What to know about the General Data Protection Regulation (GDPR)?

FAQ

www.bitkom.org

bitkom

Publisher

Bitkom e. V.
Federal Association for Information Technology, Telecommunications and New Media
Albrechtstraße 10 | 10117 Berlin

Contact

Sausanne Dehmel | Member of the Executive Board responsible for security and trust
T +49 30 27576-223 | s.dehmel@bitkom.org

Graphics & Layout

Sabrina Flemming | Bitkom

Coverimage

© artjazz – fotolia.com

Table of Contents

Introduction

The extensive provisions of the General Data Protection Regulation (GDPR) cause small and medium-sized enterprises (SMEs) initial difficulties. »Where to start with implementing the new privacy rules?«, »which processes and procedures need to be set up within the company?« and »how does a GDPR compliant data management look like?« are only few of many puzzling questions.

Many of the GDPR's concepts and principles are more or less the same as under the current EU Data Protection Directive (Directive 95/46/EC) which has been implemented by the Federal Data Protection Act (so called »Bundesdatenschutzgesetz«[1] (BDSG)) in Germany. Those who already comply with the current law shouldn't be too worried. There is no need to start from scratch!

Nevertheless, it is essential to review your data protection practices and further develop them in line with GDPR requirements by 25 May 2018 at the latest. Note that there is no blue-print solution for starting the GDPR implementing process. Every company has a different business model which also includes different data processing activities. For example, the provision on health data will have more impact on m-health app developers than on others, whereas a cloud provider might me more concerned by the new liability regime for data processors.

These FAQs aim to help companies planning their approach towards GDPR compliance. It highlights the main changes and new features in EU data protection law. The advice mainly focuses on SMEs and provides them with a checklist to effectively trigger the right processes and procedures within the company.

1 For English version see here ↗ here

When does the GDPR enter into force?

The GDPR entered into force on 25 May 2016, twenty days after the publishing in the Official Journal of the European Union. However, the law will only **apply** after a **transition period** of two years. This means that from 25 May 2018 onwards all companies within the scope of the GDPR have to be compliant and are subject to enforcement by national data protection authorities (DPAs) and courts.

Note

This two-year transition period should be urgently used to review and where necessary adapt work flows, processes, contracts and arrangements within your company as DPAs can impose fines if the requirements of the GDPR have not or not sufficiently be fulfilled.

How does the GDPR apply in Germany?

The data protection rules for companies as laid down, for instance, in the BDSG will be largely replaced by the GDPR. Furthermore, as the GDPR is an EU regulation it will be directly applicable in all EU Member States and will not require any national implementing laws. National legislators will simply enact laws to annul their current data protection legislation. However, there are a number of so called **»opening clauses«** in the GDPR which provide Member States with discretion to introduce additional national provisions to concretize and further specify the application of the GDPR:

Example Employment Data: A classic example of such an opening clause is data processing in the context of employment. According to Art. 88 (1) GDPR Member States can provide for more specific rules to ensure the protection of rights and freedoms »in respect of the processing of employees«. This formulation does neither allow for stricter nor softer rules – it simply leaves room for concretization of the rather general GDPR provisions. No comprehensive use of this opening clause and introduction of a new law is expected in Germany due to the short time limits until the application of the GDPR. However, the German legislator will probably keep the existing rule of 32 BDSG.

Note

Collective agreements like a German employer/works council agreement (so called »Betriebsvereinbarung«) are still valid according to Art. 88 (1) GDPR. Though, it is recommended to review existing agreements and assess whether they are in line with GDPR requirements. Keep in mind that data protection in the employment context is mainly governed by various judgements of German labor courts (predominantly the »Bundesarbeitsgericht«(BAG)[2]) which still need to be taken into account.

2 English ↗ **website** of BAG

Example Children's Consent under 16: The GDPR gives special protection to children's personal data. If your organization collects information about children below 16 years you will need a parent's or guardian's consent in order to process data lawfully. Member States can lower the minimum age from 16 up to 13 years.

Note

If you are an EU-wide operating company you should check first which age limit is applicable in each Member State in which you are operating. Remember that consent needs to be verifiable and you bear the burden of proof. Therefore, you should start thinking soon about putting a system in place to verify individual's ages in practice and to gather guardian consent for the data processing activity.

Example German Data Protection Officer: The German government announced that it would use the opening clause in Art. 36 (4) GDPR to maintain the German BDSG-rule which requires every company with more than 9 employees to designate a DPO taking responsibility for data protection compliance. This German rule goes beyond the minimum standard in the GDPR.

