Comments on Chapter IV – Part I Controller and processor

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.

Content

General problems

Article 22 (3a) and Recital 38 - Rules for data transfers of groups of undertakings

Data transfers between groups of undertakings are essential for efficient business management. The 95/46 Directive was missing a special provision for group-wide data processing and thereby not considering the economic cooperation and interaction of such legal entities organized in a group. This causes many problems for international companies:

Example: *Corporate groups of companies are not organized in the structure of their legal entities. Instead, workload is divided by specific product or project groups, especially with respect to human resources, customer management, legal department or other administrative purposes. In other terms, several employees might work cross-border under a project leader which is affiliated to another legal entity or central body. Therefore, it must be possible to exchange data and information of these central functions of corporate groups even without complex data protection contracts.*

Bitkom generally supports a provision which allows for data transfers within a group of undertakings as laid down in Art. 22 (3)(a) EP text and Recital 38a of the Council text.

Such clarification is urgently needed due to different interpretations within the EU member states by now: The German interpretation on the question whether companies can transfer data within a group of undertakings is very strict. In contrast, other countries (e.g. the UK) often have a different understanding which already allows for such data transfers as suggested by the EP and Council proposals. Therefore, there is a necessity for a clarification (as laid down in the EP and Council text). This will contribute to the intended goal of harmonization of the GDPR.

Bitkom proposal: In times of globalization companies are not only active "inside the Union" but also work across its borders on an international level. Therefore, such provision should make transfers also possible to countries where data is adequately protected ("adequacy decision by COM" or BCR as laid down in Chapter V). This should be regulated either in Article 3a) or in the context of Article 6 GDPR.

EP Version Article 22 (3a)	Council Version Recital 38	Bitkom Suggestion
3a) The controller shall have the right to transmit personal data inside the Union within the **group of undertakings** the controller is part of, where such processing is necessary for legitimate internal administrative purposes between connected business areas of the group of undertakings and an adequate level of data protection as well as the interests of the data subjects are safeguarded by internal data protection provisions or equivalent codes of conduct as referred to in Article 38.	38a) Controllers that are part of a **group of undertakings** or institution affiliated to a central body may have a legitimate interest to transmit personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country (...) remain unaffected.	**A simplified possibility for data transfers within group of undertakings in the EU or countries with adequate protection level should be installed:** **Option 1: Article 6 (2) + Definition of registered group of undertakings** - **Article 6 (2):** *If the controller is a legal person that is part of a registered group of undertakings and the provisions of Article 6 (1) are fulfilled, the controller may transfer personal data to other controllers that belong to the group.* - **Article 4 (16a) Definition registered group of undertakings**: *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*

		establishment of the EU. **Option 2: Article 3a) + Definition of registered group of undertakings** - **Article 3a)**: *The controller shall have the right to transmit personal data ~~inside the Union~~ within the registered group of undertakings (see definition above) the controller is part of, where such processing is necessary for legitimate internal administrative purposes between connected business areas of the group of undertakings and an adequate level of data protection as well as the interests of the data subjects are safeguarded by internal data protection provisions or equivalent codes of conduct as referred to in Article 38.* - **Recital 38a + Definition of registered group of** - **Recital 38a):** *Controllers that are part of a registered group of undertakings (see definition above) or institution affiliated to a central body may have a legitimate interest to transmit personal data within the registered group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country (...) remain unaffected.*

The term "written“ or „in writing“

The term “writing or written form” should be interpreted as under Art. 17 of Directive 95 /46 (“*in writing or in another equivalent (e.g. documented) form*”). This should be made clear. An interpretation according to Member States’ laws e.g. §126 BGB causes problems in the digital context.

Example:

EP Version Article 26	Council Version Article 26	Bitkom
1.Where processing 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 organisational measures governing the processing to be carried out and shall ensure compliance with those measures.	1. The controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a way that the processing will meet the requirements of this Regulation.	
	1a. The processor shall not enlist another processor without the prior specific or general written consent of the controller. In the latter case, the processor should always inform the controller on any intended changes concerning the addition or replacement of other processors, thereby giving the opportunity to the controller to object to such changes	1a. The processor shall not enlist another processor without the prior specific or general ~~written consent~~ ***permission*** of the controller. In the latter case, the processor should always inform the controller on any intended changes concerning the addition or replacement of other processors, thereby giving the opportunity to the controller to object to such changes.

