Appropriate modernisation of European data protection

Position on the draft European regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("general data protection regulation"

15. Mai 2012

Summary

- It must be possible to use **collective agreements** such as sectoral and company-level agreements as a basis for data processing.
- The blanket exclusion of **consent** for data processing in certain specific cases is unacceptable. For instance, it should continue to be possible to give consent in the employment relationship.
- It must continue to be possible to process the **health data** of a worker on the basis of legal certainty.
- The proposal for a regulation specifies extensive **information and notification requirements** which can lead to considerable burdens. For this reason, changes are necessary at various points.
- So far the chance has been missed to create a provision on **intra-group data transfer**. This gap must be closed.
- Disproportionate effort in relation to **order data processing** can be avoided by allowing the contractor to supply confirmation of compliance with the data protection regulation.
- The extensive **documentation obligations** would result in a considerable portion of working time in a company being spent on this aspect. This is untenable against the background of both economic and practical considerations.
- In order to enable the supervisory authority to concentrate on essential cases in the area of **data security**, it would be a good idea if infringements had to be notified only where they have serious consequences for the person concerned.
- A **data protection impact assessment** without any exceptions is superfluous and only generates new and unnecessary bureaucratic procedures.
- Introduction of a false form of **collective redress** will fail to do adequate justice to the different legal traditions in Europe. A class action leads to friction with the established principle of individual legal protection in continental Europe.
- When setting the level of a **fine**, the European Commission completely loses sight of the principle of proportionality. In

BDA is the leading social policy organisation of the German business community. It represents the interests of small, medium-sized and large companies from all sectors on all issues relating to social and pay policy, labour law, labour market policy and education. BDA works at national, European and international level for the interests of one million businesses, which together employ twenty million workers and which are linked to BDA through their voluntary membership of employer federations. These employer federations are in turn organised in the fifty-two national sectoral organisations and fourteen regional associations which are BDA's direct members.

EU-Transparenzregisternr. 7749519702-29

addition, no differentiation is made to reflect the motivation and intention underlying an infringement of data protection.

- If the European Union decides that it wants to regulate data protection in a regulation, worker data protection should also form part of this regulation. Only if it proves impossible to cover collective agreements under regulated by labour law, consent and other elements in a uniform way in the regulation will there need to be an **opening clause** for labour law. This must take account of the specificities of labour law in such a way that it continues to provide possibilities for the national legislator and parties to an employment relationship to act.

Introduction

On 25 January 2012 the European Commission presented a proposal for a regulation on data protection. With the proposal for protection of individuals with regard to the processing of data and the free movement of such data, the European Commission seeks to create a new legal framework for protecting personal data in the EU.

Many voices in the literature have rightly highlighted the Union's missing competence to legislate in this area. Article 16 paragraph 2 and article 114 paragraph 1 TFEU do not provide a sufficient basis for such a far-reaching regulatory approach. Even if a uniform framework for data flows within the Union is desirable, statutory rules to this end should not be adopted without legislative competence. This legislative competence does not exist.

BDA urges that the following points in particular should be implemented in a new concept of protection of personal data:

- It must possible to grant consent in the employment relationship.
- It must be possible to use collective agreements such as collective and company-level agreements as a basis for data processing.
- Arrangements must be put in place to facilitate intra-group data transfer.
- Bureaucratic burdens must be kept to a minimum.
- The sanction mechanisms must be scaled back to an appropriate level for data processing in employment relationships.

In light of the large number of so-called "delegated acts", a conclusive assessment of the draft regulation is not possible at this point in time. The regulation provides for "delegated acts" at twenty-six points. This means that the European Commission gives itself the power to adopt legislative acts intended to give concrete form to certain provisions of the regulation. Such wide-ranging application of this instrument is questionable. It must be dubious that the delegated acts genuinely relate to non-essential provisions as stipulated in the Lisbon treaty.

Detailed comments

Article 3 – Territorial scope

Regulatory content: In addition to data processing within the EU, the new rules would also apply for data processors outside the EU if they process personal data of individuals resident in the EU. Furthermore, the data processing must relate to the offering of goods or services in the EU or serve for the monitoring of behaviour.

Assessment: Extension of the scope of European data protection legislation to firms in non-EU countries which offer their services to EU citizens is welcome. Internet-based business models in particular do not require a registered office in the EU in order to be active here. Hence, extension of the scope will create a level playing field. However, it should be clarified in this connection how the term “residing” in article 3 paragraph 2 is to be understood.

