29 October 2015

European Data Coalition's Redline Summary Position

The European Data Coalition (Coalition) stands for a Europe that both delivers effective data protection standards for citizens and creates an environment in which European based companies are encouraged to innovate and develop Europe's digital ecosystem. The proposed Regulation on Data Protection (GDPR) was introduced with the laudable goal of updating data protection rules for the 21st century, reducing administrative burdens and harmonising the divergent approaches taken by the different Member States.

The Coalition believes that a progressive solution is within reach of the ongoing GDPR trilogue negotiations, provided the right balance between privacy and innovation is struck, and the right combination of proposals is adopted.

Art. 6/1.a (Consent) – Council position

We believe that a requirement for explicit consent for any data processing activity would in fact, perhaps counter-intuitively, undermine efforts to protect privacy. Consequently, the Coalition fully supports the Council's General Approach in maintaining the current standard of 'unambiguous consent'. This formulation leaves room for the use of 'explicit' consent in specific circumstances – notably when sensitive personal data is processed.

Art. 6/1.f (Legitimate Interest) – Council position

The inclusion of legitimate interests as a grounds for processing is welcome, as it helps avoid over-reliance on the notion of consent. Combined with the balancing test, it introduces a degree of flexibility into the GDPR, helping to ensure that emerging technologies and future needs are accounted for. The Council's version best promotes the interests of both the data subject and the data controller.

Art. 6/4 (Further Processing) – Council position

The Commission suggested that if the potential reuse of the data is incompatible with the original purposes, the data controller should still be able to justify the processing using the same grounds that can justify initial processing (e.g. consent, etc). However, unfortunately, the Commission omits "legitimate interest" as a grounds for further processing. The Coalition therefore supports the Council's version, which includes legitimate interest.

Art. 20 (Profiling) – Combination of Parliament & Council positions

The Council's position addresses several concerns associated with the Commission's proposal. The Commission proposed that the scope of Art. 20 focus on automated decision making and profiling. The Council recognised the many positive uses of data analysis in Europe and the risks associated with overzealously restricting this. The Parliament also improved on the proposal by not framing the

issue as a right not to be profiled, providing an opt-out regime and clarifying the "significant effects" test. The Coalition supports a combination of these two versions.

Art. 41 (Adequacy Decision) & Art. 42 (Appropriate Safeguards) – Combination of Commission & Council positions

The Coalition is strongly against the introduction of sunset clauses, as proposed by the Parliament. Both the Commission's and the Council's versions state that existing decisions would stay in force until amended, replaced or repealed. However, the Council's version is an improvement on the Commission's as it broadens the scope of the factors that should be considered, including participation in multilateral or regional systems (Art. 41/2.c). However, unlike the Commission, the Council adds references to "specific authorization" instead of "further authorization". The imposition of additional ("specific") requirements defeats the purpose of these instruments, creating uncertainty and potentially undermining the system. The Council's further definition of "appropriate safeguards" in Art. 42 is, however, a positive development.

Art. 44/1.h (Derogations – Legitimate Interest) – Council position

We support the preservation of the derogation contained in Art. 44/1.h that allows non-bulk, non-frequent and temporary transfers of personal data that are necessary for the purpose of the legitimate interests pursued by the data controller or data processor. The Council's version, which keeps this derogation, is the best available.

Art. 51 (One-Stop-Shop) – Commission position

The one stop shop regime is aimed at streamlining oversight of data protection in the EU. The Commission proposed that data protection cases be handled by a single regulator based in the EU country where the business has its 'main establishment', with other DPAs able to have a say in cases where the privacy rights of citizens in their country was at issue. However, concerns were raised that this system would not pass the 'proximity test' – the principle establishing that legal decisions affecting individuals should be taken as close as possible to them. The Council therefore outlined a compromise system under which only important cross border cases would be handled through the one stop shop regime. However, allowing several national authorities to be competent in a case will lead to lengthy procedures and lack of legal certainty for all involved. The Coalition supports more meaningful harmonisation and therefore favours the Commission's proposal.

Art. 77 (Joint-liability of Processor and Controller) – Council position + Coalition compromise

Here we support a system without joint and severe liability, keeping the roles and responsibilities of controller and processor distinct. The closest position to ours is the Council's, which instead of imposing joint and severe liability states that the processor shall be liable for damages "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". This is still not, however, an ideal formulation, as the term "lawful instructions" is ambiguous, pushing processors to carry out additional due diligence on data and unnecessarily replicating the efforts of controllers.

Art. 79 (Sanctions) – Council position + Coalition compromise

The Coalition believes that deterrence through fines and sanctions is necessary, but that blanket fines without a case-by-case examination are not appropriate. Instead, fines should be proportionate and capped, and calculated on the basis of data processing activities. We are against using global turnover as a basis for fines. The closest position to ours is the Council's, which lowers the amount of

sanctions, adds discretionary factors and defines more precisely the conditions for sanctions to be applied. However, unfortunately it keeps global turnover as a reference point for the calculation of fines.

