

# KEEP EUROPE GROWING

27 October 2015

## **Adopt a proportionate sanctions regime**

### **Dear GDPR triologue 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 the introduction of reasonable administrative fines. It is indeed in the private interest of both citizens and accountable companies to have a Regulation (GDPR) which works to penalise those unethical enterprises who use non-compliance as a competitive advantage over responsible companies.

This paper contains key observations of Article 79 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 Sanction Regime

The GDPR suggests basing penalties on global turnover, including revenues that are entirely unrelated to data processing. The resulting penalties, without clear, codified sanctions guidelines, could be completely disproportionate to the extent of the data processing, and the extent of any non-compliance that actually occurs. This will diminish incentives for data-driven innovation for global companies as well as discouraging "old-economy" companies from digitising and modernising.

The main focus of enforcement should be on the increased detection of data breaches and the promotion of feedback from industry so as to improve operational practices, codes of conduct, etc. Deterrence through fines and sanctions is necessary in some instances to make the Regulation credible, however it should not become de-facto the main enforcement tool when dealing with well-intended and accountable companies.

Better enforcement would ensure the implementation of the rules and users' rights by adopting sanctions against those actors, who wilfully or in a grossly negligent way do not fulfil the data protection rights of their users. Blanket fines without a case-by-case examination are counterproductive.

### Support for the Council's proposal, provided clarifications are introduced

The Coalition supports the idea that fines should be proportional and capped, and that the basis used to calculate fines should be relevant and matched to data processing activities. We are firmly against the idea of using global turnover as reference. We support the Council's position provided the basis

for the calculation of fines is reviewed. On the positive side, this position lowers the level of sanctions, adds discretionary factors and defines more precisely the conditions for sanctions to be applied.

The Coalition further recommends the development and introduction of codified and reasonable sanction guidelines into the GDPR, based on the following principles:

- Role of Data Protection Authorities (DPAs)
  - DPAs should follow a clear enforcement pyramid, i.e. Information; Persuasion; Warning letter; and Civil sanction.
  - DPAs should only have the right to engage in civil sanctions if serious harm is caused to the data subject or if the controller has disregarded previous warning letters, provided that there is a serious risk for the individual. The mere breach of formalistic requirements without supporting evidence of a damage to data subjects should not lead to civil sanctions.
  - Only the lead authority should have the power to issue penalties, consistent with the agreed one-stop-shop-model.
  
- Proportional Fines
  - Fines should be zero or minimal if the concerned organisation has taken serious steps to act responsibly and mitigate risks in its data processing activities.
  - Fines should be proportional and there should be a monetary cap limiting the absolute size of penalties.
  - Reiterated infringements should be considered as aggravating circumstances resulting in heavier sanctions up to the maximum limited established in the GDPR.
  - The basis used to calculate fines should be relevant and matched to data processing activities in order to avoid bias against diversified and specialized enterprises. The global turnover of an enterprise is an entirely unfair basis of reference which could lead to disproportionate fines for companies for which data processing is only a small fraction of their business.
  
- Funding Through Fines
  - DPAs should not finance their activities with fines accrued from civil sanctions. All proceeds from civil sanctions should be used for certification institutes and on other means to enhance privacy.

European Commission	European Parliament	Council	Coalition’s Proposed Compromise
<b>ARTICLE 79</b>			
<b>Administrative sanctions</b>	<b>Administrative sanctions</b>	<b>General Conditions for Imposing Administrative Fines</b>	<b>General Conditions for Imposing Administrative Fines</b>
1. Each supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article.	1. Each supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article. <b>The supervisory authorities shall co-</b>	1. Each supervisory authority shall be <del>empowered to impose</del> <b>ensure that the imposition of administrative sanctions</b> <del>in accordance with</del>	1. <del>Each</del> <b>The lead</b> supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article.

