ePrivacy

Whitepaper

What are the changes regarding data protection

in the future

General Data Protection Regulation?

ePrivacy GmbH, Hamburg, April 2017

Authors: Prof. Dr. Christoph Bauer, Dr Frank Eickmeier, Dr Anna Täschner

The General Data Protection Regulation (GDPR) shall apply throughout Europe from 25 May 2018. It replaces the national data protection regulations that previously applied – in Germany, this is the Bundesdatenschutzgesetz (BDSG) [German Federal Data Protection Act] and the Telemediengesetz (TMG) [German Telemedia Act] in particular. Both acts will remain in force, but as empty laws. The material issues under data protection law will in future follow from the GDPR. The so-called ePrivacy Regulation, which was submitted as a draft in January 2017, is also to be observed by online companies.

What are the most important changes resulting from the GDPR that companies in the EU should consider in the future?

1. **New data privacy statements, new obligations to provide information:**

   Art. 12 et seqq. GDPR governs new obligations to provide information, which, in many places, go beyond the previous obligations to provide information that were to be reproduced in a data privacy statement. If they have not already been added, the following points must be added to the data privacy statement:

   - name and contact details of the controller and his representative, where applicable;
   - the contact details of the data protection officer, where applicable;
   - the purpose for which the personal data should be processed, as well as the legal basis for the processing;
   - if the processing is based on Art. 6 (1) et seq. GDPR, the legitimate interests pursued by the controllers or a third party;
   - the recipient or categories of recipients of the personal data, where applicable;
   - the intention of the controller to transfer the personal data to a third country or an international organisation, where applicable;
   - the duration for which the data are stored;
   - information about the existence of a law on the provision, correction or deletion of information;
   - information about whether the provision of the personal data is legally or contractually prescribed or is necessary to conclude a contract;
   - the existence of so-called “profiling” and, in these cases, conclusive information about the logic involved as well as the scope and the effects strived for of such processing for the data subject.

   ePrivacy tip: Check whether your data privacy statement and your procedure index contain all the necessary information, and add to this if necessary.

2. New definition of personal data – what do cookie IDs have to do with this?

The concept of personal data was given a new definition in the GDPR. It is therefore recommended to review what effects this has on your business model. A lot of data that were previously considered anonymous will in future be considered data with a personal connection. “Personal data” within the meaning of the GDPR are all information that relates to an identified or identifiable natural person; a natural person will be seen as identifiable if they can be identified directly or indirectly, in particular through classification by:

- an identifier such as a name;
- an identification number;
- location data;
- an online identifier; or
- one or more special features that are an expression of the physical, physiological, genetic, psychological, economic, cultural or social identity of this natural person.

In this regard, a paradigm shift by the GDPR is important for the online sector. While previously it was disputed whether online identifiers such as cookie IDs, user IDs, MAC addresses and the like were personal data, they are now generally considered personal. The reason behind this is because they concern an “online identifier” in the sense above.

The practical effects are significant: if online IDs are considered personal data, then any collection or use of these IDs – such as within the framework of online advertising – requires the user’s consent. Therefore in these cases, the new Art. 6 (1) et seq. GDPR applies (see 3 below), which could in future have a significance for the online advertising industry that is hardly to be underestimated.

ePrivacy tip: Check whether you process data that were previously considered anonymous and in future are to be seen as personal, which are then subject to the GDPR.

3. New rules for online advertising

No changes have been made to the basic principle of data protection law by the GDPR: processing personal data is only permitted if the data subject consents or the law permits data processing (where it is allowed by law).

What is permitted by law in Art. 6 GDPR is new, however. In particular, **Art. 6 (1) et seq. GDPR** contains a rule that is far-reaching in practice and partly new. According to this, the processing of personal data is only permissible without express consent if the processing is necessary to maintain the "legitimate interests" of the controller (the party running the advert) or a third party (e.g. a co-operation partner), provided that the interests, fundamental rights and fundamental freedoms of the data subject, which call for the protection of personal data, are not outweighed, in particular if the data subject is a child. The interests of the advertising industry can also represent a legitimate interest. They are therefore not from the outset of less value than the interests of the data subjects, such as the visitors to a website.

ePrivacy tip: As a matter of urgency, check what influence the new rules will have on online advertising for your company and on what legal basis you can process personal data in the future.

4. New rules for the consent of children

Art. 8 GDPR determines that in the future, the consent of a child is only valid if the child is over the age of 16. If the child is not yet over the age of 16, this processing is only lawful if the parents grant consent.

ePrivacy tip: Check whether you process data of children under the age of 16, because you require the parents' consent for this.