1. Adopt data processing conditions that create incentives for investment in data-driven innovations

The proposed draft General Data Protection Regulation (GDPR) risks fixating perceived threats to privacy and ignoring the huge benefits of data processing. By expanding restrictions on data processing far beyond Directive 95/45/EC, the GDPR risks limiting the potential of data-driven innovations.

1.1 Consent

If only explicit consent can be used to justify data processing activities, the distinction between contract and consent will be blurred and companies will be pressured to greatly increase fully identified data subject experiences of digital/data driven services. This would result in massive consent fatigue among consumers and substantially increased costs for businesses, which would have to provide separate consent clauses, without any guaranteed increase in protection.

Consequently, the Coalition fully supports the Council's position maintaining the current standard of 'unambiguous consent'. This formulation leaves room for the use of 'explicit' consent in specific circumstances – notably when sensitive personal data is processed.

1.2 Legitimate interest

The preservation of legitimate interest as a grounds for processing is welcome, given that it can prevent over-reliance on consent for processing. However, an overly restrictive definition should be resisted. Narrowing the legitimate interest legal basis through the inclusion of a new, highly subjective "reasonable expectations" test risks sowing confusing among controllers concerning which interests they are able to claim as justification for processing. This will result in decreased investor confidence due to increased legal uncertainty, and decreased levels of investments in data driven businesses. Moreover, innovation is by its nature 'unexpected', and therefore unlikely to meet this test. Europe should not shut the door to innovation in this way.

To resolve this dispute, the trialogue negotiators should come to a compromise in which "reasonable expectation" is understood as just one of the factors to be taken into account within the balancing test. This would avoid placing undue emphasis on this difficult to define concept and guarantee the flexibility required to deliver a future-proof regulation. Furthermore, the concerns that the "reasonable expectation" test addresses are already addressed by the proposed Privacy Impact Assessment provision.

1.3 Purpose limitation

An overly constraining interpretation of purpose limitation would stifle the data-driven economy. This principle is based on the old idea that it is possible to decide on the purposes of a given data processing activity beforehand. Although traditionally analytics has been used to find answers to predetermined questions, big data analytics attempts to draw connections and relationships between data that are unexpected and previously unknown.

Under the proposed Regulation, personal data can generally only be used for those purposes that are "compatible" with the purpose for which they were initially collected. The Commission sensibly suggests that if the potential reuse of the data is incompatible with the original purposes, the data

controller should still be able to justify the processing through recourse to the grounds that can justify initial processing (e.g. consent, carrying out a legal contract, etc). However, unfortunately, the Commission omits "legitimate interest" as a grounds for further processing.

We believe the failure to include "legitimate interest" is an important oversight by the Commission. The use of this legal basis automatically provides protection to the data subject as it can only be used in conjunction with a balancing test ensuring that the interests of the data subject are not overridden. Its inclusion would represent an important addition to the efforts to ensure that the Regulation is genuinely forward looking. It would enable European businesses to adapt to the new and largely unpredictable ways in which data is used and reused in the big data era, and help them become global leaders in the field, while maintaining Europe as their home base. In light of these considerations, we strongly support the Council's approach, which includes "legitimate interest" as a ground for further processing but only in situations where the data controller's interests override those of the data subject.

1.4. Profiling

The Commission proposed a blanket prohibition on profiling, without the consent of the individual, if it "leads to measures producing legal effects concerning the data subject or does similarly significantly affect the interests, rights or freedoms of the concerned data subject". Such profiling would only be permitted either by consent, through a contract or if otherwise expressly authorised by the law of the Member State, provided suitable safeguards for the legitimate interest of the data subject exist.

The Council's General Approach proposes a narrower scope for Article 20, with the focus on automated decision making. It is the legislator's intention that the article covers data analysis capable of distinguishing data subjects from one another. In this context, it does not matter whether this practice is referred to descriptively or via a defined term such as "profiling".

The European Parliament's proposed amendments to Article 20 also introduce some positive aspects, in particular a more detailed "significant effects" test and a better formulation of the right to object to profiling. Rather than creating a "right" not to be subject to profiling, it explicitly allows it under certain conditions – the first being that it is not harmful. Lack of harm should be a sufficient condition to allow profiling, which is still subject to the other protections laid out in the Regulation. Further conditions are applied if the profiling is reasonably likely to cause harm, including a restriction of the legal bases available. Reasonable likelihood of significant harm would be established through a risk assessment. Profiling that causes insignificant harm would not restricted beyond the other provisions in the Regulation – notably the conditions applying to legal bases.

