Annex

The Federal Association for Information Technology, Telecommunications and New Media (BITKOM) represents more than 1,700 companies in Germany. Its 1,100 direct members generate an annual sales volume of 135 billion Euros annually 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.

In order to provide precise input on how to possibly address some of the unclarities and practical problems outlined in our paper with examples for possible impacts of the Regulation we propose amendments with regards to the enlisted subjects of the Regulation:

1. Scope of the Regulation
2. Lawfulness of data processing
3. Data transfers in groups of undertakings
4. Consent
5. Differentiated regulations for profiling
6. Controller Processor Relation

This is not a closed list of amendments as we are still working on amendments for the rules on self-regulation. With respect to other points we support the list of amendments drafted by our European association Digitaleurope.

1 Scope of the Regulation

Art. 4 (1) and Recitals 23, 24 Definition of Personal Data

German Association
for Information Technology,
Telecommunications and
New Media

Albrechtstr. 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

Commission Proposal	**BITKOM Proposal**
Art. 4 (1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;	Art. 4 (1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the ***controller*** ~~***or by any other natural or legal person***~~ **-,** in particular by reference to an identification number ***in combination with specific information enabling the identification*** or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;
Recital 23 'data subject' The principles of protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the individual. The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.	Recital 23 'data subject' The principles of protection should apply ***only*** to ~~***any***~~ ***specific*** information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken: (i) ~~***of only those all the***~~ means reasonably likely to be used ~~***either***~~ by the controller ~~***or by any other person***~~ to identify the individual, and (ii) ***the reasonable likeliness of a person being identified.*** The principles of data protection should not apply to data rendered anonymous ***or made unreadable*** in such a way that the data subject is no longer ***or not yet*** identifiable ***from the data.*** ***Serial numbers of products, IP addresses, International Mobile Equipment Identity codes or other such identifiers should not be regarded as personal data before a link to a natural person can be established. Such identifiers should still not be regarded as personal data even after establishment of such link when they remain standalone in the possession of a controller or processor, i.e. when they are not combined with additional data in order to identify or target activities at a natural person.***
Recital 24 When using online services, individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. This may leave traces which, combined with unique identifiers and other information received	Recital 24 When using online services, individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. This may leave traces which, combined with unique identifiers and other information received

Justification
Online identifiers and location data on their own cannot identify individuals. Also, in view of the fact that the draft Regulation places new burdens on data controllers and processors, it is important to have a clear definition for 'personal data'. We therefore suggest that location data and online identifiers as such are excluded from that definition.

It should be made clear that the theoretical possibility to identify an individual is in itself not sufficient for considering an individual as identifiable. Thus, for example, if, by the use of super-computing resources, the reasonable likeliness of identification is high for a given data set, such data set will nevertheless not be considered personal data subject to this regulation if the data controller is not reasonably likely to have access to or use such supercomputing resources to perform such identification. An overly broad definition of 'data subject' encompassing those identifiers (such as serial numbers etc.) which are not connected to a natural person does not lead to a better protection; on the contrary it takes away incentives to make data anonymous or to refrain from linking it to a natural person.

2 Lawfulness of Data Processing

Art. 6 Lawfulness of Processing

Commission Proposal	**BITKOM Proposal**
b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;	b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; ***or as otherwise appropriate to manage or effectuate the relationship between the controller and data subject***
(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. […]	(f) processing is necessary for the purposes of the legitimate interests pursued by a controller **or *by a third party***, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data~~, in particular where the data subject is a child~~.[…].

Commission Proposal	BITKOM Proposal
	(g) For the purposes of advertising, market research or in order to design telemedia services in a needs-based manner, the controller may produce profiles of usage based on pseudonyms to the extent that the data subject does not object to this. The controller must refer the data subject to his right of refusal of pseudonymous profiling measures in accordance with Art. 14. These profiles of usage must not be collated with data on the bearer of the pseudonym.