Note

A SME (/start-up) with less than 9 employees should still assess whether it needs to designate a DPO according to Art. 37 (1) GDPR (see more at page 8).

Example Collective Redress: The German legislator has already used the opening clause in Art. 80 (2) GDPR by introducing a new law on collective action for enforcement of consumer data protection rights (so-called ↗ **»Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts«** of 24 of February 2016). This law allows a wide range of third party representatives (consumer associations, chambers, etc.) to seek judicial remedies against companies. Previously, consumer associations could already bring privacy cases against companies before court, however, only in the area of privacy notices (standard terms and conditions). The new law extends this competence to areas where personal data has been unlawfully processed for advertising, market and opinion research, commercial credit bureaus, profiling, address trading or for other »comparable commercial purposes« and many data subjects are affected. In other Member States, which have not enacted such law, consumer associations can only lodge a complaint on behalf of the data subject if they have received a mandate from him or her (compare Art. 80 (1) GDPR).

Note

Expect in future that consumer associations will equally bring claims for e.g. access of personal data, rectification and erasure or damages on behalf of data subjects.

Overall, the GDPR does not leave too much room for Member States to enact additional laws in areas which are important to companies since most opening clauses refer to »public interest grounds« such as public health, national security, etc. Germany plans to publish a law in early summer 2017 to fill in some of these gaps. As most provisions of the GDPR are regulated exhaustively, **companies should already start assessing and adapting their data protection practices**. You may find compliance difficult if you leave preparations to the last minute.

Which rules remain largely unchanged?

- The Regulation keeps the main data protection concepts and principles of the current EU Directive 95/46.

  Example: Data protection principles like »purpose limitation«, »data minimization« and »transparency« remain largely unchanged.

  Note

  Although the »general principles« of data processing have not changed, they will be implemented by stricter »specific provisions« e.g. the further processing of personal data according to Art. 6 (4) GDPR (purpose limitation), the new duty of data protection by design and default according to Art. 25 GDPR (data minimization) and additional information duties according to Art. 13 and 14 GDPR (transparency).

- Data processing of personal data is still **prohibited if not explicitly allowed** by a legal basis of either the GDPR or other specific legislation (e.g. *lex specialis* of German Telecommunications Act (TKG)[3] or German Telemedia Act (TMG)). The GDPR provides the same legal grounds (e.g. consent, contract, legitimate interest, etc.) as the current Data Protection Directive.

  Note

  Up and until now, probably not all companies had identified a specific legal basis for their personal data processing activities. However, under the GDPR you have to inform your customers e.g. in the privacy notice of the legal basis used for every data processing activity including the legitimate interests of your company or a third party if data processing is based on Art. 6 (1) point (f) GDPR (see additional information on privacy notices and information access requests). Therefore, identification and documentation of all different data processing activities become very important and have practical implications. In addition, it will help you to address requests from DPAs or data subjects more easily. Remember that different legal bases come with different data protection rights. For instance, consent can be withdrawn without justification at any time whereas the right to object can only be claimed subject to specific conditions. You should reflect on the appropriate legal basis already at the stage of data collection.

3 For English version see ↗ here

- Processing of sensitive data continues to be subject to specific requirements.

Note

If you process sensitive data (such as health data, biometric data, data on criminal offences, etc.) specific requirements of Art. 9 GDPR apply (see e.g. »explicit« consent).

- The usual legal bases for transfers of personal data to non-EU countries remain largely unchanged and have been even extended.

Example: The GDPR provides for the same legal bases for internationally operating companies as the Data Protection Directive (e.g. consent, standard contractual clauses, binding corporate rules (BCRs), etc.) and even some additional ones (certification, Codes of Conduct).

Note

You should always assess first whether the EU Commission has issued an adequacy decision for the non-EU country to which you want to transfer personal data. In absence of an adequacy decision you have to find a different legal basis (e.g. standard contractual clauses) for the data transfer and inform the data subject about such transfer in your privacy notice.

European companies can also transfer personal data to US companies (or subsidiaries) which officially comply with the data protection principles of the so-called ↗ »Privacy Shield«. This new instrument has been adopted in July 2016. The US Department of Commerce publishes on its website a list of companies which have successfully self-certified under the Privacy Shield.

Bitkom: More information about data transfers can be found in Bitkom's ↗ practical guidelines on data transfer (only available in German).

- At least in Germany most companies are expected to be obliged to designate a data protection officer.

