EUROPEAN Justice Forum

Proposal for a Regulation on EU Data Protection Reform - COM(2012)11

Introduction

The European Justice Forum (EJF) is a non-profit coalition of businesses, individuals and organisations that are working to promote fair, balanced, transparent and efficient civil justice laws and systems in Europe. Its aim is to ensure that the legal environment in Europe protects both individuals and businesses alike, and that those with a legitimate grievance have not just access to justice but efficient means of redress. We wish to see a system in which innovation and enterprise can flourish and which enhances the international competitiveness of Europe.

Summary

EJF recognises, and fully endorses, the principles that the rights and freedoms of individuals must be protected whenever businesses, or public authorities, process personal data, and that data protection should be modernised, and made consistent, across the EU in response to technology changes (especially social media).

However, EJF has serious misgivings about the **system of collective complaints and remedy contained in Chapter VIII (Articles 73 to 79) of the Commission's proposal. These concerns are heightened by the amendments suggested to this Chapter by MEP Jan Albrecht in his Draft LIBE Committee report.**

These concerns fall into three main categories:

- **Lack of coherence in policy** – Parliament has rejected a sectoral-only approach to collective procedures[1] and this proposal comes before the Commission has released its forthcoming Communication 'outlining the general principles of an EU framework for collective redress';
- **The proposed articles as they stand are an invitation to speculative and abusive litigation and lack any form of safeguards.** They encourage capture of the litigation process by actors who use litigation as an investment model, such as third party funders. They fail to encourage alternative forms of dispute resolution. All this helps neither individuals to pursue their rights effectively nor businesses to defend theirs. MEP Albrecht's proposed amendments make the position worse;
- **The proposal for a fining regime is not well designed for the specificities of data protection infringements and fails adequately to encourage a culture of compliance.**

Lack of coherence

The proposal's recommendations for collective mechanisms for complaint and remedy are premature. There is a much bigger EU consumer redress policy debate that the proposal simply fails to take into account, a debate on which the Commission, Parliament and EU stakeholders have, cautiously, expended so much time and energy over the past few years. A Communication 'outlining

[1] See the European Parliament's 2012 Report

the general principles of an EU framework for collective redress' is awaited from the Commission later this year. Parliament has rejected a sectoral-only approach to collective procedures. We see no coherence in advancing stand-alone provisions for data protection as a specific sector, in Chapter VIII, before the Commission's Communication is available later this year. MEP Albrecht's proposed amendments are worse, and suffer from the same objection.

The collective complaints and redress mechanisms are defective

EJF is concerned that articles 73 to 77 in the Commission's proposal will have the effect of encouraging mass litigation – "class actions" – which is uncontrolled. This is the very phenomenon which elsewhere the Commission, and the Parliament, has rejected.[2] The proposed amendments from MEP Albrecht make the procedure more unaccountable.

Article 73.2, 73.3 and 76 give to poorly defined representative bodies rights to lodge a complaint and to a judicial remedy, *even where no individual has a concern about a breach of the regulation.* This raises a risk of speculative and vexatious complaints, and abusive litigation. This risk is exacerbated by the amendments proposed by MEP Jan Albrecht. These allow still less well defined representative bodies,[3] without reference to the interests of any affected data subject, to make claims for damages including non-pecuniary damages such as distress.

There are no safeguards to prevent abuse in the proposals. If collective complaints and redress were to form a part of these proposals there must be safeguards against abuse.[4] The first and foremost requirement is no form of collective complaint or proceeding should be permissible without a complaint by and the consent of the data subjects whose rights are said to be infringed.

Building on independent research[5] and extensive experience of litigation, EJF believes the following safeguards are essential to any form of collective complaints and redress procedure using representative parties:

- Representatives that bring collective complaints or proceedings must be properly representative of the group of individuals they represent. Criteria for what is "properly constituted" may differ widely from one Member State to another. Those criteria should be the same, and will include having the resources and expertise necessary properly to conduct the action, not having any conflict of interest between such persons or organisations and the claimants they represent, and not benefiting from such litigation beyond the recovery of out-of-pocket expenses, including attorney fees;
- All data subjects represented must be individually identified before the right to a judicial remedy is exercised on their behalf (an opt-in system). Failure to identify such individuals is against European legal principles; it artificially enlarges the 'class' of theoretical claimants; and it places an artificial pressure on a defendant to enter into a 'blackmail' settlement. It also facilitates fraudulent claims and is conflicted with the position adopted by the Parliament[6]. ;

---

[2] *Ibid.* 1

[3] 'acting purportedly in the public interest', which is a vague term.

[4] *Ibid.* 1, paragraphs 15 - 24

[5] C. Hodges, I. Benohr and N. Creutzfeldt-Banda (2012) 'Consumer ADR in Europe', Oxford: Hart Publishing; C Hodges (2008) 'The Reform of Class and Representative Actions in European Legal Systems – a new framework for collective redress in Europe', Oxford: Hart Publishing

[6] *Ibid* 1–, paragraph 20

- Contingency fees and third party litigation funding must not be allowed in the representative action. They create conflicts of interest between attorney and client or with the organisation providing the funding. They also create economic motivation to bring actions other than the receipt of normal attorney fees. They can also create streams of income from series of cases that could be securitised and marketed as financial instruments – a commercialisation of legal actions that should not be permitted, in our view;
- The 'loser pays rule' whereby the liability for costs falls on the unsuccessful party, must apply. This is the most significant deterrent against speculative litigation;
- Alternative Dispute Resolution (ADR) – the proposals reference the need for speedy resolution of problems, but currently do not encourage the use of ADR. Research has shown that ADR can deliver acceptable outcomes for consumers seeking collective redress in mass claims, in many sectors, and in many Member States.[7] There is every reason to think it would be appropriate in the context of data protection, though consumer's rights to take court action must be preserved.

Unspecific damages

Civil justice in Europe is a restorative system, not a punitive one. A claimant generally recovers in a successful court action compensatory damages that put him or her in the same position that he or she would have been in had the breach not occurred. That is a simple principle that does not offend against any system of law within the EU, and leaves it up to the courts of each Member State to determine the level of compensation. Compensation for the damage suffered correctly lies at the heart of Article 77.

The proposed amendments by MEP Jan Albrecht introduce the inclusion of non-pecuniary losses "such as distress". This suggests such a head of loss is not compensatory. The correct assessment of what is compensatory, and what is recoverable, should be left to the courts of the Member States in accordance with Article 15 Rome II Regulation (EC) No 864/2007.

