Position Paper

Vote on Amendments to Draft Data Protection Regulation in the Committee for Civil Liberties, Justice and Home Affairs (LIBE)
3 July 2013

The Federal Association for Information Technology, Telecommunications and New Media (BITKOM) represents more than 2,000 companies in Germany. Its 1,200 direct members generate an annual sales volume of 140 billion Euros and employ 700,000 people. They include providers of software and IT services, telecommunications and Internet services, manufacturers of hardware and consumer electronics, and digital media businesses. BITKOM campaigns in particular for a modernization of the education system, for an innovative economic policy and a future-oriented Internet policy.

Since the first consultations on the Regulation BITKOM has proposed to build a uniform data protection regime in Europe equivalent to the solid German standards. To realize this it is helpful to adopt successful instruments from German data protection law. But at the same time the Regulation should revise provisions that have not stood the test of time in order to strengthen the legal frame for the challenges in years to come. Members of the European Parliament in the LIBE Committee have filed various good proposals to do so. We would therefore like to point to some of the issues that are most important in our view.

Executive Summary

- Whether the application of pseudonymization and anonymization on personal data can be increased or not will depend on the incentives set by the Regulation. An adequate definition of these terms is also vital for the ability to realize useful applications concerning traffic planning, e-health, e-energy etc.
- In practice, the legality of data processing in those areas can only be assessed on the basis of the statutory permissions and consent as main legitimate grounds outlined in the Regulation. Therefore their suitability for practical use has to be checked thoroughly.
- Data processing plays a role practically everywhere IT is used. Vague provisions in this area result in difficult contract negotiations and legal insecurity for companies of all industry sectors.
- Data transfers between companies of a group are essential for efficient corporate management and should be regulated as a lean process.
- Profiling is necessary for the functioning of many services and is not as such problematic; limitations to profiling should take into account existing risks and potential disadvantages for the data subject.
- The right to be forgotten has to take into account conflicting fundamental rights and potential consequences of its implementation.
- Only a true one-stop-shop model and an efficient, streamlined consistency mechanism can guarantee the uniform implementation of the new rules.
- The relation to the e-privacy directive should be clarified. The Regulation should precede the Directive in cases where both rules would apply.
- The German model of data protection officer with direct line of report to the executive level is well-proven and should be implemented.

Federal Association
for Information Technology,
Telecommunications and
New Media

Albrechtstraße 10 A
10117 Berlin-Mitte
Germany
Tel.: +49.30.27576-0
Fax: +49.30.27576-400
bitkom@bitkom.org
www.bitkom.org

Contact
Susanne Dehmel
Head of Department
Data Protection
Tel.: +49.30.27576-223
Fax: +49.30.27576-51-223
s.dehmel@bitkom.org

Nils Hullen
Brussels Office
Rue de la Science 14
1040 Brussels, Belgium
Tel.: +32.2.609 53 21
Fax: +32.2.609 53 39
n.hullen@bitkom.org

President
Prof. Dieter Kempf

Management
Dr. Bernhard Rohleder

1 Scope of the regulation: definition of personal data, anonymous data and pseudonymous data

Data protection legislation is to ensure that there is no undue processing and disclosure of personal information that can be attributed to an individual by name and surname. The rationale of data protection is to avoid detrimental impact to an individual as a result from the collection, treatment or dissemination of information somehow related to him.

Some of the proposed amendments currently under discussion are highly misleading. The simple fact, that certain information theoretically allows the determination of a certain person, should not be sufficient to qualify that information automatically as personal data. Instead, it is crucial by what means, effort, and time the individual can be determined. As long as identification requires an unreasonable amount of resource or is impossible, there is no potential harm to the individual and the data in question cannot be considered personal in any way. This follows the spirit of Directive 95/46 which recognized the proportionality principle applied to the concept of personal data in one of its recitals. Extending the concept of personal data to data that cannot be used to ultimately identify an individual will result in two main negative outcomes:

1. It will block further development of the majority of new digital products and services. Our digital world is increasingly designed to support the individual to focus and to select the relevant. This requires a certain composition of data. In most cases anonymous or pseudonymous data are sufficient. Furthermore, modern services such as crowd-monitoring for the improvement of public transportation do require so-called big data. However, they are very unlikely to come to life in an environment where pseudonymous data are qualified as personal data.

2. More importantly, it will become impossible for citizens to differentiate between truly relevant processes and merely formal requirements when dealing with their own personal data. Should all data be treated equally by the Regulation, citizens would develop a routine of clicking boxes in order to benefit from digital products and services. Instead, the Regulation should aim at educating people. It should enable citizens to protect their own personal data where disclosure could be harmful rather than helpful.