<p>2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of co-operation with the supervisory authority in order to remedy the breach.</p> <p>3. In case of a first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed, where:</p> <p>(a) a natural person is processing personal data without a commercial interest; or</p> <p>(b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.</p> <p>4. The supervisory authority shall impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently:</p> <p>(a) does not provide the mechanisms for requests by data subjects or does not respond promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2);</p>	<p><b>operate with each other in accordance with Articles 46 and 57 to guarantee a harmonized level of sanctions within the Union.</b></p> <p>2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. <del>The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of co-operation with the supervisory authority in order to remedy the breach.</del></p> <p><b>2a. To anyone who does not comply with the obligations laid down in this Regulation, the supervisory authority shall impose at least one of the following sanctions:</b></p> <p><b>(a) a warning in writing in cases of first and non-intentional non-compliance;</b></p> <p><b>(b) regular periodic data protection audits;</b></p> <p><b>(c) a fine up to 100 000 000 EUR or up to 5% of the annual worldwide turnover in case of an enterprise, whichever is higher.</b></p> <p><b>2b. If the controller or the processor is in possession of a valid ‘European Data Protection Seal’ pursuant to Article 39, a fine pursuant to point (c) of paragraph 2a shall only</b></p>	<p><b>pursuant to this Article in respect of infringements of this Regulation referred to in Article 79a shall in each individual case be effective, proportionate and dissuasive.</b></p> <p><b>2a. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (f) of paragraph 1b of Article 53. When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:</b></p> <p><b>(a) the nature, gravity and duration of the infringement having regard to the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;</b></p> <p><b>(b) the intentional or negligent character of the infringement,</b></p> <p><b>(d) action taken by the controller or processor to mitigate the damage suffered by data subjects;</b></p> <p><b>(e) the degree of responsibility of the controller or processor having regard to technical and organisational measures implemented by them pursuant to Articles 23 and 30;</b></p> <p><b>(f) any relevant previous infringements by the controller or processor;</b></p> <p><b>(h) the manner in which the infringement became known to the supervisory authority, in particular</b></p>	<p>2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, <b>the actual harm or risk of harm to the data subject</b>, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of co-operation with the supervisory authority in order to remedy the breach.</p> <p>3. In case of a first <del>and non-intentional</del> non-compliance with this Regulation, a warning in writing may be given and no sanction <b>shall be</b> imposed, where any of the following criterias is fulfilled:</p> <p><del>(a) a natural person is processing personal data without a commercial interest; or</del></p> <p><del>(b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.</del></p> <p><b>(a) non-compliance does not cause serious harm to the data subject;</b></p> <p><b>(b) non-compliance only impacts a small number of data subjects;</b></p>
---	--	---	--

<p>(b) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4).</p> <p>5. The supervisory authority shall impose a fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, intentionally or negligently:</p> <p style="text-align: center;">(...)</p> <p>6. The supervisory authority shall impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently:</p> <p style="text-align: center;">(...)</p> <p>7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of updating the amounts of the administrative fines referred to in paragraphs 4, 5 and 6, taking into account the criteria referred to in paragraph 2.</p>	<p>be imposed in cases of intentional or negligent <b>incompliance</b>.</p> <p>2c. The administrative sanction shall take into account the following factors:</p> <p>(a) the nature, gravity and duration of the <b>incompliance</b>,</p> <p>(b) the intentional or negligent character of the <b>infringement</b>,</p> <p>(c) the degree of responsibility of the natural or legal person and of previous breaches by this person,</p> <p>(d) the repetitive nature of the <b>infringement</b>,</p> <p>(e) the degree of co-operation with the supervisory authority, in order to remedy the <b>infringement</b> and mitigate the possible adverse effects of the <b>infringement</b>,</p> <p>(f) the specific categories of <b>personal data affected by the infringement</b>,</p> <p>(g) the level of damage, including non-pecuniary damage, suffered by the data subjects,</p> <p>(h) the action taken by the controller or processor to mitigate the damage suffered by data subjects,</p> <p>(i) any financial benefits intended or gained, or losses avoided, directly or indirectly from the <b>infringement</b>,</p> <p>(j) the degree of technical and organisational measures and procedures implemented pursuant to:</p> <p>(i) Article 23 - Data protection by design and by default</p>	<p>whether, and if so to what extent, the controller or processor notified the <b>infringement</b>;</p> <p>(i) in case measures referred to in point (b) and (c) of paragraph 1 and points (a), (d), (e) and (f) of paragraph 1b of Article 53, have previously been ordered against the controller or processor concerned with regard to the same subject-matter<sup>586</sup>, compliance with these measures ;</p> <p>(j) adherence to approved codes of conduct pursuant to Article 38 or approved certification mechanisms pursuant to Article 39;</p> <p>(m) any other aggravating or mitigating factor applicable to the circumstances of the case.</p> <p>3. In case of a first and non-intentional <del>non-compliance with this Regulation</del>, a warning in writing may be given and <del>no sanction imposed</del>, where:</p> <p>3b. Each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.</p> <p>4. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in conformity with Union law and Member State law, including effective judicial remedy and due process.</p> <p>5. Member States may abstain from providing rules for administrative fines as referred to in</p>	<p>(c) the non-compliance is non-intentional.</p> <p>4. When sanctions are not ruled out due to Article 79(3), the supervisory authority shall <b>may, taking into due consideration Article 79(2)</b>, impose a fine <del>up to</del> <b>between 100 EUR and 250 000 EUR</b>, <del>or in case of an enterprise up to 0,5 % of its annual worldwide turnover</del>, to anyone who, intentionally <del>or negligently</del>:</p> <p>(a) does not provide the mechanisms for requests by data subjects or does not respond promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2);</p> <p>(b) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4).</p> <p>5. The supervisory authority shall <b>may, taking into due consideration Article 79(2)</b> impose a fine up to 500 000 EUR, <del>or, in case of an enterprise up to 2 % of its annual worldwide turnover</del>, to anyone who, intentionally <del>or negligently</del>:</p> <p style="text-align: center;">(...)</p> <p>6. The supervisory authority shall <b>may, taking into due consideration Article 79(2)</b> impose a fine up to 10 000 000 EUR <del>or, in case of an enterprise up to 2 % of its annual worldwide turnover</del>, to anyone who, intentionally <del>or negligently</del>:</p> <p style="text-align: center;">(...)</p> <p>7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of updating the amounts of</p>
--	--	--	---

