# Position Paper

**To:** **European Parliament**
**From:** Thuiswinkel.org[1]
**Date:** February 27th 2013

**Subject:** **proposal for amendments Data Protection Regulation (v.1.1)**

---

**Data Protection Regulation**
**Amendments concerning the neutrality of the Regulation and stakeholder participation**

**Introduction**
Over the years, the Article 29 Working Party has had a significant influence in implementing the EU Data Protection Directive 95/46/EC. It also has been heavily criticised by stakeholders for its interpretation thereof. Not only have some of its opinions been received as being too strict, the Article 29 Working Party also has been criticised for its total lack of transparency and stakeholder engagement, its often strict and sometimes unreasonable interpretation of the Directive as well as of the fact that at times it has openly been trying to steer the political discussion and judicial review on particular topics into a certain direction. More than once, its opinions have resulted in radical shift in the scope and application of the Directive. Because of the fact that the Article 29 Working Party is comprised of the supervisory authorities of the Member States, its opinion creates *soft law*, making the lack of stakeholder participation or political or judicial review even more pressing.

Where an Article 29 Working Party opinion merely clarifies the law and its application in specific cases, this is fine for as long as such clarifying opinions are based on widely accepted interpretations of the law and do not contain any surprises to experts in the field. An example of such clarifying opinion is WP187 on consent. However, the Article 29 Working Party has also issued opinions, which were of a much more principle or even political nature. Those opinions are often criticised by data protection experts.

Examples of such criticised opinions are:

- WP 56, where the Art. 29 Working Party held that a user's PC on which a cookie is place by a non-EU website qualifies as 'equipment located on the territory of a Member State', thus subjecting non-EU websites to the application of Directive 95/46/EC. Idem for the display of personalised ads and the creation of user profiles. Such interpretation should be rejected as it is impossible to comply with in practice. Especially in cyberspace companies should know upfront when and in what situations laws apply and not be dependent on the geographical location of the user;

- WP 74, where the Art. 29 Working Party introduced a requirement for the approval of Binding Corporate Rules (BCR) to provide the supervisory authorities with a copy of the (internal) audit reports on the data processing in case of updates of the BCR or upon request, thus expanding the powers of those authorities which by member state law did not have the power to audit controllers;

[1] Thuiswinkel.org is the Dutch association for 1700 webmerchants. www.thuiswinkel.org.

- WP117, where the Art. 29 Working Party restricted its opinion to the use of whistle blowing systems for combatting fraud and financial misconduct. Subsequently, many supervisory authorities have denied companies the possibility to use such systems to enforce the laws applicable to them as well as their internal policies on other important topics, such as child labour, environmental pollution, sexual harassment, discrimination, or even privacy and data protection. Furthermore, the Art. 29 Working Party restricted the possibility to allow anonymous reports to be made through whistle blowing systems, thus severely limiting the effectiveness of and employee trust in such systems;

- WP136, where the Art. 29 Working Party took an extremely broad view on the definition of personal data by also putting data, which do not (indirectly) identify a person under the definition of personal data, but also data which single someone out, even if such person is otherwise anonymous (e.g., IP-addresses, cookies, user-ID's, RFID-tags, MAC-addresses, and even graffiti). The Art. 29 Working Party justifies this interpretation by referring to Bodil Lindqvist (ECJ, C-101/01, 6 November 2003). However, nowhere in this case does the Court explicitly take such a position. Amendment 84 of the LIBE-report on the Regulation now also proposes to expand the scope of the Regulation to such data. Although a case can be made to justify such expansion, extending the scope this way without any restriction is one step too far. Data which single out an – otherwise anonymous – individual should only be protected by a limited number of specified provisions of the Regulation, such as the security obligation (art. 30), art. 14 (information), and 5 (principles). Applying the Regulation in full to such data would lead to unnecessary difficulties in compliance and implementation of the Regulation in organisations (see also proposals below).

- WP169/WP171, where the Article 29 Working Party was of the opinion that anyone who has factual influence over the purposes and the means of the data processing should be considered to be a controller. This interpretation expands the scope of the concept of controller to parties who up till then were only considered to be a processor as well as to parties to whom the Directive up till then was not considered to apply. For instance, in WP171, the Art. 29 Working Party stated that website publishers were covered by the information obligation of the Directive if they transfer directly identifiable information to the parties serving the ads on websites (ad network providers). Also, the Working Party states in WP171 that publishers share with ad network providers certain responsibility for the data processing that happens in the context of serving behavioural advertising. More particularly, the Art. 29 Working Party considers that this responsibility covers the first stage of the processing, i.e. the transfer of the IP address to ad network providers that takes place when individuals visit their web sites and are re-directed to the ad network provider web site. Following this opinion, many parties that were believed not to have any data protection obligations with regard to the data processed through their websites were now all of a sudden considered to be joint-controllers, leading to all kinds of practical implementation and compliance difficulties.