Our Coalition supports a combination of the Council's position on profiling and the Parliament's suggestions listed above.[1]

European Commission	European Parliament	Council	Coalition's Proposed Compromise
ARTICLE 6			
Lawfulness of processing	**Lawfulness of processing**	**Lawfulness of processing**	**Lawfulness of processing**
1. Processing of personal	1. Processing of personal	1. Processing of personal	1. Processing of personal

[1] http://europeandatacoalition.eu/wp-content/uploads/2015/06/Balance-fundamental-rights-more-effectively-%E2%80%93-or-they-will-suffer.pdf

data shall be lawful only if and to the extent that at least one of the following applies:	data shall be lawful only if and to the extent that at least one of the following applies:	data shall be lawful only if and to the extent that at least one of the following applies:	data shall be lawful only if and to the extent that at least one of the following applies:
(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;	~~(a) the data subject has given consent to the processing of their personal data for one or more specific purposes~~;	(a) the data subject has given **unambiguous** consent to the processing of their personal data for one or more specific purposes;	(a) the data subject has given unambiguous consent to the processing of their personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;	(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;	(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;	(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;	(c) processing is necessary for compliance with a legal obligation to which the controller is subject;	(c) processing is necessary for compliance with a legal obligation to which the controller is subject;	(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject;	~~(d) processing is necessary in order to protect the vital interests of the data subject~~;	(d) processing is necessary in order to protect the vital interests of the data subject **or of another person**;	(d) processing is necessary in order to protect the vital interests of the data subject or of another person;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;	(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;	(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;	(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.	(f) processing is necessary for the purposes of the legitimate interests pursued by **the** controller **or, in case of disclosure, by the third party to whom the data is disclosed, and which meet the reasonable expectations of the data subject based on his or her relationship with the controller**, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data~~, in particular where the data subject is a child~~. This shall not apply to processing carried out by public authorities in the performance of their	(f) processing is necessary for the purposes of the legitimate interests pursued by ~~a~~ **the** controller **or by a third party**, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. ~~This shall not apply to processing carried out by public authorities in the performance of their tasks~~.	(f) processing is necessary for the purposes of the legitimate interests pursued by a the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance exercise of their tasks
2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in		2. Processing of personal data which is necessary for **archiving** ~~the~~ purposes **in the public interest, or** ~~of~~ **for** historical, statistical or	2. Processing of personal data which is necessary for ***archiving*** the purposes ***in the public interest, or*** ~~of~~ ***for*** historical, statistical or

Article 83.	tasks. ~~2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83.~~	scientific ~~research~~ **purposes** shall be lawful subject **also** to the conditions and safeguards referred to in Article 83.	scientific research ***purposes*** shall be lawful subject to the conditions and safeguards referred to in Article 83.
3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in: (a) Union law, or (b) the law of the Member State to which the controller is subject. The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued.	~~3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in:~~ ~~(a) Union law, or~~ ~~(b) the law of the Member State to which the controller is subject.~~ The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued. **Within the limits of this Regulation, the law of the Member State may provide details of the lawfulness of processing, particularly as regards data controllers, the purpose of processing and purpose limitation, the nature of the data and the data subjects, processing measures and procedures, recipients, and the duration of storage.**	3. The basis ~~of~~ **for** the processing referred to in points (c) and (e) of paragraph 1 must ~~be provided for~~ **established** in accordance with: (a) Union law, or (b) **National** ~~the~~ law of the Member State to which the controller is subject. **The purpose of the processing shall be determined in this legal basis or as regards the processing referred to in point (e) of paragraph 1, be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. This legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia the general conditions governing the lawfulness of data processing by the controller, the type of data which are subject to the processing, the data subjects concerned; the entities to, and the purposes for which the data may be disclosed; the purpose limitation; storage periods and processing operations and processing procedures, including measures to ensure lawful and fair processing, including for other specific processing situations as provided for in Chapter IX.** **3a. In order to ascertain whether a purpose of further processing (...)is**	3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in: (a) Union law, or (b) the law of the Member State to which the controller is subject. The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued. **3a. In order to ascertain whether a purpose of further processing (...)is compatible with the one for which the data are initially collected, the controller shall take into account, unless the data subject has given consent, inter alia:** **(a) any link between the purposes for which the data have been collected and the purposes of the intended further processing;** **(b) the context in which the data have been collected;** **(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to**

		compatible with the one for which the data are initially collected, the controller shall take into account, unless the data subject has given consent, inter alia: **(a) any link between the purposes for which the data have been collected and the purposes of the intended further processing;** **(b) the context in which the data have been collected;** **(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9;** **(d) the possible consequences of the intended further processing for data subjects;** **(e) the existence of appropriate safeguards** ~~The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued~~.	**Article 9;** **(d) the possible consequences of the intended further processing for data subjects;** **(e) the existence of appropriate safeguards**
4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.	~~4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.~~	4. Where the purpose of further processing is ~~not~~ **in**compatible with the one for which the personal data have been collected **by the same controller**, the **further** processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. ~~This shall in particular apply to any change of terms and general conditions of a contract~~. **Further processing by the same**	4. Where the purpose of further processing is ~~not~~ ***in***compatible with the one for which the personal data have been collected ***by the same controller***, the ***further*** processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.

		controller for incompatible purposes on grounds of legitimate interests of that controller or a third party shall be lawful if these interests override the interests of the data subject.	**Further processing by the same controller for incompatible purposes on grounds of legitimate interests of that controller or a third party shall be lawful if these interests override the interests of the data subject.**
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.	~~5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.~~	~~5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.~~	

