Your World First

February 2018 | 02

Compliance – Resolutions for 2018?

Employment Law – good to know …

Companies must comply with the European General Data Protection Regulation by 25 May 2018

The subject of data privacy protection is rapidly becoming a central compliance issue that companies can no longer afford to ignore: As of 25 May 2018, breaches of European data privacy protection rules will carry fines of up to EUR 20 million or 4 % of the group annual turnover, whichever is higher. By contrast, the maximum fine currently provided for under the German Federal Data Protection Act (*Bundesdatenschutzgesetz*) is only EUR 300,000. Despite this, many companies still shy away from addressing the new developments.

We will demonstrate below what resolutions for 2018 you can and should implement now to prepare for the upcoming changes.

New legislation to take effect on 25 May 2018, liability, burden of proof

The European General Data Protection Regulation (GDPR) will take effect directly on 25 May 2018 without national transposition legislation. It will take precedence over national law. There will be no transition period after 25 May 2018.

Germany's current data protection legislation – the German Federal Data Protection Act (*Bundesdatenschutzgesetz*, BDSG) – will be superseded by a new BDSG (BDSG-neu), which will take the GDPR into account and will take effect simultaneously on 25 May 2018. Among other things, the BDSG-neu contains new rules on the privacy of employees' data, which the GDPR has placed within the remit of national lawmakers.

The topography of the European data privacy protection landscape will remain largely unchanged, but a number of fundamentally new obligations will be added. These will be accompanied by an increase in the liability risk to companies including, but by no means limited to, drastically increased fines (Article 83 GDPR). In addition to state-imposed fines and civil-law compensation claims, the new legislation will also grant injured parties damages for pain and suffering caused by breaches of data privacy regulations (Article 82 GDPR). It is particularly important to be aware of the reversal in the burden of proof: The company will be exempt from liability only "if it proves that it is not in any way responsible for the event giving rise to the damage" (Article 82(3) GDPR).

All companies are affected

The new rules will apply to all companies doing business on the European market and will pose particular challenges to companies that in the past have not attached much priority to the protection of data privacy.

These late starters will now have to set up a completely new data privacy protection architecture by 25 May 2018, a process that will require considerable resources and months of preparation. It is essential that they act swiftly.

The German supervisory authorities have stated that while they will offer a certain amount of assistance, they "will not – where breaches are found – flinch from imposing effective and proportionate sanctions as a deterrent, as required by the General Data Protection Regulation" (Thomas Kranig, President of the Bavarian State Data Protection Authority, BayLDA).

Guidance

In the following you will find a few of the aspects that employers will have to consider in the future. These are based on the questionnaire, consisting of 50 questions, that the Bavarian State Data Protection Authority recently sent to selected companies to "convey a sense of how the Bavarian State Data Protection Authority (BayLDA) intends to organize its increasing supervisory activities". The questionnaire did not include answers.

Is data protection top priority?

The supervisory authorities rightly point out that all company decision-makers should be aware of the implications of the new rules and what they mean for day-to-day operations. The necessary procedures must be incorporated into the overall organizational structure and cannot simply be imposed from above in limited areas.

The legal responsibility for this lies with company management and not, for example, with the data protection officer. If the company management is not yet (sufficiently) aware of this, it must obtain information as soon as possible.

Directors and board members may be liable without limitation, even with their personal assets. Data privacy protection is thus clearly top priority in the sense that the top managers are responsible for it.

Is there a data protection officer?

According to Article 37(1) GDPR, a company must designate a data protection officer where the company's core activities consist of data-processing operations requiring regular monitoring of individuals or where the core activity involves the processing of sensitive data. There is no minimum number of employees for this rule to apply. The data protection officer's contact details must be published and communicated to the supervisory authority (Article 37(7) GDPR).

The provisions of the BDSG-neu go further than the GDPR, however. In Germany, a data protection officer must be designated where a company usually employs at least ten people for ongoing automated processing of personal data.