Example: The GDPR requires your business to designate a DPO in only two cases – either if activities involve the regular and systematic monitoring of data subjects on a large scale (point (b)) or the core activities of your business is to process sensitive data such as health data on a large scale (point (c)). You should start assessing whether you need a DPO who takes responsibility for data protection compliance and carries out the processes and procedures mentioned in this document. However, since Germany will retain the corresponding BDSG-provision few changes to current practices are expected in this regard.

Note

If your company has less than 9 employees you should still assess whether your business activity falls within the two categories mentioned above and therefore requires a DPO despite the German employee threshold. The DPO can also be an external advisor (i.e. not part of the company's structure). Furthermore, a group of undertakings can now designate a single DPO provided that the person is easily accessible by each entity. However, the exact requirements for such a group DPO (e.g. with regard to language requirements) is not yet clear. The Art. 29 Working Party currently envisages publishing guidelines on this topic in 2016 (see page 20).

Which are the new elements and most important changes?

- The GDPR has an expanded territorial scope and also applies to non-EU companies which offer goods and services to EU citizens and process their data.

Example: A Turkish company offers goods in an online shop to EU citizens and processes their personal data. Keep in mind that the GDPR also applies to for-free-services like search engines or social networks.

Note

Even a temporary stay (residency) in the EU is sufficient which means that e.g. also tourists or foreign workers enjoy extensive data protection rights under the GDPR if their personal data is processed by companies based in Germany.

- There are some new legal definitions (Article 4).

Example:

- Comprehensive definition of data processing (Art. 4 Nr. 2) – No more threefold division (collection, processing, use)[4]
- Processor (Art. 4 Nr. 8) – no more limitation to processors within the European Economic Area
- Profiling (Art. 4 Nr. 4)
- Consent (Art. 4 Nr. 11)
- Special categories of personal data: There is e.g. a new definition of »biometric« and »genetic data« (Art. 4 Nr. 12, 13). Companies which work with e.g. facial recognition or fingerprint should not only consider these new definitions but also corresponding provisions in the GDPR.

Note

A comprehensive ↗ **overview on new definitions and changes** in comparison to the BDSG was published by the law firm Oppenhoff & Partner (only available in German)

4 Note: Each phase of »data processing« has been defined in the German BDSG (see §3 BDSG).

- The further processing of personal data for a purpose other than that for which the data have been collected is regulated differently than in the BDSG – Further processing is only allowed for compatible purposes. While already the EU Directive provided for similar rules, the former implementation in Germany differed in this regard.

  Example Further Processing: Although the principle of purpose limitation (see Art. 5 (1) (b)) remains unchanged – the wording and concept of the further processing provision in Art. 6 (4) GDPR has changed compared to the German rule in § 28 (2) BDSG. While the GDPR only permits further processing for **compatible purposes** (with some few public interest exceptions), the BDSG also allows further processing for incompatible purposes if the processing is necessary for the purposes of legitimate interests of the company except where such interest are overridden by fundamental rights and freedoms of the data subject (balancing of rights). Therefore, there is no experience with such compatibility test in Germany. It needs to be seen how narrow or wide purposes can be defined in the future to guarantee a minimum of flexibility for data processing by companies.

  Note

  A non-exhaustive list of criteria has been introduced in Art.6 (4) GDPR which should be used to assess whether a different purpose is compatible with the original purpose. The use of e.g. pseudonymization can positively affect the test of further processing of data.

- Requirements for informed and freely given consent have been gradually increased.

  Example: Consent requires to be a freely given, specific and informed e.g. ticking a box on an internet website or choosing technical settings for information society services like on social media. Pre-ticked boxes or inactivity does not fulfill such requirement according to Recital 32 GDPR. Note that if you process data for different purposes, consent needs to be given separately for each data processing activity. Otherwise, there is no free choice according to the GDPR.

  Note

  You bear the burden of proof and must be able to demonstrate that consent was given. Note that consent can also be given by electronic means. You should review your systems for seeking, obtaining and recording consent and ensure you have an effective audit trail.

- The requirements for withdrawal of consent by the individual have been lowered.

Example: A data subject shall be able to withdraw its consent easily at »any time« and »without justification«.

Note

You have to set up effective mechanisms which make withdrawing consent as easy as giving it. Therefore, you should take GDPR provisions into account when e.g. designing websites, apps or other digital services.

- No »take it or leave it« approach for consent (so called »Kopplungsverbot« i.e. prohibition of coupling in Germany).