Article 5 (a) – Principles relating to personal data processing

Regulatory content: Personal data must be processed in a manner that is transparent for the data subject.

Assessment: It is not specified more closely how processing is to be rendered “transparent”. In order to create legal certainty, this provision needs to be expanded to make it clear that transparency must be geared to objective criteria. Otherwise there could be a danger that data processing would have to be adjusted to reflect the receptiveness horizon of each data subject, something that would be unworkable in practice.

Article 6 paragraph 1 (b) and (c) – sectoral agreements, company-level agreements

Regulatory content: Article 6 paragraph 1 (b) and (c) of the draft regulation provides that processing of personal data must be possible in performance of a contract or a legal obligation.

Assessment: This fails to take adequate account of national specificities. For instance, it is the case in Germany that that collective agreements such as sectoral and company-level agreements rank equally with legislation enacted by the state and hence can provide the basis for legal data processing. Collective agreements guarantee a balanced level of data protection. In this regard, the company-level agreement serves primarily to give concrete form to unspecified legal concepts in data protection legislation for companies and their employees, and to organise legally certain procedures. For this reason, such rules meet the objective of practical data protection much better and more sustainably than statutory requirements. Hence, it must be ensured that collective agreements such as sectoral and company-level agreements can also be a legal basis for data processing.

Article 7 paragraph 4 – Consent

Regulatory content: According to article 7 paragraph 4, consent may not be a sufficient basis for data processing if there is a considerable imbalance between the position of the data subject and the controller. According to the recitals, this would be the case specifically in an employment context so that consent could no longer be advanced as a legal basis for data processing here.

Assessment: The blanket exclusion of consent to data processing in an employment context is unacceptable. It should continue to be possible to give consent in an employment relationship. Otherwise the employee would be completely deprived of the possibility to decide for himself on the use of his data. Consent is usually given in the employment context in areas where it is specifically in the interest of the employee in question to allow processing and use of his personal data. So that this possibility is not ruled out also in the future, it should at least be clarified in which individual areas of an employment relationship consent continues to be possible. In any event, consent should be irreplaceable for data processing operations linked to voluntary services provided by the employer such as childcare or catering facilities.

Article 9 – Special categories of data

Regulatory content: According to article 9 paragraph 2 (h) in conjunction with article 81, processing of health data is possible if it is done for the purpose of preventive health care or occupational safety and health. Article 9 paragraph 2 (j) provides that data on criminal convictions may be processed only under certain conditions.

Assessment: It must be ensured that health data relating to an employee can still be processed. Yet the current wording leads to legal uncertainty in practice. A clarification is needed to the effect that the cases for possible data processing enumerated in article 9 paragraph 2 apply as an alternative to special categories of personal data. Otherwise there would be a danger of illegal conduct, for instance if the employer stores details of health-related absences in personnel data systems for the purpose of calculating remuneration, since health data within the meaning of article 4 paragraph 12 may be processed only for the purpose of preventive health care in accordance with article 9 paragraph 2 (h) in conjunction with article 81 et al. As special categories of personal data, health data already enjoy sufficient protection which ought not to be extended.

For many companies, it is essential to collect data on criminal convictions, for instance in order to meet compliance requirements or in the framework of application procedures. It would be desirable to have a provision which allows processing of such data for these purposes.

Articles 12, 14, 15 and 18 – Information and communication obligations

Regulatory content: The draft regulation lays down extensive information and communication obligations on the controller fest. According to article 12 paragraph 1, it should be possible apply measures for informing the data subject electronically if personal data are processed automatically. Information in accordance with paragraph 2 must also be possible electronically. According to article 18 paragraph 1, the data subject should have the right to obtain a copy of the processed data in an electronic and structured format structured which is commonly used. The electronic form can be specified by the European Commission.

Assessment: It is clear from the information and communication requirements that the European Commission has in its sights primarily companies whose main business object is the collection of personal data, along the lines of a “lex facebook”. However, the bureaucratic obligations are completely unsuited for data processing in an employment context, in particular in the case of small and medium-sized enterprises.

The provisions in article 12 of the draft regulation can lead to a considerable burden for small and medium-sized enterprises in particular if appropriate electronic precautions have to be taken so that procedures can be processed electronically. The introduction of an electronic form is superfluous especially in smaller businesses with daily direct contact between the data controller and the data subject. Neither does the reference to standard forms and standard procedures make things much easier. Whether and, if so, how the European Commission is to make use of the possibility to incorporate simplifications for micro, small and medium-sized enterprises is not clear at the present time.