European Commission	European Parliament	Council	Coalition's Proposed Compromise
ARTICLE 20			
Measures Based On Profiling	**Profiling**	**Automated Individual Decision Making**	**Automated Individual Decision Making**
1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour. 2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph	1. **Without prejudice to the provisions in Article 6** every natural person shall have the right **to object to profiling in accordance with Article 19. The data subject shall be informed about the right to object to profiling in a highly visible manner.** ~~shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation,~~	1. ~~Every natural person~~ **The data subject** shall have the right not to be subject to a ~~measure~~ **decision based solely on automated processing, inlcuding profiling**, which produces legal effects concerning ~~this natural person~~ **him or her** or significanly affects ~~this natural person~~ **him or her**~~, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour~~. ~~2~~ **1a**. ~~Subject to the other provisions of this~~	1. ~~Every natural person shall~~ **The data subject may** be subject to a ~~measure~~ **decision** ~~which produces legal effects concerning this natural person or significantly affects this natural person, and~~ which is based solely on automated processing intended to evaluate certain personal aspects relating to ~~this natural person~~ **him or her** or to analyse or predict in particular ~~the natural person's~~ **his or her** performance at work, economic situation, location, health, personal preferences, reliability or behaviour **only if the decision**: ~~2. Subject to the other provisions of this Regulation, a person may~~

1 only if the processing: (a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or (b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or (c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards. 3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9. 4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject. 5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to	~~location, health, personal preferences, reliability or behaviour.~~ 2. Subject to the other provisions of this Regulation, a person may be subjected to ~~a measure of the kind referred to in paragraph 1~~ **profiling which leads to measures producing legal effects concerning the data subject or does similarly significantly affect the interests, rights or freedoms of the concerned data subject** only if the processing: (a) is ~~carried out in the course of~~ **necessary for** the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied ~~or where~~ **provided that** suitable measures to safeguard the data subject's legitimate interests have been adduced, ~~such as the right to obtain human intervention~~; or (b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or (c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards. 3. ~~Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person~~ **Profiling that has the effect of discriminating against individuals on the basis of race or ethnic origin, political opinions,**	~~Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing~~ **Paragraph 1 shall not apply if the decision**: (a) is ~~carried out in the course of the~~ **necessary for** entering into, or performance of, a contract, **between the data subject and a data controller** ~~where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention;~~ or (b) is ~~expressly~~ authorized by a Union or Member State law **to which the controller is subject** and which also lays down suitable measures to safeguard the data subject's **rights and freedoms and** legitimate interests; or (c) is based on the data subject's **explicit** consent~~,~~ ~~subject to the conditions laid down in Article 7 and to suitable safeguards~~. **1b. In cases referred to in paragraph 1a (a) and (c) the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision:** 3. ~~Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person~~ **Decisions**	~~be subjected to a measure of the kind referred to in paragraph 1 only if the processing:~~ **(a) does not significantly harm him or her or produce legal effects concerning him or her; or** (~~a~~**b**) is ~~carried out in the course of~~ **necessary for** the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied ~~or where~~ **provided that** suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or (~~b~~**c**) is expressly authorized by a Union or Member State law **to which the controller is subject** and which also lays down suitable measures to safeguard the data subject's **rights and freedoms and** legitimate interests; or d) is based on the data subject's **prior and explicit** consent ~~subject to the conditions laid down in Article 7 and to suitable safeguards~~. **2. In cases referred to in paragraph 1(b), 1(c), and 1(d), the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to obtain an explanation of the decision, to express his or her point of view and to contest the decision.** 3. ~~Automated processing of personal data intended~~

safeguard the data subject's legitimate interests referred to in paragraph 2.	**religion or beliefs, trade union membership, sexual orientation or gender identity, or that results in measures which have such effect, shall be prohibited. The controller shall implement effective protection against possible discrimination resulting from profiling. Profiling** shall not be based solely on the special categories of personal data referred to in Article 9. ~~4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.~~ 5. ~~The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for~~ **Profiling which leads to measures producing legal effects concerning the data subject or does similarly significantly affect the interests, rights or freedoms of the concerned data subject shall not be based solely or predominantly on automated processing and shall include human assessment, including an explanation of the decision reached after such an assessment. The** suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2 **shall include the right to**	**referred to in paragraph 1a** shall not be based ~~solely~~ on special categories of personal data referred to in Article 9**(1), unless points (a) or (g) of Article 9(2) apply and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.** ~~4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.~~ ~~5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.~~	~~to evaluate certain personal aspects relating to a natural person shall not be based solely on~~ **Profiling that has the effect of discriminating against data subjects on the basis of** the special categories of personal data referred to in Article 9, **or that is reasonably likely to have such effects, shall be prohibited**. ~~4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.~~ 5. The Commission shall be empowered to adopt ~~delegated acts~~ **Recommendations in accordance with Article 86** for the purpose of further specifying ~~the criteria and conditions for~~ suitable measures to safeguard the data subject's legitimate interests referred to in paragraph**s 1 and** 2.

	obtain human assessment and an explanation of the decision reached after such assessment. **5a. The European Data Protection Board shall be entrusted with the task of issuing guidelines, recommendations and best practices in accordance with point (b) of Article 66 (1) for further specifying the criteria and conditions for profiling pursuant to paragraph 2.**		

2. Promote a consistent application of the GDPR throughout the EU

The one-stop-shop regime is intended to streamline oversight of data protection in the EU. Currently, businesses operating across the trading bloc can be forced to answer to data protection authorities (DPAs) in each EU country. To address this issue, the Commission proposed the one-stop-shop regime to enable data protection cases to be handled by a single regulator based in the EU country where the business has its 'main establishment'. Other DPAs would be able to have a say in cases where the privacy rights of citizens in their country are at issue.

