Not only can they view their data at any time, but can also actively influence that data. According to Articles 13 and 14, companies have the obligation to explain to the data subjects in detail what exactly is going to happen with the data before the data are collected (**information obligation**, see item 5 (b) above). If the data subject's data was already collected by the company, the subject has the **right of access** to the data for free as per Article 15 (see exceptions in Section 34 BDSG-new) as well as the right to rectification of incorrect data as per Article 16. If storage of the data in question is no longer necessary, consent is withdrawn or the processing is unlawful, the data subject can also demand **erasure** of the data in accordance with Article 17 (see the additions to this as per Section 35 BDSG-new). The company must then also inform the companies to which it has sent the data in question (**right to be forgotten**, Article 17 (2)). According to Article 18, instead of erasing the data, **restriction of processing** is another option when the data in question has to remain stored for legal reasons. Finally, the data subject also has the **right to object** in accordance with Article 21, such as when the data are being processed based on legitimate interests. In accordance with Article 12 (3), the above rights must be complied with within one month after receipt of the request.

Practical tip: *The data subjects have extensive rights and can even expect a response from the company within one month. You should therefore create internal systems that make it possible to respond to data subjects' requests concerning data protection very quickly and with minimum effort. If you use providers you should ensure that the contracts include their obligation to cooperate with requests from data subjects.*

10. Data protection officer

The GDPR stipulates the obligation to appoint a company data protection officer („DPO") only in exceptional cases, including, among other things, in the case where the comprehensive and systematic monitoring of people is one of the company's core activities. However, German lawmakers have adopted their own

rule for this and specified in Section 38 BDSG-new that all companies with at least 10 employees who are permanently employed to automatically process personal data (e.g. because they work with their own e-mail account) must appoint a DPO. The DPO must be appointed based on his/her professional qualifications and expertise in the field of data protection law as well as his/her ability to meet legal requirements. His/her contact details must be published (this is new) and communicated to the supervisory authorities. The DPO reports directly to the highest management level and cannot be recalled or discriminated against because of his/her position.

Practical tip: *The data protection officer does not mandatorily have to come from inside the ranks of the company. A consulting firm or a law firm can also be appointed as an „external data protection officer." This way you also outsource the liability for the areas of „monitoring, informing and advising" to the service provider, which lowers your own risk.*

11. Sanctions

The GDPR provides the supervisory authorities with a wide range of sanction options. In contrast with the old BDSG, the supervisory authorities are instructed to impose sanctions for infringements of data protection laws (Recital 148), unless the infringements are minor ones. Administrative fines of **up to EUR 20 million or 4% of the company's global sales (or group's global sales)** may be imposed against the company in question as well as against an IT service provider the company hires (contract data processor), provided it is responsible for the data protection violation. Relevant previous violations have an effect on the amount of the fine as well as a company's lack of cooperation with the supervisory authority. Section 43 BDSG-new governs its own sanctions in the area of consumer credit if a company fails to properly comply with notification and information requirements. Section 42 BDSG-new includes provisions that punish criminal behavior, such as prohibited commercial behavior and acts with the intention of enrichment and malice.

Practical tip: *The supervisory authorities will not immediately impose administrative fines in the millions; SMEs that commit common violations such as defective contract data processing can more likely expect fines of thousands or tens of thousands. However, the consequences to a company's reputation from data breaches are much worse, because the media enjoys reporting on these. Companies should also take into account that a well regulated data protection system is an ideal basis for the current wave of digitalization, because transparent and tidy data administration makes it possible to quickly and effectively use digital tools such as predictive analytics or artificial intelligence.*

12. Outlook

The GDPR and the new BDSG enter into force on May 25, 2018. The supervisory authorities have already announced that they will not grant any grace periods (sanction-free transition periods to implement the laws). Companies should also note the upcoming ePrivacy Directive, which also enters into force on May 25, 2018. It will replace the existing ePrivacy Directive 2002/58 and Directive 2009/136 on the use of cookies and essentially introduces the obligation of using an opt-in solution for the use of cookies on websites (in other words, getting visitors' express consent which, however, can also be done by using predefined browser settings).

Publisher

1&1 IONOS Cloud GmbH
Greifswalder Str. 207
10405 Berlin, Germany

Contact partner:

Mark Neufurth
Senior Content Marketing Manager
E-Mail: mark.neufurth@cloud.ionos.com

Copyright

RA Dr. Hans M. Wulf
SKW Schwarz Rechtsanwälte

1&1 IONOS Cloud GmbH
Greifswalder Str. 207
10405 Berlin, Germany

Phone: +49 30 57700-850
Fax: +49 30 57700-8598
E-mail: enterprise-cloud@ionos.com

Executive management:
Christoph Steffens,
Matthias Steinberg, Achim Weiss

District Court Berlin Charlottenburg, Germany
Registration number: HRB 125506 B
VAT number: DE 270700052