Comments on Chapter III – Rights of the data subject

25/08/2015

Bitkom represents more than 2,300 companies in the digital sector, including 1,500 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. 78 percent of the companies' head-quarters 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 focusing the modernization of the education sector and a future-oriented network policy.

Bitkom's position papers will be also published on its website.

Overview

Transparency and modalities

Identification problems using electronic format: The Commission's proposal prescribed, that the application process of the right to information and other rights should always be made possible in electronic form. In contrast, today it is standard practice by a controller to send information by letter even if requested electronically. Thereby, it can be verified that the person requesting information is also the concerned data subject. This can often not be guaranteed if using an e-mail address.

Example: *Providing information electronically is only unproblematic if the concerned data subject has directly an account with e-mail address with the controller and has additionally verified his or her personal details. Otherwise there might be the risk of a data protection breach – providing (sensitive) data to a third person.*

Article 12 - Procedures and mechanisms for exercising the rights of the data subject

EP Version Article Article 12	Council Version Article 12	Bitkom
1. Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically where possible.	1. The controller shall take appropriate measured to provide any information referred to in Article 14 and 14a and any communication under Articles 15 to 19 and 32 relating to the processing of personal data to the data subject in an intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or by other means, where appropriate electronically. Where the data subject makes the request in electronic form, the information may as a rule be provided in electronic form, unless otherwise requested by the data subject. When requested by the data subject, the information may be given orally provided that the identity of the data subject is proven, (...)	Bitkom supports the additions made be EP and Council.

Article 13a - Standardised information policies (Icons)

Although Bitkom recognizes the wish to condense information on terms on conditions into a label or icon or similar format, there are fundamental issues that have to be considered if one intends to follow such an approach:

1. **Article 13a –A consumer protection provision:** Bitkom emphasizes that Article 13a) should only apply in a B2C not B2B – context. The latter are technical and highly complex in nature. Should the legislator decide to integrate this provision, a simplification by Icons would insufficiently present factual circumstances and thereby falsify the actual case. In addition, there is no inequality in bargaining power. In case of a compromise in trialogue discussions, it should be made clear that this Article only applies in a B2C- context.

2. **Interaction between Icons and privacy policies:** Article 13a leaves open in which relation privacy policies and icons stand to each other. Is there any duty for the controller to already provide information in form of an Icon even before data processing takes place? Should the EP version be adopted, which we do not recommend, many legal questions need to be addressed also with regard to a certification process.

3. **Label or icons might mislead consumers due to their simplified form:** There is a contradiction between the legal necessity to inform the consumer in detail and the objective of presenting the information in a format that actually enables consumers to read and understand the terms and conditions. However, this contradiction cannot be solved by pressing complex data privacy policies into the form of overly simplified icons. Such icons are not self-explanatory and need to be interpreted. This interpretation will unavoidably lead to confusion and misunderstandings between controller and data subject unless the latter reads the privacy policy in combination with the Icon which in the end would lead to more not less information.

   Example: *The proposed icons contain negative explanations "...are not" which means they inform about what does not happen instead of actually stating what happens. This fact already makes them quite hard to understand. Symbols, such as the one with the 'lock', the one on 'data minimization' or the 'sign for not using data for other purposes' are not self-explanatory. In addition, most of them are only repeating what is written in the law as obligation for the controller anyway. They do not in any way give more information.*

4. **Standardized Icons are difficult to be applied across all industry sectors:** The GDPR applies not only to ICT companies but also to all other sectors of industry. One-size-fits all icons, as proposed by the EP, mainly focus on the ICT-industry and do not meet the needs of different industries. They might be also interpreted differently among Member States as certain sectors have further, more-detailed rules on data protection based on national law. The GDPR allows for such sectoral differentiations by its opening clauses. However, if such concept is adopted there should be at least only an abstract obligation in the Regulation; the concrete implementation should be carried out in a self-regulatory process in each industry as proposed in in Art 38 GDPR.

5. **Standardized Icons in general are not easily adaptable to new technologies:** There is an ever growing complexity of data processing in a connected world. Innovation is moving fast and EU decision-makers already have problems to keep pace with the digital transformation. Icons had to be constantly adapted and further developed in line with the technological progress. This problem can be only solved by working closely together with industry.