To address several concerns raised by the Member States, the Council suggested a compromise which is weaker in uniting the EU's divergent national systems. Under the plans, only important cross border cases would be handled in accordance with the one-stop-shop regime. Allowing several national authorities to be competent in a case would lead to lengthy procedures and lack of legal certainty for controllers, processors and even data subject seeking redress.

The Coalition supports a more meaningful harmonisation effort and therefore believes that the Commission's proposal should be preserved. Moreover, to promote the goal of legal certainty, it is crucial to establish guidance on what constitutes a "main establishment" in the context of identifying the lead DPA overseeing data processing activities. It is our view that the definition of the main establishment should be based on a common set of objective criteria for processors and controllers, allowing for the selection of the undertaking or the entity within the group of undertaking, which would be best placed to ensure compliance with the one stop shop decision across the EU. After all, the one stop shop mechanism is supposed to be broader than just establishing non-compliance also including authorization and approval measures, making it hard to justify why processors are taken out of its scope.

We are further disappointed that the definition put forward on transnational processing, which suggests to keep the threshold of cases benefiting from the one stop shop mechanism at a considerably high level. It is our view, which the possibility of benefiting from this structure should be available to all cases that are not exclusively of local nature.

European Commission	European Parliament	Council	Coalition's Proposed Compromise
ARTICLE 51			
Competence	**Competence**	**Competence**	**Competence**
1. Each supervisory authority shall exercise, on the territory of its own Member State, the powers conferred on it in accordance with this Regulation.	1. Each supervisory authority shall **be competent to perform the duties and to** exercise, ~~on the territory of its own Member State~~, the powers conferred on it in accordance with this Regulation **on the territory of its own Member State, without prejudice to Articles 73 and 74. Data processing by a public authority shall be supervised only by the supervisory authority of that Member State**.	1. Each supervisory authority shall **be competent to perform the tasks and** exercise, ~~on the territory of its own Member State~~, the powers conferred on it in accordance with this Regulation **on the territory of its own Member State**.	1. Each supervisory authority shall exercise, on the territory of its own Member State, the powers conferred on it in accordance with this Regulation.
2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.	deleted	2. Where the processing ~~of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.~~**is carried out by public authorities or private bodies acting on the basis of points (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 51a does not apply.**	2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.
3. The supervisory authority shall not be competent to supervise processing operations of courts acting in their judicial capacity.	3. The supervisory authority shall not be competent to supervise processing operations of courts acting in their judicial capacity.	3. ~~The s~~**S**upervisory authority shall not be competent to supervise processing operations of courts acting in their judicial capacity.	3. The supervisory authority shall not be competent to supervise processing operations of courts acting in their judicial capacity.

3. Lay the foundations for open and secure international data transfers

3.1. Adequacy decisions and Appropriate Safeguards (including Binding Corporate Rules)

The Coalition encourages the Commission to continue to promote and expand mutual recognition through adequacy assessments of third countries' privacy regulations. This will limit the need for individual Member State authorities to approve cross-border data flows, as well as the need for controllers or processors to rely on complex alternative transfer mechanisms. Furthermore, adequacy decisions should impose reciprocal obligations to keep the third countries' personal data flows open into the EU and improve the business conditions for EU based data processing.

When international harmonisation of privacy regulations cannot be realistically achieved, the Coalition supports the ambition of the EU Institutions to foster the use of effective legal transfer mechanisms such as Binding Corporate Rules (BCRs) for both controllers and processors or Standard Contractual Clauses (SCCs) to facilitate trans-border data flows.

The introduction of sunset clauses as proposed by the European Parliament's suggested amendments in Chapter V would result in unnecessary regulatory uncertainty and make it prohibitively costly for private companies to invest in these transfer mechanisms. Compliance with well-established and trusted data transfer arrangements under Directive 95/45/EC already resulted in significant investment by European businesses.

Both the Commission and the Council take a more appopriate approach to existing transfer mechanisms, allowing them to continue until amended, replaced or repealed by the Commission. The Coalition supports this approach as it safeguards investment and international trade.[2]

3.2. Prohibition of data disclosure requests by third countries

Article 43a (new) on data disclosure requests from third countries would create extraterritorial conflicts of law for European companies operating inside and outside the EU. This would leave companies in impossible situations, moreover it provides no meaningful legal protection for citizens. The deletion of this article is strongly recommended.

3.3. Legitimate interest as a mechanism for international data transfers

The Regulation should account for the global nature of today's data value chains and the increasing role of global digital markets. In today's economy, products and applications are based on systems constructed in both EU and non-EU countries. As developers and support personnel in many cases reside in various countries, allowing them to perform their work remotely is a necessity given today's global distribution value chains.