Justification

b) There are cases, where there is no contract (yet) and where it is not possible or appropriate to ask the customer in advance to request the desired processing of data.
Example: If an online retailer wants to offer payment per invoice after delivery of the ordered goods, usually he needs to check on the reliabilty of the customer very quickly. There is no request of the customer to do so, but the online retailer needs to do so in order to be able to offer this, otherwise the risk would be too high and he could offer the service to no one.

f) Credit agencies and industry warning systems that are partly already legally required to prevent money laundering or fraud (cf. Art. 25 c German Banking Act) retrieve their data, as commonly conceived, not based on the interest of the bodies providing the data or the credit agency storing the data or the warning system, but based on the legitimate interest of third parties in the systems. If the legal basis protecting the interests of third parties ceases to exist, credit agencies and warning systems would not be able to become active at all since the transfer of corresponding data (in the interest of third parties) would no longer be permitted. In this respect, companies would lose the possibility to check credit ratings or use systems in the framework of compliance measures (for the significance of credit agencies, also check European Court of Justice of 23 Nov. 2006 – case 238/05).

Furthermore, the protection of a child is already given when it comes to the balance of rights between the controller or a third party and the data subject. Nevertheless, such interests have to be taken into due consideration, especially if the data subject is a child. But the wording as it is now could also imply that there is no legitimate processing possible at all if the data subject is a child, even if the processing is carried out (also) in the interest of the child.

g) Pseudonymous profiling should be deemed as lawfully for reasons of advertising, market research or to design media services in a needs-based manner (i.e. user interfaces, websites etc.), as long as the profile data is stored separately from the individual data and the pseudonymous profiles can not be linked to a indentifiable natural person subsequently. Pseudonymous profiles are essential for providing tailor-made online advertising. The economic benefit of online advertising is crucial for all Internet offers, among others, in the field of

quality journalism which is available to users free of charge. If such a possibility of funding through advertising is prevented although the processing organ (website operators or third parties transferring advertising banners) cannot track back the actual person, innovative business models on the Internet would be obstructed in all conceivable spheres.

3 Data Transfers in Groups of Undertakings

NEW Art. 6 (2) a) and new Art. 4 (16a)

Commission Proposal	BITKOM Proposal
	Art. 6 (2) a) If the controller is a legal person that is part of a registered group of undertakings and the provisions of Art. 6 (1) f are fulfilled, the controller may transfer personal data to other controllers that belong to the group.
	Art. 4 (16a) "registered group of undertakings"means a group of undertakings seated in the EU and countries with adequate protection level, that has registered as group at the Data Protection Authority of the main establishement within the EU.

Justification
Corporate groups of companies are not organised in the structure of their legal entities. Human ressources and also customer management are usually organized between different companies of the group. Therefore there is a strong need for unbureaucratic data transfers within such corporate groups.
The new provisions for BCRs might help a little in international context, but the system is still too complicated to fulfill the needs of companies. Therefore a simplified possibility for data transfers within groups of undertakings in the EU or countries with adequate protection level should be installed.

4 Consent

Art. 7 Consent (Recitals 32, 33, 34) and Art. 4 (8)

Commission Proposal	BITKOM Proposal
Art. 4 (8) 'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed	Art. 4 (8) 'the data subject's consent' means any freely given specific, informed and ***unambiguous*** ~~***explicit***~~ indication of his or her wishes by which the data subject, either by a statement or by a ~~**clear**~~ affirmative action, signifies agreement to personal data relating to them being processed
Art. 7 (1) The Controller shall bear the burden of proof for the data subject'sconsent to the processing of their personal data for specified purposes.	Art. 7 (1) deleted
Art. 7 (4) Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.	Art. 7 (4) Consent shall not provide a legal basis for the processing, ~~***where there is***~~ ***when, due to*** a significant imbalance between the position of the data subject ***and the controller, the data subject could not refuse his consent without suffering harmful consequences of a material nature attributable to the controller.***
Recital 32 Where processing is based on the data subject's consent, the controller should have the burden of proving that the data subject has given the consent to the processing operation. In particular in the context of a written declation on another matter, safeguards sould ensure that the data subject is aware that and to what extent constent is given.	Recital 32 Where processing is based on the data subject's consent, the controller should have the burden of proving that the data subject has given the consent to the processing operation. ***The burden of proof is only on the fact that consent was actually given to the processing operation in question. The controller is not obliged to determine the identy of the person who gives consent.*** In particular in the context of a written declation on another matter, safeguards sould ensure that the data subject is aware that and to what extent constent is given.
Recital 34 Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its	Recital 34 **Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller,** ***resulting in the data subject not having a true option of refusal without being subject to harmful consequences, taking into account the interest of the data subject. Such situations may exist, among others, in relation to certain aspects of employment relationship, in context of essential services or when dealing with public authorities.*** ~~***This is especially the***~~