The fining regime and compliant behaviour

Articles 78 and 79 raise a number of fundamental policy objections, and need to be revised:

- A regulatory model with a deterrence-based approach at its heart will not incentivise businesses to create long-term compliant behaviours. It is a matter of obvious and common sense that prevention is better than cure/punishment;
- A mandatory fining regime does not assist in delivering redress to data subjects who have suffered damage. It does not allow supervisory authorities to use the power and threat of fines to encourage business to "*do the right thing*" in the event of a breach;
- Having a mechanism that allows the supervisor to take into account the compliance regimes of the data controller before the breach, and the plans of the data controller to put things right or pay compensation, will radically increase compliance if the data controller can get a significant reduction in the fine. Or, in other words, businesses that have made little or no effort at compliance ought to face more significant and greater penalties than a business that has taken care to avoid problems in the first place;

[7] Ibid 5

- There are well-known cases where, for example, the Commission and national competition authorities have reduced or waived fines where infringers have made compensation arrangements.[8]

Conclusions

The Commission has stated that it intends for this draft legislation to give business greater certainty and to lower costs. We believe that these particular provisions, and the proposed amendments, will do exactly the opposite.

EJF believes that the revision of the data protection regime in Europe provides a real opportunity to incentivise businesses to embrace fully a positive attitude to compliance and "doing the right thing". However, we do not believe that the current provisions will achieve these desired outcomes because the draft legislation does not provide any incentives for compliance. It prioritises mass litigation at the expense of ADR, and it offers an inappropriate deterrence policy borrowed from competition enforcement theory that fails to address the very different landscape of data protection.

As a result, EJF recommends that:

- In the interest of coherence, all elements relating to collective complaints and redress, namely Articles 73(2), 73(3) and Article 76 (1), be deleted from the Proposal[9] in anticipation of the Commission's forthcoming Communication on the subject;
- Were collective procedures to remain in the proposal then there should be safeguards, including ADR, whichshould be encouraged as a means to fast and efficient dispute resolution, with litigation reserved as a last resort; and
- The legislation should incentivise compliant behaviour *and* provide the tools for quick & effective resolution of problems between data subjects and businesses, rather than bluntly punishing wrongdoing. The threat of serious and large fines should be, in our view, the mechanism of last resort of ensuring regulatory compliance.

---

[8] *Banksys* case in Belgium – authority satisfied by commitments and compensation to complainants; Commission's *Pre-Insulated Pipe Cartel case* - one party's fines reduced by €5m after it paid compensation. German competition authority closed case after reaching agreement with 29 gas suppliers to refund €127m to customers (note that the Bundeskartellamt guidelines on fine amount specifies taking into account compensation payment in calculating fines). The Commission decided not to proceed against Angus Fire Armour after it gave undertakings to the Commission and paid compensation to Macron Fire Protection

[9] This is the position in line with that already adopted by the European Parliament's IMCO Committee in its Opinion, namely, amendments 198 and 201

EJF COMMENTS AND SUGGESTIONS

Committee on Civil Liberties, Justice and Home Affairs
2012/0011(COD)
16.1.2013

DRAFT REPORT
on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
(COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Jan Philipp Albrecht

Amendment 60

Proposal for a regulation
Recital 101

Text proposed by the Commission	*Amendment*
(101) Each supervisory authority should hear complaints lodged by any data subject and should investigate the matter. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject.	(101) Each supervisory authority should hear complaints lodged by any data subject ~~*or by association acting in the public interest*~~ and should investigate the matter. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject ~~*or the association*~~ of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject.

Or. en

Justification

See related amendments to Article 73(2).

Amendment 310

Proposal for a regulation
Article 73 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Any body, organisation or association ***which aims to protect data subjects' rights and interests concerning the protection of their personal data and*** has been properly constituted according to the law of a Member State shall have the right to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects if it considers that a data subject's rights under this Regulation have been infringed as a result of the processing of personal data.	*delete*

Or. en

Justification

The proposed provisions for a representative complaint mechanism, can in turn lead to collective proceedings. Consideration of such collective mechanisms should await the emergence of the Commission's Communication on Collective Redress. Any such mechanisms would need extensive provisions and safeguards to protect from the substantial risks of abuse.

Amendment 310a

Proposal for a regulation
Article 73 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Independently of a data subject's complaint, any body, organisation or association referred to in paragraph 2 shall have the right to lodge a complaint with a supervisory authority in any Member State, if it considers that a personal data breach has occurred.	*delete*

Or. en

Justification

Allowing representative bodies to act without authorisation of any data subjects in lodging a complaint introduces the potential for speculative and vexatious complaints. Such a mechanism needs extensive provisions and safeguards to protect from the substantial risks of abuse.

Amendment 312

Proposal for a regulation
Article 76 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Any body, organisation or association referred to in Article 73(2) shall have the right to exercise the rights referred to in Articles 74 and 75 on behalf of one or more data subjects.	*delete*

Or. en

Justification

This introduces a collective redress mechanism which is detached from any consideration of the principles that may emerge from the Commission's forthcoming Communication on Collective Redress).

Amendment 313

Proposal for a regulation
Article 77 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the controller or the processor for the damage suffered.	1(a). Any person who has suffered damage, ~~***including non-pecuniary loss,***~~ 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.

Or. en

Justification

Compensation for non-pecuniary loss introduces non-restorative aspects and is uncertain. A person who suffers damage as a result of a relevant infringement should be compensated for the damage suffered and it is up to the court seised to determine that compensation.

Amendment 316

Proposal for a regulation
Article 79– paragraph 2

Text proposed by the Commission	*Amendment*
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 cooperation with the supervisory authority in order to remedy the breach.***	2. The administrative sanction shall be in each individual case ~~effective,~~ proportionate ~~and dissuasive~~.

Or. en

Justification

Supervisory authorities need to be able to operate flexibly and consider each individual case. Some sanctions may need to be dissuasive, and some persuasive. The proposals from the Commission and the Committee are too restrictive and tie the hands of the supervisory authority.

Amendment 317

Proposal for a regulation
Article 79 – paragraph 2 a (new)

Text proposed by the Commission	*Amendment*
	~~*2a. In order to determine the type, the level and the amount of the administrative sanction, the supervisory authority shall take into account all relevant circumstances, with due regard to the following criteria:*~~
	~~*(a) the nature, gravity and duration of the infringement,*~~
	~~*(b) the intentional or negligent character of the infringement,*~~
	~~*(c) the degree of responsibility of the natural or legal person and of previous infringements by this person,*~~
	~~*(d) the technical and organisational measures and procedures implemented pursuant to Articles 23 and 30,*~~
	~~*(e) the specific categories of personal data affected by the infringement*~~
	~~*(f) the repetitive nature of the infringement*~~
	~~*(g) the degree of harm suffered by data subjects,*~~
	~~*(h) the pecuniary interest leading to the infringement by the person responsible and the level of the profits gained or losses avoided by the person responsible, insofar as they can be determined,*~~
	~~*(i) the degree of cooperation with the supervisory authority in order to remedy the infringement and mitigate the possible adverse effects of the infringement, and*~~
	~~*(j) the refusal to cooperate with or obstruction of inspections, audits and controls carried out by the supervisory authority pursuant to Article 53.*~~

Or. en

Justification

See amendments to Article 79(2).

Amendment 318

Proposal for a regulation
Article 79 – paragraph 3

Text proposed by the Commission	*Amendment*
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:***	3. In case of a ~~*first and*~~ non-intentional ***breach of*** this Regulation, a warning in writing may be given and no sanction imposed.
(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.	