Example: Art. 7 (4) GDPR read in combination with Recital 34 prohibits a company from making the performance of a contract conditional on consent to the processing of personal data that is not necessary for the performance of a contract (so-called »take it or leave it«). This rule goes far beyond the existing § 28 (3) point (b) BDSG which only applies in monopoly situations. In practice, this could mean that you have to offer your service both with and without consent.

- Extended obligations for information in privacy notices and information access requests.

Example: You have to provide data subjects certain information when processing their personal data which can be done e.g. through a privacy notice. New in the GDPR is e.g. the requirement to provide for legal basis for processing of data, the period for which the data will be stored or - if that is not possible – at least the criteria used to determine that period. Furthermore, prior to any further processing you have to inform the data subject (again) in case of purposes different from the ones the data had been collected for (see Art. 13 and 15 GDPR).

- New duty of data portability for data which the data subject has itself provided: Such data needs to be made portable in a »structured, commonly used and machine-readable format« and, if requested and »technically feasible«, even transmitted directly from one company to another.

Note

As of May 2018, you should be able to deal with requests from customers who want to receive personal data which they have provided to you e.g. when registering for your service. You have to provide this data in a »structured, commonly used and machine-readable format«. This might be difficult depending on your business model (e.g. social media, platforms or other digital services). Therefore, the so called »Art. 29 Working Party« (see more information below) will issue a guidance document on how to interpret this broad provision.

- Extended right to erasure (also new duty to inform third parties about data subject access requests).

Example: If your database is inaccurate and you have passed on this information to other parties, you have to inform these parties about this inaccuracy so they are also able to correct the data.

Note

You should always document which personal data you process, where it came from and who you share it with. Otherwise, it will be difficult to fulfill the requirements of the GDPR. Furthermore, you need to think about how to delete personal data and put procedures in place (e.g. who will make the decision about deletion? derivation of deletion periods?). In case of e.g. information access request by a data subject, it will help you to locate and delete the data more quickly.

- Extended right to object.

Example: The data subject can object to data processing, especially for direct marketing purposes, including profiling.

Note

The right to object needs to be presented »clearly and separately« from other information and needs to be brought to the attention e.g. by highlighting it in the privacy notices.

- »Joint controllers« where two or more controllers jointly determine the purposes and means of processing, have so far been unknown to the BDSG (although this concept was already addressed in the Data Protection Directive).

Example: According to Art. 4 (7) GDPR a company does not necessarily have to process personal data alone but multiple actors can interact in the processing of data and allocate roles and responsibilities. Nowadays, even SME's outsource professional services to other entities as they lack specific competence and capacity. The development of such expertise would also lead to disproportionate investments for the company. The participation of parties to the joint determination is not limited in numbers: Art. 26 GDPR refers to »two or more controllers« and thus sets no limit. However, it is necessary that the different parties determine with regard to the specific processing operations either the purposes or other essential elements of the means. The joint control must not lead to a restriction of data protection rights and participating parties have to clarify transparently the distribution of control (e.g. ensuring information, right of access, etc.). The concept of »joint controller« must be differentiated from a situation where a controller operates »alone« and the situation where a »processor processes data on behalf of the controller« (in Germany so called »Auftragsdatenverarbeitung« or under the GDPR just »Auftragsverarbeitung«).

Note

The Art. 29 Working Party has already published guidance on the concept of »joint controllers« in 2010 (see Art.29 Working Party, ↗ WP 169 v. 16 February 2010). This paper also explains the difference between a »single controller«, »joint controllership« and »data processing on behalf of a controller«.

Bitkom: Bitkom is currently working on an overview on this topic which also includes a more detailed explanation of the concept of »joint controllership«. This Paper will be published later this year.

- The legal relationship and duties between controllers and processors (see section above) have partly changed. Especially data processors have received more obligations under the GDPR such as new documentation duties and a direct liability towards the data subject in case of a data breach.

Example: According to Art. 82 (1) and (4) GDPR a data subject can claim damages not only from a »controller« as under the old Data Protection Directive but also directly from a »processor«. Thus, every party of a processing chain is fully liable towards the data subject which means that it has to compensate the entire damage even if not responsible for it. However, every party can claim back any paid compensation from other processing parties involved in the same processing (Art. 82 (5) GDPR) if it has not or only partly been responsible for the damage. Note that DPAs can also directly impose fines against data processors if they infringe GDPR requirements e.g. if a data processor works without a contract.