5. New: Profiling, and why user profiles do not fall under this

The term "profiling" is new in the GDPR. The legislator wishes for each person to have the right not to be subjected to a decision to evaluate personal aspects concerning their person, which is based exclusively on automated processing and is binding for the data subject or significantly affects them in a similar way. This could

be, for example, an automatic rejection of an online credit application or an online recruitment procedure without any human intervention.

So-called “profiling” is included as such processing. It means any form of automated processing of personal data assessing the personal aspects relating to a natural person, in particular to analyse or forecast aspects regarding work performance, financial position, health, personal preferences or interests, reliability or behaviour, place of residence or change of location of the data subject.

This only applies, however, if this has legal effects for the data subject or the person is affected significantly in a similar way. In plain language, this means that not all forms of user profiles fall under this within the framework of online advertising. This is because these generally have no “legal effects”.

ePrivacy tip: Check whether you operate according to the definition of profiling given and whether this has a legal effect on or significantly affects the data subjects. If yes, you should obtain legal advice.

6. New rules on order processing

There are new rules on order data processing that will simply be called “order processing” in future. There are indeed many principles that have been familiar for a long time in Germany and will continue to apply. There are, however, some changes that make it necessary to make an adjustment to the “order processing contracts”.

The privileged collection, processing or use of personal data by order according to the BDSG (Section 3(8) Sentence 3 and Section 11 BDSG), according to which the service provider employed per order is not a third party, but rather a so-called “internal relationship” determined by law without checking limits for data transfer, is found again in a similar form in the GDPR. This is because according to Art. 4 No. 10 GDPR, an order processor is not a third party. What is new, however, is that the GDPR does not contain any limitation on the privilege of order processing in the EU/EEA area, which previously followed from the limitation in Section 3(8) Sentence 3 BDSG.

The GDPR does, however, place more responsibility and duties on the order processors in future. The central provision for order processors in the GDPR in future

is Art. 28 GDPR. In paragraph 1 of the Article, it is first required to review the suitability of an order processor. According to this provision, the controller may only employ order processors who offer sufficient guarantees that they possess the appropriate technical and organisational measures ("TOMs") for sufficient data protection.

As before, a contract must as a rule be concluded with the order processor, which can be concluded in writing or – a new feature – in electronic form.

For all order processors, there will in future be the new obligation to maintain a record of processing activities pursuant to Art. 30 (2) GDPR for all categories of activities carried out by order of a controller. These must be provided to the supervisory authorities on request, e.g. during audits.

The term "joint controller" is also new. If two or more controllers jointly determine the purpose and the means of processing according to Art. 26 GDPR, then they are "joint controllers". They then set out in an agreement in a transparent form as to which of them will fulfil which obligation according to the GDPR, in particular what concerns maintaining the rights of the data subject and who fulfils which duties to provide information.

ePrivacy tip: If you as the client commission a service provider, check again whether you are provided with the provider's TOMs and whether they are sufficient. If you are active as an order processor, begin in good time to create a processing record for the activities carried out by order.

7. Enhanced data protection default settings, Art. 25 GDPR

Another new feature is the obligation for all companies to make default settings that enhance privacy in the future. According to Art. 25 GDPR, there is the obligation to undertake suitable technical and organisational measures that ensure that, as a result of the default settings, fundamentally only those personal data, the processing of which is necessary for the particular determined purpose of the processing, are actually processed. This obligation only applies for the volumes of the personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default, personal data

are not made accessible without the individual's intervention to an indefinite number of natural persons.

ePrivacy tip: Check whether your IT fulfils the requirements mentioned in future.

8. Revise your procedure record – but not everybody needs the record anymore!

Art. 30 GDPR establishes new requirements for a procedure record, which will in future be called the "Record of all processing activities". According to Art. 30 GDPR, each controller must maintain such a "Record of all processing activities", provided that the processing activity is under its responsibility. In future, the record shall contain the following information:

- the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
- the purposes of the processing;
- a description of the categories of data subjects and of the categories of personal data;
- the categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations;
- where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation;
- where possible, the envisaged time limits for erasure of the different categories of data;
- where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

The record is to be maintained in writing; this can also be in electronic form. The controller (or the order processor, for which these rules also apply to the greatest possible extent) shall make the record available to the supervisory authority on request.

CAUTION: The duties mentioned do not apply for companies or organisations that employ fewer than 250 employees, unless:

- the processing undertaken by them hides a risk for the rights and freedoms of the data subjects;
- the processing is not only occasional; or
- processing of special categories of data is carried out according to Article 9 (1) or personal data are processed through criminal law judgements and crimes within the meaning of Article 10.