**Role of the Article 29 Working Party and EDPB**

Article 29 of Directive 95/46/EC fails to specify the role of the Article 29 Working Party. It merely states that the Working Party *"has an advisory status"*. This lack of specificity, encouraged by its independent status and diversity in the application of the Directive among Member States, has led the Article 29 Working Party to understand its role as being broad and comprehensive. In doing so, the Article 29 Working Party at times has overstepped the (invisible) boundaries of its advisory role by issuing interpretations of a more principle nature, which in fact should be the (exclusive) power of the courts, more specifically the European Court of Justice. Also, at times, it has issued opinions, which were more political in nature. Such interpretations however should be the (exclusive) power of the European legislator (Council, Parliament and Commission). Supervisory authorities and the Article 29 Working Party, and in the future the European Data Protection Board (EDPB), should only *apply* the law, not drive its development or the political debate.

The examples above show that over the years, the Art. 29 Working Party, without any stakeholder participation or judicial review, has gradually broadened the scope of data protection law to area's where experts did not expect the Directive to apply. Or it applied the law in ways that experts believed to be too strict. Because the Directive did not provide for a countervailing power with regard to the application and interpretation of the Directive by the Article 29 Working Party, it would even be fair to say that the Article 29 Working Party have 'monopolised' the legal and – up to a point also the political – debate on privacy and data protection law in Europe, especially with respect to the application of the Directive to the private sector. This conclusion is even further supported by the fact that the Directive requires Member States to obtain the prior advice of the supervisory authorities on legislative proposals, thus providing an incentive for the supervisory authorities and the Article 29 Working Party to have a political agenda. At the same time the political role of the Article 20 Working Party is also informally strengthened by politicians and others, who routinely ask its members to be keynote speakers at political events and policy-oriented conferences.

**Missed opportunity**

Now that the EU Data Protection Framework is being revised, there is also an opportunity to review the role and way of working of the Article 29 Working Party. Unfortunately, in its report the Commission didn't spend much attention to the way the Article 29 Working Party has operated in the past. Moreover, in order to ensure a harmonized approach to the enforcement of the Regulation, the Commission proposes to even further strengthen the role of the European Data Protection Board (the successor of the Article 29 Working Party). Although increased consistency in the application of the Regulation in the Member States is highly welcome given the current patchwork of laws in the Union, it is certainly a missed opportunity not to have assessed the way the supervisory authorities have operated in the Member States and the role of the Article 29 Working Party in the interpretation of Directive 95/46/EC prior to the draft of the Regulation.

**Draft LIBE report**

The draft LIBE-report on the Regulation further strengthens the role of the EDPB, as it proposes to delegate many regulatory powers to the EDPB instead of the Commission. However, some of these powers are problematic from a democratic perspective, especially because the decisions of the EDPB are binding on controllers and processors. Yet, the EDPB is not required to consult with relevant stakeholders: data subjects, controllers and processors.

Examples of such powers are:

- The power to establish a list of data processing operations, which require prior consultation of the supervisory authority (Amendment 218). This poses the risk of major administrative burdens to industry;
- The power to adopt a measure binding a supervisory authority (Amendments 62 and 289). It may be expected that this power will be used to *overrule* favourable decisions of supervisory authorities in case other supervisory authorities object to such decisions. This creates legal uncertainty for business for the duration of the period that the decision may be challenged and the challenge is subsequently resolved;
- The power to advise the institutions of the European Union, especially the Council and the Parliament (Amendment 64 and 298). This reinforces the incentive for the EDPB to have a political agenda, where it is not a political body;
- The power to specify the criteria and the requirements for the methods to obtain verifiable consent of a child's parents for processing a child's personal data online (Amendment 111). This is a very difficult issue and requires careful consultation of relevant stakeholders, including business;
- The power to specify the criteria, conditions and appropriate safeguards for the processing of special categories of personal data (Amendment 116). Such power may not only severely hamper sectors which routinely process special data, such as the medical sector or the insurance sector, in the efficient and effective operation of their business, but also those businesses, which occasionally process special data in the course of their business operations, such as webshops selling consumer healthcare products;
- The power to specify criteria and requirements for appropriate measures and mechanisms related to Privacy by Design and Privacy by Default (Amendment 179). Not only could this power hinder

technological innovation, Amendment 178, which requires the producers of data processing systems and software to implement Privacy by Design, *in combination* with Amendment 179 would imply that the EDPB is empowered to regulate critical data processing infrastructures (e.g., the Internet) without any stakeholder participation from government or business. The same would apply to Amendment 194 (the power to specify the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations);

- The power to specify "the criteria and requirements for the core activities of the controller or the processor" with respect to the obligation to designate a Data Protection Officer (DPO) (Amendment 228). This amendment is poorly drafted, as the wording may imply that the EDPB is empowered to regulate the core activities themselves instead of – as probably meant – the criteria for determining the core activities which would qualify a controller or processor to appoint a DPO;
- The power to specify the resources of the DPO (Amendment 234). This impacts the autonomy of the government or business to allocate scarce budget and resources as it sees fit; and
- The power to further specify the criteria and requirements for Binding Corporate Rules (Amendment 257). This allows the EDPB to develop additional requirements for controllers or develop new supervisory powers not mentioned in the Regulation (See also the statements with regard to the Article 29 Working Party and auditing powers above).