Bitkom: Not only liability but also documentation duties have been extended under the GDPR. Therefore, processors, too, have to maintain a record of processing activities (called »Verfahrensverzeichnis« under the BDSG) and make this record availably if requested by a DPA. Bitkom has provided ↗ guidance on how such records could look like (only available in German).

Note

Note that this guidance only refers to a »controller« and not a »processor« as the Data Protection Directive as well as the BDSG only obliges the former to keep such records. If you are a processor, you should start thinking about how to create a record of processing activities in line with GDPR requirements (see Art. 30 (2) GDPR). Bitkom is currently revising its guidance on documentation.

- The Regulation follows a stronger risk-based approach with regard to technical and organizational measures (see security of processing in Art. 32 GDPR), which makes documentation of risk analysis obligatory.

Note

To determine the appropriate technical and appropriate measures (TOMs) for each data processing activity (Art.32 GDPR), the company needs to take into account the likelihood and severity of the risk for the right and freedoms of data subjects. To proof that such comprehensive risk assessment has been conducted, the company should document its considerations or at least the final result. Furthermore, an efficient process should be integrated to carry out such risk analysis. Bitkom is currently working on a paper which gives more guidance.

- New duty to carry out and document a privacy impact assessment (PIA) for high risk situations. However, the general obligation to notify a DPA has been deleted (so called »Vorabkontrolle« in §4d (5) BDSG).

Example: A privacy impact assessment (PIA) should be based on an adequate risk assessment management (see information above). Should you in your risk analysis come to the conclusion that the specific data processing activity will result in a »high risk« to the rights and freedoms of the data subject, you have to conduct a PIA, especially if extensive data is used for profiling, a large scale use of sensitive personal data is processed or systematic monitoring of public areas. Note that a PIA is also required where a new technology is deployed. You should start developing a procedure on how to conduct a PIA, who will do it and which other stakeholders need to be involved.

Note

You have to contact the DPA prior to processing to seek its opinion (Art. 36 GDPR), if your PIA indicates that the specific processing activity would result in a high risk and you either do not or cannot take measures to mitigate the risk. Note that national DPAs can publish so called »black« and »white lists« with data processing activities which never or always require a PIA.

Bitkom: The Art. 29 Working Party has announced to publish guidance on this topic in 2016. Bitkom is currently working on a paper which makes suggestions on how to carry out a risk analysis and how to conduct a PIA based on the results.

- Extension of duty to report personal data breaches. A company must report every data breach to the DPA within 72h where there is a »risk« that the individual will suffer some form of damage (e.g. identity theft or fraud). In some cases you also have to notify the individuals whose data has been subject to the breach if the latter is likely to result in a »high risk« to their rights and freedoms.

  Example: So far, German companies have already been required to report unlawful access to data to DPAs if the breach concerned »sensitive« data (e.g. health or financial data) and there was a threat of serious harm to the data subject's rights (§ 42a BDSG).

Note

It is highly recommended to develop internal guidelines and put procedures in place to detect, report and investigate personal data breaches. A certain structure will guarantee that you fulfill your duty within the short time frame. There are some minimum requirements (see Art. 33 (3) GDPR) on the content of such report which should be taken into account. Furthermore, companies are obliged to document data breaches.

Note

In addition to BDSG-requirements, under the e-Privacy Directive (implementation through § 109a TKG) all »electronic communication services« are obliged to report data breaches to the Federal Network Agency (so called »Bundesnetzagentur«) and the Federal Data Protection Officer (so called »Bundesdatenschutzbeauftragter«). In the GDPR, a new instrument with similar, however not identical legal requirements on reporting data breaches, was introduced. The e-Privacy Directive is currently reviewed by the EU Commission which is expected to publish a proposal by the end of 2016. It is likely that respective provisions in the e-privacy Directive will be repealed as already covered by the GDPR and companies only have to follow one mechanism.

- The competent data protection authority is determined according to the »main establishment«. This is where your organization has its main administration or the legal entity where decisions about data processing are made.

  Example: The main establishment is determined according to where your organization has its main administration or where decisions about purposes and means of data processing are made. Especially large companies with complex structures, processing data in various countries (such as group of undertakings) should map out and review where main decisions of different data processing activities are taking place.

Note

A national DPA e.g. the Hesse DPA is still competent for investigating cases which only relate to an establishment on its territory or substantially affect German data subjects (»lead supervisory authority«). However, if the processing operation also affects people in other Member States such as Spain or France, those concerned DPAs can be involved in a complex »cooperation and consistency procedure« (often referred to as »One Stop Shop«). If no consensus is reached by the involved DPAs in such procedure, the newly established »European Data Protection Board« (EDBP) (see below) will issue a binding and final decision.