Or. en

Justification

See amendments to Article 79(2).

Amendment 319

Proposal for a regulation
Article 79 – paragraph 4

Text proposed by the Commission	*Amendment*
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*:*	4. The supervisory authority ~~*shall*~~ *may* impose a fine ***that shall not exceed*** 250 000 EUR, or in case of an enterprise 0,5 % of its annual worldwide turnover, to anyone who intentionally or negligently ***infringes*** Article 12(1) and (2).
(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).	

Or. en

Justification

Supervisory authorities need to be able to operate flexibly and consider each individual case. The proposals from the Commission and the Committee are too prescriptive and tie the hands of the supervisory authority by mandating a fine.

Amendment 320

Proposal for a regulation
Article 79 – paragraph 5

Text proposed by the Commission	*Amendment*
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:***	5. The supervisory authority ~~*shall*~~***may*** impose a fine ***that shall not exceed 500 000 EUR,*** or in case of an enterprise 1 % of its annual worldwide turnover to anyone who intentionally or negligently ***infringes Articles 11, 12(3) and (4), 13, 14, 15, 16, 17, 18, 24, 28, 31(4), 44(3), 80, 82, 83.***
(a) does not provide the information, or does provide incomplete information, or does not provide the information in a sufficiently transparent manner, to the data subject pursuant to Article 11, Article 12(3) and Article 14;	
(b) does not provide access for the data subject or does not rectify personal data pursuant to Articles 15 and 16 or does not communicate the relevant information to a recipient pursuant to Article 13;	
(c) does not comply with the right to be forgotten or to erasure, or fails to put mechanisms in place to ensure that the time limits are observed or does not take all necessary steps to inform third parties that a data subjects requests to erase any links to, or copy or replication of the personal data pursuant Article 17;	
(d) does not provide a copy of the personal data in electronic format or hinders the data subject to transmit the personal data to another application in violation of Article 18;	
(e) does not or not sufficiently determine the respective responsibilities with cocontrollers pursuant to Article 24;	
(f) does not or not sufficiently maintain the documentation pursuant to Article 28, Article 31(4), and Article 44(3);	
(g) does not comply, in cases where special categories of data are not involved, pursuant to Articles 80, 82 and 83 with	

rules in relation to freedom of expression or with rules on the processing in the employment context or with the conditions for processing for historical, statistical and scientific research purposes.

Or. en

Justification

Supervisory authorities need to be able to operate flexibly and consider each individual case. The proposals from the Commission and the Committee are too prescriptive and tie the hands of the supervisory authority by mandating a fine.

Amendment 321

Proposal for a regulation
Article 79 – paragraph 6

Text proposed by the Commission	*Amendment*
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:*	6. The supervisory authority ~~*shall*~~*may* impose a fine ***that shall not exceed*** 1 000 000 EUR or, in case of an enterprise 2 % of its annual worldwide turnover, to anyone who intentionally or negligently ***infringes the provisions of this Regulation other than those referred to in paragraphs 4 and 5.***
(a) processes personal data without any or sufficient legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7 and 8;	
(b) processes special categories of data in violation of Articles 9 and 81;	
(c) does not comply with an objection or the requirement pursuant to Article 19;	
(d) does not comply with the conditions in relation to measures based on profiling pursuant to Article 20;	
(e) does not adopt internal policies or does not implement appropriate measures for ensuring and demonstrating compliance pursuant to Articles 22, 23 and 30;	
(f) does not designate a representative pursuant to Article 25;	
(g) processes or instructs the processing of personal data in violation of the obligations in relation to processing on behalf of a controller pursuant to Articles 26 and 27;	
(i) do(h) does not alert on or notify a personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the data subject pursuant to Articles 31 and 32;es not carry out a data protection impact assessment pursuant or processes personal data without prior authorisation or prior consultation of the supervisory authority pursuant to Articles 33 and 34;	

(j) does not designate a data protection officer or does not ensure the conditions for fulfilling the tasks pursuant to Articles 35, 36 and 37;

(k) misuses a data protection seal or mark in the meaning of Article 39;

(l) carries out or instructs a data transfer to a third country or an international organisation that is not allowed by an adequacy decision or by appropriate safeguards or by a derogation pursuant to Articles 40 to 44;

(m) does not comply with an order or a temporary or definite ban on processing or the suspension of data flows by the supervisory authority pursuant to Article 53(1);

(n) does not comply with the obligations to assist or respond or provide relevant information to, or access to premises by, the supervisory authority pursuant to Article 28(3), Article 29, Article 34(6) and Article 53(2);

(o) does not comply with the rules for safeguarding professional secrecy pursuant to Article 84.

Or. en

Justification

Supervisory authorities need to be able to operate flexibly and consider each individual case. The proposals from the Commission and the Committee are too prescriptive and tie the hands of the supervisory authority by mandating a fine.

European Federation of Journalists

EUROPEAN MAGAZINE MEDIA ASSOCIATION

ENPA EUROPEAN NEWSPAPER PUBLISHERS' ASSOCIATION

Proposed General Data Protection Regulation: Exemption for Data Processing for Journalistic Purposes (Article 80)

Press Freedom in Europe in severe danger

EFJ - the European Federation of Journalists, EMMA - the European Magazine Media Association and ENPA - the European Newspaper Publishers' Association, are extremely concerned by the ongoing Council negotiations regarding Article 80 of the proposed General Data Protection Regulation. We note that new changes regarding the wording are being discussed, but worryingly the key issue still remains unaddressed: the Council text does not include a **robust and directly applicable exemption** for data processing for journalistic purposes. This exemption is indispensable for a free press in Europe.

The Council text in its current version – just like the text of the Parliament – does not guarantee any protection for press freedom, but leaves it entirely up to the Member States to "reconcile" the right to the protection of personal data with the right to freedom of expression. The wording of the **Council text even implies** that data protection rules are **to be applied to journalistic data processing**.

Not only would the adoption of this Council wording be a tremendous step backwards and fall far behind the current level of protection of press freedom, it would represent the **abolition of the current *acquis communautaire* on European press freedom**.

At Council level, the proposed changes to the Article 80 text which have been under discussion would result in a weakening of the guarantees set out in the original Commission proposal and as compared to the Directive 95/46/EC. The wording of an optional "reconciling" presents the risk of leaving too much flexibility for Member States when it comes to the implementation of Article 80. It would also create a **risk of governments' misuse** of this provision in Member States where protection of press freedom remains weak. As mentioned above, the wording even implies that data protection rules could apply to journalistic data processing. Therefore, those Member States willing to uphold press freedom on a national level, might even be hindered to do so by the Regulation.

Moreover, the Council should not follow the **European Parliament's approach**, which rendered the Article 80 exemption meaningless given that the primary purpose of this exemption – in both the current Data Protection Directive (95/46/EC), as well as the Commission proposal – is the protection of journalistic activities. The Parliament's text, however, omits any specific reference to journalistic data processing, in an attempt to cover other forms of expression online (including blogs, forums, etc.), and makes the exemption sound almost optional ("whenever this is necessary") rather than being binding.

