ORGALIME

Position Paper

Brussels, 7 February 2014

Proposal for a Regulation on the personal data protection: processing and free movement of data (General Data Protection Regulation, 2012/0011(COD))

I. Introduction

Orgalime welcomes the European Commission's proposal for a Regulation 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) and we support the overall objectives of the data processing reform, including greater harmonisation in the area of implementation and the concept of the one-stop-shop, as well as greater consumer confidence in the online environment.

Orgalime furthermore welcomes the fact that the European Parliament is debating thoroughly the proposal for a General Data Protection Regulation that is expected to bring important changes to the European Union's rules on data protection.

We agree with the general direction taken by the Commission, acknowledging that, while the objectives of Directive 95/46/EC remain relevant, a thorough review has become indispensable owing to the technological and social changes which have occurred in the digital environment.

At the same time, Orgalime is reluctant to endorse many new obligations imposed on companies by the proposal at hand. The Commission and the Parliament, when debating the revision of the data protection legal framework, should not forget that a company's data is the lifeblood of its business. Customer data, financial and legal records, sales figures, as well as the day-to-day correspondence – constitute vital information required to run a company successfully. Orgalime therefore believes that there should be a differentiation in the scope of regulating of different stakeholders, whether it is, for example, a student transferring his data on the social media, or a company that keeps the information safe and ensures compliance with relevant data protection rules and legislation.

We see that the future legislation should be built on a risk-based approach, instead of forcing everyone to comply with heavy and costly bureaucracy, regardless of the nature or quantity of data

www.orgalime.org

ORGALIME aisbl | Diamant Building | Boulevard A Reyers 80 | B1030 | Brussels | Belgium
Tel: +32 2 706 82 35 | Fax: +32 2 706 82 50 | e-mail: secretariat@orgalime.org
Ass. Intern. A.R. 12.7.74 | VAT BE 414341438

they possess or the method of processing. It is not possible to build a one-size-fits all framework for data protection. We need less prescriptive and more flexible regulation that also recognises that companies are sensitive to the need to provide proper protection of the personal data that they process for their customers and employees. Over the last decade, sensitivity both of the public and of company employees as to how their personal data is collected and processed has significantly increased. Companies have both legal and commercial reasons to comply with data protection laws, including a desire to be successful in the marketplace and to be seen as an employer of choice by employees.

II. Key concerns and suggestions

Our key concerns and suggestions to further improve the Commission's proposal are summarised below, and include reporting obligations, administrative burdens, number of delegated and implementing acts, as well as the level of sanctions.

1. Too many extra obligations and too much administrative burden undermine innovation

By introducing the Regulation, the European Commission wants to reduce the costs for companies. However, it is evident that the proposal has the opposite effect. The Regulation imposes a great number of additional obligations that will create greater administrative burden and will undermine innovation in the sectors concerned. To give a concrete example: the cost for a business of a privacy assessment (imposed by art. 33) is estimated at between 10.000 and 30.000 EUR.

It is of major concern to Orgalime that the proposal not only focuses on the Controller, but, in many articles, the Commission also involves the Processor who processes data under the authority of the Controller. Article 77 even determines their liability as a "joint liability".

As the Controller determines the purposes of the processing, he is liable towards the controlling authority and towards the data subject. Article 26 gives a good overview of the duties of the Processor and points out that the Controller has to make arrangements with the Processor and that those arrangements have to be governed by a contract.

Orgalime thinks that all references to the concept of the Processor other than in article 26 only aim to impose the same obligations on the Processor and the Controller. Orgalime is strongly opposed to this shift of obligations from the Controller to the Processor, and we doubt the added value for the data subject that may result from this shift of obligations. The joint liability will only blur the rules on who is the one responsible for proper data protection and further increase the administrative burden and costs for all parties.

In conclusion, in Orgalime's view a clear delimitation of the responsibilities of the different parties is essential for a well functioning framework.

ORGALIME aisbl | Diamant Building | Boulevard A Reyers 80 | B1030 | Brussels | Belgium
Tel: +32 2 706 82 35 | Fax: +32 2 706 82 50 | e-mail: secretariat@orgalime.org
Ass. Intern. A.R. 12.7.74 | VAT BE 414341438

2. Reporting of a personal data breach

The second point of concern is the reporting obligation of a personal data breach to the supervisory authority. Orgalime asks for a more precise description of the scope of this article. Also, a notification within 24 or even within 72 hours is unreasonably short for both parties – the company and the supervisory authority (Article 31). Orgalime is of the opinion that, as provided for in the e-privacy directive, the Regulation should not prescribe a specific period of time. In our view the notifications to supervisory authorities are a formality and red tape that represents an unnecessary cost for business.