Justification

Art. 4 (8)

The term ‘unambiguous’ is better suited as it does not lower but rather increases the requirements of ‘consent’ compared to ‘explicit’ (because of the combination with the requirement of ‘affirmative action’) and it has a much better chance to be understood in a consistent way in all the Member States.

Art. 7 (1) and Recital 32

The rule on the burden of proof in Art. 7 (1) creates an unnecessary disadvantage for controllers and will force them to collect and archive more data in order to be able to proof given consent. Already now usually companies have to proof that consent was given, if that is the legal basis for their processing – they have to provide processes for the declaration of consent and its filing. If they can proof that there is a filed consent, the burden of proof should go to the data subject that might still deny any declaration of consent. The possibilties of anonymised usage of internet services should not lead to a one-sided disadvantage for the Controller. Furthermore the relation between Art. 7 (1) and Art. 10 is unclear as Art. 10 says that the controller doesn’t have to collect additional data merely for the purpose of complying with provisions of the regulation.

Art. 7 (4) and Recital 32

The provision of Art. 7 (4) is problematic as company agreements or individual consent by the employee are an important and common instrument to regulate data protection issues between companies and their employees, voluntary services by an employer for his employees that require data processing of some sort were excluded by the proposed provision.

5 Differentiated Rules on Profiling

Commission proposal	**BITKOM Proposal**
Art. 20 (1) Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.	Art. 20 (1) Every natural person shall have the right not to be subject to a ***~~measure~~ decision*** which produces legal effects concerning this natural person ***~~or significantly affects this natural person~~***, and which is based solely on automated processing intended to evaluate ***~~certain personal aspects relating to this natural person or to~~*** analyse or predict the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.

Justification

Additional, distinct measures for processing of personal data through automated means are only justified for cases where the measure produces legal effects; any other profiling that constitutes processing of personal data is normal processing and already subject to all the provisions of the Regulation. The list in article 20 needs to be a closed one.

6 Controller and Processor

Art. 26 Processor

Commission Proposal	BITKOM Proposal
1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.	1. Where ***a*** processing ***operation*** is to be carried out on behalf of a controller ***and would involve personal data that would permit the processor to reasonably identify the data subject,*** the controller shall choose a processor providing sufficient ~~***guarantees***~~ ***assurances*** to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.
2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:	~~2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:~~
(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;	~~(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;~~
(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;	~~(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;~~
(c) take all required measures pursuant to Article 30;	~~(c) take all required measures pursuant to Article 30;~~
(d) enlist another processor only with the prior permission of the controller;	~~(d) enlist another processor only with the prior permission of the controller;~~
(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;	~~(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;~~
(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;	~~(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;~~
(g) hand over all results to the controller after the end of the processing and not process the personal data further after the end of the agreed processing otherwise;	~~(g) hand over all results to the controller after the end of the processing and not process the personal data further after the end of the agreed processing otherwise;~~
(h) make available to the controller and the supervisory authority all information necessary to	~~(h) make available to the controller and the supervisory authority all information necessary to~~