1. Solutions

The best approach would be to amend Article 80 so as to create a directly applicable and binding exemption on processing of personal data for journalistic purposes, as proposed by the European Parliament's opinion-giving committees (ITRE and JURI). This would subsequently avoid a scenario whereby a Member State could abuse the flexibility of Article 80 or even use it as an argument for the application of the regulation to journalistic data processing. The exemption also needs to clearly identify the Chapters, which are not to be applied to journalistic data processing. These Chapters need to be taken out as a whole

and not leave room for misunderstanding as the Commission proposal did (e.g. "the general principles in Chapter II, the rights of the data subject in Chapter III", etc.). Moreover, Chapter VIII, regulating remedies, liability and sanctions, has to be included in the exemption.

The direct enforcement of the exemption is consistent with the principle of subsidiarity. Journalistic activities, although exempted from specific Articles of the Data Protection Regulation, would continue to be regulated by national libel, defamation and media laws, including those relating to privacy and other fundamental rights, which are guaranteed in each Member State.

A clear and robust exemption for journalistic activities would not hamper the protection of other forms of expression. Without distorting the main purpose of the journalistic exemption, it would be possible to add a second paragraph to Article 80 covering blogs, forums, etc. We believe it is essential to keep an explicit reference to journalistic activities, in light of the legislation and ethical rules governing the extensive responsibilities that professionals in the media sector already have to comply with, as compared to others. It is important to uphold this distinction.

2. What could a robust and clear exemption in Article 80 look like?

a) *Current Council Text*

The **current Council text** is unacceptable for the reasons mentioned above, basically because it places press freedom in Euope in severe danger.

Article 80

The national law of the Member State shall (...) reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression, including the processing of personal data for journalistic purposes and the purposes of **academic,** artistic or literary expression.

b) *Ideal solution*

The **ideal solution** foresees a direct applicability of the exemption. Non-journalistic freedom of expression is protected in a separate paragraph:

Article 80

1. Chapter II *(*General principles*)*, ***Chapter III*** *(rights of the data subject)*, ***Chapter IV*** *(controller and processor)*, ***Chapter V*** *(*Transfer of personal data to third countries and international organisations*)*, ***Chapter VI*** *(*Independent supervisory authorities*)*, ***Chapter VII*** (Co-operation and consistency*)* ***and Chapter VIII (Remedies, liability and sanctions) shall not apply to the*** processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression in order to reconcile the right to the protection of personal data with the rules governing freedom of expression.

2. Paragraph 1 shall apply correspondingly to the processing of personal data for purposes of non-journalistic expression of opinions or allegations of facts.

Alternative paragraph 2 (giving Member States a greater margin of appreciation):

2. Member States shall provide for exemptions or derogations from the provisions mentioned in paragraph 1 of this article for the processing of personal data not covered by sentence 1 of this paragraph, whenever this is necessary in order to reconcile the right to the protection of personal data with the rules governing freedom of expression.

c) *Minimum Solution*

If a directly applicable exemption cannot be agreed upon, the following **minimum solution** has to take into account as follows:

(1) There must be a clear obligation and no discretion for Member States in implementing the exemption for data processing for journalistic purposes.
(2) The exemption must cover as a minimum any processing "for journalistic purposes. There must be no suggestion of any unclear balancing process being required.
(3) Chapters have to be clearly identified in an encompassing way, including VIII
(4) Non-journalistic data processing must be protected separately and distinguished from journalistic data processing.

Article 80
1. Member States shall provide for exemptions or derogations from ***Chapter II (General principles), Chapter III (Rights of the data subject), Chapter IV (Controller and processor), Chapter V (Transfer of personal data to third countries and international organisations), Chapter VI (Independent supervisory authorities), Chapter VII (Co-operation and consistency) and Chapter VIII (Remedies, liability and sanctions)*** for the processing of personal data carried out ~~solely~~ for journalistic purposes or the purpose of artistic or literary expression in order to reconcile the right to the protection of personal data with the rules governing freedom of expression.

2. The obligation for member states in paragraph 1 applies to processing of personal data not covered by paragraph 1 whenever this is necessary in order to reconcile the right to the protection of personal data with the rules governing freedom of expression.

[or, as another option of including non-journalistic freedom of expression]

2. Member States shall provide for exemptions or derogations from the provisions mentioned in paragraph 1 of this article for the processing of personal data not covered by sentence 1 of this paragraph whenever this is necessary in order to reconcile the right to the protection of personal data with the rules governing freedom of expression.

Contacts:

[redacted]

A next-generation privacy framework

Examples in action and precedents

vodafone

Introduction

The principles of European data protection provide a sound foundation for regulation. But economic, societal and technological changes have brought to light fundamental shortcomings: Our regulatory model is inflexible, overly process-oriented, and heavily reliant on legal formalities. It overly burdens stretched national governments, puts European businesses at a competitive disadvantage, and fails to achieve real privacy protections for European citizens.

Industry must do better at respecting consumer privacy. But the regulatory framework must create the right incentives for it to do so. Personal information is essential to the information economy, but the European regulatory framework as it is cannot ensure sustainable economic development or even keep pace with protecting the rights of individuals.

Accountability must be an alternative to prescriptiveness, not an overlay.

We cannot overstate the importance of accountability to improving industry's privacy and data protection performance. Accountability – the outward demonstration of responsibility – has a very important part to play in encouraging the creation of internal governance and assurance processes that deliver better privacy outcomes. But these processes will develop only when they are a substitute for and not an overlay to a prescriptive, legalistic compliance regime.

We explain here how a principles-based accountability model – using many of the features of the existing regulatory framework (codes of conduct, certification schemes and privacy impact assessments) and combined with strong and effective enforcement – can build a solid ground within a next-generation privacy framework.

Accountability is not a new concept, and the challenges faced by policy makers in the privacy sphere are not necessarily unique. Policy makers here can learn from other sectors, such as corporate governance or environmental regulation, so we discuss some precedents that can help guide this Regulation.

How do we build a better Regulation?

To address the shortcomings of the Directive, the Regulation must be reoriented towards a principles-based 'accountability model'. What this means in general terms is that the Regulation should reiterate the principles upon which privacy is to be respected (here we see no need to diverge substantially from the principles of the Data Protection Directive and other international instruments). But rather than prescribing the means for organisations to live up to the principles, the Regulation must identify the outcomes that are expected, give companies the flexibility to create the internal governance that achieves those outcomes, and use certification programmes, third-party audits and judicious oversight and enforcement to ensure that those outcomes are met.

Contents

See Amendment 1 in the attached annex

1. Set high-level principles and expected outcomes in the Regulation.

We believe the existing framework of both the Directive and the Regulation achieves this. The principles are there, and they are solid. The expectations have been set for meeting data subjects' rights with respect to access, transparency and control.