Furthermore, the obligation to report material breaches to the Data Protection Authorities (DPA) should be flexible enough not to interrupt the organization's efforts to deal with an eventual breach. Organizations are always free to seek guidance from DPAs in the event of data breach.

3. Main establishment or One Stop Shop principle

According to the "one-stop-shop" principle, when the processing of personal data takes place in more than one Member State, there should be a single supervisory authority responsible for monitoring the activities of the controller or processor throughout the Union and taking the related decisions. Orgalime welcomes this concept, and agrees that the lead authority principle is a key element in simplifying data protection rules across the borders of Member States. Orgalime believes however, that the existing provisions of the one stop shop concept require clarification to ensure that the drafting reflects the Commission's desire to encourage simplification. Therefore, in Orgalime's view, a good definition of the "main establishment" concept is needed in order to harmonise the actions of the supervisory authority.

4. Delegated acts: great legal insecurity

Orgalime regrets that too many issues in the draft Regulation are left to be dealt with by delegated and implementing acts. The number of delegated and implementing acts should be reduced and limited to those provisions addressing non-essential issues. In the current state of the proposal, more than 40 articles refer to "delegated acts". In our view, delegated acts are only acceptable if they clarify non essential parts of the legislation that are rather technical. We therefore believe that the number of provisions referring to delegated acts should be reduced and taken out of those articles that already contain detailed obligations.

5. Mandatory Data Protection Officer

Orgalime opposes the creation of a mandatory Data Protection Officer (DPO) function, as we fear this would cause unnecessary financial burdens to small companies without, at the same time, adding much value to the data protection. Especially for SMEs, which the regulator should remember represent over 99% of companies, this obligation is by far too excessive and, while it is reasonable to motivate companies to appoint a Data Protection Officer by reducing bureaucracy, it

ORGALIME aisbl | Diamant Building | Boulevard A Reyers 80 | B1030 | Brussels | Belgium
Tel: +32 2 706 82 35 | Fax: +32 2 706 82 50 | e-mail: secretariat@orgalime.org
Ass. Intern. A.R. 12.7.74 | VAT BE 414341438

should not be made mandatory in any way. We therefore believe that SMEs should be exempt from the obligation to appoint a Data Protection Officer insofar as data processing is not their core business activity.

6. Sanctions and more discretionary competence of the national supervisory authority

Based on the proposed Regulation – the national supervisory authorities will receive more power. The Regulation gives them the power to impose penalties that can run up to 1.000.000 EUR or 2% of a company's annual worldwide turnover. Although Orgalime understands that enforcement is essential and therefore sanctions are necessary, we believe that these sanctions should be proportionate with regard to the effective shortcomings.

Orgalime also stresses that the supervisory authority has no discretion as to whether or not a fine should be imposed. In our view, in cases where there is no fraud or gross negligence, the lack of discretionary competence is not beneficial to the system.

7. The transfer of personal data to third countries and the Binding Corporate Rules

Orgalime wishes to keep on using the exception of the consent of an employee as "a legal ground" for a transfer. As for the application of Binding Corporate Rules, Art. 43 imposes a supplementary condition: these legally binding corporate rules should be applicable on each member of the group and each member within the Controller's or Processor's group should comply with these rules.

Orgalime believes that it is not realistic to require from every subdivision of the group to take the necessary measures to implement the Binding Corporate Rules, to respect them and to prove that there are compliant.

III. Conclusion

Orgalime would like to stress that the General Data Protection Regulation needs enough time for evaluation in the Council and in the European Parliament. We would advise against rushing into an agreement not preceded by a thorough discussion between the institutions, and with all potentially affected stakeholders. We therefore welcome the fact that the European Parliament is thoroughly debating the proposal. While we agree with the general direction taken by the Commission in the data protection reform, we are reluctant towards the proposals to impose disproportionate new obligations imposed on companies by the Regulation. This would be disproportionate and a clear violation of the "think small first principle" which is a core principle that is supposed to be enshrined in all new European regulation.

ORGALIME aisbl | Diamant Building | Boulevard A Reyers 80 | B1030 | Brussels | Belgium
Tel: +32 2 706 82 35 | Fax: +32 2 706 82 50 | e-mail: secretariat@orgalime.org
Ass. Intern. A.R. 12.7.74 | VAT BE 414341438