- The GDPR introduces significantly increased fines – up to 20 million Euro or 4 % of worldwide annual turnover per data breach.

Example: The German BDSG set a moderate cap of 300 000 EUR per data protection breach. The new fines of the GDPR can be much higher. Note that the GDPR refers to the worldwide annual turnover of the company of the preceding financial year. According to Recital 150 »company« shall be defined as in Article 101 and 102 TFEU. As those Articles are also used in competition law, some scholars have interpreted that the level of fines depends on the turnover of the »group of undertakings« and not only the responsibly entity (»controller«). However, the literal interpretation does allow for any conclusion. Note that DPAs can also impose fines for several data protection breaches which can go beyond the level of an individual data protection breach.

Note

Companies especially groups of undertakings should assess the risk of maximum fines on basis of their annual turnover and regard this outcome in their compliance risk management. Make sure all of your branches have an effective data protection management in place.

Note

It is likely that data protection breaches of companies, especially in case of cross-border activities, will be more easily detected by DPAs through the newly established cooperation procedure. In the past many legal proceedings of e.g. German DPAs had failed due to lack of jurisdiction which was only attributed to one authority in the EU.

Which processes and documents do I have to review?

- Documentation of data processing activities (especially with respect to the new duty of data processors, possibly additional documentation requirements with regard to risk analysis, risk assessment and privacy impact assessment (PIA))
- Privacy Notices (essential extension of information duties)
- Declarations of consent (stricter formal requirements) and consent mechanisms such as withdrawal of consent
- Review of employer/works council agreements (at least in Germany)
- Process to implement right to object
- Contracts between controller and processer (liability, documentation)
- Process to implement reporting of data protection breaches
- Process to enable data portability in commonly used and machine-readable format
- Performance of training courses for the provisions of the GDPR and changes in the company
- Implementation of effective risk management to identify and choose appropriate technical and organizational measures
- Implementation of privacy impact assessment (PIA)
- Monitoring of national legislative processes and training

Note

Through specific reference in the general principles, **the GDPR places accountability obligations on data controllers**. The new accountability principle requires the company to be able to demonstrate compliance by showing e.g. that it has put in place effective data protection policies and procedures. Therefore, you need to have an effective data protection management system which includes the above-mentioned processes like documentation on the basis of which you can proof compliance to DPAs. A lack of sufficient documentation on the GDPR implementation in your business can directly affect the level fines in case of non-compliance.

What are the costs and effort I should expect?

The cost and effort for companies will vary depending on how many data processing activities and contracts they have to assess and which relevance and effect respective GDPR provisions have on the processes and procedures of the company. Furthermore, it depends on how extensively and clearly your company has documented processes and implemented data protection management so far.

Some factors which could be taken into account when assessing expenditure of implementing GDPR within company:

- Number of data processing activities already documented in a record – number of data processing activities which have not been documented yet? Creation of new documentation record? How many departments need to be involved?
- Time to revise one (ore more) privacy statements and time to review X processes for which additional consent is needed
- Negotiation with works council for additions /change of works council agreement(s)
- Number of data processing contracts x time to review + (if necessary) time for renegotiation of contracts
- Revision of all current processes, involvement of all stakeholders
- Training of employees
- Principle of accountability causes considerable expenditure for documentation

Which company departments should be informed about the changes?

Not only the DPO but also other key decision makers in your company should be made aware of and informed about changes in the law:

- **Executive Management:** The Executive Management should be aware of changes in your data protection practices as implementing GDPR could have significant impact on the company's structure and resources.
- **Law and Compliance:** Many contracts probably need be adapted. Furthermore, you should inform your compliance department which needs to take data protection compliance in their risk analysis more serious as the level of fines for non-compliance has increased considerably.
- **IT-Security:** As regards the new mandatory »data protection risk assessment« for the employment of technical/organizational measures, it is recommendable to verify how these could be

aligned and complement »IT security risk assessments«, which are already conducted within the company.

- **Finance:** Restructuring and adaption of processes may cause considerable costs to your company which need to be taken into account by your finance department.

- **Research and Development:** Provisions like »data protection by design and default« impose requirements on, inter alia, product development and implementation. Therefore, data protection principles should be considered at an early stage in processes and procedures to guarantee an effective data protection management.

- **HR and Work Council:** In case of works council agreement on certain data protection practices in your company, consider the co-determination rights of the works council according to §87 (1) Nr.6 of the German Works Constitution Act (BetrVG). Furthermore, you should train your employees.