Against this background, BITKOM strongly supports LIBE-Amendments that promise a manageable, future-oriented application of the provisions-to-be to relevant cases only:

With regard to the definition of data subject and anonymised data we recommend **AM 734** together with **AM 14** (the definition in 14 should be moved into Article 4 (1)) as well as **AM 391, 405 and 716, 720.** With regard to the definition of pseudonymous data we recommend **AM 732.** Furthermore there should be a clarification as in **AM 683, 686, 687 or 696** on the scope of the regulation**.**

2 Lawfulness of processing and Consent

BITKOM supports the concept of an informed consent, fostering a harmonized approach of data protection in Europe, and providing a balanced framework for a prospering digital economy.

Legal grounds for a lawful data processing should be adjusted to the existing needs of data subjects and controllers in a digital environment. Flexible provisions should be based, among others, on the balance of interests, also of third parties (**AM 455, 873, 874, 878**). Legal grounds for data processing should further incentivize the pseudonymization of personal data and privacy enhancing measures (**AM 887, 897, 898, 900, 904**). They should take into account the increasing need for fraud prevention (**AM 894**), network and information security purposes (**AM 886, 899**) and compliance obligations (**AM 857/859/862**). The use of publicly available data is also relevant in practice, therefore **AM 890 und 895** should be included. Collective agreements are a common basis for legitimate data processing within companies and should be considered as well (**AM 856**).

Rules on consent should focus on transparency and usability, providing legal certainty for data subjects and controllers alike. Conditions for consent should be adjusted accordingly to the risk of the data processing (**AM 105 428, 429**). An informed, unambiguous but implicit consent should be possible if appropriate according to the risk of the data processing (**AM 105, 757, 758, 762, 765**). Further on, legal certainty is a crucial prerequisite for new business models, an innovative Digital Single Market and jobs and growth as such. A given consent, based on the free and informed decision of the relevant data subject, must stay a reliable legal ground for data processing. Vague concepts as a “significant imbalance”, which is foreseen to render a valid consent void, should be abandoned (**AM 983, 984, 985, 986, 987, 988**). Contractual obligations should also be a reliable basis for consumers and data controllers. The withdrawal of consent must not be a backdoor for the termination of existing contractual obligations or for the deletion of data, which are subject to legitimate use of the data processor (**AM 438, 976, 977, 980)**.

3 Controller – Processor Relation

The responsibilities between controller and processor have to be better-defined. The single responsibility of the controller (compare with Art. 6 par. 2 and Art. 17 Directive 95/46/EG) has proved of value. This clear separation concerning the singular responsibility of the controller is continued in **AM 522, 523, 524** as well as in **AM 746, 747, 748**. The current privilege of the controller that says, that data transfers to the processor do not have to fulfil the provisions in Art. 6, is based on his singular responsibility and can be found in **AM 525**. The data subject also has to know his or her single point of contact for the right of information and access e.g. Therefore, the documentation obligations can also be reduced to the one who is the point of contact for the data subject and therefore obliged to give information according to Art. 14 of the Regulation. **AM 1825 and 1826** reflect that. A clear separation of responsibilities also forces the controller to fulfil his responsibility already when choosing a service provider. Therefore also a common liability of processor and controller isn’t appropriate, as the processor is only allowed to act on the instructions of the controller and has no means to control the controller whether he actually is legitimized to process the data. **AM 2818, 2822 and 2823** consider this and take into account the interests

of the data subject as well as the distribution of decision-making authority between the controller and the processor.

4 The need for Data Transfers in Groups of Companies

The special relation between companies of a group also raises needs for data transfers between these companies. If an adequate level of data protection has been ensured (e.g. through binding corporate rules, a serious code of conduct or within Europe through uniform legal provisions) the so far necessary agreements on processing on behalf within a corporate group should become dispensable, in order to avoid red tape through redundant contractual agreements. Especially it should be possible to transfer key functions such as customer service, legal department, revision or human resources in one legal entity of the group without having to conclude extensive contractual agreements for data protection purposes. Legal provisions should be adapted to the needs of groups of companies and privilege those companies that establish binding corporate rules. In addition, binding corporate rules should also extend to sub-processors, in order to cover the provision of cloud services. We therefore support **AM 795 and 860/864, 901, 2426, 2467, 2348, 2349 and 2350. Furthermore AM 2415, 2421 (following 2349) and 2422 should be considered.**

5 Profiling

The focus of Article 20 should be on prohibiting only profiling that is harmful to the individual, and welcome amendments that seek to define an appropriate and realistic threshold for harm (i.e. which is unfair or discriminatory or which has significant adverse effects). As a basic principle, processing that is legitimate should be allowed. Profiling that discriminates on the basis of sensitive categories of data should be prohibited, without prejudice to the provisions of Article 9.2

We support amendments that aim to restrict profiling that may be harmful to the individual (i.e. unfair or discriminatory or which has significant adverse effects) such as **AM 1544, 1547, 1553**; all other profiling activities would fall under the general provisions of the Regulation where personal data processing takes place (**AM 1579, 1588, 1590**). We also support amendments that seek to make profiling based on pseudonymous data legitimate on all instances (**AM 1556, 1568**). This is a risk-based approach that would in practice adequately protect the individual whilst not unnecessarily restricting the use of profiling techniques and technologies that are essential to business, the economy, competitiveness and growth.