Example: The human resources department employs five HR managers who save HR files on the server. Six sales employees work with electronic customer databases.

In Germany, an employee who becomes a data protection officer – if required by law – enjoys special protection against dismissal, similarly to a works council member.

Under the GDPR, the data protection officer's scope of responsibility has been expanded to include monitoring compliance with the data protection rules (Article 39(1)(b) GDPR). The new monitor obligation has caused the question to be raised by legal scholars as to whether this establishes a guarantor's obligation and an independent liability, like in the case of a compliance officer. Some supervisory authorities take the (non-binding) view that this is not the case.

Can we be sure that all processes related to personal data processing are legal?

In practice, this is often a difficult question to answer, particularly the first time it crops up. There is no generally applicable legal basis that covers all processes pertaining to an employment relationship. Each case must be judged on its own merits, the main criterion being the purpose for which data processing takes place.

- The basic system has not changed

The fundamental principle remains: The processing of personal data requires a legal basis; otherwise it is illegal (so-called prohibition with reservation of consent). "Personal data" means any information relating to an identified or identifiable natural person (Article 4(1) GDPR).

Examples: Name, date of birth, gender, marital status, address, account number, days off sick, religion, training, qualification, photograph, email address, IP address, current residence.

The term processing is similarly broad. It includes "collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." (Article 4(2) GDPR). In the context of employment, because of the special German

rule, also data available on paper are covered (§ 26(7) BDSG-neu).

Examples: Saving master data (name, address, date of birth, etc.), viewing personnel files, retrieving information through HR software, Google research on applicants, employee appraisals, use of performance data for determining bonuses, publishing contact data on company website, removing disciplinary warnings, selection of redundancy candidates based on social criteria, management of staff reintegration, recording time worked, video records, gate controls, GPS location, use of computers with personalized access.

The rules do not apply to anonymous information, thus information that does not refer to an identified or identifiable natural person. The same applies to personal data that has been rendered anonymous in such a way that the data subjects cannot or can no longer be identified (Recital 26 GDPR). This definition has become very narrow: Under current law (§ 3 No 6 BDSG), data is sufficiently anonymous if it can be correlated to an individual "only with disproportionate effort in terms of time, cost and labor."

- General data privacy protection principles under employment law

In an employment context, a justification pursuant to § 26 BDSG-neu (currently: § 32 BDSG) based on a works agreement, consent or generally under Article 6 GDPR is possible. Special rules apply where data is to be sent outside the company, such as to the parent company and/or outside the European Union.

– Employee data may be processed only where necessary to establish, operate or terminate the employment relationship. Ultimately, the employer's interest in data processing must be weighed up against the employee's privacy rights (principle of proportionality).

  Example: If the company advertises a vacancy, the HR department may save the applicants' contact data in order to send a rejection or invitation to an interview. However, it may not make such data available to the communications department so that it can send advertising to the applicant.

  The revised German legislation will continue the currently applicable § 32 BDSG including any related case law. The explanatory memorandum provides for a reservation for other areas to be covered by other statutory instruments (e.g. prohibiting secret monitoring, use of biometric data for authentication and authorization purposes), but any new rules should concern only principles that have already been incorporated into law through case law. In other words, rulings of the Federal Labor Court are still relevant.

– Collective agreements such as collective bargaining agreements and works agreements may form a legal basis for processing employees' personal data. This is consistent with rulings rendered by the Federal Labor Court and is now expressly governed by § 26(4) BDSG-neu.

  Example: The company wishes to introduce software containing a module for staff development. If the employer and the works council enter into a works agreement to this effect, the works agreement can, assuming it is appropriately worded, become the legal basis for processing employee data.

  German lawmakers did not introduce specific requirements for collective agreements, but merely referred to Article 88(2) GDPR. Works agreements must thus reflect the – loosely defined – GDPR provisions, which include, in particular, transparency and proportionality.

  Example: The works agreement does not clearly define the purpose of the data and their intended use. The works agreement is not a suitable legal basis for data processing.