- **Resource implications**: Implementing the GDPR could have significant resource implications, especially for larger and more complex organizations. Remember when planning the implementation process of GDPR that your employees have to also fulfill their daily tasks.

Who provides guidance on interpretation?

- The **recitals of the GDPR** are to be read in connection with the respective articles and should be used for interpretation of the GDPR.

- **Art. 29 Working Party:** The Art.29 Working Party was set up under the EU Data Protection Directive. It has advisory status, acts independently and regularly publishes information on data protection (such as opinions, recommendations and reports) on their ↗ website. On 2 February 2016 the Art. 29 Data Working Party set out its first ↗ action plan for the implementation of the GDPR.

- One of the main tasks for EU data protection authorities will be to form the so called new **»European Data Protection Board (EDPB)«** which will in future have legal personality and replace the Art. 29 Working Party. The Board is composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor whose office will provide also for the secretariat. The Board will foster coordination and cooperation amongst data protection authorities (cooperation and consistency mechanism) e.g. through common enforcement action against companies which affect consumers from more than one Member States. Yet it is not clear who will represent Germany in the EDPB as it has not only one but 17 DPAs (each state + one federal).

- Furthermore, the Art. 29 Working Party will publish guidelines for companies. The first topics to be addressed are the following:
  - **Privacy Impact Assessment:** The GDPR obliges companies for the first time to make a privacy impact assessment (PIA). First approaches have been developed even before the adoption of the GDPR e.g. in ↗ France by the »Commission Nationale de l'Informatique et des Libertés« (CNIL) or in the ↗ UK by the »Information Commissioner's Office« (ICO). Furthermore, first concepts have been developed in international standardization (see ISO DIS 29134 Management Standard Privacy Impact Assessment). The Art. 29 Working Party will probably develop current approaches in line with GDPR requirements.
  - **Right on data portability:** The right to data portability, whereby the data subject not only has the right to »receive« the personal data concerning him or her in a structured, commonly used and machine-readable format but also the right to get the data transmitted directly from company to another, is new. This right was originally based on the idea to enable social network and other platform users to get their data from the platform when moving to another service. However, the final GDPR article has been defined so broadly that is unclear how the concept will apply to other web services. The Art. 29 Working Party will provide some clarity here.
  - **Certification:** Processors can get certifications for data processing activities by either an accreditation body or a DPA to proof that they have an effective data protection management in place.
  - **Data Protection Officer:** In contrast to Germany, most EU Member States have not obliged companies to designate a DPO. Therefore, the Art. 29 Working Party has probably prioritised this topic. Note that there is a strong expertise of DPOs in Germany. The GDPR only contains minor changes in this regard, thus German companies can build existing approaches.

  New priorities will be determined by the Art. 29 Working Party in 2017 and 2018.

- **European Data Protection Supervisor:** The European Data Protection Supervisor (EDPS) is an independent supervisory authority whose objective it is to ensure a harmonized and high data protection level within the EU. On its ↗ website the EDPS publishes – next to all kinds of privacy-related information – information on the GDPR. The EDPS has defined its role regarding the implementation of the GDPR in its ↗ strategy for 2015 – 2019: Firstly, the EDPS office will provide the Secretariat for the »European Data Protection Board (EDPB)« and will closely work together with EU data protection authorities (e.g. to develop guidance and training). Secondly, the EDPS will engage in the development of subsequent sector-specific legislation, and lastly develop a web-based repository of information on data protection as a resource for privacy stakeholders.

- **Data Protection Authorities in Germany:**
  - **Federal Commissioner for Data Protection and Freedom of Information:** The Federal German Commissioner has published a short guidance on the GDPR. You can find the so

called ↗ » BfDI Info 6 zur Datenschutz-Grundverordnung« on its website as well as a good overview »Datenschutz kompakt« ↗ here.

- **Düsseldorfer Kreis/Data Protection Conference:** The so called »Duesseldorfer Kreis« is an informal committee of the German Data Protection Authorities (also called Conference) for the private sector to arrange nationwide principal questions of data protection. The committee is named after its meeting place: Duesseldorf, a city in North Rhine-Westphalia. The State Commissioner on Data Protection of North Rhine-Westphalia is the chair of Duesseldorfer Kreis. You can find a complete listing of decisions of Duesseldorfer Kreis since 2006 on the website of the ↗ German Commissioner of Data Protection (BfDI). Here you will find a few ↗ central decisions.