   Compromise Suggestion: *The Council Presidency has suggested in its document from the 4th September that "the use of Icons should be on a voluntary basis" and that the „definition and content of these icons is not to be done in the Regulation but rather by tasking the Commission or the EDPB." Bitkom supports both notions in case of a compromise. However, as already stated above, both Commission and EDPB need to work closely together with representatives of industry in a multi-stakeholder approach or icons need to be drafted via self-regulation.*

Bitkom believes that a standardization of data protection regulations and provisions for privacy policies (such as harmonized information requirements) will help to reduce consumer's cost for reading and understanding. More harmonized rules in the EU, as the General Data Protection Regulation proposes, will contribute to the understanding of data subjects. Icons, in contrast, are a good idea in theory but cannot be imposed by legislation in a practicable and useful way. In case of a compromise, Bitkoms' concerns should be taken into account.

EP Version Article 13 a	Bitkom
1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with the following particulars before providing information pursuant to Article 14: (...)	Bitkom supports the deletion of Article 13 a.

Information and access to the data subject

Article 14 and 14a – Information requirements

Article 14 (3a) is connected to Article 6 (4), the provision on further processing for incompatible uses. Therefore, both provisions should depend on each other.

EP Version Article 14a	Council Version Article 14a	Bitkom
	2. The controller shall provide the information referred to in paragraphs 1 and 2: 3a) Where the controller intends to further process the data (...) for a purpose other than the one for which the data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.	Bitkom already laid down in its comments on Chapter II that "further processing in the legitimate interest of the controller" is crucial for big data analysis and the development of online-services. In this context, we recognize the need to provide enough transparency to the data subject.

Article 14 and 15 – Professional Secrecy

Professional Secrecy: Bitkom supports the EP text to refer to professional secrecy with respect to the right and duty to provide information. Such differentiation is needed to meet the demands of special occupations.

EP Version Article 14	Council Version Article 14	Bitkom
5. Paragraphs 1 to 4 shall not apply, where: da) the data are processed in the exercise of his profession by, or are entrusted or become known to, a person who is subject to an obligation of professional secrecy regulated by Union or Member State law or to a statutory obligation of secrecy, unless the data is collected directly from the data subject.		**Bitkom supports the EP text.**

EP Version Article 15	Council Version Article 15	Bitkom
2c. There shall be no right of access in accordance with paragraphs 1 and 2 when data within the meaning of point (da) of Article 14(5) are concerned, except if the data subject is empowered to lift the secrecy in question and acts accordingly. .		**Bitkom supports the EP text.**

Article 17 – Right to erasure / "Right to be forgotten"

The draft regulation gives every person the right to demand "to be forgotten". The objective of this right is to give the data subject – in particular in view of the internet – the possibility to limit or completely restrict the availability and use of data. Bitkom fully recognizes this wish but also points to the practical feasibility of such right.

The right to block data: In line with Art. 12 b of the Directive 95/46, the right to block data should still be possible where erasure is not possible or is only possible with disproportionate effort due to specific type of storage.

Duty to inform third parties: According to Article 17 (2) GDPR a duty to deletion exist also for cases in which the person concerned is no longer controlling the data. In order to ensure that all copies of information once published within a service can be deleted, the controller has to track the data subjects' contents. This runs counter to the actual aim of data protection. Therefore, Bitkom supports the addition to inform "known" controllers which would better reflect reality and avoid difficult tracking.

Furthermore, the wish to remove every link on the internet, will often fail due to technical reasons and the speed content is shared nowadays. Due to this reason, Bitkom supports that notion that the controller only has to take "reasonable steps" (as proposed by EP and Council text) and the addition of the Council text to take "available technology and the cost of implementation" into account. Due to the problem to fully remove data from the World Wide Web, the term "right to be forgotten" is misleading and should be avoided as laid down in the EP text. Bitkom supports an approach in line with the current data protection Directive to obtain "rectification, erasure and blockage of personal data".

Bitkom also support the EP proposal of making the exercise of the right to be forgotten contingent on the possibility to verify the identity of the entity making the request (Article 17.1a of the EP).

