



**Mr Félix Braz**  
Minister for Justice of Luxembourg  
13, rue Erasme  
L-2934 Luxembourg  
LUXEMBOURG

11 December 2015

Dear Minister,

***BUSINESSEUROPE message on the expected adoption of the General Data Protection Regulation***

Creating a connected digital single market is one of the top priorities for the Juncker Commission. A true digital single market could contribute an additional €415 billion to European GDP and create thousands of jobs, but this will only happen if the EU makes the right choices.

The General Data Protection Regulation that you will agree upon in the next few weeks will be crucial for the development of the digital single market and for Europe's competitiveness. Data are driving innovation in all sectors of the economy. The use of data delivers efficiency to companies, allows the creation of new business models and offers a whole range of new innovative services to consumers. The Internet of Things, connected cars, cloud computing and smart houses are based on the collection, use and analysis of data - including personal data. We cannot miss this opportunity.

If the negotiations on the Regulation lead to a result consistent with these objectives, European companies will truly be at the forefront of the digital revolution. This opportunity is in your hands. If it is lost, Europe's competitiveness could be seriously damaged.

BUSINESSEUROPE urges the trilogue negotiators to take into account the following recommendations to help Europe regain its global competitiveness:

- 1. Create a proportionate regime of sanctions.** Legislators must avoid putting in place a system with disproportionate sanctions, which do not reflect the harm suffered by the citizens and the impact on the market in case of a violation. Effective deterrence for intentional breaches is important, but it must be proportionate and consistent within the EU.
- 2. Clarify the system of liability between controller and processor, avoiding joint and several liability.** Companies need legal certainty concerning liability. A system with joint and several liability for both controller and processors would clearly introduce significant uncertainties and burdens on companies, whilst also increasing uncertainties for data subjects. The redress mechanisms for data subjects will be less clear and the risks to the protection of personal data could be greater, as controllers might be discouraged from taking essential precautions because they can pass their liabilities onto processors. The Regulation must clearly specify who is liable for what and in which situations.
- 3. Avoid fragmentation in the digital single market.** Companies need a truly harmonised EU framework on data protection, with a meaningful and efficient one-stop shop system (in line with the original Commission proposal), coherent implementation and interpretation of the rules and consistency in the decisions of each national Data Protection Authority, also in relation to international data transfers.



4. **Limit burdens for companies.** Requirements for prior authorisation/consultation, data protection impact assessments, data breach notification, appointment of data protection officers, must all reflect a true risk-based approach. Obligations must be proportionate to the risks for the data subject and the regulation must refrain from adopting an overly broad definition of 'high risk'. The possibility to transfer data within undertakings can also lead to less administrative burdens and must be explicitly permitted by the Regulation.
5. **Allow further processing and the use of pseudonymous data.** The ability to process data for other purposes than the ones the data were collected for ("further processing") is at the foundation of the development of big data and must be permitted by the Regulation in accordance with the possibility to provide an adequate level of protection of personal data. Moreover, pseudonymisation is essential for the creation of innovative services and business models. Processing pseudonymised data significantly decreases the risks for the rights and interests of citizens. The possibility to process pseudonymous data must therefore be clearly allowed and encouraged by the Regulation.
6. **Provide for stable and adequate legal basis for processing.** Companies and data subjects need legal certainty with regard to data processing. The Regulation should not hinder legitimate data processing, nor extensively formalise the relation between data subject and the controller. Explicit consent should thus be required only for processing of sensitive data. Processing based on legitimate interest should not be overly restricted.
7. **Ensure effective mechanisms to transfer data internationally.** The legislative framework must provide appropriate and comprehensive means to transfer data internationally, as this is absolutely crucial for trade and international cooperation. National Data Protection Authorities must ensure consistency within Europe in their approach on international data transfers, to avoid creating situations where companies based in several Member States are confronted with conflicting requirements.

A more developed position with additional elements and suggestions is at annex. We trust you will take our views into consideration.

We are sending similar letters to the other trilogue negotiators in the European Parliament and the Council.

Yours sincerely,



Markus J. Beyrer