General Obligations for controller and processor

Almost no company processes data only internally due to efficiency reasons. Instead, professional service providers perform tasks that cannot be fulfilled by companies themselves as they are often lacking competence and capacity.

Some of the provisions, for instance, **Article 30**, which introduces a legal obligation for the processor to implement appropriate technical and organizational measures, can be generally welcomed. Others provisions, as some sections of **Articles 24, 26, 28,** duplicate duties and obligations on information and documentation, and thereby inadequately increase the efforts of alignment documentation duties for both parties - controller and processor. Furthermore, other provisions **as Article 77**[1] **– in case of a joint and several liability -**, have such far-reaching consequences and negative implications on costs and administrative burden that the competition of the European economy in, for instance, the cloud computing sector is threatened. Especially in complex data processing environments, where different controllers and processors play a role in processing personal data (e.g. connected car), liability and responsibility must be clearly allocated, in order to avoid that some obligations or rights stemming from the Regulation are not ensured by any of the parties.

Bitkom calls on the legislators to take a coherent approach which takes due account of the Digital Single Market. Clear regulations for data processing are essential to the further development of areas such as cloud computing and value creation for the whole European economy. Whether new business models are rather promoted or obstructed depends on the practicality of these rules.

[1] Bitkom will comment on this in its position paper on Chapter VIII.

Controllers

Article 22 Responsibilities of the controller

Bitkom supports the approach that the controller should ensure and demonstrate compliance with the Regulation. The wording of the Council text is clear and precise and lays down all important elements of the responsibility of the data controller.

EP Version Article 22	Council Version Article 22	Bitkom
1. The controller shall adopt appropriate policies and implement appropriate and demonstrable technical and organisational measures to ensure and be able to demonstrate in a transparent manner that the processing of personal data is performed in compliance with this Regulation, having regard to the state of the art, the nature of personal data processing, the context, scope and purposes of processing, the risks for the rights and freedoms of the data subjects and the type of the organisation, both at the time of the determination of the means for processing and at the time of the processing itself. 1a) Having regard to the state of the art and the cost of implementation, the controller shall take all reasonable steps to implement compliance policies and procedures that persistently respect the autonomous choices of data subjects. These compliance policies shall be reviewed at least every two years and updated where necessary. **3**. The controller shall be able to demonstrate the adequacy and effectiveness of the measures referred to in paragraphs 1 and 2. Any regular general reports of the activities of the controller, such as the obligatory reports by publicly traded companies, shall contain a summary description of the policies and measures referred to in paragraph 1.	1. Taking into account the nature, scope context and purposes of the processing as well as the likelihood and severity of risk for the rights and freedoms of individuals, the controller shall implement appropriate measures and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation. 2a. Where proportionate in relation to the processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller. 2b. Adherence to approved codes of conduct pursuant to Article 38 or an approved certification mechanism pursuant to Article 39 may be used as an element to demonstrate compliance with the obligations of the controller **Deleted**	Bitkom generally supports the Council text. **Section 2a Council text**: Bitkom generally welcomes the reference to the proportionality principle. **Section 1a EP text:** Bitkom questions the practicability and necessity of prescribing a two-years period: ***These policies shall be reviewed ~~at least~~ ~~every two years~~ regularly and updated where necessary*** **Section 3 EP text:** This section is too vague and leads to legal uncertainty. It is not clear how the controller shall be able to demonstrate the effectiveness of the measures?

Article 24 Joint controllers

The proposal of the European Data Protection Supervisor's (EDPS) highlights contractual freedom between joint controllers which can distribute rights and obligations between them by means of an arrangement. In light of this contractual freedom, it must be also possible for joint controllers to determine (internally) who shall be liable vis-à-vis a third party, i.e. the data subject. The latter is generally not interested in the complex arrangement itself but only needs to know who he needs to address in case of a problem. This information must be clearly communicated to him.

Furthermore, the proposal highlights that "joint and several liability" is not the rule but the exception in the absence of an arrangement. It thereby gives the incentive for joint controllers to ensure a clear distribution of obligations and rights and adequately guarantees the data subject rights in certain cases.

Bitkom supports the proposal of the EDPS which strikes the right balance between private autonomy of joint controllers and the protection of the rights and freedoms of the data subject.