EP Version Article 17 Right to erasure	**Council Version Article 17 Right to erasure and to be forgotten**	**Bitkom**
1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to him or her and the abstention from further dissemination of such data, and to obtain from third parties the erasure of any links to, or copy or replication of, those data where one of the following grounds applies: (...)	1. The controller shall have the obligation to erase personal data without undue delay especially in relation to personal data which are collected when the data subject was a child, and the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay where one of the following ground applies: (...)	Bitkom supports the deletion of the misleading term of „Right to be forgotten". Furthermore, Bitkom supports the reintegration of the „right to block data".

1a. The application of paragraph 1 shall be dependent upon the ability of the controller to verify that the person requesting the erasure is the data subject.		Bitkom supports the addition of the EP text in 1 a).
2. Where the controller referred to in paragraph 1 has made the personal data public without a justification based on Article 6(1), it shall take all reasonable steps to have the data erased, including by third parties, without prejudice to Article 77. The controller shall inform the data subject, where possible, of the action taken by the relevant third parties.	2a. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the data, that the data subject has requested the erasure by such controllers of any links to, or copy or replication of that personal data.	Bitkom supports the Council text in 2a) and an addition of "known" controllers. This better reflects internet reality and technical feasibility and avoids the obligation to track the data subject.
4.Instead of erasure, the controller shall restrict processing of personal data in such a way that it is not subject to the normal data access and processing operations and cannot be changed anymore, where:		
da) the particular type of storage technology does not allow for erasure and has been installed before the entry into force of this Regulation.	**Deleted**	Bitkom generally supports an adoption of the "right to block data" as mentioned above. However, if trialogue discussions point in a different direction, Bitkom supports Article 17 (4) (da) EP text with the deletion of the last half sentence which partly compensates for the loss of data blockage.

Article 18 – Right to data portability

The duty to transfer customer data of a concerned person electronically to a competitor goes significantly further then other rights like the right to information and right to erasure which similarly enable the data subject to gain controller over his or her data. It causes not only technical problems but distorts competition. This is especially because of the fact that the suggestion does not differentiate between cases (e.g. online platforms) but applies to all companies which store data. This could lead to absurd results.

Example: *Online-Shop has the duty to transfer data (information of customer) from its ordering process in format the competitor can use for its business. This could reveal trade secrets and thereby distort competition.*

Should a compromise be reached between different versions, the text should clarify on which situation the right to data portability applies. Furthermore, a balance of interest must be introduced to take also the interests of the controller or processor (like trade secrets) into account.

Commission	EP Version Article 15	Council Version Article 18	Bitkom
(...)	2a. Where the data subject has provided the personal data where the personal data are processed by electronic means, the data subject shall have the right to obtain from the controller a copy of the provided personal data in an electronic and interoperable format which is commonly used and allows for further use by the data subject without hindrance from the controller from whom the personal data are withdrawn. Where technically feasible and available, the data shall be transferred directly from controller to controller at the request of the data subject.	1. The data subject shall have the right to receive the personal data concerning him or her which he or she has provided to a controller in a structured and commonly used and machine-readable format, without hindrance from the controller to which the data have been provided, *where*. 2a	Data sets are an important, if not existential, resource of companies and a product of significant investments in online services. Therefore, a duty that goes beyond mere portability by a "machine-readable" format, significantly distorts competition. A right balance between competition law and data protection must be found by deleting the word "machine-readable".
3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).			**Standards, Modalities and Procedures:** It is not appropriate in Art. 18 (3) to delegate technical standards, modalities and procedures to the Commission by delegated acts. Such technical questions can only be solved in dialogue with the controller and processor which have to implement such standards. A multi-stakeholder approach would be a better option.

Article 19 Right to object

"Justified" grounds for the objection: Bitkom encourages the legislator to revert to the original 1995 Directive wording, which requires a "justified" objection. The lack of justification renders it impossible to weigh the legitimate interest of the controller or processor against the interest of the data subject. Furthermore, ill-informed objections would be given automatic standing which a controller may not be able to overturn, or which will have required that the processing is to be suspended while the objection is clarified. Such activities would reduce legal uncertainty and increase the potential for business disruption for any entity relying on the legitimate interest legal basis.

Compelling legitimate grounds of the controller: It is unclear why the Council uses a different legal test compared to Art. 6 (1) (f) GDPR. Bitkom supports the deletion of the word "compelling".

