BUSINESSEUROPE

POSITION PAPER

15 September 2015

BUSINESSEUROPE INPUT FOR TRILOGUE DISCUSSIONS ON THE GENERAL DATA PROTECTION REGULATION

1. RISK-BASED APPROACH

(→ CONDITIONAL SUPPORT FOR EP AND COUNCIL TEXTS, DEPENDING ON THE ISSUES AND SUBJECT TO CHANGES)

A well-defined risk-based approach is needed, as it has the potential to substantially improve outcomes for data subjects while reducing administrative burdens for companies. **We welcome the introduction of this approach by the Council. However, some elements of the Council text need to be corrected to achieve a workable and meaningful risk-based system.**

> ***"The total costs of the documentation requirements according to the EP LIBE Committee report on the General Data Protection Regulation can be estimated at not less than €15 000 + VAT in the first two years of conducting business activity by an entrepreneur."***
>
> Economic consequences for SMEs of the EU Regulation on the protection of personal data according to the project approved by the LIBE Committee, Polish Confederation Lewiatan and Chamber of Digital Economy Polska, 2013

We welcome particularly the Council reasonable approach on data protection impact assessment and the EP and Council texts on prior authorisation/prior consultation, because they take into account the different levels of sensitivity and risks involved in the data processing. In particular, we support the Council approach when it defines the cases which require an obligation of prior consultation, for instance in the absence of measures to be taken by the controller to mitigate the risk. The EP approach on prior consultation is welcome, insofar as it allows for internal consultations with the data protection officer (if appointed). This possibility rightly reflects the principle of risk based approach, because the controller, who is fully responsible for the data processing, has the right to assess if there is any possibility to minimise the risks associated with a given processing. This is particularly justified in the case of controllers who use professional legal services to assist the data collection and processing or who nominate a data protection officer. These solutions might mitigate the risks involved with the data processing. On the contrary, the consultation requirement in the Council version would result in suspension of the business for 6 to 10 weeks before the advice by the authority is given, forcing businesses to wait until already overburdened authorities evaluate their submission for consultation.

BUSINESSEUROPE a.i.s.b.l
AVENUE DE CORTENBERGH 168 – BE 1000 BRUSSELS – BELGIUM
TEL +32 (0)2 237 65 11 – FAX +32 (0)2 231 14 45 – E-MAIL MAIN@BUSINESSEUROPE.EU
WWW.BUSINESSEUROPE.EU
EU Transparency register 3978240953-79

Moreover, we caution against the introduction of an overly broad definition of 'high risk' processing, and insist on the **need for one clear and unambiguous definition**. If the definition of 'high risk' is too vague or broad, it can be attributed to any kind of processing of sensitive data or large scale processing, thus undermining the very idea of risk-based approach.

We also urge negotiators to truly pursue one of the fundamental objectives of the reform and ensure a consistent and harmonised approach on data protection in Europe. It is fundamental to reject proposals whereby every national authority could draft its own list of processing, requiring an impact assessment or other provisions that clearly go against the spirit of a consistent approach and the digital single market. **If such guidance is required, it should be better given through general recommendations by the European Data Protection Board, not by national DPAs on case by case basis.**

> ***"A quarter of consumers do not read the information they are provided digitally. (…)The complexity and the technicality of the language are also key reasons why users do not read the information that they are given."***
>
> Europe Economics, Digital Content Services for Consumers: Assessment of Problems Experienced by Consumers, 2011.

According to the draft Commission proposal, the controller must provide data subjects with **extensive amount of information related to the processing of their personal data.** This will considerably lengthen, and make more unintelligible, the information clauses of digital services contracts. These provisions will create complexity for companies (and users) operating across the Union. In this context, the provisions of the Parliament's text are too prescriptive. They do not allow the controller to adapt the requirements (amount of information provided to the data subject, processing procedures and their documentation, measures to ensure compliance, including the decision to hire the data protection officer) to the scale and nature of data processing. They impose a standardised template – applicable to all data controllers – overlooking the extent to which they use new technologies, scale and nature of data processing. This may result in putting too much burden on SMEs.

Furthermore, the EP approach concerning the requirement to appoint a data protection officer in the case of processing data of more than 5 000 people per year is disproportionate and would apply to situations of data collection for most websites (i.e. for the purpose of newsletter mailings) or small shops equipped with camera surveillance. This obligation would also apply to any entity that buys or legally build databases containing data of more than 5 000 people in order to advertise its products and services. In this context, we support the Council approach which allow for more flexibility.

