

Comments on Chapter VIII – Remedies, Liabilities and Sanctions

25/08/2015

Page 1

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.

Overview

Horizontal Topics:	3
Article 73 - Right to lodge a complaint with a supervisory authority.....	5
Court Proceedings	6
Article 76 – Representation of data subjects – Opening Clause for collective redress..	6
Article 77 Right to compensation and liability	8
Sanctions, Penalties, Administrative Fines	11

Horizontal Topics:

Vague legal terminology: Vague legal terms are used throughout Chapter VIII which go against a constituent and coherent approach of a European data protection.

Example Article 73 (2) EP Version: “Any body”

EP Version Article 73 Right to lodge a complaint with a supervisory authority	Council Version Article 73 Right to lodge a complaint with a supervisory authority	Bitkom
<p>2. <u>Any body, organisation or association which acts in the public interest</u> and has been properly constituted according to the law of a Member State shall have the right to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects if it considers that a data subject’s rights under this Regulation have been infringed as a result of the processing of personal data.</p>		<p>EP version: The term “acts in the public interest” is too vague. Member States have different constitutional traditions and different understandings on what is understood as “acting in the public interest”. This is contrary to the intended aim of harmonization.</p> <p>Bitkom suggestion: It must be further determined which entities shall have the right to lodge a complaint like “Any body, organization or association which <u>acts on behalf of the data subject</u>”.</p>

Example Article 77 (1): “Any person”

EP Version Article 77 Right to compensation and liability	Council Version Article 77 Right to compensation and liability	Bitkom
<p>1. <u>Any person</u> who has suffered damage, <u>including non-pecuniary damage</u>, as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to <u>claim</u> compensation from the controller or the processor for the damage suffered.</p>	<p>1. <u>Any person</u> who has suffered <u>material or immaterial</u> damage as a result of a processing which is not in compliance with this Regulation shall have the right to receive compensation from the controller or the processor for the damage suffered.</p>	<p>Legislators should not use different legal terms throughout the text. Reference to the “data subject” as defined legal concept is therefore preferable.</p> <p>Bitkom suggestion: “Any data subject”</p>

The term "written" or „in writing“: The term “in writing or in 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.¹

EP Version Article 77 Right to compensation and liability	Council Version Article 77 Right to compensation and liability	Bitkom
2. Where more than one controller or processor is involved in the processing, each <u>of those controllers or processors</u> shall be jointly and severally liable for the entire amount of the damage, <u>unless they have an appropriate written agreement determining the responsibilities pursuant to Article 24.</u>		

¹ Bitkom has commented on this in previous position papers: <https://www.bitkom.org/Themen/Vertrauen-Sicherheit/Datenschutz/Trilogverhandlungen/>.

Single Provisions:**Article 73 - Right to lodge a complaint with a supervisory authority**

EP Version Article 73 Right to lodge a complaint with a supervisory authority	Council Version Article 73 Right to lodge a complaint with a supervisory authority	Bitkom
<p>1. Without prejudice to any other administrative and judicial remedy <u>and the consistency mechanism</u>, every data subject shall have the right to lodge a complaint with a supervisory authority in any Member State if they consider that the processing of personal data relating to them does not comply with this Regulation.</p> <p>2. Any body, organisation or association which acts in the public interest and has been properly constituted according to the law of a Member State shall have the right to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects if it considers that a data subject's rights under this Regulation have been infringed as a result of the processing of personal data.</p> <p>3. Independently of a data subject's complaint, any body, organisation or association referred to in paragraph 2 shall have the right to lodge a complaint with a supervisory authority in any Member State, if it considers that breach <u>of this Regulation</u> has occurred.</p>	<p>1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a <u>single supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement, if the data subject considers that the processing</u> of personal data relating to him or her does not comply with this Regulation.</p> <p>2.Deleted</p> <p>3.Deleted</p> <p><u>5. The supervisory authority to which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 74 (...).</u></p>	<p>Bitkom supports the Council text.</p> <p>See comments above.</p>

Court Proceedings

Article 76 – Representation of data subjects – Opening Clause for collective redress

Collective redress, whereby a wide range of third party representatives can seek legal judicial remedies without any safeguards for the controllers and processors causes many problems:

- **Harmonization:** An opening clause as laid down in Article 77 (2) Council text, which allows for diverging laws on judicial redress in the Member States, undermines the intended goal of harmonization and level playing field in the GDPR. France and Germany², for instance, have already enacted new bills for privacy class actions on a national level in a derogatory way from the GDPR, whereas other Member States take a critical viewpoint.
- **Supervision by data protection authorities:** Data protection and consumer protection are overlapping but not identical. They have different protection goals, legally protected objects and underlying principles. Data protection authorities (DPAs), which are specifically assigned with powers by the Directive 95/56, are best placed to evaluate whether a data protection breach, which has been reported by the data subject, took place and whether to bring such case to a court.