Because in the online industry many companies do not only "occasionally" carry out data processing, but rather this is the main purpose of their commercial activity, for them this means that they are as a rule not released from the obligation to create the record. Any company that is involved in the online advertising industry with issues like targeting, user profiles, cookie IDs and the like is still obligated to draw up an appropriate record of processing activities.

ePrivacy tip: Check whether you have to draw up a processing record and start in good time. If you already maintain a record, check whether you need to add anything, where applicable. Consider that in future there will be more severe punishments if you cannot submit a record for an audit by the authorities.

9. New: The so-called data protection impact assessment

The so-called data protection impact assessment, Art. 35 GDPR, is new. According to this provision, where a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a "high risk" to the rights and freedoms of the natural data subjects, the controller – i.e. the company – shall, prior to the processing, "carry out an assessment of the impact of the envisaged processing operations on the protection of personal data". The advice of the data protection officer is to be sought (Art. 35 (2) GDPR).

The data protection impact assessment is required in the following cases in particular:

- a systematic and extensive evaluation of personal aspects relating to natural persons, which is based on automated processing, including profiling, and on which decisions are based that produce **legal effects** concerning the natural person or similarly significantly affect the natural person;

- processing on a large scale of special categories of data referred to in Article 9 (1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

- a systematic monitoring of a publicly accessible area on a large scale.

The supervisory authority shall establish and make public a list of the kind of processing operations that are subject to the requirement for a data protection impact assessment.

The first requirement mentioned above contains an important limitation for the **online industry**. According to this, any automated processing of data – which occurs regularly in the online industry – only requires a data protection impact assessment if this either produces **legal effects** concerning the natural person or particularly sensitive data are processed. The delivery of programmatic advertising on the basis of possible created user profiles does not, however, as a rule create any legal effect; as a rule, no special types of personal data are processed either. In many cases of online advertising, it will therefore not be necessary to undertake a data protection impact assessment. It is all the more important, however, for the individual company to establish whether the requirements are met or not.

If a data protection impact assessment is required, then it should contain at least the following (Art. 35 (7) GDPR):

- a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

- an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other data subjects.

ePrivacy tip: Check whether you need to carry out a data protection impact assessment by assessing the risk for the data subjects. This should generally not be the case unless you run profiling or process special kinds of data. Keep up to date when the supervisory authorities issue the black or white list, and then check whether the type of procedure you use is listed there.

10. Right to erasure (right to be forgotten), Art. 17 GDPR

Art. 17 GDPR introduced a new right, the so-called “right to be forgotten”. The usual rights to erase one’s own personal data remain, however.

In this regard, Art. 17 (1) GDPR determines first that any data subject shall have the right to obtain from the respective controller the erasure of personal data concerning him or her without undue delay where one of the following grounds applies:

- The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.
- The data subject withdraws consent.
- The data subject objects to the processing and there are no overriding legitimate grounds for the processing.
- The personal data have been unlawfully processed.
- The erasure of personal data is required to fulfil a legal obligation.

ePrivacy tip: Prepare to erase data on request from the data subject and set up an appropriate process.

11. Right to data portability

The right to data portability, Art. 20 GDPR, is new. According to this, any data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller – such as Facebook – in a structured, commonly used and machine-readable format. Furthermore, he or she has the right to transmit those data to another controller (such as Google+) without hindrance from the controller to which the personal data have been provided.

ePrivacy tip: Check whether your business model is affected by data portability and prepare for this in good time, where applicable. Possibly discuss with other companies how they implement this requirement. Bitkom recently published a statement on this subject.

12. New obligation to provide notice of data breaches

As governed previously in Section 42a BDSG, there is still a duty to provide information if knowledge of particular personal data is obtained unlawfully.

Pursuant to Art. 33 GDPR, in the case of a personal data breach, the controller shall without undue delay and – this part is new – where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority. This does not apply only if the personal data breach is unlikely to result in a risk "to the rights and freedoms of natural persons". Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. Also new is the obligation governed in Paragraph 5, according to which the controller must document all personal data breaches. The documentation must make it possible for the supervisory authorities to review compliance with the provisions of Art. 33 GDPR.

Each notification must contain the following information:

- a description of the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

- the name and contact details of the data protection officer or other contact point from where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

ePrivacy tip: Check whether you already have an emergency plan in case of a data leak. If not, you should make up for this and, where applicable, inform the competent employees. Also consider the case where there is a data breach on Friday evening, which means that the notification must be made by Monday evening. The emergency plan can, for example, be part of your company's data protection and data security concept.