2. ONE-STOP SHOP
(→ SUPPORT FOR THE COMMISSION TEXT)

It is essential that the final Regulation preserves the one-stop shop as designed by the original Commission proposal. The one-stop shop should provide a clear and workable instrument to deal with cross-border issues, with only one authority responsible for adopting decisions.

Since the beginning of the negotiations, BUSINESSEUROPE has been advocating for a meaningful, clear and workable legal framework for the one-stop shop, with simple and easy procedures. The one-stop shop is the main element that could truly help businesses in taking advantage of the potential of data-driven innovation. This principle has been designed to simplify compliance for businesses and authorities, and to ensure consistency in the application of legislation at national level

While we support the efforts of the Council to reach a consensus amongst Member States, we believe the compromise obtained fails to encapsulate a true one-stop-shop mechanism. We support the introduction of provisions that would address the question of conflict of competence between different authorities, but we believe negotiators must ensure that any process ends with only one decision. Allowing several national authorities to be competent in a case would lead to lengthy procedures and lack of legal certainty for controllers, processors and even data subject seeking redress. Given the number of national authorities that might be involved, we are concerned about the possibility of multiple parallel court proceedings when the decision is appealed. Moreover, admitting local judicial review might result in simultaneous procedures and divergent rulings issued by national courts in appeal from the same decision.

3. PSEUDONYMOUS DATA (ART. 4)
(→ SUPPORT FOR EP AND COMMISSION TEXTS, DEPENDING ON THE ISSUES)

We welcome the EP approach which introduces the concept of pseudonymous data in the Regulation, **not differentiating whether data is pseudonymous from the onset or became such following a pseudonymisation process. The use of pseudonymous data would ensure the much needed flexibility to process data that cannot directly identify the data subject, while ensuring at the same time a reasonable level of protection for citizens.**

Currently the difference between pseudonymous and anonymous data on the basis of the 95/46 Directive and the upcoming draft data protection Regulation is not drawn in the same way in all Member States. Named identifiers appear to be considered anonymised data in some countries, and identifiable data in others. Pseudonymous data could be a decisive factor and innovation driver for big data, Internet of Things, e-health, smart energy and other services, at the same time significantly decreasing the risks for the rights and interests of data subjects. The processing of pseudonymous data as a legitimate ground in the area of big data can be particularly useful. As long as the controller keeps the necessary keys to avoid re-identification and takes the technical, organisational and contractual measures to avoid such re-identification, following a risk based approach and accountability principles, this can be a satisfactory solution for data subjects. By now, the draft data protection Regulation lacks however clear incentives in

using these kinds of data. The Regulation should include clear references to pseudonymisation as an incentive to alleviate obligations. In line with a proper risk-based approach, if companies process pseudonymous data it means they are taking technical, contractual and organisational measures, enhancing the principle of accountability, to reduce any risk to the privacy of the individual.

The Council compromise ignores the possibility of processing data that the controller already obtains in pseudonymous form, and requires some sort of action in order to give it the attribute of pseudonymity. This removes the main benefit of having provisions dealing with less identifiable forms of data, because when any data is collected, it would have to be assumed to be fully identifiable. Only the subsequent action of the controller can make the data pseudonymous. There would therefore be no incentive for companies to use "less identifiable" information, for instance with cookies, or the use of IP addresses. Instead, companies would collect "fully" personal data and keep it segregated from "pseudonymised" data.

4. CONSENT
(→ SUPPORT FOR COUNCIL AND EP TEXTS, DEPENDING ON THE ISSUES)

On the issue of consent, **we welcome the Council compromise which is balanced and avoids mandating explicit consent in all circumstances**. **This approach better reflects the reality of the digital environment, where consent is in some cases informed and freely given, even if not explicit.** In this context, it is necessary a new definition of consent or changes in recital 25 proposed by the Council. A one-size-fits-all requirement does not take into account in which context, for instance the technical circumstances, consent was obtained and which risks are involved. Asking for explicit consent for every single processing could result in individuals bombarded by constant requests several times a day. This would create a "tick-the-box" approach, with consumers not being aware anymore of what they consent to. At the same time, data controllers would be unable to rely on consent to processing even where the conduct of data subjects clearly indicates freely given and informed consent. The experience is positive in those Member States in which the tacit consent is allowed

It is also important to highlight that the withdrawal of consent must not affect the lawfulness of processing of data based on other grounds then consent itself.