EP Version Article 24	Council Version Article 24	EDPS	Bitkom
1. Where several controllers jointly determine the purposes, and means of the processing of personal data, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them. The arrangement shall duly reflect the joint controllers' respective effective roles and relationships vis-à-vis data subjects, and the essence of the arrangement shall be made available for the data subject. In case of unclarity of the responsibility, the controllers shall be jointly and severally liable.	1. Where two or more controllers determine the purposes and means of the processing of personal data, they are joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 14 and 14a, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement shall designate which of the joint controllers shall act as single point of contact for data subjects to exercise their rights. 2. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the (...) controllers. 3. The arrangement shall duly reflect the joint controllers' respective effective roles and relationships vis-à-vis data subjects, and the	1. Where two or more controllers jointly determine the purposes and means of processing of personal data, they shall identify their respective responsibilities for compliance with the obligations under this Regulation in accordance with Union or Member State law, in particular as regards the exercising of the rights of the of the data subject and their respective duties by means of an arrangement between them. In the absence of an arrangement, the controllers shall be jointly and severally liable.	Bitkom generally supports the suggestions of the EDPS which modifies the EP version only slightly.

	essence of the arrangement shall be made available for the data subject. Paragraph 2 does not apply where the data subject has been informed in a transparent and unequivocal manner which of the joint controllers is responsible, unless such arrangement other than one determined by Union or Member State law is unfair with regard to his or her rights (...).		

Recital 62

Bitkom welcomes the clarification of the EP text as interpretation varies amongst Member States.

EP Version Recital 62	**Council Version Recital 62**	**Bitkom**
62) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processor, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller. **The arrangement between the joint controllers should reflect the joint controllers' effective roles and relationships.** **The processing of personal data under this Regulation should include the permission for a controller to transmit the data to a joint controller or to a processor for the processing of the data on his or her behalf.**	62) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processor, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, including where a controller determines the purposes, and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.	Bitkom supports the clarification of the EP text stating that for the transfer of data to the processor no additional legal permission is needed. The lack of harmonization within EU MS' practice renders such clarification important.

Processsors

Article 26 Processors

The Commission has generally proposed in Article 26 to make processors more accountable towards the controller by assisting them in ensuring compliance in particular with security and related obligations. The text introduces many new requirements for data processors and states how these should be included in the contractual arrangements. Some of these additions are unworkable in practice and therefore should be deleted:

Section 1 a – EP text

EP Version Article 26	Council Version Article 26	Bitkom
1.Where processing 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 organisational measures governing the processing to be carried out and shall ensure compliance with those measures.	1. The controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a way that the processing will meet the requirements of this Regulation. 1a. The processor shall not enlist another processor without the prior specific or general written consent of the controller. In the latter case, the processor should always inform the controller on any intended changes concerning the addition or replacement of other processors, thereby giving the opportunity to the controller to object to such changes	Bitkom supports Section 1 of the EP text as it is clearer, more unequivocal in formulation and highlights the data subject rights. **Bitkom highly supports the deletion of section 1a) Council text and does not recommend a compromise.**

Prescriptive one-size-fits-all requirements in law as laid down in Article 1a Council-text cannot take due account of the different data processing situations which significantly vary in complexity and nature. Prescribing compulsory written consent of the controller as well as mandatory information and opt-out requirement does not take account of whether such requirements are necessary, suitable or proportionate in the specific case:

Example: *The processor commissions a body to carry out the inspection or maintenance of its automated procedures or data processing systems, in the course of which the possibility of personal data being accessed cannot be excluded.*[2]

Example: *The processor instructs a sub-processor to change the operating system of a computer.*

Example: *A call-center wants to replace its telephone system.*

[2] In §11 Section 5 BDSG (German Data Protection Act) this specific case is regulated in contrast to the GDPR. Providers who do not have an interest in the data, but need to access them from time to time, e.g. for remote maintenance, should be generally exempted from Article 26 and 28. A corresponding regulation like §100 German Telecommunications Act should be integrated. It states that the service prover does not act as processor: "*As far as necessary, the service provider may generate and use the inventory data and traffic data of participants and users to identify isolate and remove errors*."

In such situations, where a possibility of access to personal data is relatively low, costs of stringent requirements are not proportionate to the benefits. In contrast, other situations definitely require that the processor informs the controller of intended changes concerning the addition or replacement of other processors.

Article 1a cannot adequately address thousands of data processing operations, where information and control rights between controller, processors and sub-processors need to be arranged according to the situation. These parties need a clear distribution of obligations and rights according to their contractual relations. It is e.g. important to adequately determine which criteria the processor has to take into account when choosing a sub-processor. Model contracts on data processing lay down in more detail which aspects need to be considered in a contractual relationship and can be tailored to meet the needs of different industries.