The Coalition is supportive of the Council's willingness to preserve the derogation contained in Art. 44/1.h. Others have mistakenly made the case that this clause risks lowering the level of protection currently provided under the EU *acquis*. Such arguments, however, do not adequately account for the restrictiveness of the conditions under which this transfer mechanism would operate. This derogation would not cover mass transfers or frequent small-scale transfers of end-user data. Its fundamental objective is to address business-to-business situations when a temporary, non-bulk and non-frequent data transfer of personal data is necessary for the completion of a support function, troubleshooting action or routine control. If this exception is discarded, the vital flexibility enabling

[2] http://europeandatacoalition.eu/wp-content/uploads/2015/06/Keep-Europe-open-to-international-data-transfers.pdf

business-to-business outsourcing and catering to industrial internet data processing needs would disappear.

European Commission	European Parliament	Council	Coalition's Proposed Compromise
ARTICLE 41			
Transfers with an Adequacy Decision	**Transfers with an Adequacy Decision**	**Transfers with an Adequacy Decision**	**Transfers with an Adequacy Decision**
(…)	(…)	(…)	(…)
5. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2), or, in cases of extreme urgency for individuals with respect to their right to personal data protection, in accordance with the procedure referred to in Article 87(3).	5. The Commission ~~may~~ **shall be empowered to adopt delegated acts in accordance with Article 86 to** decide that a third country, or a territory or a processing sector within that third country, or an international organisation does not ensure **or no longer ensures** an adequate level of protection within the meaning of paragraph 2 of this Article, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred. ~~Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2), or, in cases of extreme urgency for individuals with respect to their right to personal data protection, in accordance with the procedure referred to in Article 87(3).~~	3a. Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5.	3a. Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5.
(…)	(…)	(…)	(…)
8. Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by the	8. Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force until five years after the entry into force of this Regulation unless amended, replaced	5. The Commission may decide that a third country, or a territory or a ~~processing~~ **specified** sector within that third country, or an international organisation ~~does not~~ **no longer** ensures an adequate level of protection within the meaning of paragraph 2 ~~of this Article, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred. Those~~ **and may, where necessary, repeal, amend or suspend such decision without retro-active effect. The** implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2) or, in cases of extreme urgency ~~for~~	5. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred. ~~Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2), or, in cases of extreme urgency for individuals with respect to their right to personal data protection, in~~

Commission.	or repealed by the Commission before the end of this period.	~~individuals with respect to their right to personal data protection,~~ in accordance with the procedure referred to in Article 87(3). **5a. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the Decision made pursuant to paragraph 5.** (…)	~~accordance with the procedure referred to in Article 87(3).~~ 5a. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation ~~giving rise to the~~ **before taking a** Decision ~~made~~ pursuant to paragraph 5. **The Commission shall ensure appropriate publicity for this consultation.**

European Commission	European Parliament	Council	Coalition's Proposed Compromise
ARTICLE 42			
Transfers by way of Appropriate Safeguards	**Transfers by way of Appropriate Safeguards**	**Transfers by way of Appropriate Safeguards**	**Transfers by way of Appropriate Safeguards**
(…) 5. Where the appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor shall obtain prior authorisation for the transfer, or a set of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such transfer. Such authorisation by the supervisory authority shall be in accordance with point (a) of Article 34(1). If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57. Authorisations by a supervisory authority on	(…) 5. Authorisations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until two years after the entry into force of this Regulation unless amended, replaced or repealed by that supervisory authority before the end of this period.	(…) 5b. Authorisations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid, until amended, replaced or repealed by a Commission Decision in accordance with paragraph 2.	~~(…)~~ 5b. Authorisations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid, until amended, replaced or repealed by a Commission Decision in accordance with paragraph 2.

the basis of Article 26(2) of Directive 95/46/EC shall remain valid, until amended, replaced or repealed by that supervisory authority.			

European Commission	European Parliament	Council	Coalition's Proposed Compromise
ARTICLE 44			
Derogations	**Derogations**	**Derogations**	**Derogations**
1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that: (…) (h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.	**1.** In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that: (…) ~~(h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.~~	1. In the absence of an adequacy decision pursuant to **paragraph 3 of** Article 41, or of appropriate safeguards pursuant to Article 42, **including binding corporate rules,** a transfer or a ~~set~~ **category** of transfers of personal data to a third country or an international organisation may take place only on condition that: (…) (h) the transfer**, which is not large or frequent,** is necessary for the purposes of the legitimate interests pursued by the controller **which are not overridden by the interests or rights and freedoms of the data subject** ~~or the processor, which cannot be qualified as frequent or massive~~, and where the controller ~~or processor~~ has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced ~~appropriate~~ **suitable** safeguards with respect to the protection of personal data~~, where necessary~~.	1. In the absence of an adequacy decision pursuant to Article 41, or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that: (…) (h) the transfer**, which is temporary, not large or frequent,** is necessary for the purposes of the legitimate interests pursued by the controller or the processor **which are not overridden by the interests or rights and freedoms of the data subject** ~~which cannot be qualified as frequent or massive~~, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data.
RECITAL 86			
Provisions should be made for the possibility for transfers in certain	Provisions should be made for the possibility for transfers in certain	Provisions should be made for the possibility for transfers in certain	Provisions should be made for the possibility for transfers in certain

circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients.	circumstances where the data subject has given his **explicit** consent, where the transfer is ~~necessary~~ **occasional** in relation to a contract or a legal claim, **regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers** where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients, **taking into full account the interests and fundamental rights of the data subject.**	circumstances where the data subject has given his **explicit** consent, where the transfer is ~~necessary~~ **occasional** in relation to a contract or a legal claim, **regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers** where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients.	circumstances where the data subject has given his **explicit** consent, where the transfer is ~~necessary~~ **occasional** in relation to a contract or a legal claim, where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients. **When a controller in a third country needs to transfer back the personal data from an EU-based processor, such a controller shall have the right to transfer back the personal data without restrictions**.

4. Maintain clear and separate roles and responsibilities for controllers and processors

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, providing companies with clarity regarding roles and responsibilities, and ensuring consumers know who to turn to in case of a problem. Therefore, the existing liability principles should be maintained in the new Regulation. Nevertheless, processors should continue to assume direct liability when they operate outside of a contract with a controller. When this occurs the processor becomes a controller in its own right, assumes direct responsibility for the processing and is subject to the penalties laid out in the processing contract.

We caution against the introduction of a "one-size-fits-all" joint liability model that blurs the responsibilities in the data processing value chain. Joint liability is a model that has failed in the past. It was introduced in the 2001 model clauses for the transfer of personal data and proved to be overly burdensome for all parties involved. This led to a low uptake of the model clauses and a revision by the Commission in December 2004, later upheld in 2010. The Article 29 Working Party has also

expressed its doubts over the concept, stating that joint liability is burdensome and risks preventing controllers from using standard contractual clauses.

We understand that the joint liability proposal aims to protect data subjects in cases where the controller ceases 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. In the event that a controller disappears, the data subject should be able to turn to the processor through a scheme of subsidiary liability. This means that the data subject is guaranteed redress in all circumstances. This system has been tested and proven efficient over time, allowing the market to thrive while protecting the rights of data subjects. We support the Council's position, provided the concerns above are improved.[3]

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 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.	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 ~~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.	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 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**	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 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

[3] http://europeandatacoalition.eu/wp-content/uploads/2015/06/GDPR-Maintain-clear-and-separate-roles-and-responsabilities-for-controllers-and-processors.pdf

		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 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.**	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.**

5. Adopt a proportionate sanctions 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 potential 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 placed 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 objective when dealing with well-intended and accountable companies.

Better enforcement should ensure the implementation of the rules and users' rights through more robust enforcement 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.

The Coalition supports the idea that fines should be proportionate and capped, and that the basis used to calculate fines should be matched to data processing activities. We are firmly against the idea of using global turnover as the basis for penalties. We support the Council's position provided that the basis for the calculation of fines is reviewed. On the positive side, the Council's position lowers the level of sanctions, adds discretionary factors and defines more precisely the conditions for sanctions to be applied.[4]

European Commission	European Parliament	Council	Coalition's Proposed Compromise
ARTICLE 79			
Administrative sanctions	**Administrative sanctions**	**General Conditions for Imposing Administrative Fines**	**General Conditions for Imposing Administrative Fines**
1. Each supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article. 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	1. Each supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article. **The supervisory authorities shall co-operate with each other in accordance with Articles 46 and 57 to guarantee a harmonized level of sanctions within the Union.** 2. The administrative sanction shall be in each individual case effective, proportionate and	1. Each supervisory authority shall ~~be empowered to impose~~ **ensure that the imposition of** administrative ~~sanctions~~ **fines** ~~in accordance with~~ **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**. **2a. Administrative fines shall, depending on the**	1. ~~Each~~ **The lead** supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article. 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 actual harm or risk of harm to**

[4] http://europeandatacoalition.eu/wp-content/uploads/2015/06/GDPR-Adopt-a-proportionate-sanctions-regime.pdf

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. 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: (a) a natural person is processing personal data without a commercial interest; or (b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities. 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: (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); (b) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4). 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,	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.~~ **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:** **(a) a warning in writing in cases of first and non-intentional non-compliance;** **(b) regular periodic data protection audits;** **(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.** **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 be imposed in cases of intentional or negligent incompliance.** **2c. The administrative sanction shall take into account the following factors:** **(a) the nature, gravity and duration of the incompliance,**	**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:** **(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) the intentional or negligent character of the infringement,** **(d) action taken by the controller or processor to mitigate the damage suffered by data subjects;** **(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;** **(f) any relevant previous infringements by the controller or processor;** **(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;** **(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**	**the data subject,** 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. 3. In case of a first ~~and non-intentional~~ non-compliance with this Regulation, a warning in writing may be given and no sanction **shall be** imposed, where any of the following criterias is fulfilled: ~~(a) a natural person is processing personal data without a commercial interest; or~~ ~~(b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.~~ **(a) non-compliance does not cause serious harm to the data subject;** **(b) non-compliance only impacts a small number of data subjects;** **(c) the non-compliance is non-intentional.** 4. **When sanctions are not ruled out due to Article 79(3),** the supervisory authority ~~shall~~ **may, taking into due consideration Article 79(2),** impose a fine ~~up to~~ **between 100 EUR and** 250 000 EUR~~, or in case of an enterprise up to 0,5 %~~