  As of 25 May 2018, the requirements will apply to both new and old works agreements. There will be no transition periods. Companies will therefore be well advised to take a closer look at existing works agreements and take the new requirements into account in any current negotiations.

– Consent can still form the basis for data processing, but only if given voluntarily for a specific purpose and if given on the basis of an

informed decision. As before, it will thus still be unlawful for blanket consent to be given for any conceivable scenario. It must be possible to prove the validity of any consent that has been given (Article 7(1) GDPR).

Whereas the GDPR does not require such consent to be given in any specific form, consent pursuant to § 26(2) BDSG-new must generally be provided in writing. Moreover, employees must be informed in text form (e.g. by email) of the purpose of the data processing and of their right to revoke their consent.

What is new is that voluntary consent can, in principle, be given within the employment relationship. The Act provides examples of what is meant by "voluntary": for example, if the employee is granted a financial advantage, such as permission to use IT for private purposes.

Example: The company allows employees to use the internet for private purposes. After having been provided with detailed information, the employees consent to certain data (time of use, websites visited, etc.) being collected for certain purposes (data security, avoiding criminal offenses).

However, as in the past, caution must be exercised with regard to consent in an employment context. Consent may be revoked at any time with future effect.

Example: An employee revokes previously given consent to process her personal data in the context of a new software solution on personality analysis. The company needs an alternative legal basis in order to continue processing such data.

The supervisory authorities currently take the view that where consent was validly given in the past, it will continue to apply provided that it was given validly in the legal situation prevailing at the time and voluntarily (according to the GDPR) and that the consenting person was at least 16 years old (Düsseldorf working group decision of 13/14 September 2016). For many companies, however, this is no reason to lean back and relax: many declarations of consent are invalid under the current law (for example, as a blanket provision in an employment contract). Companies should thus make sure, if possible, that there is an additional legal basis for the data processing.

A justification may also fall within the general rule of Article 6(1) GDPR, for example, to satisfy a legal obligation or if data processing is necessary to safeguard the legitimate interests of the company/a third party and such interests prevail over the interests or basic rights and liberties of the data subject.

Example: Transfer of employee data to the buyer where a company is to be sold before the change in employer.

– Despite corporate and economic links, group companies are treated as unrelated entities under data privacy protection law. In other words, a subsidiary may pass data on an employee to the parent company only if one of the aforementioned legal bases (works agreement, consent, Article 6 GDPR) apply or if there is a data-processing contract, on which Article 28 GDPR imposes strict requirements.

  However, groups do enjoy a "minor group privilege:" according to Recital 48 to the GDPR, data processing for internal administrative purposes is acknowledged as a legitimate interest, so the weighing up of interests will often favor the group company.

– The transmission of data outside the European Union is subject to additional criteria on top of the basic processing consent (legal instrument, works agreement, consent) (Article 44ff. GDPR).

  It is fairly straightforward to transmit data to a non-EU country that the European Commission has certified as granting adequate protection. Because the certification decisions continue to apply, Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay can still be regarded as "safe third countries for data protection purposes."

  Example: The group headquarters is in Canada. The German subsidiary has granted it remote access to certain (non-sensitive) employee data. Transmission to

Canada, which is a "safe third country", is unproblematic (first review level). However, like for data transmission within Germany, it is still necessary to review whether processing (provision) as such is justified (second review level), for example, under Article 6(1)(f) GDPR as read with Recital 48, if, for example, the purpose is to set up a group-wide skill database.

The Commission has found that the EU-US Privacy Shield ensures an adequate level of data privacy protection, which has provoked sharp criticism.

Data may also be transmitted where the parties have entered into a binding agreement incorporating EU Standard Contractual Clauses, which also continue to apply (Article 46(5) sentence 2 GDPR). Data may be transmitted without consent if the clauses continue to apply unchanged. Data may also be transmitted subject to binding internal data privacy protection rules (Binding Corporate Rules), codes of conduct, certification and individually negotiated clauses, provided that such rules have received the prior consent of the supervisory authority.

