BUSINESSEUROPE

THE DIRECTOR GENERAL

To: Members and Substitutes of the Civil Liberties, Justice and Home Affairs (LIBE) Committee at the European Parliament

18 October 2013

Re: LIBE Committee vote on the General Data Protection Regulation

Dear Member of the European Parliament,

I am writing to you in view of the upcoming Committee vote on the proposed General Data Protection Regulation.

BUSINESSEUROPE recognises that businesses' and consumers' access and use of data is a vital part of everyday life. The new digital economy is data-driven. Data processing is the backbone of a knowledge-based society that can turn information into fundamental societal and individual benefits. This opportunity will also dramatically affect industrial efficiency. Data driven innovation can be a key driver for jobs and growth and personal data can leverage €330 billion a year in the EU by 2020.

BUSINESSEUROPE has significant concerns with a number of provisions of the proposed data protection regulation, which must be adjusted to ensure this legislation does not have a detrimental impact on innovation and growth. We urge Members of the Parliament not to choose speed over quality. The current Parliament compromise amendments fail to address the shortcomings of the proposed regulation and BUSINESSEUROPE is concerned that haste could lead to the adoption of an inadequate data protection framework.

It is fundamental that the new data protection regulation renews its commitment to privacy, enables innovation and allows Europe to take advantage of the growth potential stemming from the use of data. This was repeated by Vice-President Reding recently, when she stated that data protection and innovation should go hand in hand as they are complementary. However, the current draft regulation fails to grasp this growth and innovation opportunity.

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 3976240953-79

BUSINESSEUROPE

This is in particular the case for:

- The excessive administrative burdens that the proposal generates for businesses;
- The impossibility to use consent as a legal basis for data processing in employment context;
- The lack of a risk based approach in the current Commission proposal;
- The negative perception on profiling;
- The risk of hindering international data transfers.

The annex to this letter develops further these aspects as well as others, which we would like to see addressed.

A number of elements of the proposed reform, such as the aim of achieving greater harmonisation and a level playing field for all players at global level, together with the introduction of the "one-stop-shop" principle, are steps in the right direction. Personal data must be granted the same level of protection, regardless of the location or the nature of the product provided. A thorough application of the "one-stop-shop" principle will benefit companies and especially start-ups in Europe and encourage more innovative business.

BUSINESSEUROPE is confident that you will carefully consider those elements and we remain at your full disposal if you wish to discuss these or other points further.

Yours sincerely,

Markus J. Beyrer

BUSINESSEUROPE

ANNEX

SPECIFIC COMMENTS

BUSINESSEUROPE welcomes the current reform, as it is essential to update the 1995 framework in order to adapt to the new challenges of the digital economy. We believe that privacy and competitiveness do not present a zero-sum, "either/or" choice. In this context, you will find below our recommendations to match these two key objectives.

The need for a risk-based approach

The draft regulation often imposes the same compliance obligations regardless of how or why personal data is used. This approach threatens to curtail many innovative and beneficial data processing activities that consumers desire and demand. It is fundamental to adopt a risk-based approach, taking into account the nature, scope, context and purposes of the processing operations, as well as the levels of risk arising for data subjects. We believe the focus of the regulation should be on restricting dangerous, discriminatory or otherwise undesirable uses of data, while permitting the beneficial uses of such data. By adopting a risk-based approach, it is also possible to ensure that measures to prevent or mitigate risks of processing are proportionate with the risks identified. This will also allow resources to be allocated in the most efficient ways.

Consent that works for citizens

It is important that consumers can make informed choices regarding the processing of their personal data. However, it is vital that the provisions on consent do not hinder a sensible and flexible processing of data, as this would lead to a box-ticking exercise rather than an effective way for data subjects to control their data.

In addition, consent must be considered a valid basis for data processing in general, including in employment context. The draft regulation currently being discussed would make it impossible to process data on the basis of consent in employment context. This would be extremely difficult for employers, who could face situations where it is impossible for them to process data even when an employee agrees, only because there is no other legal basis for processing. Employees themselves could be negatively affected by this provision, because in many cases processing of employees personal data is done in their own interest (e.g. health, holidays, parental leave, educational and skills profiles and wages).

The value of data over time must not be underestimated

The use of historical data is necessary for the existence of a number of specific businesses, such as online services, credit registers and insurances. Enforcing a systematic and general right to be forgotten would undermine their business models, and would make it even more difficult for them to provide a number of customer services, such as consumer credit or the ability to subscribe to a tailor-made insurance contract. Moreover, a restrictive right to be forgotten would undermine the ability for citizens to access and share information online. The provisions surrounding the right to

be forgotten must therefore take this into account, in order not to harm potential innovation further down the line. In particular, it shall be specified that the right to be forgotten can only be exercised where there is no other legal ground for processing than the data subject's consent and the consent has been withdrawn or the processing does not comply with the regulation.

Careful approach to administrative burdens

With the provisions on the right to data portability, the new rules would require significant resources and imply huge costs for businesses which are not proportional with the benefits to the consumer. At a time when we should be taking full advantage of any competitive edges Europe may have, the right to data portability should be deleted.

BUSINESSEUROPE also urges policymakers to introduce more flexibility around the provisions for data protection impact assessments, data breach notification requirements and for the appointment of data protection officers, to ensure that these deliver tangible benefits to the consumer without placing unnecessary burdens upon businesses such as additional costs and time constraints.

Profiling to benefit consumers

There are many legitimate reasons why profiling takes place, often for the benefit of consumers, including fraud or ID theft prevention. Consequently, the negative perception towards profiling must be addressed, given that it helps to customise products to individual preferences and needs, making them more relevant to the consumer. The emergence of personal location data has created a wide range of innovative services, such as emergency response services for car accidents, and has the potential global value of more than €500 billion for consumers and business end-users.[1] The availability of innovative services will only take place in Europe if we are equipped with an appropriate regulatory framework for profiling.

The provisions in the current Commission draft appear to stem from an overriding concern with the world of social media – but we need to be careful to ensure this does not overshadow the positive uses of data. The robust protection of data subjects will be better served if the regulation focuses on how profiles are used, instead of on the mechanisms used to create profiles. The regulation should be amended to make clear that profiles can continue to be used for beneficial purposes.

A balanced approach to sanctions

Even though effective and high-quality enforcement is essential, the sanctions proposed in the Commission draft 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. In our view, in cases of first and non-intentional non-compliance, a warning procedure should be applied to all companies, no matter their size, particularly if the risk of data protection breach is eliminated and the data controller has taken all measures to avoid them in the future.

[1] « Big data: The next frontier for innovation, competition, and productivity", McKinsey report, May 2011, http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation

Cross-border data transfers must be workable

In order to fully capture the potential of the data-driven economy, companies will need to combine data from different sources. Due to the intrinsic global nature of the digital economy, it is fundamental that data can easily flow not only within Europe, but also outside, in particular with regards to company groups located in different Member States. For instance, in the case of cloud computing, often the servers are based outside Europe and enabling easy data transfer to third countries is at the very core of the nature of cloud services. This does not necessarily undermine the level of protection of such data. It is therefore vital that the regulation further eases, rather than hinders data flows between different parties and throughout different countries.

* * *