The EP text provides in art 7.4 that the execution of a contract or the provision of a service shall not be made conditional on the consent to the processing of data that is not necessary for the execution of the contract or the provision of the service pursuant to Article 6(1) (b). This provision risks undermining the development of information society services which are provided for free in exchange of personal data. Such models are particularly common in the online world, but have been used also in offline situations (for example, a hairdresser may offer discounted haircut to customers willing to provide their home address on which promotional offers can be sent). These kinds of arrangements function to the benefit of companies, customers and therefore they must not be forbidden.

5. LEGITIMATE INTEREST AND FURTHER PROCESSING (ART. 6)

(→ SUPPORT FOR THE COMMISSION TEXT ON FURTHER PROCESSING* AND FOR *COUNCIL TEXT ON LEGITIMATE INTEREST)

A legal basis for further processing is essential for many current and future business models. BUSINESSEUROPE supports the clarification of the Commission to base processing for incompatible purposes either on consent or "another ground for lawful processing", which refers to all legal bases in Article 6, (in line with the current Directive 95/46), rather than the Council text, **because it provides a clearer test that is only required for incompatible purposes.** Instead, the current Council text complicates this first step by including a burden of proof and restricting further processing to the same controller. This would unjustifiably complicate the use of big data with no added value for data protection.

In order to support Europe's data economy and take full use of new insights provided by big data in healthcare, energy, transport, it is important to not restrict further processing unnecessarily. Data-driven and big data innovations are based on further processing. Data are collected from individual and objects, analysed and combined to create inferred data. The incentive to lawfully share data with secondary and tertiary parties is strong, as it leads to increased efficiency and to the development of new products and services. It is important to ensure that the principle of data minimisation does not collide with the development of data-driven innovation, which can benefit business, consumers and society.

We also express our support for the Council approach on legitimate interest. We strongly encourage the EU institutions to avoid the overly restrictive approach suggested by the Parliament. We would like to recall that the legitimate interest legal basis for processing is a key provision that allowed the 95/46 Directive being flexible enough to adapt to the latest innovations of the digital economy.

6. PROFILING (ART. 20)

(→ CONDITIONAL SUPPORT FOR COUNCIL TEXT, SUBJECT TO CHANGES)

We urge the EU institutions to avoid creating a framework which could restrict profiling across various industry sectors irrespective of the objectives pursued. The current Council compromise is a step forward compared to the Commission and the Parliament proposals, but it can be improved.

In the context of discussions on privacy, profiling has generally been considered as a practice that consumers must be protected from. According to BUSINESSEUROPE, this is not entirely the case. Nowadays, the ability to process and analyse data through the creation of profiles is absolutely essential for the digital economy.This is done in a significant number of domains: credit card fraud detection in the banking industry; clinical decision support, disease prevention, surveillance and population health management in the health industry; merchandising, demand-driven forecasting, pricing strategy, overall operations improvement and warranty management in the retail industry; product and process quality improvement and predictive maintenance in the automotive industry; smart metering in the energy sector; tax and revenue benefits and fraud detection.

7. RIGHT TO BE FORGOTTEN (ART. 17)

(→ CONDITIONAL SUPPORT FOR COUNCIL TEXT SUBJECT TO CHANGES AND SUPPORT FOR EP ON IDENTITY VERIFICATION)

We generally support the Council more flexible approach on the right to be forgotten. However, despite the amendments made to the text, neither the version of the Parliament nor that of the Council answer the question about how the controller – wanting to fulfill its obligation –could identify other controllers who process data that were made public. Even if this is possible, the controller cannot force any entities acting independently to perform such actions. We also support the EP proposal of making the exercise of the right to be forgotten contingent on the possibility to verify the identity of the entity making the request (Article 17.1a of the EP). In this context, it is important that the Regulation addresses essential issues, especially the ones that are not addressed in the current 95/46 Directive, without leaving unclear matters to be dealt with in the delegated acts.

8. DATA PORTABILITY

BUSINESSEUROPE not support the principle of data portability. Obligations of data portability would create heavy burdens on data controllers without a proportionate benefit for data subjects.

9. INTERNATIONAL TRANSFERS OF DATA

(→ SUPPORT FOR THE COUNCIL AND FOR THE EP TEXTS, DEPENDING ON THE ISSUES)

International data transfers are fundamental for any business activity, in any sector and for companies of any size. **It is fundamental that the Commission decisions on third countries' data protection adequacy reflect today's business reality. Such decisions must be taken timely, ensure predictability and allow stakeholders to express their views.** In the last years, the Commission has not taken any adequacy decision despite the fact that many third countries have developed sound data protection legal frameworks. Quick processes are need for European companies to transfer data to these countries.