	<p>(ii) Article 30 - Security of processing</p> <p>(iii) Article 33 - Data protection impact assessment</p> <p>(iv) Article 33 a - Data protection compliance review</p> <p>(v) Article 35 - Designation of the data protection officer</p> <p>(k) the refusal to cooperate with or obstruction of inspections, audits and controls carried out by the supervisory authority pursuant to Article 53,</p> <p>(l) other aggravating or mitigating factors applicable to the circumstance of the case.</p> <p><del>3. In case of a first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed, where:</del></p> <p><del>(a) a natural person is processing personal data without a commercial interest; or</del></p> <p><del>(b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.</del></p> <p><del>4. The supervisory authority shall impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently:</del></p> <p><del>(a) does not provide the mechanisms for requests by data subjects or does not respond promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2);</del></p> <p><del>(b) charges a fee for the information or for</del></p>	<p>paragraphs 1, 2 and 3 of Article 79a where their legal system does not provide for administrative fines and the infringements referred to therein are already subject to criminal sanctions in their national law by [date referred to in Article 91(2)], while ensuring that these criminal sanctions are effective, proportionate and dissuasive, taking into account the level of administrative fines provided for in this Regulation.</p> <p>Where they so decide, Member States shall notify, to the Commission, the relevant parts of their criminal law.</p> <p style="text-align: center;"><b>Article 79a</b></p> <p>1. The supervisory authority <del>shall</del> <b>may</b> impose a fine <del>up to that shall not exceed</del> 250 000 EUR, or in case of an enterprise <del>undertaking up to</del> 0,5 % of its <del>total</del> worldwide annual turnover, <del>to anyone of the preceding financial year, on a controller</del> who, intentionally or negligently:</p> <p>(a) does not respond <del>the mechanisms for requests by data subjects or does not respond promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2)</del> <b>within the period referred to in Article 12(2) to requests of the data subject;</b></p> <p>(b) charges a fee in violation of <b>the first sentence of paragraph 4 of Article 12.</b></p> <p>52. The supervisory authority <del>shall</del> <b>may</b> impose a fine <del>up to that shall not exceed</del> 500 000 EUR, or in case of an</p>	<p><del>the administrative fines referred to in paragraphs 4, 5 and 6, taking into account the criteria referred to in paragraph 2.</del></p>
--	---	---	---

	<p>responses to the requests of <del>data subjects</del> in violation of Article 12(4).</p> <p>5. The supervisory authority shall impose a fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its <del>annual worldwide</del> turnover, to anyone who, intentionally <del>or</del> negligently:</p> <p>(...)</p> <p>6. The supervisory authority shall impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its <del>annual worldwide</del> turnover, to anyone who, intentionally <del>or</del> negligently:</p> <p>(...)</p> <p>7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of updating the <b>absolute</b> amounts of the administrative fines referred to in paragraphs 4, 5 and 6 <b>paragraph 2a</b>, taking into account the criteria <b>and factors</b> referred to in paragraphs 2 <b>and 2c</b>.</p>	<p>enterprise <b>undertaking</b> up to 1 % of its total worldwide annual turnover, <del>to anyone of the preceding financial year, on a controller</del> or processor who, intentionally or negligently:</p> <p>(...)</p> <p>63. The supervisory authority may impose a fine <del>up to</del> <b>that shall not exceed</b> 1 000 000 EUR or, in case of an enterprise <b>undertaking</b> up to 2 % of its <b>total</b> worldwide annual turnover, <del>to anyone of the preceding financial year, on a controller</del> or processor who, intentionally or negligently:</p> <p>(...)</p> <p>3a. <b>If a controller or processor intentionally or negligently violates several provisions of this Regulation listed in paragraphs 1, 2 or 3, the total amount of the fine may not exceed the amount specified for the gravest violation.</b></p> <p>7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of updating the amounts of the administrative fines referred to in paragraphs 4, 5 and 6, taking into account the criteria referred to in paragraph 2.</p>	
--	--	--	--

## Conclusion

The best way to safeguard the right to privacy is to implement an enforcement strategy that is focused on increased detection of data breaches while simultaneously fostering trust between industry and regulators in an effort to promote accountability. Such a participatory enforcement approach is preferable to simple deterrence.

We ask the trialogue negotiators to adopt a proportionate sanctions regime and ensure legal certainty and a level playing field for companies and consumers across the EU, who need to be assured that all 28 DPAs apply the same criteria for assessing a breach.

Yours sincerely,

A handwritten signature in black ink, appearing to read "Rene Summer". The signature is fluid and cursive, with a long horizontal stroke extending to the right.

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](http://www.europeandatacoalition.eu) or contact us at [info@europeandatacoalition.eu](mailto:info@europeandatacoalition.eu)