In contrast, the development of national laws on judicial redress in Europe shows that a broad range of other third parties like consumer associations, chambers, etc. are granted with equal powers in the area of data protection law. Such parallel mechanism can trigger the independence of DPAs and lead to contradictions in interpretations. Furthermore, more institutions get insights into data processing processes, trade secrets or data of data subjects as such which have, in contrast to DPAs, no strong duty of confidentiality. There could be also reputation damage if e.g. consumer associations bring claims against companies even if accusations are subsequently proven unfounded. **Bitkom cautions against an opening clause, which would allow MS to grant similar rights to an unlimited range of third parties to lodge complaints and seek judicial remedies on behalf of the data subject.**

- **Concretely and directly affected data subjects:** Data protection rights are constructed as rights for persons who are concretely and directly affected. A mandate of the data subject to a DPA as, for instance, suggested in Section 1 of Article 76 EP version is needed. National laws, like the German proposal, allow for an abstract enforcement of rights by consumer associations and other entities without specific reference to the data subject itself. **Bitkom opposes this approach. DPAs and other associations should be entitled to represent only those that have given their consent on any action before court.**

² So called „Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von Verbraucherschützenden Vorschriften des Datenschutzrechts“.

EP Version Article 76 Common Rules for Court Proceedings	Council Version Article 76 Representation of the data subject	Bitkom
<p>1. Any body, organisation or association referred to in Article 73(2) shall have the right to exercise the rights referred to in Articles 74, 75 and 77 if mandated by one or more data subjects.</p> <p>2. Each supervisory authority shall have the right to engage in legal proceedings and bring an action to court, in order to enforce the provisions of this Regulation or to ensure consistency of the protection of personal data within the Union</p> <p>3. Where a competent court of a Member State has reasonable grounds to believe that parallel proceedings are being conducted in another Member State, it shall contact the competent court in the other Member State to confirm the existence of such parallel proceedings.</p> <p>4. Where such parallel proceedings in another Member State concern the same measure, decision or practice, the court may suspend the proceedings.</p> <p>5. Member States shall ensure that court actions available under national law allow for the rapid adoption of measures including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved.</p>	<p>1. The data subject shall have the right to mandate a <u>body, organisation or association, which has been properly constituted according to the law of a Member State and whose statutory objectives include the protection of data subjects' rights and freedoms with regard to the protection of their personal data, to lodge the complaint on his or her behalf</u> and to exercise the rights referred to in Articles 73, 74 and 75 on his or her behalf.</p> <p>2. <u>Member States may provide that any body, organisation or association referred to in paragraph 1, independently of a data subject's mandate (...), shall have in such Member State the right to lodge a complaint with the supervisory authority competent in accordance with Article 73 and to exercise the rights referred to in Articles 73, 74 and 75 if it considers that the rights of a data subject have been infringed as a result of the processing of personal data that is not in compliance with this Regulation.</u></p> <p>3. Deleted</p> <p>4. Deleted</p> <p>5. Deleted</p>	<p>Section 1 EP version: Bitkom denies the reference to Article 73 (2) “any body organization or association which acts in the public interest”. Suggestion: “Any body, organization or association which acts on behalf of the data subject”.</p> <p>Section 1 EP version “if mandated by one or more data subject”: There is a concern that the interpretation of this text also functions as opening clause for class action. If one person mandates its right, the body, organization or association should not be allowed to bring judicial proceedings of this data subject on behalf of others when they have not directly mandated the entity too.</p> <p>Section 1 Council version: Bitkom generally prefers Section 1 of the Council text.</p> <p>Section 2 Council Version: Bitkom strongly denies the opening clause in Section 2.</p> <ul style="list-style-type: none"> - Only if a data subject has mandated his right, no abstract enforcement of data protection rights - Right to a judicial remedy against a controller or processor (Art. 75) specifically needs to be deleted.