Example: *In the CRA-sector this provision would cause damage by opening way to potential frauds as data subjects might object to the processing of information about payment defaults. This would lead to data subjects having incomplete or inaccurate credit files, which would impact both their ability to attain credit and the lenders ability to assess risk.*

EP Version Article Article 19	Council Version Article 19	Bitkom
1. The data subject shall have the right to object at any time to the processing of personal data which is based on points (d), and (e) of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.	1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her which is based on points (...) (e) or (f) of Article 6(1), the first sentence of Article 6(4) in conjunction with point (e) of Article 6(1) or the second sentence of Article 6(4). The controller shall no longer process the personal data (...) unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, (...) rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.	Bitkom supports an integration of the word "justified" grounds as laid down in Article 14 in the Directive 95 /46. The current model, whereby the data subject needs to justify their objections, should prevail. Bitkom supports the deletion of the word "compelling".

Article 20 - Right to profiling

Changing the wording of Article 15 of the Data Protection Directive 95/46 in the Regulation draft requires clarification which profiling is still permitted. The interpretation of the different concepts of "profiling" (EP), "automated decision making" (Council) or "measures based on profiling" (Com) varies among stakeholders - not only within industry but also the EU institutions. Therefore, Bitkom points out that both options (EP and Council) may pose problems in practice depending on the interpretation.

1. The GDPR debate let to a negative connotation of profiling, which neglects that it is widely used in all kind of industries and often provides positive results for the data subject or consumer in general.

   Example*: Examples like credit scoring are often negatively used against profiling and raise fear among consumers. However, credit ratings in many cases are a prerequisite of companies e.g. to offer payment methods such as "purchase on account" on the internet where payment takes place only after delivery. Consumers value this possibility especially in cases where they order from a new service.*

   Bitkom cautions against an approach which considers profiling only from a negative angle.

2. Bitkom generally supports the right to "request human intervention". There are many cases which should be covered by Article 20 GDPR such as situations, which clearly affect the data subject's rights and freedoms. In such a case the right to request human intervention is absolutely legitimate.

   Example: *A bank refuses the payment by credit card from a consumer.*

   In contrast, other situations like pure data analytics for optimizing websites or various systems using an algorithm should not fall under the scope of this Article as long it does not negatively affect the data subject's rights. Profiling is just a way of data processing and, therefore, it only makes sense to have specific provisions to the extent it may cause special risks or negative effects for the data subject.

   Example: *There is no necessity to re-evaluate (by human intervention) whether e.g. a hotel booking site or another search engine has provided the right search result.*

It also needs to be discussed whether – in all circumstances – human intervention should be made obligatory as suggested by Article 20 (5) of the EP-text ("shall include"). In some circumstances 'human intervention', such as contesting the decision, is necessary only in the aftermath of a decision, and only needed, if the decision does not satisfy the request of the data subject.

Example: *Credit rating agencies provide information between 250.000.000 – 300.000.000 times (in Germany) on the basis of automated processing. In most cases the credit, such as purchasing a mobile phone on credit, is granted within seconds at the point-of-sale. With mandatory human assessment this will not be possible anymore.*

All in all, Bitkom cautions against an approach which covers all "automated processing"- situations and subjecting them to same conditions of Article 20 GDPR. A context-based approach (see also comments on profiling based solely on the processing of pseudonymous data in section below) should be implemented by, for instance, making clear in a recital which situations are covered by this Article and which not.

EP Version Article 20 Profiling	**Council Version Article 20 Automated individual decision making**	**Bitkom**
1. Without prejudice to the provisions in Article 6, every natural person shall have the right to object to profiling in accordance with Article 19. The data subject shall be informed about the right to object to profiling in a highly visible manner.	1. The data subject shall have the right not to be subject to a decision (…) based solely on automated processing, including profiling, which produces legal effects concerning him or her or significantly affects him or her.	Bitkom concerns regarding Article 19 are laid down earlier in this paper. Furthermore, it is not clear what the words "highly visible manner" means.
2. Subject to the other provisions of this Regulation, a person may be subjected to profiling which leads to measures producing legal effects concerning the data subject or does similarly significantly affect the interests, rights or freedoms of the concerned data subject only if the processing:	1a. Paragraph 1 shall not apply if the decision:	
a) is necessary for the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied**,** provided that suitable measures to safeguard the data subject's legitimate interests have been adduced; or	a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; or	
b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or	b) is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's legitimate interests; or is based on the data subject's explicit consent.	Such opening clause for MS law should be reconsidered in light of harmonization which the GDPR intends to achieve.
c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to	c) Is based on the data subjects's explicit consent.	Bitkom has commented on "consent" in its position paper in Chapter II.

