BUSINESSEUROPE

THE DIRECTOR GENERAL

Mr. Juozas Bernatonis
Minister for Justice
Ministry of Justice of the Republic of Lithuania
Gedimino ave. 30
LT-01104 Vilnius
LITHUANIA

2 December 2013

Dear Minister,

BUSINESSEUROPE message on the General Data Protection regulation in view of the discussions at the Justice and Home Affairs Council on 5-6 December 2013

A framework to protect personal data *and* boost European companies' competitiveness

Companies need a workable framework to deliver on the huge potential of the data-driven economy. Rules on data protection have to be balanced, future proof and easy to understand and apply.

BUSINESSEUROPE is strongly concerned that the General Data Protection Regulation currently being discussed fails to address this challenge and does not strike the right balance between protection of European citizens and free movement of data in the single market. Both the current proposal and the report recently voted by the European Parliament would create disproportionate restrictions to data processing and data flows, which would have detrimental effects on innovation and growth and consequential negative impact on European citizens.

Accordingly, BUSINESSEUROPE supports the approach of Member States to have in-depth discussions before considering any decisions on the revision of the current rules. Data protection legislation impacts all segments of the economy and companies of all sizes. We strongly believe that the final agreement cannot be rushed, leaving room for a deeper discussion on the most complex issues. Quality must prevail over speed in reaching an agreement.

However, BUSINESSEUROPE supports the *one-stop-shop mechanism*, to be discussed by the Justice Council, as one of the positive elements of the proposal. A more harmonised data protection framework in Europe, combined with an effective one-stop-shop mechanism, will facilitate free movement of data in the digital single market.

AV. DE CORTENBERGH 168
BE-1000 BRUSSELS
BELGIUM
VAT BE 863 418 279

BUSINESSEUROPE a.i.s.b.l.
WWW.BUSINESSEUROPE.EU

TEL +32(0)2 237 65 11
FAX +32(0)2 231 14 45
E-MAIL: MAIN@BUSINESSEUROPE.EU
EU Transparency register 3978240953-79

In this context, we urge the Justice Council to take into account the following considerations in its discussions on 6 December.

An effective one-stop-shop mechanism

BUSINESSEUROPE strongly welcomes the *one-stop-shop mechanism* in the Commission draft proposal, intended as the jurisdiction of a single data protection authority (DPA) over businesses operating across multiple European countries for compliance. This is a major improvement to the current EU rules on data protection, as it will make their application more consistent throughout the internal market, thereby ensuring a level-playing-field for companies, increasing legal certainty and reducing administrative burdens for controllers and processors in the EU.

It is therefore essential that the regulation provides **a clear and workable legal framework for the one-stop-shop**, with simple and easy procedures. The Justice Council must take these considerations into account while discussing this issue.

In particular, BUSINESSEUROPE asks for:

1) Laying down clear and appropriate criteria for organisations to determine their "main establishment";
2) Defining clear and harmonised competences, duties and powers of DPAs in all Member States;
3) Clarifying roles and interactions between the "competent DPA" and other DPAs. Blurring the role of competent authority or involving many DPAs in issuing decisions will make the procedures burdensome to the detriment of both companies and citizens.
4) Guaranteeing consistency of decisions in the EU, especially defining the role of the European Data Protection Board and the European Commission in the mechanism;
5) Ensuring that the one stop shop principle applies to all companies which fall within the scope of the Regulation.

The one-stop-shop would really reduce unnecessary administrative requirements for companies. Therefore, we urge the Council to fulfil the original purpose of this mechanism. Businesses need to avoid the risk of undesirable multiple fines and multiple lawsuits in multiple Member States.

Need to avoid sectoral collective redress measures

The Council will address the right to lodge a complaint with a supervisory authority in its discussions on 6 December. BUSINESSEUROPE supports effective redress for those concerned by breaches of EU law. This is vital for boosting consumers' confidence in the digital single market. It is in the interest of companies that adequate redress mechanisms exist and function well.

However, we do not believe this can only be achieved through more litigation. Other, non-judicial, redress mechanisms are available and should be taken into consideration very seriously. In addition, the economic costs imposed on society by judicial systems of collective redress and the increase in litigation it entails should be evaluated.

Furthermore, we call for consistency with the Recommendation on collective redress adopted by the European Commission in June 2013, leaving it to Member States to decide how to integrate any horizontal collective redress measure in the way that best suits their legal system. Consequently, we recommend that the Justice Council refrain from supporting any sector-specific proposal at EU level, as this would clearly clash with the content of the Recommendation.

Finally, the proposal to introduce collective redress provisions for data protection entails a serious risk of encouraging business models based upon buying and exploiting claims, mostly to the advantage of intermediaries and representative bodies, and not of individuals.

Additional elements to be addressed by the Council

BUSINESSEUROPE has a number of additional concerns which need to be addressed to avoid jeopardising European competitiveness and hindering innovation. It is critical that the Council addresses these shortcomings during the upcoming discussions.

- ***Reduce burdensome requirements for companies***

BUSINESSEUROPE regrets that the report recently voted by the European Parliament adds heavier administrative burdens compared to the Commission proposal, which already included considerable requirements. It is fundamental that the Council introduces more flexibility around the provisions on information and documentation obligations, data protection impact assessments, data breach notification and data protection officers. These provisions must really deliver tangible benefits to the consumers and reflect different types of business and business models, without creating additional costs and time constraints.