intentionally or negligently: (…) 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: (…) 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.	**(b) the intentional or negligent character of the infringement,** **(c) the degree of responsibility of the natural or legal person and of previous breaches by this person,** **(d) the repetitive nature of the infringement,** **(e) the degree of co-operation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement,** **(f) the specific categories of personal data affected by the infringement,** **(g) the level of damage, including non-pecuniary damage, suffered by the data subjects,** **(h) the action taken by the controller or processor to mitigate the damage suffered by data subjects,** **(i) any financial benefits intended or gained, or losses avoided, directly or indirectly from the infringement,** **~~(~~j) the degree of technical and organisational measures and procedures implemented pursuant to:** **(i) Article 23 - Data protection by design and by default** **(ii) Article 30 - Security of processing** **(iii) Article 33 - Data protection impact assessment** **(iv) Article 33 a - Data protection compliance review** **(v) Article 35 - Designation of the data protection officer** **(k) the refusal to cooperate with or obstruction of**	**against the controller or processor concerned with regard to the same subject-matter586, compliance with these measures ;** **(j) adherence to approved codes of conduct pursuant to Article 38 or approved certification mechanisms pursuant to Article 39;** **(m) any other aggravating or mitigating factor applicable to the circumstances of the case.** ~~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:~~ **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.** **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.** **5. Member States may abstain from providing rules for administrative fines as referred to in 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**	~~of its annual worldwide turnover,~~ to anyone who, intentionally ~~or negligently~~: (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); (b) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4). 5. The supervisory authority ~~shall~~ **may, taking into due consideration Article 79(2)** impose a fine up to 500 000 EUR, ~~or, in case of an enterprise up to 2 % of its annual worldwide turnover,~~ to anyone who, intentionally ~~or negligently~~: (…) 6. The supervisory authority ~~shall~~ **may, taking into due consideration Article 79(2)** impose a fine up to 10 000 000 EUR ~~or, in case of an enterprise up to 2 % of its annual worldwide turnover,~~ to anyone who, intentionally ~~or negligently~~: (…) ~~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.~~

	inspections, audits and controls carried out by the supervisory authority pursuant to Article 53, **(l) other aggravating or mitigating factors applicable to the circumstance of the case.** ~~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:~~ ~~(a) a natural person is processing personal data without a commercial interest; or~~ ~~(b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.~~ ~~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:~~ ~~(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);~~ ~~(b) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4).~~ ~~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:~~ ~~(…)~~ ~~6. The supervisory authority shall impose a fine up to 1 000 000 EUR or, in case of~~	**sanctions are effective, proportionate and dissuasive, taking into account the level of administrative fines provided for in this Regulation.** **Where they so decide, Member States shall notify, to the Commission, the relevant parts of their criminal law.** **Article 79a** **1**. The supervisory authority ~~shall~~ **may** impose a fine ~~up to~~ **that shall not exceed** 250 000 EUR, or in case of an ~~enterprise~~ **undertaking** ~~up to~~ 0,5 % of its **total** worldwide annual turnover~~, to anyone~~ **of the preceding financial year, on a controller** who, intentionally or negligently: (a) does not respond~~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)~~ **within the period referred to in Article 12(2) to requests of the data subject**; (b) charges a fee in violation of **the first sentence of** paragraph 4 of Article 12. ~~5~~**2**. The supervisory authority ~~shall~~ **may** impose a fine ~~up to~~ **that shall not exceed** 500 000 EUR, or in case of an ~~enterprise~~ **undertaking** ~~up to~~ 1 % of its total worldwide annual turnover~~, to anyone~~ **of the preceding financial year, on a controller** or processor who, intentionally or negligently: (…) ~~6~~**3**. The supervisory authority may impose a	

	~~an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently:~~ ~~(…)~~ 7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of updating the **absolute** amounts of the administrative fines referred to in ~~paragraphs 4, 5 and 6~~ **paragraph 2a**, taking into account the criteria **and factors** referred to in paragraph**s** 2 **and 2c**.	fine ~~up to~~ **that shall not exceed** 1 000 000 EUR or, in case of an ~~enterprise~~ **undertaking** ~~up to~~ 2 % of its **total** worldwide annual turnover~~, to anyone~~ **of the preceding financial year, on a controller** or processor who, intentionally or negligently: (…) **3a. 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.** ~~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.~~	

Conclusion

A failed GDPR would establish an enormous disconnect in Europe from the requirements of a modern, advanced digital knowledge economy, putting at significant risk the development of a data-driven innovation economy, as aspired to in the DSM strategy. It therefore comes down to a straight choice between an ambitious DSM and a failed GDPR.

Let's make the right choice and assure a bright future for Europe's digital economy. There is still time in the ongoing trilogues to adopt the right combination of proposals on the table, **as suggested above – let us make sure we make the right choice.**

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