- **Bavarian Data Protection Authority:** The Bavarian data protection authority published a series of short ↗ GDPR:
  - Video monitoring according to GDPR (06.07.2016)
  - Art. 42 GDPR – Certification (22.06.2016)
  - Art. 32 GDPR – Security of processing (10.6.2016)
  - Art. 17 GDRP – Right to erasure (»Right to be forgotten«) (19.7.2016)
  - Art. 30 GDPR – Directory of data processing activities (documentation) (2.8.2016)
  - Art. 9 GDPR –Special categories of personal data (17.08.2016)
  - Sanctions on GDPR (01.09.2016)

- **Data protection authorities of other countries:**
  - **United Kingdom:** The ICO will play an important role on the interpretation of data protection despite the Brexit. On its ↗ website the ICO has published an ↗ overview of its strategy for the **guidance** that it will be issuing regarding the **GDPR**, a ↗ 12-steps-checklist for companies as well as a general ↗ overview of the GDPR.
  - **France:** On 15 June the French DPA (CNIL) issued a ↗ guidance document on the GDPR which focuses on the main **challenges** that organization may face when **implementing the Regulation**. The guidance document focuses on data subjects rights, accountability, data transfers, and enforcement. Furthermore, on 16 June, the CNIL launched an ↗ online consultation regarding the interpretation and implementation of the GDPR. The consultation focuses on 4 areas: DPOs, Data portability, PIAs and Certification.
  - **Spain:** On 29 June, the Spanish data protection authority (**AEPD**) published a **recommendations** document on the implementation of the GDPR. The Recommendations focus on consent, information notice, data protection impact assessments, certification, data protection officers' certifications and relationship between controllers and processors. The DPA also announced that it is currently working on the **development of tools** which will help controllers understand and comply with the GDPR. You can find the recommendations ↗ here.

- **Denmark:** On 21 June, the Danish DPA (Datatilsynet) published a **Q&A document** on the GDPR. The Q&A document covers **12 questions** and is specifically targeted at data controllers covering the topics of data subject rights, consent, children's data, legal grounds for data processing and data breach notification. The Danish DPA is advising controller to use the Q&A document as a **checklist** for GDPR compliance. You can find the Q&A document ↗ here.
- **Finland:** On 2 June, the Finnish Ministry of Finance's State Administration of Information and Cyber Security Management Team (VAHTI) published a document aimed at **assisting organisations in their preparation for GDPR compliance**. The document provides recommendations for companies during the 2-year transition period. The Ministry of Justice also noted that it will set up a **Working Group** to investigate the necessary **amendments** needed to make sure that national legislation is in line with the GDPR. You can find the press release ↗ here and report ↗ here.

- **Bitkom Publications:**
  - **Data Processing on behalf of a controller:**
    Template for a data processing contract: ↗ »Mustervertragsanlage zur Auftragsdatenverarbeitung« (available in German and English). These practical guidelines and templates are currently adapted to the requirements of the GDPR.
  - **Documentation:**
    Practical Guidlines: ↗ »Das Verfahrensverzeichnis BDSG – Ein Praxisleitfaden (Version 3.0). Stand März 2016« (only available in German). These practical guidelines are currently adapted to the requirements of the GDPR.
  - **International data transfers:**
    - Practical guidelines: ↗ »Übermittlung personenbezogener Daten – Inland, EU-Länder, Drittländer« (only available in German). These practical guidelines are currently adapted to the requirements of the GDPR.
    - ↗ Safe-Harbor: Judgement of the CJEU and its consequences. FAQs (only available in German).

Bitkom represents more than 2,400 companies in the digital sector, including 1,600 direct members. With more than 700,000 employees, our members generate a domestic turnover of 140 billion Euros a year, exporting high-tech goods and services worth another 50 billion Euros. Comprising 1,000 small and medium-sized businesses as well as 300 start-ups and nearly all global players, Bitkom' members offer a wide range of software technologies, IT-services, and telecommunications or internet services. They produce hardware and consumer electronics or operate in the sectors of digital media and the network industry. 79 percent of the companies' headquarters are located in Germany with an additional amount of 9 percent in other countries of the EU and 9 percent in the USA as well as 4 percent in other regions. Bitkom supports an innovative economic policy by focussing the modernization of the education sector and a future-oriented network policy.

Federal Association for Information Technology, Telecommunications and New Media

Albrechtstraße 10
10117 Berlin | Germany
T 49 30 27576-0
F 49 30 27576-400
bitkom@bitkom.org
www.bitkom.org

bitkom