The extension of information and communication rights set out in articles 14 and 15 as compared with the provisions of the data protection directive are questionable. Additional obligations are placed on the data controller which will burden him considerably. Thus, it is provided

in article 14 paragraph 1 (c) and article 15 paragraph 1 (d), for instance, that the data controller must notify the subject whose data are stored. The storage period for these data varies sharply in the employment context. Communication is possible only with a considerable bureaucratic effort. At a time when red tape is being cut and is not supposed to be replaced, such a requirement is counterproductive. This is all the more the case because article 15 places no time limit on the data subject's right to information. In order to enable work in a cooperative atmosphere, this right should be restricted to one exchange of information per calendar year.
Also bureaucratic is the obligation set out in article 14 paragraph 3 to communicate the source of personal data which is not collected from the data subject himself. This information obligation is not included in directive 95/46/EC. It will generate a considerable amount of extra work, not least because this information is not limited to available information as it is in article 15 paragraph 1 (g).

The removal of the information obligation provided for in article 5 (a) where the data subject already has the information set out in article 14 paragraphs 1 to 3 is too narrow. In practice, this means that information will have to be provided much more often than provided for in § 33 paragraph 2 BDSG, without any perceptible objective justification. This provision of the German data protection law has proved adequate. Hence, the information obligation in article 14 should not come into play if the data subject has been made aware of the storage or communication of personal data.

The right to data portability contained in article 18 is not necessary to protect the data subject's right of personality. It is useful for the data subject to be able to read and, if necessary, comment on stored data. A uniform format does not offer the data subject any added value.

Article 20 – Profiling

Regulatory content: A natural person may not be subject to a measure based on purely automated data processing. This is the case if the measure can have a legal effect or materially harm the data subject's legitimate interests, and is applied for specific purposes. Provision is made for exceptions.

Assessment: This provision may be of significance for automated selection procedures in which, for instance, minimum grades are recorded. Under article 20 paragraph 2 (a), a person may then be subject to a measure if at the same time precautions such as a right to direct personal contact are taken in order to safeguard the data subject's legitimate interests. Such a right is very wide-ranging and would pose considerable challenges for companies where there are large numbers of applications. In practice, it has proved completely adequate for the person to be able to put his point of view – as provided for in article 15 paragraph 2 (a) of data protection directive 95/46/EC.

Article 23 – Data protection by design and by default

Regulatory content: Having regard for the state of the art, the data controller deploys procedures as well as technical and organisational measures such as to meet processing needs as well as to meet the requirements of the regulation.

Assessment: The use of technical and organisational procedures and measures should be more strongly aligned on a risk-oriented approach. The processing of special categories of personal data justifies higher requirements than the processing of simple address data.

Article 26 – Contract processors

Regulatory content: Article 26 of the draft directive sets out what arrangements have to be made before the data controller can subcontract processing to another person. The controller must ensure compliance with safeguard measures.

Assessment: The proposal provides that the controller must ensure that the contract processor complies with safeguard measures. But it leaves him in the dark as to when this obligation is deemed to have been met. This can be achieved only with disproportionate effort, especially for smaller businesses. The latter make frequent use of contract data processors, e.g. by subcontracting wage administration to a third party. To this end, they need legal certainty. For that reason, it should be sufficient if the organisation which subcontracts data processing to meet its requirements under the regulation if the subcontractor provides a confirmation of compliance with the data protection regulation. The workload generated by constant checks can be avoided in a non-bureaucratic way through such a confirmation. Article 26 must not lead to legal implementation problems similar to those experienced with § 11 BDSG, the equivalent German provision that is currently in force. Article 26 paragraph 1 second half of the sentence should therefore be deleted.

Article 28 – Documentation

Regulatory content: Data controller, contract processor and representative must meet extensive documentation obligations.

Assessment: Whereas hitherto such extensive obligations have been included only in the framework of the notification obligation of article 19 of data protection directive 95/46/EC and/or Article 4e BDSG, and can cease to apply under certain conditions, the documentation obligation now envisaged would apply more generally. Exceptions for companies are foreseen only if the company has fewer than 250 employees and data processing is an ancillary activity. The result of this is that wide-ranging documentation would have to be introduced in many cases. In companies where dealing with personal data is a day-to-day activity, these documentation obligations would lead to a large portion of working time being spent on documentation. This is untenable against the background of both economic and practical considerations. The creation rather than reduction of bureaucracy at this point is highly questionable.