Another possibility is for the data subject to consent to data transmission to a non-EU country. Finally, data transmission may be lawful in special cases, which are generally subject to strict interpretation, such as when the transmission is necessary to perform the contract or to pursue claims.

It is important that to note that a change in the reason for the data processing may require a different legal basis. Data processing must be compatible with the original purpose (Article 5(1)(b) GDPR).

Are processing activities of a company known and will they be documented/can they be documented at short notice?

According to Article 30 GDPR, a record similar to the previous (internal) record must be kept of processing activities. The record must include:

- 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 (in third countries),
- any data transmission to a third country,
- where possible, the envisaged time limits for erasure of the different categories of data and
- where possible, a general description of the technical and organizational security measures (referred to in Article 32(1) GDPR).

The supervisory authorities have announced that they will provide suitable templates.

Exemptions apply to companies with fewer than 250 employees, which do not have to keep a record unless the processing:

- entails a risk to the rights and liberties of data subjects,
- is not merely occasional or
- concerns particularly sensitive data (e.g. health, origin, union membership).

In practice, this exemption is unlikely to be significant. The national supervisory authorities take the view that regular processing of employee data must be regarded as "not merely occasional."

The record, which has to be submitted to the supervisory authority at its request, is only one element for satisfying the duty of accountability: Anyone who processes data must demonstrate compliance with the strict principles relating to processing of personal data as set out in Article 5(1) GDPR.

The supervisory authorities rightly point out that the record will play an important role: only by having a detailed knowledge of one's own data processing activities is it possible to take targeted action to ensure that the processing of personal data complies with legal requirements. Therefore, companies who do not currently have a record are strongly advised to produce one by 25 May 2018 or – if they do have a record – to revise it.

Is it known how and when a data protection impact assessment has to be carried out?

Article 35 GDPR requires a data protection impact assessment where a type of processing – especially where new technologies are used – is likely to result in a high risk to the rights and freedoms of natural persons, in which case the processes, purposes and legitimate interests must be described. The necessity and proportionality of processing, risks to data subjects and planned protective measures including demonstration of efficacy must be described.

It does not clearly defined what is meant by "high risk" for rights and freedoms of natural persons. Article 35(3) GDPR mentions special categories of data, including the systematic and extensive evaluation of personal aspects relating to natural persons based on automated processing that form the basis for a specific decision.

Examples: Collectable data can be profiling, assessment processes, promotion lists, skill databases, big data applications (which are not confined to aggregated data).

It is intended that supervisory authorities will compile positive/negative lists of when a data privacy protection impact assessment is or is not necessary (Article 35(4), (5) GDPR). Such lists do not exist to date, but the Article 29 Data Protection Working Party has drawn up a set of guidelines (WP 248) containing a preliminary list of criteria. These require a company to carry out a data protection impact assessment before monitoring the activities of employees and the workplace.

The supervisory authority must be consulted if the data protection impact assessment indicates that the planned processing is likely to result in a high risk in the absence of measures to mitigate the risk (Article 36(1) GDPR).

Under the revised law, the responsibility to carry out an assessment lies with the data controller (company); it is only necessary to seek the advice of a designated data protection officer (Article 35(2) GDPR).

Can the stricter requirements regarding the obligation to inform data subjects be met in time?

The company must inform the data subjects (applicants, employees, temporary employees, apprentices, etc.) about the processing of their personal data. Where data is collected directly from the data subjects, information is provided immediately (Article 13(1) GDPR), for example, when the employment contract is signed. If the data is collected from third parties, the data subject must be informed within one month (Article 14(3)(a) GDPR).

The company's duty to provide information on data processing essentially includes the details included in the record of processing activities, particularly the purpose of the processing and the categories of data recipients. It may therefore be advisable for companies with fewer than 250 employees to keep such a record.