**Proposals**

The new Regulation should aim to introduce a more balanced system of interpretation of European data protection law. This could be achieved by taking the following measures:

- **The Regulation should ensure that the supervisory authorities in their enforcement activities are not (by default) biased towards the interests of the data subjects, but also take into account the interests of society and data processors and controllers;**

- **The Regulation should ensure a fair and transparent stakeholder participation in the application of the Regulation in order to make the application more acceptable to all relevant stakeholders involved with personal data processing.**

Below a number of amendments are proposed, which aim to achieve both goals.

**Amendment 1**

| **Proposal for a regulation**<br>**Title** | |
|---|---|
| *Text proposed by the Commission* | *Amendment* |
| REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on **the protection of individuals with regard to** the processing of personal data and on the free movement of such data (General Data **Protection** Regulation) | REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the processing of personal data and on the free movement of such data (General Data **Processing** Regulation) |

***Justification***

*This amendment aims to clarify the neutrality of the Regulation with regard to the various interests involved, as the purpose of data protection law is to strike a balance between the interests of the various stakeholders involved in the data processing. On the one hand, there are the interests of society as a whole or of an individual business, etc. to*

*process personal data (i.e. avoiding harm, enforcement of laws and rules, maximizing economies, efficiency and value, and enhancing trust in individuals). On the other hand, there are the interests of the data subject not to have his personal data processed or to have them processed in a fair manner in order to avoid harm, ensure non-discrimination, ensure freedom from injustice, or to ensure individual autonomy and privacy. This amendment aims to ensure that the supervisory authorities and the EDPB do not - by default - feel the need to be biased to the interests of the individual data subject, but also fairly take into account the interests of society and data processors and data controllers in their enforcement activities.*

**Amendment 2**

| **Proposal for a regulation**<br>**Recital (139)**<br><br>*Text proposed by the Commission* | <br><br>*Amendment* |
|---|---|
| In view of the fact that, as underlined by the Court of Justice of the European Union, the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced with other fundamental rights, in accordance with the principle of proportionality, this Regulation respects all fundamental rights and observes the principles recognised in the Charter of Fundamental Rights of the European Union as enshrined in the Treaties, notably the right to respect for private and family life, home and communications, the right to the protection of personal data, the freedom of thought, conscience and religion, the freedom of expression and information, the freedom to conduct a business, the right to an effective remedy and to a fair trial **as well as** cultural, religious and linguistic diversity. | In view of the fact that, as underlined by the Court of Justice of the European Union, the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced with other fundamental rights, in accordance with the principle of proportionality, this Regulation respects all fundamental rights and observes the principles recognised in the Charter of Fundamental Rights of the European Union as enshrined in the Treaties, notably the right to respect for private and family life, home and communications, the right to the protection of personal data, the freedom of thought, conscience and religion, the freedom of expression and information, the freedom to conduct a business, the right to an effective remedy and to a fair trial, cultural, religious and linguistic diversity **as well as the fundamental rights and freedoms of enterprises, including but not limited to their freedom to conduct a business**. |

***Justification***

*In addition to Amendment 1, this proposal builds on paragraph 3.3 of the explanatory memorandum to the Regulation. Recalling the Charter of human rights, the amendment aims to strike a balance between individuals rights/freedoms and companies rights/freedoms.*

**Amendment 3**

| **Proposal for a regulation**<br>**Article 46** | |
|---|---|
| *Text proposed by the Commission* | *Amendment* |
| 1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application of this Regulation and for contributing to its consistent application throughout the Union, **in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the Union.** For these purposes, the supervisory authorities shall co-operate with each other and the Commission. | 1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application of this Regulation and for contributing to its consistent application throughout the Union. For these purposes, the supervisory authorities shall co-operate with each other and the Commission. |