Articles 31 and 32 – Data security

Regulatory content: With regard to infringement of the protection of personal data, the draft sets out strict rules. For instance, where feasible the supervisory authority has to be notified within twenty-four hours of the breach coming to light. Furthermore, a likely detriment to the privacy or of data protection by the breach would have to be notified to the data subject.

Assessment: The European Commission has here disregarded the fact that not every breach has serious implications for the data subject. To allow the supervisory authority to concentrate on important cases, it would be a good idea if only such breaches need to be notified which have entail a serious detriment to the data subject. Moreover, not every breach of the protection of personal data justifies strict legal consequences. The German law concentrates on those cases where particular types of personal data are involved, data linked to professional confidentiality, data linked to criminal acts or public order offences as well as data linked to bank or credit card accounts.

In addition, this twenty-four hour deadline creates a straitjacket. The term “without

undue delay" is sufficient. This leaves leeway to take account of each individual case.

It is also important to bear in mind that the obligation to notify the data subject is beset with uncertainties. Thus notification to the supervisory authority should be accompanied by notification of the data subject himself "when the data breach is likely to adversely affect the protection of the data or privacy of the data subject". The introduction of the ill-defined legal concept of "likely" leads to legal uncertainty. In addition, the formulation of the above quotation as a whole is ambiguous.

Moreover, it must be ensured that a notification by the data controller to the supervisory authority can only be used in any subsequent sanction procedure with the data controller's consent, in application of the ban on self-incrimination.

Articles 33 and 34 – Data protection impact assessment

Regulatory content: In the case of processing operations which present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, article 33 stipulates that the data controller must first carry out an impact assessment. This is submitted to the supervisory authority in accordance with article 34 paragraph 6. If the processing operations could present high risks, the supervisory authority must be consulted in advance in accordance with article 34 paragraph 2 (a).

Assessment: A data protection impact assessment without any exceptions such as the presence of a statutory obligation or consent is superfluous and creates not only new and unnecessary bureaucratic procedures. Due to the general formulations, it is unclear what areas actually require such an impact assessment. This legal uncertainty to which the data controller is exposed, in combination with the extensive obligations to which he is subject (e.g. description of processing operations, risk assessment, remedies, guarantees, obtaining an opinion from data subject or representative), leads to a considerable increase in red tape and uncertainty. This is even more so because a severe fine can be imposed in the event of an infringement of article 33, as set out in article 79 paragraph 6 (t).

Article 35 et seq. – Data protection officer

Regulatory content: The draft regulation provides that a data protection officer has to be designated in companies with more than 250 employees. According to article 35 paragraph 2, the appointment of a single group data protection office is permissible. The provisions covering the data protection officer are expanded, e.g. the name and contact details of the data protection office have to be made known to the public.

Assessment: The principle of bureaucracy avoidance should also apply with respect to the data protection officer. The interest of the public in being informed about a data protection officer is out of all proportion to the possible workload this imposes on the data controller, and in addition it is entirely unclear how this information is to be provided.

In order create an additional incentive to appoint a data protection officer, certain requirements should lapse when a data protection officer is appointed, e.g. in the framework of the information and communication obligations in articles 14 and 15, prior authorisation in application of article 34 or the extensive documentation requirements in accordance with article 28.

Articles 26 paragraph 5, 43 and 44 – Intra-group data transfer

Regulatory content: Article 26 paragraph 5 provides that the European Commission can in future adopt simplified provisions for processing personal data for the purposes of control and reporting within the group. In addition, article 43 provides that binding corporate rules can be authorised by the supervisory authority in liaison with the European Commission and European Data Protection Committee, which are then deemed to provide suitable guarantees for data transfer in third countries.

Assessment: Exchange of data is indispensable for groups of companies. This requires a legally certain basis. Accordingly, the approach of simplifying intra-group data transfer taken in the draft regulation goes in the right direction. Nevertheless, the European Commission has not taken the opportunity to create a provision on intra-group data transfer which ensures legal certainty for data transfer not only within the EU but also beyond. The new data protection provisions envisaged with the regulation must be used to close this gap.

