27 October 2015

Maintain clear and separate roles and responsibilities for controllers and processors

Dear GDPR trialogue stakeholders of the European Institutions,

The European Data Coalition acknowledges and respects the need to protect EU citizens' data. One aspect of such protection is that data subjects are able to claim compensation for damages resulting from data breaches. Chapter VIII on Remedies, Liabilities and Sanctions in the draft Regulation (GDPR) is central to establishing the roles of the data controller and processor in the data chain in a clear and predictable way.

This paper contains key observations regarding Article 77 of the GDPR made by the Coalition. It is our intention to both identify areas of concern, and also suggest solutions to guarantee the success of a data-driven innovation economy in Europe.

Proposed full joint and several liability of processor and controller

Under the current 95/46/EC Directive, the responsibility and liability vis-à-vis the data subject lies with the data controller. This system has stood the test of time as the consumer knows whom to turn to in case of a problem, and companies have clarity on roles and responsibilities. Therefore, the existing liability principles should be maintained in the new Regulation (GDPR). We strongly advise against the introduction of a "one-size-fits-all" joint liability solution that blurs the responsibilities in the data processing value chain, as the joint liability system in this context is misguided, produces disproportionate negative effects and offers questionable incremental value for data subjects. This position is based on the following considerations:

- **Processors should continue to assume direct liability, as is the case under the 95/46 Directive, when operating outside the instructions of a controller**: This merits reiteration. There is a misconception that processors that oppose joint liability take this stance to avoid responsibility. This is simply not true. In situations where a processor operates outside the contract with a controller, the processor is automatically a controller and assumes direct responsibility, as well as being subject to the penalties laid down in the processing contract.

- **The EU Data processing market is not broken and hence no controller is "forced" to choose a cost minimizing non-compliant processor**: The market provides an ample supply of compliant data processors for controllers to choose from. Therefore, the GDPR should continue to provide controllers with the right incentives to have clear, simple contractual arrangements with processors, as currently done under the 95/46 Directive.

- **Data Protection Authorities (DPAs) suggest more awareness is needed rather than change of roles and responsibilities:** Joint liability in this case attempts to fix a nonexistent problem. Decisions by European Data Protection Authorities have clarified[1] for both controllers and processors the requirements controllers must make of processors under the present 95/46 Directive. This indicates that the solution needed is increased awareness rather than a change of roles and responsibilities.

- **The 95/46 Directive is explicit that controllers bear responsibility towards the data subject**: As the controller is the organisation that collects the data in the first place, it is logical that this entity should bear the responsibility for defining the appropriate legal basis and purpose of the processing, and ensuring that if such processing is outsourced to another party (the processor), appropriate contractual safeguards are put in place.

  The user is not necessarily aware of how exactly the processing of its data is handled, and should not be required to have a full understanding of this process. From his/her perspective, the entity to which he/she entrusted the data should bear full responsibility for ensuring that it is appropriately protected and handled according to the purpose and legal ground it was collected for.

  Furthermore, the processor only disposes of the information entrusted to it by the controller. Introducing joint liability would force the processor to seek out additional information, which could create prohibitive information costs for the processor under conditions of information asymmetry.

  The processor should be responsible if it does not respect its contractual or legal obligations. However, the user should not be put in the potentially impossible situation of having to understand the dynamics between the controller and processor, understand what went wrong, who is responsible, etc. As mentioned above, controllers ensure they choose a processor that is able to handle the data entrusted on the controller with care, and that will bear its responsibility vis-a-vis the controller in case of a problem. There is enough choice on the market to be able to achieve this.

- **Offering processing solutions is not the same as offering defective products causing harm**: A database service or other processing service is intrinsically neutral and has no inherent safety risk. Any risk depends on the usage and as such the instructions given by the controller. It is important to bear in mind that the controller is the only party with the full information on the intended purpose and use of the data, as well as on the information communicated to the data subject. The processing may be perfectly fit for one usage but inappropriate for another.

- **Joint liability clashes with the data minimisation principle**. **A processor would need to have the same information as the controller in order to be able to determine whether it can offer a particular service and accept joint liability.** As described above, and in line with the data minimisation principle, the processor does not have the full information on the processing activity, only the residual information that the controller choses to communicate and share with it. Sharing additional information may also expose the controller to information disclosure that it considers to be trade secrets, increasing the risk of cybersecurity threats for all European based data processing.

[1] Example see: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140402_microsoft.pdf

- **The Article 29 Working Party has also expressed its doubts concerning the concept**, stating that joint liability is burdensome and risks preventing controllers from using standard contractual clauses.[2]

We understand that the joint liability proposal aims to protect data subjects in cases where the controller has ceased to exist. We agree that in such unique cases, the data subject must be protected and we believe that the 2010 model clauses provide an effective solution to such a situation[3]. In the event that a controller disappears, the data subject can turn to the processor through a scheme of subsidiary liability. This means that a data subject is guaranteed redress in all circumstances.

Support for the Council's version, provided clarifications are introduced

The contributions from the European Parliament and the Council have introduced some improvements, as both move away from a regime of full joint and several liability. However, the Parliament's text still does not adequately clarify the different roles and responsibilities held by the controller and processor in the data chain.

We agree with the Council's approach that in the case of data breaches, it is the data controller that should be primarily liable for damages. Direct processor liability should be limited to when the processor operates outside of a contract with a controller.

