37

PROCESSOR OBLIGATIONS AND LIABILITIES

Proposed amendments

We welcome the progress made on the various aspects of the draft General Data Protection Regulation. However, we believe that further changes are necessary to clarify the obligations and liabilities of data processors.

To that end, below we propose amendments to Articles 77 (right to compensation), 28 (records of categories of personal data processing activities), 30 (security of processing), 33 (data protection impact assessment) and 34 (prior authorization and prior consultation), taking into account the text partially endorsed by the Council in October 2014, the European Parliament amendments, and the Commission's original text[1].

The amendments below focus exclusively on the provisions in the proposal for a General Data Protection Regulation that are directly relevant to the question of processor liability. The fact that we do not offer comments on a particular provision should not be considered an endorsement of these provisions.

Our proposed amendments are marked in red italics, and our deletions are also in red and marked with ~~strikethrough~~. We also indicate in red where our amendments are proposed compromise amendments (integrating text of all three institutions) and where they are proposed amendments to the European Parliament or Council text.

Article 77

(Right to compensation and liability)

Commission text	EP text	Council text (3 October 2014)	Compromise amendment
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 controller or the processor for the damage suffered.	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 right to ***claim*** compensation from the controller or the processor for the damage suffered.	1. Any person who has suffered damage as a result of ~~**an unlawful**~~ processing operation ~~**or of an action incompatible**~~ **which is not in compliance** with this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.	1. Any 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~~ *claim* compensation from the controller ~~or the processor~~ for the damage suffered.

[1] As we agree with the Council's proposal to delete Article 29 (co-operation with the supervisory authority), no amendments are proposed to these provisions.

Commission text	EP text	Council text (3 October 2014)	Compromise amendment
			1a. Where the data subject can demonstrate that the damage suffered has been directly caused by a processor having acted outside or contrary to the controller's instructions, the data subject shall have the right to claim compensation from the processor for such damage.
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.	2. Where more than one controller or processor is involved in the processing, each ***of those controllers or processors*** shall be jointly and severally liable for the entire amount of damage ***unless they have an appropriate written agreement determining the responsibilities pursuant to Article 24***.	2. Where more than one controller or processor **or a controller and processor are ~~is~~** involved in the processing **which gives rise to the damage**, each controller or processor shall be jointly and severally liable for the entire amount of damage. **This is without prejudice to recourse claims between controllers and/or processors.**	2. Where more than one controller is involved in the processing, each controller shall be jointly and severally liable with the other for the entire amount of the damage
			2a. Where more than one processor is involved in the processing, each processor shall be liable only for the damage it has caused directly and as a result of having acted outside or contrary to the controller's instructions.
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.	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.	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.	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~~ *it is* not responsible for the event giving rise to the damage.

Article 28

(Records of categories of personal data processing activities)

Commission text	EP text	Council text (3 October 2014)	Amendment to Council text
4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors: (a) a natural person processing personal data without a commercial interest; or (b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.	***delete***	4. The obligations referred to in paragraphs 1 and 2a shall not apply to: (a) (...); or (b) an enterprise or a body employing fewer than 250 persons, unless the processing it carries out is likely to result in a high risk for the rights and freedoms of data subject such as (...) discrimination, identity theft or fraud, [breach of (...) pseudonymity,] financial loss, damage to the reputation, loss of confidentiality of data protected by professional secrecy or any other economic or social disadvantage for the data subjects, taking into account the nature, scope, context and purposes of the processing; or	4. The obligations referred to in paragraphs 1 and 2a shall not apply to: (a) (...); or (b) an enterprise or a body employing fewer than 250 persons, unless the processing it carries out is likely to result in a high risk for the rights and freedoms of data subject such as (...) discrimination, identity theft or fraud, [breach of (...) pseudonymity,] financial loss, damage to the reputation, loss of confidentiality of data protected by professional secrecy or any other economic or social disadvantage for the data subjects, taking into account the nature, scope, context and purposes of the processing; or *(c) tasks where any processing of personal data is nominal and incidental and presents no risk to data subjects.*

Article 30

(Security of processing)