suitable safeguards.	1 b) In cases referred to in paragraph 1a (a) and (c) the data controller shall implement suitable measures to safeguard the data subjects' rights and freedoms and legitimate interest, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.	
3. Profiling that has the effect of discriminating against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, sexual orientation or gender identity, or that results in measures which have such effect, shall be prohibited. The controller shall implement effective protection against possible discrimination resulting from profiling. Profiling shall not be based solely on the special categories of personal data referred to in Article 9.	2. Decisions referred to in paragraph 1a shall not (...) be based on special categories of personal data referred to in Article 9(1), unless points (a) or (g) of Article 9(2) apply and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.	
5.Profiling which leads to measures producing legal effects concerning the data subject or does similarly significantly affect the interests, rights or freedoms of the concerned data subject shall not be based solely or predominantly on automated processing and shall include human assessment, including an explanation of the decision reached after such an assessment. The suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2 shall include the right to obtain human assessment and an explanation of the decision reached after such assessment.	deleted	
5a. The European Data Protection Board shall be entrusted with the task of issuing guidelines, recommendations and best practices in accordance with point (b) of Article 66(1) for further specifying the criteria and conditions for profiling pursuant to paragraph 2.		

Article 4 – Definition of profiling

EP and Council have made proposals for a definition of „profiling“ which include the term „performance at work“. This reference should be reconsidered as it might cause practical problems.

Example: *An employee applied for a job within the group in another country. HR department asked him to pass a language online test in order to see whether he has sufficient language skills. He failed and was automatically not put on the short list.*

Example: *A bank house asks in an online recruitment questionnaire to proof skills in mathematics by providing results of the school leaving examination. Applications without a defined level will automatically be rejected.*

EP Version Article 4	**Council Version Article 4**
(3a) 'profiling' means any form of automated processing of personal data consisting of using those data to evaluate personal aspects relating to a natural person, in particular to analyse and predict aspects concerning performance at work, economic situation, health, personal preferences, or interests, reliability or behaviour, location or movements;	(12 a) 'profiling' means any form of automated processing of personal data consisting of using those data to evaluate personal aspects relating to a natural person, in particular to analyse and predict aspects concerning performance at work, economic situation, health, personal preferences, or interests, reliability or behaviour, location or movements;

Recitals 58a – profiling

Anonymised and pseudonymised profiling: Giving privilege to anonymised or pseudonymised data enables the processing organ to create user profiles, e.g. for advertising, market research or for adequate design of Internet services, without violating the rights of the data subject concerned. This privacy-enhancing creation of profiles is clearly different from profiles that connect user activities to an individual and can therefore legally take place also without the explicit consent of the person involved.

EP Version Recital 58	Council Version Recital 58a	Bitkom
Profiling based solely on the processing of pseudonymous data should be presumed not to significantly affect the interests, rights or freedoms of the data subject. Where profiling, whether based on a single source of pseudonymous data or on the aggregation of pseudonymous data from different sources, permits the controller to attribute pseudonymous data to a specific data subject, the processed data should no longer be considered to be pseudonymous.	Profiling as such is subject to the (general) rules of this Regulation governing processing of personal data (legal grounds of processing, data protection principles etc.) with specific safeguards (for instance the obligation to conduct an impact assessment in some cases or provisions concerning specific information to be provided to the concerned individual). The European Data Protection Board should have the possibility to issue guidance in this context.	In particular profiling based solely on the processing of pseudonymous data, should be presumed not to significantly affect the interests, rights and freedoms of the data subject. Where profiling, whether based on a single source of pseudonymous data or on the aggregation of pseudonymous data from different sources, permits the controller to attribute a profile consisting of pseudonymous data to a specific data subject, without the use of additional information, such a profile should no longer be considered to contain pseudonymous data.