Article 77 Right to compensation and liability

Nowadays, almost no company processes data on its own due to efficiency reasons. Instead, professional service providers perform tasks which cannot be fulfilled by companies themselves as they often lack competence and capacity. Clear regulations for data processing are essential to the further development of cloud computing and value creation for the whole European economy. Whether new business models are promoted or rather obstructed depends on the practicality of these instructions.

A clear allocation of responsibility and liability between controller and processor is therefore essential. Today, not only German law but also the data protection directive prescribes a clear model, in which the responsibility and liability vis-à-vis the data subject lies with the controller. Neither industry nor regulators, including the Article 29 Working Party, have found any reason to think the current distinction is no longer relevant or workable. Blurred and mixed roles increase the cost and complexity of data processing, thereby delaying new business models and duplicating the complexity and cost for all concerned parties. **Bitkom strongly advocates moving away from a regime of joint and several liability.**

Data processing on behalf of the controller is central to all service providers not only in the ICT industry. The consequences of changing the current model are therefore extremely far reaching:

- **Call-Center:** *Companies (controller) often outsource their customer care or advertisement to external call-centers (processor). Those centers are then offering services based on the instructions they receive from the controller. In case the data processing is invalid, because e.g. the consent requirements are insufficiently fulfilled, not only the controller but also the processor becomes liable under a joint liability regime. However, it would be unduly difficult especially for small processors to control and check the controller's actions.*

The far-reaching consequences and negative implications on costs, administrative burden and competition for the European economy are often underestimated. Cloud service providers play an increasingly important role not only in the business environment but also in public administration:

Cloud Computing: *The processor very often does not have the possibility to verify the content of the data, e.g. if it only transmits them in an encrypted form, stores or archives them. In the case of cloud computing, an infrastructure provider has no access to the data processed in its container. Making the infrastructure provider responsible and liable for the data of its customers forces it to look into the data and thus contravenes the basic premise of data protection, i.e. to limit access to personal data.*

Bitkom fears that mixed and blurred responsibilities will have a significant negative impact on the Digital Single Market Strategy not only with respect to the cloud computing sector but also regarding innovations and technological developments:

Connected Car: *In the near future, manufacturers will increasingly supply digital services (in contrast to physical products) in a connected car; for example, map services, e-call, black boxes or autonomous driving systems. This processing chain gets even more complex if the data processor also works together with sub-processors. Under the current system the data subject needs to address his claim to the manufacturer of the car in case of a defect. This is reasonable because he also has a direct relationship via contract with the controller. Under a regime of joint and several liability the data subject could bring a claim against each small processor e.g. app developer which would become liable for the entire damage in the data processing chain.*

Comments on Parliament & Council Texts:

If a compromise between EP and Council text is to be struck, the following aspects should be taken into consideration:

- **Section I as general principle:** Section I of Article 77 should be understood as general principle that damage can be claimed by a data subject in case processing is not in compliance with this Regulation. It should not be understood as establishing a general system of joint and several liability.
- **Section II as special case of Section I:** Section II must highlight that “joint and several liability” is not the rule but the exception.
- **EP text:** The reference “in the absence of an arrangement” provides the incentive for ‘joint controllers’ to ensure a clear distribution of obligations and rights (private autonomy and freedom of contract) and adequately guarantees the data subject’s rights. Section 2 EP text could be extended to processors (Art. 26), so the ‘controller and processor’ only become jointly and severally liable when they have no appropriate agreement in place.
- **Council text:** Bitkom supports the consensus of the Council in Section 2 that in practice the controller should be primarily liable for damages suffered as a consequence of data protection violations. Processor liability could be limited to circumstance where e.g. the processor disregards contractual obligations or acts beyond the contract or other legally binding acts with the controller. These few cases of processor liability should be specifically spelled out.

However, the following sections 3, 4 and 5 still move towards a joint and several liability approach and should be reviewed.

Bitkom encourages EP and Council to look at the Opinion 1/2010 from the Article 29 Working Party on the concepts of “controller” and “processor”. (WP169) which promotes a clear allocation of responsibility and liability.