The procedure described in articles 43 and 58 for authorisation of binding corporate rules for data transfer in third countries is unnecessarily complex and time-consuming. The involvement of the European Commission and European Data Protection Committee by the supervisory authority does not seem to be necessary in light of the past experience of supervisory authorities with authorisation of binding corporate guidelines. The competence enshrined in article 51 for the sovereign territory of its Member State should not be undermined when it comes to authorisation of binding corporate rules. In addition, the empowerment of the European Commission to adopt delegated acts in relation to criteria and requirements for binding corporate rules and criteria for their authorisation means that unknown aspects can feed into the procedure even now. Since authorisation of corporate rules is a core aspect of intra-group data transfer, this area should be removed from the possibility for delegated acts.

The data transfer foreseen in article 44 paragraph 1 (h) to meet a legitimate interest does not go far enough for this provision to serve as a basis for data transfer between group companies in a third country. Such a transfer is only possible if it cannot be qualified as frequent or massive. Yet, when tasks are bundled within a group, the outcome is bound to be a frequent exchange of data. Hence, this unnecessary restriction should be removed.

Article 51 – Competence of supervisory authority

Regulatory content: The supervisory authority at the location of the main establishment of the data controller or contract processor is competent for his processing activities in all EU Member States.

Assessment: The underlying idea that only one supervisory authority should have competence for an undertaking is welcome. This principle should apply for all supra-regionally active undertaking, independent of whether they operate within a Member State, within the EU or in connection with a third country.

Article 73 et seq. – Legal remedies

Regulatory content: Not only data subjects but also institutions, organisations and associations which have set themselves the goal of protecting personal data would have access to the extensive rights to lodge complaints granted by the regulation as well as the possibility to submit decisions by the supervisory authority for judicial review on behalf of one or more data subjects.

Assessment: The introduction of a false form of collective redress will fail to do adequate justice to the different legal traditions in Europe. Nor is there any need for such an instrument, since every data subject and also every interest organisation can already turn to the supervisory authority and adequate protection is therefore in place.

The provision whereby, for instance, organisations can also challenge decisions by the supervisory authority in court on behalf of several data subjects is tantamount to the introduction of a class action. Such an instrument leads to friction with the established principle of individual legal protection in continental Europe, including in Germany, which flows on from the right of personality. Data subjects are sufficiently protected by the possibility of a joint action (§§ 59 et seq. ZPO – German Code of Civil Procedure) as well as of a linked case in accordance with § 147 ZPO.

Article 78 and 79 – Sanctions

Regulatory content: Under article 79, the supervisory authority can impose sanctions which are effective, proportionate and dissuasive. The level of fines is linked to the global annual turnover of the company and can be up to 2% of this amount. The European Commission can update these amounts.

Assessment: The sanctions proposed by the European Commission of up to 2% of global annual turnover constitute a clear sharpening as compared with the sanctions regime currently applicable. In setting the level of a fine, the European Commission completely loses sight of the principle of proportionality it has set for itself, since the sanction can no longer be set within justifiable dimensions with respect to the breach. It overlooks the fact that the business object of most undertakings is not data processing. Rather, it is much more of an ancillary object in the employment context.

At the very least, a differentiation with regard to the motivation behind a data protection infringement is necessary. In the current draft of the regulation, the three levels of sanctions (0.5%, 1% and 2%) make no differentiation as regards intentional or negligent conduct – rather, the two types of conduct are equated to each other and can only be taken into account in the framework of the supervisory authority's discretion in setting the level of a fine.

Furthermore, a differentiation should be made as to whether or not an infringement has been committed with a pecuniary motive. This applies even more for a sanctions regime which is linked to global annual turnover – as it is in the sanctions system for competition law. Fines which could run into billions cannot be justified. This is particularly the case if the data protection infringement is negligent and without a pecuniary motive.

There also needs to be a discussion on the level of sanctions and the link to global annual turnover with no qualifications. Even in EU competition law, whose sanctions regime has clearly been taken as a model, this criterion is increasingly being criticised.

Article 82 – Data processing in the employment context

Regulatory content: Member States can regulate employee data protection within the limits of the regulation, inter alia, for the purposes of recruitment, performance and termination of the employment relationship.

Assessment: If the Union decides to regulate data protection in a regulation, employee data protection should also form part of this regulation. Only if it proves impossible to cover collective agreements regulated by labour law, consent and other elements in a

uniform way in the regulation will there need to be an opening clause for labour law. This must take account of the specificities of labour law in such a way that it continues to provide possibilities to act for the national legislator and parties to an employment relationship.

Contact:

BDA | DIE ARBEITGEBER
Bundesvereinigung der Deutschen Arbeitgeberverbände

Arbeitsrecht
T +49 30 2033-1200
arbeitsrecht@arbeitgeber.de