13. Security and data processing

The GDPR shall also obligate every controller to take suitable technical and organisational measures in order to guarantee a level of security that is appropriate to the data protection risk. These measures must take into consideration the state of the art, the implementation costs, the nature, the scope, the context and the purposes of the processing as well as the various probabilities of occurrence and severity of the risk for the rights and freedoms of natural persons. The measures can include the following, among others:

- A pseudonym for and encoding of personal data.
- The ability to ensure the confidentiality, integrity and availability of data.
- The ability to be able to quickly reproduce the availability of personal data and access to them in the case of a physical or technical incident.
- A procedure to regularly review, assess and evaluate the effectiveness of the technical and organisational measures to guarantee the security of the processing.

ePrivacy tip: Check your already existing technical and organisational measures and ensure that in future, a regular review and therefore the accompanying documentation are ensured for the future.

14. New tasks and obligations of the data protection officer

In future, it will still be necessary in Germany to appoint a data protection officer. In Germany, the obligation to appoint a data protection officer is governed differently than under the GDPR, in the so-called Allgemeine Bundesdatenschutzgesetz (ABDSG) [the General Federal Data Protection Act]. According to this, a data protection officer must be appointed if at least 10 persons are permanently engaged in the processing of personal data. The tightened protection against dismissal, as is already governed in the BDSG, will continue to apply even after the GDPR comes into effect. What is new is that Art. 37(7) GDPR envisages that the "controller or the processor" shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

According to Art. 83(4) GDPR, infringements of these obligations can be fined up to €10 million or 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

ePrivacy tip: If you have not appointed a data protection officer in the past, check whether you need to do this, publish his contact details and share these with the supervisory authorities.

15. New fines and sanctions

Fines are currently set in the BDSG according to the severity of the infringement at up to €50,000.00 or €300,000.00. In Art. 83 et seqq., the GDPR increases this extensively. The new fines under the GDPR, depending on the severity of the infringement, can reach up to €10 million or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher. In the case of infringements of the provisions under Art. 5, 6, 7 and 9 – so in particular, in the case of processing personal data – the fines can range up to €20 million or in the case of an undertaking, up to 4% of the total worldwide annual turnover.

ePrivacy tip: Realise that infringements of data protection law will in future be reinforced with much larger fines than before; inform your employees about this, where applicable.

16. Extension of liability to foreign companies

In future, liability under the GDPR will be extended to foreign companies, even if they do not maintain any of their own branches in a Member State of the European Union. Pursuant to Art. 3 GDPR, it is sufficient that foreign companies either offer data subjects in the EU goods or services or – and this could be important for the online marketing industry – that these companies "observe" the behaviour of data subjects insofar as their behaviour is carried out in the EU. Companies in the online advertising industry that employ technologies to track online activities in particular, e.g. tracking, profiling and targeting, are even liable according to the provisions of the GDPR if they do not run any of their own branches in the EU.

ePrivacy tip: Check whether you work with companies to which this applies and inform them about this, where applicable. In this way, you can increase your readiness.

17. Extended obligations regarding documentation and evidence

The General Data Protection Regulation envisages significantly extended obligations regarding documentation in many cases for controllers and order processors. Art. 5(2) GDPR prescribes that the controller shall be responsible for, and be able to demonstrate compliance with, Art. 5 (1) GDPR. If a responsible company infringes this requirement, there are fines of up to 4% of sales, as mentioned above.

According to Art. 24 (1) GDPR, the person responsible for the processing must be able to demonstrate that processing of personal data is performed in accordance with the GDPR. Order processors must provide the responsible persons with all the necessary information so that the responsible person can prove that he satisfied the duties governed in Art. 32 et seqq. GDPR.

ePrivacy tip: Check whether you can fulfil the extended obligations regarding documentation, in case the supervisory authorities request evidence. This includes documentation of the risk assessment in the course of the review whether an impact assessment is necessary (see above), among other things. If you are active as an order processor, you must take into account that your client will ask you for the corresponding documents, such as a processing overview or TOMs.

18. Data protection management systems

The requirements on companies, on their data protection organisation and data protection processes will increase significantly in future. This lies above all in so-called risk-based data protection, which was established in many places in the GDPR. The requirements of Art. 24 and 25 GDPR, as well as the greatly increased fines, will in many cases make it necessary to develop so-called data protection management systems in the future. A data protection management system is to be understood as the entirety of all documented and implementation regulations, processes and measures that serve to systematically control the handling of personal data in the company in compliance with data protection laws.

ePrivacy tip: Check whether the introduction of a data protection management system could be appropriate for you and weigh the alternative options carefully and in good time.