EP Version Article 77 Right to compensation and liability	Council Version Article 77 Right to compensation and liability	Bitkom
<p>1. Any person who has suffered damage, <u>including non-pecuniary damage</u>, as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to <u>claim</u> compensation from the controller or the processor for the damage suffered.</p> <p>2. Where more than one controller or processor is involved in</p>	<p>1. Any person who has suffered <u>material or immaterial</u> damage as a result of a processing which is not in compliance with this Regulation shall have the right to receive compensation from the controller or the processor for the damage suffered.</p> <p>2. <u>Any controller (...) involved in the processing shall be liable for the damage caused by the processing which is</u></p>	<p>Section 1 both texts suggestion: “Any data subject” - > see comments above</p> <p>Section 2 Council text: Could be a compromise.</p>

³ Opinion 1/2010 on the concepts of “controller” and “processor”: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

<p>the processing, each of those controllers or processors shall be jointly and severally liable for the entire amount of the damage, <u>unless they have an appropriate written agreement determining the responsibilities pursuant to Article 24.</u></p> <p>3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage.</p>	<p><u>not in compliance with this Regulation. A processor shall be liable for (...) the damage caused by the processing only where it has not complied with obligations of this Regulation specifically directed to processors or acted outside or contrary to lawful instructions of the controller.</u></p> <p>3. <u>A controller or the processor shall be exempted from liability in accordance with paragraph 2, (...) if (...) it proves that it is not in any way responsible (...), for the event giving rise to the damage.</u></p> <p>4. <u>Where more than one controller or processor or a controller and a processor are involved in the same processing and, where they are, in accordance with paragraphs 2 and 3, responsible for any damage caused by the processing, (...) each controller or processor shall be held (...) liable for the entire damage.</u></p> <p>5. <u>Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage in accordance with the conditions set out in paragraph 2.</u></p> <p>6. <u>Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under national law of the Member State referred to in paragraph 2 of Article 75.</u></p>	<p>Section 2 EP text: If version of EP is kept, Article 26 could be added in last sentence.</p> <p>Section 3 Council text: It is unclear what “in any way” should mean under legal terms. It should be therefore deleted.</p> <p>Section 3, 4, 5 of Council text: Should be reviewed again.</p>
--	--	--

Sanctions, Penalties, Administrative Fines

Strong integration of the proportionality principle: Sanctions should be applied by data protection authorities in a form which is reasonable, appropriate and proportionate. The proportionality principle should be strongly integrated in the text of the GDPR.

- **Discretionary Factors:** Bitkom welcomes the integration of discretionary factors such as the nature, gravity or duration of in-compliance and whether the infringement was intentional or negligent. Companies, which e.g. willfully do not comply with the Regulation (e.g. where non-compliance is used as a risk strategy and competitive advantage), must be treated differently than companies which negligently infringe the GDPR.
- **Level of sanctioning disproportionate to vagueness of rules:** The level of sanctioning (in the EP version up to 5% of the worldwide turnover) is disproportionate to the vagueness of some provisions in the GDPR (e.g. privacy by design).
- **Close cooperation with data processing entities:** DPAs should mainly focus on close cooperation with data processing entities to improve operational practices and prevent future data protection breaches. This will provide incentives for innovation as companies receive support to modernize and strengthen their data protection management. Especially Companies, outside the ICT sector and where the core business model is not directly linked to the collection and processing of data might negligently infringe the GDPR due to a lack of skills in this area.

— **Fines should be relevant and matched to data processing activities:**

- **“Turnover:”** Fines should not focus on worldwide “turnover” for the calculation. There are dramatic differences between the profit margins of trading companies and service providers. Companies with a higher turnover do not necessarily make profit. Start-ups in particular and new business models can be ruined by high penalties that are linked to turnover figures.
- **“Worldwide:”** Each controller or processor should be liable for its data processing and the infringements caused by its legal entity. Bitkom rejects the idea of global sanctioning.

EP Version 79 Administrative sanctions	Council Version 79 a) Administrative Fines	Bitkom
<p>1. Each supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article. <u>The supervisory authorities shall cooperate with each other in accordance with Article 46 and 57 to guarantee a harmonized level of sanctions within the Union.</u></p>	<p>1. The supervisory authority (...) <u>may</u> impose a fine <u>that shall not exceed</u> 250 000 EUR, or in case of an <u>undertaking</u> 0,5 % of its <u>total</u> worldwide annual turnover <u>of the preceding financial year, on a controller</u> who, intentionally or negligently:</p>	<p>Undertaking should be replaced by “enterprise” as this is defined in Art. 4 and this entity is usually is the same as the responsible controller. It is important that the <u>risk of fines lies with the company that acts as controller</u> – only this company can determine the circumstances of the processing and should thus be held responsible for faults and misuse.</p>