Profiling which is commercially indispensable or obligatory by law should be allowed explicitly (**AM 1574, 1584, 1585, 1586, 1589**). Further Amendments we support are: **AM 511, 1594, 1600, 1604, 1612-1616.**

6 Right to Be Forgotten

The Right to be forgotten and erasure as proposed by the European Commission and reinforced in some LIBE amendments creates operational implementation questions and does not fully outline the impact of these requirements on a) other fundamental rights recognized under the EU Charter of Fundamental Rights and the European Convention on Fundamental Rights b) the role of intermediaries under EU law. We therefore support **AM 1380, 1381, 1385, 1390, 1391, 1399, 1400, 1403, 1410, 1412 and 1414.**

7 One-Stop Shop and Coherency-Mechanism

The introduction of the one-stop-shop principle is helpful and important. But the competence of data protection authorities in the draft only depends on the (legal) person. If a company (e.g.a corporate group) consists of several legally separated organisations such as two GmbHs in Germany, a S.A. in France, a Ltd. In UK and a SpA in Italy, these are five controllers and they keep their four to five data protection authorities. The role of the authority at the place of the main establishment mainly concentrates on authorizations and the coordination of joint enforcement. A "one-stop-shop" doesn't exist for companies with diversified structure under company law. **AM 786** allows for the achievement of a true one-stop-shop by providing for clear, tangible, consistent and verifiable criteria to determine the main establishment, which have proven to be workable as they are used today to determine the appropriate DPA for BCRs. It also proposes one uniform 'main establishment test' for controller and processor. **AM 790/791** clarifies and strengthens the one-stop shop concept by determining that the DPA of a company's main establishment has exclusive competence for the supervision and for enforcement action. It provides legal certainty for data subjects and businesses. **AM 793/794**: In respect of the EU principle of non-discrimination, this amendment clarifies that non-EU controllers who appoint an EU representative benefit from the one stop-shop principle in the same way as EU-established controllers, considering that they are subject to the same rights and obligations of the draft Regulation.

By clarifying that the DPA of the country, where the non-EU controller's representative is established, is exclusively competent **AM 2588 2589 / 2590** strengthens the one-stop-shop principle. **AM 2591 / 2592** clarifies that where the Regulation applies to an EU-based controller or processor and a non-EU based controller within the same corporate group, only one DPA should be competent, namely the DPA of the country of the EU-based controller's or processor's main establishment. By clarifying the procedure in case of a data subject's request or complaint, **AM 2599** strengthens the one-stop-shop principle. This will ensure that the benefits of harmonisation, legal certainty and effective redress are conferred to the data subject. **AM 2599, 2618 / 2619, 2627 / 2628, 2633 / 2634, 2635 / 2636, 2662 / 2664** are in line with a robust one-stop-shop principle, these amendments clarify that the powers described in these provisions are incumbent on the "competent" authority in the sense of Article 51.

8 Relation of Regulation and E-Privacy-Directive

In order to avoid double or contradicting legislation the relation between the data protection regulation and the e-privacy Directive has to be clarified. The current version of Art. 89 is unclear. It says that the e-Privacy Directive precedes the Regulation in matters that are subject to specific obligations with the same objective. But it is not clear how to interpret this in practice. Concerning stock data, traffic data and localization data special legislative solutions for telecommunication providers should be avoided. In order to create a level playing field a clear and clarifying and thus legally certain adaption of the scope of application of the sector specific e-Privacy Directive is necessary. We support a primacy in application of the Data Protection Regulation where an identical case of application falls under both scopes. The primacy in application should be clarified through the Regulation by deletion of the corresponding provisions in the e-Privacy Directive (**AM 3127, 3129**). A revision of the e-Privacy Directive at a later

stage, in order to adapt it to the Regulation, doesn't provide the necessary legal certainty.

9 Data Protection Officer

The concept of a company data protection officer has been very successful in Germany. The concept is widely recognised – data protection authorities approve it as well as the companies themselves. His strong position and direct line of report to the executive level make the data protection officer an effective and independent supervision authority within a company. To strengthen the position of the data protection officer, continuous professional training, independency (**AM 2228**) and professional secrecy should be guaranteed (**AM 231, 2271, 2276, 2277, 2282, 2283**). The trust in the institution of a data protection officer can be fostered, if there is at least one data protection officer available in each member state (**AM 2195**). The appointment of a data protection officer should be advantageous for companies – e.g. by replacing notification and consultation obligations as under existing national data protection law (**AM 2019, 2861**). This would strengthen self-control within the economy and would at the time help to reduce red tape. It should be clearly stated, that a data protection officer can not only be an employee of the controller but also be an independent external service provider (**AM 2219**).