2. *Create a regulatory regime that leaves room for codes of conduct.*

The Regulation as proposed continues to overlay the basic principles of data protection with a prescriptive regime intended to impel industry to take specific steps intended to achieve compliance with those principles. But the prescriptive approach in the current regime has not achieved the desired outcomes, and more of the same is unlikely to create change.

Beneath the overarching principles set by the Regulation, the policy framework must establish a 'tool-kit' of measures and regulatory instruments that will equip regulators to play an active role with industry, civil society and others to agree proportionate and effective measures that ensure outcomes are achieved using risk management methodology.

The bones of a better approach were included in the Directive, in Article 27 on Codes of conduct (now Article 38 of the Regulation). But codes of conduct have largely been ignored by both industry and regulators, precisely because the prescriptive regime leaves little incentive to invest the time and resources in an alternative that does nothing to lighten the burden. For the spirit of Article 38 to be achieved, the Regulation must embrace an effective system of codes of conduct, but must also include the right incentives to use that system. With the right framework in the Regulation, regulators, companies, sectors or industries are properly incentivised to agree specific codes of conduct that implement data protection principles. And we've seen in other contexts that the process of negotiating those agreements will spur innovative approaches to achieve the principles of the Regulation, while at the same time lightening the burden on industry.

3. *Conduct formal reviews of codes of conduct in an evidence-based and open environment.*

Regulators should be bound to review applications for codes in a transparent, open and accountable process (including, for instance, the hearing of evidence from interested parties) and issue determinations. Determinations should be subject to appeals to a tribunal or court, in turn helping to create real case law interpreting Regulation.

A core part of any such dialogue should be the hearing of evidence from interested parties, including consumer and user groups. This is particularly important as consumer attitudes and behaviours change faster than regulators can keep up, leading to the risk that the legal framework is ignored by large parts of the population, or that it loses legitimacy.

A public forum will enable all stakeholders to frame the dialogue according to the evidence of risks and concerns presented, and therefore ensure the resulting code is proportionate. Failing a deal, regulators must be empowered to act, but the public evidence should remain a vital component of any unilateral determination of what is proportionate regulatory action.

Precedent: Environmental Regulatory Covenants

A successful co-regulatory code of conduct approach can be found in environmental regulation. In the process of regulatory covenants, regulators and industry work from common principles to identify areas of risk and agree ways to achieve outcomes that address those risks. Regulatory covenants have been successfully used to resolve a lack of progress, innovation and "internalisation" of regulatory requirements by industry on environmental issues – common complaints about privacy as well.[1]

What is the parallel between privacy and the environment? Both are subject to "externalities" – harms for the physical / digital environment that are borne disproportionately by society rather than those who create the harms. Factories could contaminate rivers with effluent resulting from industrial processes, a cost borne by those living in the area but not easily transferred to the producer. So the excessive collection, generation or sharing of personal data may create costs to society (including the individuals concerned) that are not fully borne by the digital producer.

Environmental regulators had difficulty finding ways to transfer more of the burden to the producers, while also encouraging them to invest in innovative, less polluting technologies and processes. Early on, overly prescriptive legislation had the unintended effect of encouraging firms to seek legal loopholes or engage in riskier practices, rather than accept the overarching principles of environmental protection and work towards a sustainable future for all.

This narrative will be familiar for those regulating privacy. The frustrations with data protection law largely derive from a sense that corporations are ignoring its spirit and focus instead on ways to weave through the rules. Regulatory covenants are helpful in this context because, by empowering industry to jointly create compliance mechanisms, they compel industry to internalize the principles and also to innovate – to look for new ways to achieve the principles while lightening the burden on their businesses.

In the privacy field, we believe that regulatory covenants will be the most effective way to encourage privacy-by-design, by enabling companies to create new privacy enhancing technologies that meet the principles of the law and reduce the risks and the demands of traditional, labour-intensive compliance mechanisms.[3]

Compliance with an approved code of conduct should be treated as compliance with the Regulation unless and until overturned by a court.

See Amendment 6, Article 38.

4. *Accredit independent assessors and seal programmes that perform the oversight function. Develop incentives for industry to use them and report on their results.*

Regulated organisations should be encouraged to commission accredited independent assessors to review their privacy programmes and provide reports to regulators and to the public on their compliance. Those who commit to independent assessment and transparent reporting should receive a waiver of the Regulation's more prescriptive elements on documentation and prior authorisation – the assessment and reporting would replace these now redundant oversight mechanisms.

See Amendment 5, Article 34

The Regulation must incentivise uptake by making commitment to accountability and an effective internal privacy management programme (as we describe later) a mitigating factor in any sanctions imposed. Of course, organisations that do not, for whatever reason (be it size, maturity of the programme or perceived risk) see the value of an accountability programme should be able to continue under the existing regime.

For instance, the Working Party or EDPB could be empowered to certify independent assessors to conduct assurance monitoring and reporting, and organisations could be encouraged (or even required, in some circumstances) to retain such independent assessors to monitor and report on their compliance with the principles set out in any second-generation framework.

See Amendment 7, Article 39

Because the supervisory authority retains ultimate control over the accreditation of assessors, this framework enables a scaling of the supervisory regime using market forces. Those who can afford to (because the economic gains justify it) will pay an independent assessor so that they can act quickly in the marketplace, spurring rather than impeding technological innovation and shifting the regulatory cost to the market rather than the public purse.

Those who choose not to pursue an independent assessment can of course continue to rely on the supervisory authorities' oversight using the traditional prescriptive mechanism – the existence of an alternative approach should free up resources so that the authorities can act in a timely manner, making this a better approach for all involved.

See Amendment 2, Article 22(3), Amendment 3, Article 28(1)-(2), (4)

Precedent: Article 29 Working Party points to financial, competition laws

Outside of the environmental space, the Article 29 Working Party in its 2010 document on accountability discussed various additional precedents in financial services and competition compliance spaces for the model we discuss here.

"Outside the world of data protection, there are some examples of accountability - as a program specifying a data controller's policies and procedures to ensure compliance with laws and regulations. For example, compliance programs are mandatory under financial services regulations. In other cases, compliance programs are not mandatory but are encouraged, such as in the field of competition law. For example, in Canada, the Competition Commissioner has developed elaborate policies on corporate compliance programs. The decision on whether or not companies apply a program is voluntary. However, the Canadian Competition Commissioner stresses the importance of compliance as a risk mitigation tool and stresses the legal, reputational and economic benefits."[7]

How must organisations comply?

The elements of internal accountability governance have been discussed by many other commentators. We'd like to elaborate here on what we built and the precedents we borrowed from that guided us, as a potential model for the regulatory framework that can encourage other companies to follow.