Bitkom supports a deletion of Article 1 a) as it significantly intervenes in the contractual freedom of controller and processor and prescribes requirements which cannot be applicable to all case constellations.

Article 26 Processors (Section 2 and 3)

EP Version Article 26	Council Version Article 26	Bitkom
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. The controller and the processor shall be free to determine respective roles and tasks with respect to the requirements of this Regulation, and shall provide that the processor shall:	2.The carrying out of processing by a processor shall be governed by a contract or legal act under Union or Member State law binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the rights of the controller and stipulating in particular that the processor shall:	**Section 2:** **EP text:** Positive addition in the EP text to highlight the freedom of contract and allows for the needed flexibility to adjust contractual terms to the context and particular circumstances. **Council text:** This addition is contrary to the goal of harmonization and will lead to different rules in MS.
a) process personal data only on instructions from the controller, unless otherwise required by Union law or Member State law;	a) process the personal data only on instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing the data, unless that law prohibits such information on important grounds of public interest;	**a) Deletion of Council text:** No necessity for such information requirement
	(h) make available to the controller (...) all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits conducted by the controller. The processor shall immediately inform the controller if, in his opinion, an instruction breaches this Regulation or Union or Member State data protection provisions.	Council text Similar under current German data protection law.
	2a) Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.	Bitkom supports the deletion of the red-highlighted Council text since it is in contradiction to the core principle of the legal construction of a controller-processor relationship.

Article 26 (4) – EP text

The consequence for the processor to become a controller with all right and duties if he processes data "other than instructed" or "becomes the determining party in relation to the purposes and means" must be rejected due to some practical considerations:

"Other than instructed": Such approach which does not allow the processor to change the data processing in a non-risk manner needs to be rejected. The Article 29 Group has also pointed out that the processor needs some flexibility regarding the data processing. Based on this Article the processor would carry the liability for the slightest change in data processing:

Example: *A call-center receives the instruction by its controller to call customers only until 5 pm. New Employee (A) forgets about this arrangement and calls customer (B) at 5.30 pm.*

Example: *Processor adapts its IT-security to the latest technologies and thereby processes the data other than instructed.*

Determining party in relation to the means: Art 26(4) implies that the controller would need to provide very detailed instructions as to what personal data the processor shall process. In practice, this is often not the case. Based on this Article the processor would carry the liability for not receiving highly detailed instructions from the controller:

Example: *The "means of data" protections are often not specifically determined in a contract (e.g. format, etc.). Does that mean that the processor becomes automatically a controller because he is the determining party of the "means"?!*

Where a processor does breach such instructions, it is logical that the processor is considered to be a controller (and possibly liable) in respect of that processing but there is no reason to include the original data controller as a joint controller in this instance.

Bitkom supports the deletion of Article 26 (4) EP text.

EP Version Article 26 (4)	**Council Version Article 26 (4)**	**Bitkom**
4. If a processor processes personal data other than as instructed by the controller or becomes the determining party in relation to the purposes and means of the data processing, the processor shall be considered to be a controller in respect of the processing and shall be subject to the rules on joint controllers as laid down in Article 24.	**Deleted**	**Bitkom highly supports the deletion of this section and does not recommend a compromise.** **Though, in case of a compromise Bitkom recommends to adapt the text:** *4. If a processor ~~processes personal data other than as instructed by the controller or~~ becomes the determining party in relation to the purposes and means of data processing, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers as laid down in Article 24.*

Article 28 Documentation

Effective data protection requires that legal entities have sufficiently documented understanding of their data processing activities. The documentation requirements in Art 28 remain at rather high level and appear 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 to 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.

Processors should have an obligation to maintain documentation of their processing in respect of their IT architecture. However, to avoid that documentation duties are generally duplicated which would increase the efforts of alignment documentation duties inadequately for both parties,

Bitkom supports the deletion of "processor" in Section 1 of Article 28. 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.

Article 28, Section 1

EP Version Article 28 Documentation	Council Version Article 28 Records of categories of personal data processing activities	Bitkom
1.Each controller and processor shall maintain regularly updated documentation necessary to fulfill the requirements laid down in this Regulation	1. **Each controller** and, if any, the controller's representative, shall maintain a record of all *categories of personal data* processing activities under its responsibility. This record shall contain the following information:	**Bitkom supports the deletion of the term processor.**