***Justification***

*See justification to Amendment 1.*

**Amendment 4**

| **Proposal for a regulation**<br>**Article 87 - new**<br><br>*Text proposed by the Commission* | <br><br>*Amendment*<br><br>1. A European Data Protection Dialogue is hereby set up.<br><br>2. The European Data Protection Dialogue shall be composed of:<br>(a) a chair, appointed by the Parliament;<br>(b) 12 representatives of European trade organisations, which act in the interest of data controllers or processors established in the Union;<br><br>(c) 12 representatives of European organisations, which act in the interest of data subjects;<br><br>(d) 12 independent experts appointed by the European Commission.<br><br>3. The members of the European Data Protection Dialogue, as referred to in paragraph 2(b), (c) and (d) are appointed by the Commission on invitation. The Commission shall invite relevant organisations and experts, while ensuring that the various interests and expertise are represented as much as possible. Invited organisations may nominate one or more representatives. A representative or expert is appointed for four years and can be re-appointed for another four years. In case of an interim vacancy of a representative as referred to in paragraph 2(b) or (c), the organisation which originally provided the representative for such position may nominate a new representative.<br><br>4. The Commission shall consult the European Data Protection Dialogue prior to establishing any measure or taking any decision pursuant to this Regulation. The Commission, the European Data Protection Board and any supervisory authority shall take the utmost account of the opinion of the European Data Protection Dialogue.<br><br>5. In addition to paragraph (3), the European Data Protection Dialogue may issue an opinion on any matter relevant to the application of the Regulation, if it so wishes. Any member as referred to in paragraph (2) may request the European Data Protection Dialogue to issue an opinion on a matter. The Data Protection Dialogue shall send such opinion to the |
|---|---|

| | |
|---|---|
| | Commission, the Council, the Parliament and the European Data Protection Board.<br><br>6. The European Data Protection Dialogue may set up Committees to prepare a draft opinion on matters as referred to in paragraphs (4) and (5). The European Data Protection Dialogue and its Committees may hear testimony from relevant stakeholders and experts and may conduct a public consultation on a matter. The Committees shall submit their draft opinions to the European Data Protection Dialogue prior to their publication.<br><br>7. The European Data Protection Dialogue decides with a simple majority. The minority is given the opportunity to complement the opinion with one or more dissenting summary opinions. The final sentence of paragraph (4) is not applicable to dissenting opinions.<br><br>8. The Commission shall act as the secretariat of the European Data Protection Dialogue. Article 73(2) and (3) shall apply mutatis mutandis to the support provided by the Commission to the European Data Protection Dialogue.<br><br>9. Nor the chair nor the experts, as referred to in paragraph 2(a) and (d) can be members or staff of the Parliament, the Council, the Commission, the European Data Protection Board or a supervisory authority. Experts should have extensive knowledge of the substance and application of data protection law, data processing technology, business or public administration.<br><br>10. Each member of the European Data Protection Dialogue shall designate a substitute. Substitutes may participate in the preparation of opinions in the Committees. The European Data Protection Dialogue elects two deputy chairs from amongst its members. The European Commission shall maintain and make public a list of the names, affiliations and other relevant positions of the chair, the deputy chairs, the members and their substitutes.<br><br>11. The chair shall convene the meetings of the European Data Protection Dialogue and prepare its agenda. The European Data Protection Dialogue shall lay down the attribution of tasks between the chair and the deputy chairpersons as well as between the Committees in its rules of procedure. |

| | |
|---|---|
| | 12. Discussions of the European Data Protection Dialogue and any documents used in preparation of its draft opinions are confidential, unless otherwise decided by the chair. |

***Justification***

*The Regulation has an extremely wide impact on society. This poses a risk that relevant interests and concerns are overlooked by the Commission or the European Data Protection Board in issuing their decisions or that their decisions have intended consequences. The European Data Protection Council, as proposed in this amendment, acts as a means to generate the interests and concerns of relevant stakeholders and experts in the regulatory process. The opinions of the European Data Protection Council are not binding, but they provide meaningful information to the decision makers in the Commission, the Council, the Parliament and the European Data Protection Board. The members of the European Data Protection Council are selected from European trade associations and European NGO's (consumer organisations, unions, digital rights groups, etc). To ensure their independence, the experts, as referred to in paragraph 2(d) cannot be members or staff from the legislative bodies and supervisory authorities. They should have in-depth knowledge of the relevant issues surrounding the application of the Regulation.*

**With regard to the Amendments in the draft LIBE report**

- Amendment 218 should be opposed (see explanation above);
- Amendments 62 and 289 should be opposed (see explanation above);
- Amendments 64 and 298 should be opposed (see explanation above);
- Amendment 111 should be opposed (see explanation above);
- Amendment 116 should be opposed (see explanation above);
- Amendment 179 should be opposed (see explanation above);
- Amendment 194 should be opposed (see explanation above);
- Amendment 228 should be drafted and read: "…….the criteria and requirement for **determining** the core activities of the controller or the processor,…….;
- Amendment 234 should be opposed (see explanation above);
- Amendment 257 should be opposed (see explanation above).