1. *Culture, not "tick-box" compliance*

The companies who have made the most progress in reorienting their approach to privacy have been those that make privacy a matter of corporate culture rather than just legal "tick-box" compliance. We take as precedent the UK Bribery Act 2010 (see sidebar), which encourages regulated industry to take steps to internalise their commitment to compliance by, for example, setting the tone at the very top of the organisation and creating a sense of ownership and responsibility throughout the organisation (not just with lawyers and compliance experts) through training and communication.[4]

See Amendment 2, Article 22(2)(b)

2. *Operationalising privacy risk management*

Environmental regulations have one aspect that has been widely credited with truly internalising compliance within a company – the Environmental Management System, which applies advanced business management practices to the environmental aspects of a company's operations. It turned companies' internal environmental compliance programmes from

Precedent: UK's Bribery Act 2010

The UK's antibribery regime is made up of a high-level legal requirement to have in place adequate procedures designed to prevent a breach in the law, along with an implementation guide that sets out principles rather than prescriptive rules. These principles are:

Proportionate Procedures. An organisation has procedures to prevent bribery proportionate to the bribery risks it faces and to the nature, scale and complexity of its activities. The procedures should be clear, practical, accessible, effectively implemented and enforced.

Top-level commitment. Top-level management (a board of directors, the owners or an equivalent) are committed to preventing bribery. They foster a culture within the organisation in which bribery is never acceptable.

Risk assessment. The organisation assesses the nature and extent of its exposure to external and internal risks of bribery on its behalf. The assessment is periodic, informed and documented.

Due diligence. The organisation applies due diligence procedures in a proportionate and risk-based approach to mitigate identified bribery risks.

Communication and training. The organisation ensures that its bribery prevention policies and procedures are embedded and understood throughout the organisation through internal and external communication, including training, that is proportionate to the risks it faces.

Monitoring and review. The organisation monitors procedures designed to prevent bribery and makes improvements where necessary.

Companies subject to the Act have a strong incentive to demonstrate commitment to these principles at the highest level of their organisation: if they can show that adequate procedures were in place to prevent bribery, then it is a full defence. Several years on, we have seen UK businesses build flexible, comprehensive global programmes, with significant executive support, because of the nature of the regulatory framework in which they operate.[6]

a process largely reactive to governmental regulations or public outcry, to a proactively managed part of their operations.[5]

Such a turnaround is clearly needed in privacy management as well. European companies are too heavily invested at this point in traditional data protection compliance models, overseen by relatively low-level lawyers who have reactive interpretation of law as their responsibility (often one of several). Instead, companies should be incentivised through the regulation to create Privacy Risk Management programmes.

Regulation and its supervisory authorities can support, and give incentives for, the adoption of privacy risk management programmes by private entities and governmental organizations. They can create international databases of information on how companies are doing on programme implementation. They can impose lower penalties on companies with a bona fide programme. They could provide information and technical assistance to those companies interested in doing so.

A company, through its programme, would commit to assessing its impact on personal privacy, setting ambitious goals for protecting personal information, systematically developing strategies to meet these goals, monitoring progress and continually improving in its protection of personal information. Any privacy code of conduct should naturally require the adoption of a privacy risk management programme as one of its terms.

See Amendment 2, Article 22(2)(a)

3. *Widespread use of impact assessments*

Many of the proposals we have put forward here will require organisations to move from a legalistic approach to a risk-based approach. That is, to focus less on interpreting strict and inflexible rules and instead shift resources and focus to creating a deeper understanding of privacy risks and developing effective solutions to address those risks. The best way to achieve a risk-based approach is through the use of the Privacy Impact Assessment. The effective use of impact assessments can deliver better privacy practices and can incentivise innovation in approaches to privacy risks. The Regulation must create incentives for industry to adopt impact assessments, and regulators must encourage their use as part of a privacy risk management culture.

One sure way to encourage organisations to adopt impact assessments is to reward their use. For example, if an organisation can verify that it has diligently implemented an impact assessment it should act as a mitigating factor when examining any alleged breach of the Regulation.

See Amendment 4, Article 33

4. *External evidence of internal programmes*

The draft Regulation includes a positive move away from existing filing, prior authorisation and notification regimes to a requirement to retain documentation of compliance. But the current draft's overly prescriptive documentation rules leave little room for companies to build the kind of programme we discuss here. The Regulation must require organisations to show exter-

Precedent: Mandatory and voluntary public reporting regimes

Reporting regimes have been mandated successfully in other sectors (for example, their long use in areas of accounting and finance). There is also an extensive practice of voluntary reporting, for example in corporate responsibility through independent assurance standards like AA1000 APS (Principles Standard), launched in 2008, which provide a recognized basis for organisations to report on their compliance with principles.[8]

Although tarnished in this economic environment, the fundamental model for this kind of oversight is clearly the regulation of accounting and the financial services. It can be argued that the failure of this model there was not due to inherent weaknesses in the model itself, but in the failure of the oversight and enforcement role. We believe that the framework discussed here, when combined with the dedicated regulatory bodies of the existing Directive, can prove a powerful combination.

nal evidence of their internal privacy management programmes, and must provide incentives for organisations whose size or risk profiles justify the retention of independent assessors to verify their programmes and publish reports on their overall compliance. One strong incentive would be removing other prescriptive requirements for those organisations that do so. This would be a far more effective mechanism in creating transparency and accountability than the existing requirements. Documentation requirements of the kind we propose will also serve as a solid foundation for the kind of oversight and enforcement we discuss below.

See Amendment 2, Article 22(3)

How will the Regulation be enforced?

Any regulatory model will succeed or fail on the strength of its oversight and enforcement model. Organisations must be held to account for their record in implementing the data protection principles and achieving the outcomes required by the Regulation, by whatever means they have adopted.

Supervision is currently the monopoly of the national regulator, and this creates both a resource and skills bottleneck. It is clear that we need to explore alternatives to direct supervision by regulators. National regulators frequently cite lack of resources as a major impediment to their supervisory role. The increased use of codes of conduct, as we call for above, will place further pressure on the scarce public resources of our regulators.

The solution is to create the independent monitoring and assurance programmes we discussed earlier. In this supervisory model, regulators are required to accredit independent assessors who can be commissioned by companies to review their privacy programmes. Such assessors are then empowered to provide reports to regulators and even to the public.

In a similar vein, 'privacy seals' and trust programmes can provide independent assessment on a more limited basis, such as for specific products or technologies, as illustrated by the good work of organisations like EuroPrise.

See Amendment 7, Article 39

Importantly, this model will stimulate the creation of a secondary market in privacy compliance assessment, reducing the pressure on regulators as a resource bottleneck, but remaining accredited and approved by the regulator. It will lead to the development of a professional community of skilled privacy assessors with the goal of helping enterprises (public and private) develop the internal culture and professional support structures necessary to embed privacy compliance within their organisations.

Independent assessors would also be in a position to gather feedback and learning from the assessment process that can, without compromising the confidentiality of individual companies, act to inform and educate both the regulator and policy makers more generally about what is happening on the ground.

Conclusion

We are strongly pro-regulation. Industry will never improve its privacy track record without clear obligations and strong enforcement. But more prescriptiveness is not the answer. Privacy is too important to be marginalised in the corporate legal department.

Strange though it may sound, the new Regulation must embrace ambiguity – uncertainty in regulation is not necessarily a flaw. Designed into the right framework, it can impel companies to empower strategic professionals to make risk-based, business-oriented decisions that produce better outcomes than prescriptive rules could. And it must be accompanied by strong and effective enforcement, with significant impacts for companies that get it wrong. Policymakers have to be bold to allow ambiguity. But it's not a compromise, it's an essential element of a successful regulatory framework.