- ***Ensure a balanced approach to sanctions***

Effective and high-quality enforcement is essential. BUSINESSEUROPE does not believe this can be best achieved by the sanctions proposed in the Commission draft and reinforced by the Parliament. These sanctions are excessive and might have serious negative impacts on companies' ability to innovate. Any sanction levied should be proportionate to the impact on data subjects (for instance, an actual damage for the data subject) and take into account the circumstances of noncompliance, distinguishing between intentional and unintentional behaviours. A one-size-fits-all approach, following the model of sanctions for anti-competitive behaviour, is not appropriate in the context of data protection. In competition law, the sanction system is based on

economic studies and understanding of the negative impacts of anti-competitive behaviour to the market dynamics. This justifies the turnover-based way of calculating fines. Data protection rules must be addressed in a different way.

This list of additional concerns is not exhaustive. You will find in the annex to this letter the list of BUSINESSEUROPE top ten concerns on the data protection proposal.

As data protection is essential for citizens, companies, growth and jobs, any revision of EU data protection rules should establish an appropriate European framework. Data protection legislation is complex and impacts all segments of the economy. The new rules will remain in place for many years and must be future proof.

BUSINESSEUROPE support the approach of Member States to have sufficient in-depth discussions before adopting a final decision. It will be essential to pursue the negotiations following the rule "thoroughness proceeds rapidness".

Yours sincerely,

Markus J. Beyrer

BUSINESSEUROPE

ANNEX

BUSINESSEUROPE TOP TEN PRIORITIES ON THE GENERAL DATA PROTECTION REGULATION

KEY MESSAGES

1. **The definition of personal data must be clear and not excessively broad**
2. **Consent must be possible to process employees' personal data in employment context**
3. **Documentation, data protection impact assessment and prior authorisation requirements should be proportionate**
4. **Profiling should not be regarded as a negative measure per se**
5. **Data protection officer requirements must not be too prescriptive**
6. **International data transfers must not become disproportionally burdensome**
7. **Introduction of collective redress in the regulation is not appropriate**
8. **The system of sanctions must not be excessive**
9. **Right to be forgotten and to data portability must be workable**
10. **The competence of supervisory authorities and the definition of main establishment must be clarified**

WHAT DOES BUSINESSEUROPE AIM FOR?

1. **The definition of personal data must be clear and not excessively broad**
   It is fundamental to ensure a clear and unambiguous definition of what is *personal data*, in accordance with the objective of the regulation. An excessively broad definition could have unintended negative consequences for the digital economy, for instance preventing the use of IP addresses for security and authentication purposes.
2. **Consent should be possible in employment context to process employees' personal data**
   Consent of the employee is the most workable basis to process data in employment context and it must be maintained, because other options proposed do not provide the same degree of legal certainty. If employees cannot consent on the processing of their personal data, the effect could harm their own interests (e.g. for recrutiment purposes, trainings and/or other entitlements).

AV DE CORTENBERGH 168
BE-1000 BRUSSELS
BELGIUM
VAT BE 863 418 279

BUSINESSEUROPE a.i.s.b.l.

WWW BUSINESSEUROPE EU

TEL +32(0)2 237 65 11
FAX +32(0)2 231 14 45
E-MAIL MAIN@BUSINESSEUROPE EU
EU Transparency register 3978240953-79

3. **Documentation, data protection impact assessment and prior authorisation requirements should be proportionate**
Maintaing documentation for every processing operations, even the ordinary ones which do not present specific risks, does not respond to the need of protecting European citizens. In some cases, an authorisation must be obtained prior to the processing of personal data, which would both overburden the data protection authorities (in charge of granting the authorisation) and undermine the smooth functioning of businesses.

4. **Profiling should not be regarded as a negative measure per se**
Profiling is often a basis for a good customer service (for instance in case of services that remember consumers' preferences) and is even necessary in certain businesses, such as banking or insurance. Disproportionate limitations on profiling would therefore harm the functioning of entire sectors and could ultimately have a negative impact for consumers.

5. **Data protection officer requirements must not be excessively prescriptive**
The obligation of appointing a data protection officer for the public sector and companies with more than 250 employees, without allowing a degree of flexibility to each organisation, is excessively prescriptive. Effective data protection can be achieved with different concrete solutions. Also, the threshold of 250 employees is probably not the most pertinent – the extent of data processing in some cases is independent from the number of employees.

6. **International data transfers must not become disproportionally burdensome**
Business models in the digital economy increasingly rely on international transfers of data (for instance, in the case of cloud computing, often the servers where the data are stored are placed in third countries). The increased requirements for consent in international data transfer may disrupt emerging digital business model with a negative impact on innovation.

7. **Introduction of collective redress in the regulation is not appropriate**
In absence of a specific framework on collective redress, the general data protection regulation is not the right place to introduce this possibility. This provision, in particular if linked to a sensitive issue such as privacy, could lead to flourishing of business models solely based upon buying and exploiting claims.

8. **The system of sanctions must not be excessive**
Administrative sanctions are high (in the Commission proposal, up to 1 000 000 euros or 2% of an enterprise's worldwide turnover) and defined on the basis of competition law approach. This is not acceptable in the case of data protection, as the type of conduct and the impact of those violations on the market are not comparable to anticompetitive behaviours.

9. **Right to be forgotten and to data portability must be workable**
The right to be forgotten has to be reconsidered in situations where historical data are fundamental (e.g. credit registers and insurances), or when the obligation to delete relates to data stored in place where the collector of data has no control. Provisions on data portability must also reflect the technological reality and respect technological neutrality, not imposing to companies requirements that are virtually impossible to fulfil.

10. **The competence of supervisory authorities and main establishment must be clarified**
To ensure the benefits of the "one-stop shop" approach, it is fundamental that one single competent authority is comprehensively informed about all aspects relevant in a specific case. The wording of the regulation must provide a clear definition of *main establishment* of the controller and the processor, as well as setting out specific ways to identify the competent supervisory authority.

* * *