Data subjects must also be informed of the legal basis for the data processing (Article 13(1)(c) GDPR). If the data is to be sent to a non-EU state, this must also be stated. Companies must thus make disclosures on European Commission decisions regarding adequacy (e.g. EU-US Privacy Shield) and/or the guarantees (e.g. conclusion of EU standard contractual clauses, Binding Corporate Rules). In the latter case, the data subject must be given an opportunity to obtain or read the guarantees. This shows once again that companies that have not clarified their data flow and legal basis will not be able to comply with statutory obligations. Data subjects must also be informed how long the personal data will be stored or at least of the criteria used to determine that period. This is based on the principle that personal data must be deleted as soon as there is no further need for them to be kept to fulfil the purpose. Each case must be judged on its own merits. Some data, such as data relating to unsuccessful job applicants in light of the short period during which objections may be raised, will no longer be needed after only a few months (§ 15(4) German General Act on Equal Treatment (AGG)). Other data may still be relevant for years, for example, two years for proof of hours worked (§ 16(2) German Working Hours Act (ArbZG)) and at least five years for social security insurance records (§ 28f(1) as read with § 28p German Social Code IV (SGB IV)).

Moreover, the controller must also provide data subjects with information on their right to information, correction and deletion and to lodge a complaint with the supervisory authorities and their right to revoke consent. They must also receive information on whether the provision of personal data is a statutory or contractual requirement or is a prerequisite for entering into a contract, whether the data subject is obligated to provide the personal data and the possible consequences of not doing so.

The extensive information duties will probably mean, among other things, that in future a "package insert" will have be provided with employment contracts.

Will you be able to report any data protection breach to the supervisory authority within 72 hours?

Section 42a BDSG currently provides for the obligation to report the loss of certain sensitive personal data (including bank or credit card accounts) in some circumstances to the supervisory authority and, where applicable, to the data subject or even to place notices in daily newspapers. Breaches of these obligation may carry a fine.

Example: An employee inadvertently sends an email with an unencrypted Excel spreadsheet containing employees' account data to an unknown third party.

Under the new Articles 33, 34 GDPR, the sanctions will be much more severe – a fine of up to EUR 20 million or 4 % of global turnover. A breach must generally be reported to the competent supervisory authority within 74 hours of discovery. This obligation applies to all "personal data" irrespective of the quality of the data. An exception applies only if the breach of the obligation to protect the privacy of personal data is unlikely to result in a risk to the rights and freedoms of natural persons. However, the risk does not have to be "significant," so the breach may have to be reported even if the data in question was encrypted.

Example: The HR manager loses a memory stick with sensitive employee data. The data is encrypted, but the encryption technology is out of date.

Companies are strongly advised to ensure they have procedures in place to prevent data losses where possible. The main problem is that data breaches frequently occur without the company's knowledge. Company policies/works agreements, etc., should therefore always require data to be sent in an encrypted form and include duties to report breaches. Staff should be trained and made aware of the issues.

Keep calm and act!

It is undisputed that the new rules will require greater effort on the part of companies. The first step is to establish at an early stage what needs to be done. The next step – implementation – must then be taken: The financial consequences of simply ignoring the new regulations could be dramatic. Clearly defined rules on responsibility and procedures and the awareness of data privacy protection risks can help to avoid fines and civil-law liability claims.

Data controllers are therefore strongly advised to act now – in collaboration with external experts – and do whatever needs to be done to ensure the compliance with the General Data Protection Regulation within the company. Then, and only then, will they be prepared for the deadline on 25 May 2018.

Please do not hesitate to contact us at any time if you have any questions regarding the European General Data Protection Regulation.

Kind regards

CMS Germany
Employment & Pensions Practice Area Group

C/M/S/ Law-Now™

Law.Tax

Your free online legal information service.

A subscription service for legal articles
on a variety of topics delivered by email.
cms-lawnow.com

C/M/S/ e-guides

Law.Tax

Your expert legal publications online.

In-depth international legal research
and insights that can be personalised.
eguides.cmslegal.com

---

cms.law