Justification

The proposed text introduces a host of new requirements for data processors and states how these should be included in the contractual arrangements. Some of these additions are unworkable in practice. For example, a controller may want to ensure that additional sub-processors - which may be numerous – apply effective data protection but it should be clear this does not mean they should assess each in turn prior to their employment. As the processor has the closer relationship, they are better placed to make such a judgment. In relation to handing over results at the end of processing, there may be no results as such to hand over if the data minimisation principle has been effectively applied. Making data available to the supervisory authority should be handled by the controller. Certain information may be subject to a confidentiality obligation under law or contract and hence a processor may not be at liberty to disclose such information to a supervisory authority. Moreover, such data should not be required to be transmitted on a regular basis as this would overburden authorities and further increase the administrative burden. Finally, Art 26(4) implies that the controller would need to provide very detailed instructions as to what personal data (data attribute by data attribute) the processor shall process. In reality, this is often not the case, yet based on this article the processor would carry the liability for not receiving extremely detailed instructions from the controller. Where a processor does breach such instructions, it is logical that the processor is considered a controller in respect of that processing but there is no reason to include the original data controller as a joint controller in this instance.

Art. 28 Documentation

Annex

Amendments to the Draft Data Protection Regulation
page 12

Commission Proposal	BITKOM Proposal
1.Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility.	1. Each controller ~~***and processor***~~ and, if any, the controller's representative, shall maintain documentation of ~~***all***~~ ***the main categories of*** processing ~~***operations***~~ under its responsibility.
2. The documentation shall contain at least the following information:	2. **Such** documentation shall contain at least the following information:
(a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;	(a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;
(b) the name and contact details of the data protection officer, if any;	(b) the name and contact details of the data protection officer, if any;
(c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);	(c) the **generic** purposes of the processing. ~~including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);~~
(d) a description of categories of data subjects and of the categories of personal data relating to them;	(d) a description of categories of data subjects and of the categories of personal data relating to them;
(e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;	((e) the ~~***recipients or***~~ categories of recipients of the personal data~~***. ,including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;***~~
(f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;	(f) where applicable, transfers of ***personal*** data to a third country or an international organisation~~,~~ ~~***including the identification of that third country or international organisation***~~ and, in case of transfers referred to in point (h) of Article 44(1), a reference to ~~***the documentation of appropriate***~~ safeguards ***employed***;
(g) a general indication of the time limits for erasure of the different categories of data;	(g) a general indication of the time limits for erasure ***or data retention policy applicable to*** ~~***of***~~ the different categories of data;
(h) the description of the mechanisms referred to in Article 22(3).	~~***(h) the description of the mechanisms referred to in Article 22(3).***~~
3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.	~~***3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on the basis of a request outlining the reasons for requiring access to the documents, to the supervisory authority.***~~
4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors:	4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers ~~***and processors***~~:

Justification

Effective data protection requires that organisations have sufficiently documented understanding of their data processing activities. The documentation requirement in Art 28.2 remains at rather high level and appears to largely duplicate the notification provisions in Art. 14.

Instead of satisfying bureaucratic needs, the aim of the documentation should be to help controllers and processors meet their obligations. Companies have many ways of documenting their data processing environment and no specific method should be mandated. Often such documentation exists through multiple means. A very detailed documentation procedure would remain an almost instantly outdated snapshot of a constantly changing reality characterized by complex data processing arrangements in a multiparty environment. Controllers cannot maintain detailed documentation of the IT architecture of the processors. Accordingly, processors should have an obligation to maintain such documentation of their processing. It should be left to the controllers and processors – in agreement with the lead DPA - based on the Accountability principle to determine which documentation is adequate and best suited for specific processing activities to comply with this Regulation and achieve the desired protection.

Recital 62

Commission Proposal	**BITKOM Proposal**
In order to demonstrate compliance with this Regulation, the controller or processor should document each processing operation. Each controller and processor should be obliged to co-operate with the supervisory authority and make this documentation, on request, available to it, so that it might serve for monitoring those processing operations.	In order to demonstrate compliance with this Regulation, the controller ~~***or processor***~~ should document ***different categories of*** ~~***each***~~ processing ~~***operation***~~ ***under its responsibility***. Each controller ~~***and processor***~~ should be obliged to co-operate with the supervisory authority and make this documentation, on request, available to it, so that it might serve for monitoring those processing operations.