[1] Examples of regulatory covenants in six European countries were described in a 2011 report of the European Environment Agency, which states, "By 1996 more than 300 EAs

had been concluded at the national level in the EU." http://www.eea.europa.eu/publications/92-9167-052-9-sum

[2] One clear example is the Dutch Energy Efficiency Benchmarking Covenant, which set a flexible approach for meeting goals to reduce greenhouse gas emissions and governs 80% of Dutch industrial energy use. http://www.benchmarking-energie.nl/

[3] We have borrowed heavily here from the input of Dennis Hirsch, Geraldine W. Howell Professor of Law, Capital University Law School. Dr. Hirsch served as 2010 Fulbright Senior Professor at the University of Amsterdam, Faculty of Law, Institute for Information Law. He argues that there are similarities between the challenges faced by sustaining the environment and the challenges for information society, and that policy makers could learn from experiences in the more mature field of environmental regulation. See Dennis D. Hirsch, Capital University Law School, 'Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law', Georgia Law Review, Vol. 41, No. 1 (2006).

[4] As an example of best practice, see Vodafone's privacy risk management system as described at http://www.vodafone.com/content/dam/vodafone/about/privacy/vodafone-privacy-programme.pdf.

[5] See Hirsch, above.

[6] http://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf

[7] http://ec.europa.eu/justice/policies/privacy/docs/wp-docs/2010/wp173_en.pdf

[8] http://www.accountability21.net/

WFA WORLD FEDERATION OF ADVERTISERS

allegrogroup

Considerations on Article 38 - Codes of Conduct Proposal for a Data Protection Regulation

This purpose of this document is to present the case for a bigger role for codes of conduct in the creation of an effective co-regulatory landscape for the protection of data across the Union. It also seeks to express concerns that the current wording of Article 38 on codes of conduct within the draft General Data Protection Regulation will restrict the growth of codes and hamper their ability to, in support of the Regulation, effectively protect consumer's data and facilitate digital innovation.

Executive Summary

Codes of conduct are well suited for the purpose of enhancing data protection and privacy standards in the digital world. At their best, they are dynamic, inclusive, accountable and increasingly sophisticated policy tools designed to complement legislation.

The important role that codes of conduct can play in this context was acknowledged within Article 27 of the 1995 Data Protection Directive; yet this article has not had the desired effect. Indeed, we would go so far as to say that the article, originally designed to encourage the creation of codes of conduct, has acted as an inhibitor to the emergence and growth of effective codes.

It is clear that Article 27 has failed to deliver any critical mass of self-regulatory initiatives. The FEDMA code is to-date, the only one which has formally been approved under Article 27; a process which took 5 years to complete. The RFID PIA Framework supported by a Commission-led expert group and requiring the endorsement of the Article 29 WP, still took over 3 years.

In light of the speed of change across the digital landscape, an approval process of this length seriously risks delaying the introduction of solutions and making any approved code obsolete at the point of approval. It also undermines one of the core strengths of codes of conduct; their ability to react quickly to address concerns as they evolve.

In addition, Europe's self-regulatory framework for online behavioural advertising, managed by EDAA, was never submitted to the Article 29 Working Party, partly due to the limited appreciation of the full range of purposes which codes of conduct can serve.

Unfortunately, the proposed wording of Article 38, on the drawing up of codes of conduct, in the General Data Protection Regulation is heavily based on the 95 Directive. As such, we believe this Article in its current form risks repeating the same mistakes as its predecessor.

Therefore we strongly encourage all stakeholders, to consider positive amendments to the text to:

- Explicitly acknowledge the significance of codes of conduct and the full range of purposes they can serve
- Specify the obligations of all actors to ensure legal certainty
- Provide proportionate incentives for industry to embrace codes of conduct
- Ensure the full integration of codes of conduct across relevant chapters of the Regulation

Existing examples of best practice

Europe has a strong intellectual foundation for the growth of effective codes of conduct. Self and co-regulation are common practice at the EU level and in the majority of its Member States.

The EU institutions first formally set out a role for self- and co-regulation in 2003, in the inter-institutional agreement on law-making. In February 2013, the European Commission published the Principles for Better Self-and Co-Regulation, which set out five main procedural and substantive conditions for self-and co-regulation to be effective:

- **Compliance with community law.**
- **Added value for the general interest** – Codes of conduct must not serve specific interest but have to add value for the general interest.
- **Transparency** – Codes of conduct need to be publically available.
- **Representativeness** - The number of drafting partners of code of conducts affects their credibility and effectiveness; codes must therefore be endorsed by a critical mass of industry players.
- **Monitoring** – Monitoring and evaluating the success of the objectives set out in codes of conduct are considered to be crucial to their success.

When combined, these principles create a robust and accountable policy-tool that complements legislation.

The nature and purpose of codes of conduct

For a legislation to effectively promote codes of conduct and acknowledge their broad value it should explicitly recognise the full range of purposes which they can serve.

One obvious purpose for codes of conduct, and the one which is currently acknowledged in the draft Regulation, is the effective application of the provisions included in the Regulation.

Another purpose which codes of conduct can serve is in their ability to establish standards and provisions, in areas relating to protection of personal data, but not explicitly referred to in the regulation. This would also contribute substantially to the future-proofing of the Regulation allowing it to adapt and evolve. Industry should be able to obtain the same official recognition and support from member states, data protection bodies and the Commission for such codes.

In full, we see codes of conduct as having at least the following purposes, which we believe should be stipulated in the article:

A. **Legal compliance and effective implementation:** ensuring the effective calibration and application of the law;

B. **Substantive protection:** the implementation of measures beyond the provisions of set out in the law, pertaining to the data protection;

C. **Single Market logic:** the harmonisation of practices throughout the Single Market;

D. **International harmonisation**: the spread of Union data protection standards beyiond the Union;

E. **Consumer engagement**: enhancing trust in data protection practices, notably through consistent experiences.

Codes as complementary not competitive

To be clear, codes of conduct are not designed to replace or compete with legislation. They are complimentary policy tools which are capable of enhancing standards in fluid, fast moving and complex environments.

This is especially the case in the digital world, where the growth of the market and the speed of technological innovation makes codes of conduct a critical component, along with legislative underpinnings, in addressing emerging policy concerns. They also place some of the resource burden required to achieve progress on industry. The sheer mass of digital activity also makes leveraging industries resources and expertise a very sensible proposition.

Codes of conduct are a voluntary framework, entered into freely. This should not undermine the value of codes as, if the code is effective, formally acknowledged and properly incentivised, participation in the code would make commercial sense.

Amending Article 38 within the GDPR

- *Explicitly acknowledge the significance of codes of conduct and the full range of purposes they can serve*

The draft Data Protection Regulation contained no explicit endorsement of codes of conduct. Without such a reference codes of conduct will continue to be received with undeserved skepticism by key actors and through them, broader society.