Commission text	EP text	Council text	Amendment to EP text
1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal	1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing, ***taking into account the results of a data protection impact***	1. **Having regard to available technology and the costs of implementation and taking into account the nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for the rights and freedoms**	1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing, ***taking into account the***

Commission text	EP text	Council text	Amendment to EP text
data to be protected, having regard to the state of the art and the costs of their implementation.	***assessment pursuant to Article 33***, having regard to the state of the art and the costs of their implementation.	**of individuals**, the controller and the processor shall implement appropriate technical and organisational measures, **[including (...) pseudonymisation of personal data]** to ensure a level of security appropriate to the risk ~~represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation~~.	***results of a data protection impact assessment pursuant to Article 33***, having regard to the state of the art and the costs of their implementation.
	1a. Having regard to the state of the art and the cost of implementation, such a security policy shall include: ***(a) the ability to ensure that the integrity of the personal data is validated;*** ***(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data;*** ***(c) the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident that impacts the availability, integrity and confidentiality of information systems and services;*** ***(d) in the case of sensitive personal data processing according to Articles 8 and 9, additional security measures***	**1a. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by data processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.**	1a. Having regard to the state of the art, *the respective roles of the controller and processor,* and the cost of implementation, such a security policy shall include: *(a)-(e) EP text* ***support***

Commission text	EP text	Council text	Amendment to EP text
	to ensure situational awareness of risks and the ability to take preventive, corrective and mitigating action in near real time against vulnerabilities or incidents detected that could pose a risk to the data; ***(e) a process for regularly testing, assessing and evaluating the effectiveness of security policies, procedures and plans put in place to ensure ongoing effectiveness.***		
2. The controller and the processor shall, following the evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data.	2. The ~~controller and the processor shall, following an evaluation of the risks, take the~~ measures referred to in paragraph 1 ~~to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data~~ ***shall at least:*** ***(a) ensure that personal data can be accessed only by authorised personnel for legally authorised purposes;*** ***(b) protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure; and***	~~2. The controller and the processor shall, following the evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data.~~	2. The ~~measures referred to in paragraph 1 shall at least~~ *processor shall, as it deems appropriate and permissible under business confidentiality requirements, provide to controllers information explaining how the processor protects personal data against accidental destruction or accidental loss and how it prevents any unlawful forms of processing, in particular any unauthorized disclosure, dissemination or alteration of or access to personal data.* *(a)-(c) EP text* ***delete***

Commission text	EP text	Council text	Amendment to EP text
	(c) ensure the implementation of a security policy with respect to the processing of personal data.		

Article 33

(Data protection impact assessment)

Commission text	EP text	Council text	Amendment to EP text
1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.	1. Where ~~processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes,~~ ***required pursuant to point (c) of Article 32a(3)*** the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the ***rights and freedoms of the data subjects, especially their right to*** protection of personal data. ***A single assessment shall be sufficient to address a set of similar processing operations that present similar risks.***	1. Where **a type of** processing, **in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, damage to the reputation, [breach of (...) pseudonymity], loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage,** the controller **(...)** shall, **prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.**	1. Where ~~*required pursuant to point (c) of Article 32a(3)*~~ the controller ~~*or the processor acting on the controller's behalf carry out an assessment of the impact of the envisaged*~~ *assesses that the nature, scope and purpose of* envisaged processing operations ~~*on the*~~ *present specific risks to* the rights and freedoms of data subjects, especially their right to protection of personal data, *the controller shall inform the processor.* ~~*A single assessment shall be sufficient to address a set of similar processing operations that present similar risks.*~~ *The controller may request that the processor conduct a separate assessment of the impact of the processing operation on the right to the protection of personal data in relation to the specific processing operations for which the processor is responsible.*

Article 34(8) new

(Prior authorisation and prior consultation)

Commission text	EP text	Council text	Amendment to EP text
			8. The controller shall be primarily responsible to comply with the obligations set out in points 2 and 6 of this Article 34. The processor shall be responsible to comply with these obligations only when requiring the controller to do so would be unfair and unreasonable taking into account all circumstances.