The Council's version, which we believe is the strongest available, does however contain some weaknesses that were perhaps overlooked and should still be improved upon. The combination of paragraphs 2 and 3 of Article 77 as proposed by the Council would imply a reverse burden of proof whereby the data processor would have to prove "*that it is not in any way responsible (…), for the event giving rise to the damage*". In the case that neither the controller nor the processor could prove their innocence, it would result from paragraph 4 that the "*controller or processor shall be held (…) liable for the entire damage*", meaning that the data subject could still direct its full claims to anyone involved in the data chain.

European Commission	European Parliament	Council	Coalition's Proposed Compromise
ARTICLE 77			
Right to Compensation and Liability	**Right to Compensation and Liability**	**Right to Compensation and Liability**	**Right to Compensation and Liability**
1. Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the	1. Any person who has suffered damage**, including non-pecuniary damage,** as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the	1. Any person who has **suffered material or immaterial** damage as a result of ~~an unlawful~~ **a** processing ~~operation or of an action incompatible~~ **which is not in compliance** with this	1. Any ~~person~~ **data subject** who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive

[2] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp84_en.pdf

[3] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF

controller or the processor for the damage suffered. 2. Where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage. 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.	right to ~~receive~~ **claim** compensation from the controller or the processor for the damage suffered. 2. Where more than one controller or processor is involved in the processing, each **of those** controller**s** or processor**s** shall be jointly and severally liable for the entire amount of the damage**, unless they have an appropriate written agreement determining the responsibilities pursuant to Article 24**. 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.	Regulation shall have the right to receive compensation from the controller or the processor for the damage suffered. 2. ~~Where more than one~~ **Any** controller ~~or processor is~~ involved in the processing ~~each controller or processor~~ shall be ~~jointly and severally~~ liable for ~~the entire amount of~~ the damage **caused by the processing which is 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.** 3. ~~The~~ **A** controller or the processor ~~may~~ **shall** be exempted from ~~this~~ liability ~~in whole or in part~~ **in accordance with paragraph 2**, if ~~the controller or the processor~~ **it** proves that ~~they are~~ **it is** not **in any way** responsible, for the event giving rise to the damage. 4. Where more than one controller or processor **or a controller and a processor** ~~is~~ **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 ~~jointly and severally~~ **held** liable for the entire ~~amount of the~~ damage**.** **5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that**	compensation from the controller ~~or the processor~~ for the damage suffered. 2. Where more than one controller ~~or processor~~ is involved in the processing, each controller ~~or processor~~ shall be ~~jointly and severally~~ liable for the entire amount of the damage**, unless they have an appropriate written agreement determining the responsibilities pursuant to Article 24. A processor shall be liable for the damage caused by the processing only where it acted outside or contrary to lawful instructions of the controller.** 3. The controller or the processor ~~may~~ **shall** 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. **4. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the controller, because the controller has ceased to exist in law, the data subject may issue a claim against the processor for harm caused by it and for which the processor was responsible, unless any successor entity has assumed the respective legal obligations of the data controller by contract of by operation of law, in which case the data subject can enforce its rights against such entity.**

		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. **6. 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.**	

Conclusion

The Coalition does not support a system with joint and several liability for both the controller and processor, as this would impose significant burdens upon companies, be fundamentally unfair and disproportionate, and create confusion in the data chain.

The Council's proposed amendments are an improvement on the Commission's text, provided clarifications are introduced in paragraphs 2, 3 and 4. This clarifications should ensure that the processing entity is only liable when operating outside of its contract with the data controller, having thereby assumed direct responsibility for any eventual damage.

Yours sincerely,

Rene Summer
Coalition Spokesperson

ABOUT THE COALITION

Our Coalition is made up of nineteen European companies, from SMEs to Global Multinationals and non-profit organisations operating in a variety of sectors on a national, regional and global scale. With an aggregate turnover (2013) of over € 158 billion and some 752,000 employees worldwide, our footprint allows us to bring growth, progress and jobs to the EU's economy. Our membership includes…

… a global leader in power and automation solutions…
… the leading Central and Eastern European e-commerce company…
… a productivity solutions provider of compressors, vacuum solutions, construction and mining equipment…
… a non-profit organisation dedicated to collecting money to prevent and combat child cancer diseases…
… a global leader in household appliances…
… two providers of communications technology and services…
… a designer, engineer, manufacturer and distributor of outdoor power products…
… an investment company…
… a SME provider of online marketing through search engine marketing, conversion and lead generation…
… an e-commerce company providing payment services for online storefronts…
… an engineering group in tooling, materials technology, mining and construction …
… an enterprise software corporation…
… a global provider of heavy trucks and buses, engines and services…
… a global provider of renewable solutions in packaging, biomaterials, wood and paper…
… the leading university in technology and digital arts programmes…
… a provider of business software and services to more than 340 000 business in the Nordics…
… a producer and distributor of trucks, buses and construction equipment…
… the leading company in advanced mobile services…

Our businesses are profoundly different but deeply united by the need for clear roles and responsibilities, open cross-border data flows, balanced codified sanction guide lines, effective one stop shop and absence of overly prescriptive rules as fundamental conditions for long-term growth, competitiveness and prosperity, for both us and the economies in which we operate.

For further information please visit us www.europeandatacoalition.eu or contact us at info@europeandatacoalition.eu