Currently, the only indications within the draft Regulation of the value of codes of conduct are:

- A statement that industry should be encouraged to use them (Recital 76, Article 38);
- An unclear reference to one of the value propositions of codes of conduct – namely that they can contribute to legal compliance ("facilitate the effective application of", or "intended to contribute to the proper application of" the Regulation – Recital 76, Article 38).

We would encourage an explicit acknowledgement, similar to the Audiovisual Media Services Directive (R44), of the value of codes of conduct and the responsibility of all stakeholders in encouraging the creation of best practice codes.

We would also welcome an acknowledgement that codes of conduct can, in certain circumstances, be the most appropriate tool, whether for the effective application of the Regulation or otherwise, in order to achieve policy goals.

- *Specify the obligations of all actors to ensure legal certainty*

Industry must have legal certainty on what is expected of it and on what can be expected from other actors in the process in order to encourage the take-up of codes of conduct.

This is particularly critical in relation to the obligations of the relevant supervisory authorities regarding prompt review, response and promotion for the code. Guidance on the specific requirements from industry, such as impact assessments, number and nature of signatories, monitoring proposals, required consultations, would also be contribute to the streamlining of the process.

Currently, clarity around actor's obligations is absent. Paragraph 2 of Art. 38, states:

> *"Associations and other bodies representing categories of controllers or processors in one Member State which intend to draw up codes of conduct or to amend or extend existing codes of conduct may submit them to an opinion of the supervisory authority in that Member State. The supervisory authority may give an opinion whether the draft code of conduct or the amendment is in compliance with this Regulation. The supervisory authority shall seek the views of data subjects or their representatives on these drafts."*

The original text fails to clarify any procedural obligations or apparent timeframe on the part of the authority involved. According to this wording, for example, a supervisory authority could choose to withhold an opinion on the code of conduct following submission. What should happen if the supervisory authority did not approve the code?

It is essential that all actors involved have greater clarity over what they can expect from this process and how it influences industries ability to effectively implement codes of conduct.

- ***Provide proportionate incentives for industry to embrace codes of conduct***

In order for codes of conduct to be effective they require a critical mass of engagement. In order to ensure maximum buy-in there should be genuine incentives for data controllers and processors to make a collective and voluntary commitment to create and adhere to a code of conduct and then to submit this code to a relevant authority. Without these incentives we risk reducing the ability of codes to harmonise processes.

The importance of incentives has been acknowledged by a number of member states and there has been broad support in the Council to more clearly identify and increase the number of incentives which should be made to apply to the use of codes of conduct.

Effective self-regulation may be incentivised in various ways. For example, adherence to a code of conduct could be used to create a category of processors and controllers for which, whilst in no way removing the fundamental obligations of the signatories, could be leveraged or used, for example, to reduce administrative burdens in the context of PIA's.

Another incentive could quite simply be an acknowledgement by the Commission, DPA' and Member States that in certain circumstances codes are <u>best</u> placed (ahead of a Delegated Act or EDPB guidance) to adapt the Regulation to a specific context. This could then supported by better integration of codes of conduct language into other articles in the regulation. The list which currently exists in Council' Article 38(1a) would be a good basis for this.

Codes of conduct could prove to be the solution to those cases that present practical issues, such as the Right to be forgotten in the online world, or clarify the obligations of controllers, just to name two.

Without contributing needlessly to the sea of icons which exist, another incentive could see the controlled development of a seal or icon, promoted by the Commission, which could be used by industry to create a reputational advantage.

The types of incentives available for signatories of codes should be clearly laid out in the Regulation.

Conclusions:

Legislators now have the opportunity to realise the potential which codes of conduct' represent.

We encourage all stakeholders to clearly express within the Regulation:

- The important role which codes of conduct can play in finding the right mix of legislation and code of conduct in the formation of a policy landscape;
- The full range of purposes which codes of conduct can play;
- The obligations of the actors involved;
- The incentives which signatories of the code of conduct should expect.

The Parliament's adopted amendments go some way to better integrating codes of conduct into other areas of the draft Regulation and clarifying actors' obligations but a lot more can still be done to improve the effectiveness of this Regulation in creating codes which are beneficial for all parties involved.

Suggestions for article text:

The following paragraphs describe in some detail the kind of text that we believe would be an appropriate framework for codes of conduct. We do not provide actual legislative text here, because we prefer to build consensus around the principles first:

Recital 76

- The recital should mandate a wide array of authorities to explicitly recognise the important role of codes of conduct in creating consistent and effective protection of personal data throughout the Union and encourage those authorities to promote their use.

- The recital should explicitly acknowledge that codes may serve purposes other than legal compliance. For example, the implementation of protections other than those set out in the Regulation but which pertain to the protection and processing of personal data

Recital 76(a)

- The recital should clearly state the importance of offering proportionate incentives for industry to adopt codes of conduct and to submit these to the relevant authority for opinion in order to ensure critical mass of signatories and encourage harmonisation of standards through codes.

Article 38

- The first paragraph should list the various purposes that codes of conduct can serve, including legal compliance, protections outside those specifies in the law, harmonization in the interests of the single market, spread of EU standards beyond the EU, and creation of consistent consumer experiences in order to build trust.

- Another paragraph, as proposed by the Commission, should list specific topics, within the Regulation, where legislators wish to see codes applied. This should be exhaustive.

- A further paragraph should set out criteria for the general validity of codes. We would propose compatibility with the law, transparency, critical mass, accountability/monitoring and dispute resolution.

- The basic steps of the process for the voluntary submission of codes for opinions from relevant authorities should be laid out. This should address both single-country and multi-country scenarios and include:
    - A requirement that the submitting parties specify which purposes the code is designed to fulfill;
    - Specifying which organization or body is mandated, as the relevant authority, to deliver an opinion (data protection authorities to opine on data protection aspects, competition authorities on competition aspects, consumer authorities on consumer aspects, etc.), and which other interested parties should be consulted as part of this process;
    - Explicitly stating that there should be no undue delay. References to timeframes for response would further encourage legal certainty for business and ensure swift progress can be made.

Article 38(a)

- This article should, in line with the Council' proposal, specify the appropriate requirements for a body mandated with monitoring compliance with a code. This should include:
    - Expertise in the relevant subject matter
    - Procedures to assess eligibility for and compliance with the code
    - Complaints handling facility
    - Ability to prove that no conflict of interest exists in monitoring the code

The World Federation of Advertisers (WFA) is the only global organisation representing the common interests of marketers. WFA champions responsible and effective marketing communications. The advertising sector currently has some of the most mature and robust self-regulatory frameworks in existence, including the European Advertising Standards Alliance and the European Digital Advertising Alliance.

Contact: [redacted]

The Allegro Group is the leading Central and East European e-commerce company. From its Polish home in Poznań, the group has expanded to cover close to a score of European countries, including 9 EU Member States. It operates e-marketplaces, e-retail sites, e-classifieds sites, online comparison shopping businesses, and a global online payments business.

Contact [redacted]