Other systems of data transfers must be made smoother and easier. In the modern information technology dependent economy, it is not sustainable to submit transfers of personal data using the approved mechanisms to any prior approvals. In particular, there is no reason to make a distinction between standard contractual clauses and binding corporate rules (BCRs), transfers under both mechanisms should not require authorisation or approval. It is also recognised that the BCRs for processors cannot have the same content as BCRs for controllers, due to different scope and nature of obligations under this Regulation.

The Parliament's proposal in art. 43 (1.a) on BCRs, requiring that that employee representatives are formally involved in the creation of the BCR, is unworkable and should be deleted.

The Parliament's proposal in Article 42 to place obligations on the controller or processor to seek approval in advance of transferring data to countries that are not considered to have an adequate level of protection in accordance with new Article 43(a), or the so-called 'Anti-FISA' provision, places companies in a difficult position for their business activities, especially where there is a conflict of law situation. These matters should be addressed at an inter-Governmental level.

European businesses are also supportive of the Council's willingness to preserve the derogation contained in Art. 44.1(h). Crucially, this derogation applies to non-bulk or non-mass transfers of personal data; non-frequent small scale transfers of personal data, or not permanent transfers of personal data. Furthermore, the purpose of the transfers envisioned under the derogation is not to process or disseminate personal data, but rather to enable support functions, troubleshooting or routine controls. For such functions, the transfer of personal data is purely incidental.

10. TRANSFERS OF DATA WITHIN UNDERTAKINGS
(→ SUPPORT FOR EP TEXT)

Exchange of data is indispensable within groups of undertakings, to ensure indispensable the competiveness of European companies acting not only within the European Single Market, but also across its borders. This is also valid for any institution affiliated to a central body. In this context, we strongly welcome the EP approach in art. 22.3a, stipulating that a group of undertakings should have this possibility. This position should be upheld during the trilogue discussions. In recital 38a the Council provides that controllers which are part of a group of undertakings are allowed to transmit personal data within the group of undertakings for internal administrative purposes. We welcome that the Council is going in the right direction, but this recital would not be a sufficient legal basis to ensure such transfers.

11. LIABILITIES (ART. 77)
(→ CONDITIONAL SUPPORT FOR COUNCIL TEXT, SUBJECT TO CHANGES)

BUSINESSEUROPE does not support a system with joint and several liability for both controller and processors, which would clearly introduce significant burdens on companies and authorities with no concrete gain for the data subject.

In this context, the Council attempts to improve the Commission draft are welcome. There are however elements which need some improvement, as Article 77 (2) in the Council position refers to 'lawful instructions' of the controller to the processor and this concept is open to wide and different interpretations. This would increase the risk for processors. As a response, processors would have to carry out more due diligence on data and where it comes from, or accept a high level of risk. This poses a particular risk when dealing with SMEs as controllers, as they may not be equipped to understand/respond to due diligence requests and consequently for processors to decide not to service some parts of the market. Alternative language could be 'contractual instructions of the controller' instead of 'lawful instructions'.

It is also fundamental to ensure a subsidiary liability system whereby the data subject turns to the data controller as his/her first port of call for redress. The processor is liable to the controller if he act contrary and beyond instructions. Making a processor liable to the data subject for its obligations under this regulation would in practice turn processors, not controllers, into the data subject's sole port of call for redress. Where both controller and processor are involved in processing, the controller must have a possibility to recover the damages that are due to the processor. For instance, in the framework of a contract between a controller and a processor, the contract should foresee the necessary guarantees to allow the controller to possibly recover the damages that are due to the processor.

The most frequent scenarios of data incidence are personal data breach due to an IT security incident (covered by Art 30, under the obligation to establish adequate security measures). In the typical case of an outsourcing cloud computing contract, the incident will normally happen in the processor's infrastructure. Based on the current Council proposal for Article 77(2), in case of such an incident, the controller could exempt himself completely. As a consequence, the data subject can only raise a claim against the processor, not the controller as it is the case today. This goes against the logic of customer relations, since a person would have to turn to the IT providers of his bank/hospital rather than his bank/hospital. Also, the controller has no incentive to keep up its data security measures since it can exempt itself according to Article 77(3). Any damages to the data subject are claimed directly to his IT providers, not himself.

12. SANCTIONS AND COLLECTIVE REDRESS (ART. 73-79)

(→ CONDITIONAL SUPPORT FOR COUNCIL TEXT, SUBJECT TO CHANGES)

We welcome the approach contained in the Council text, which lowers the amount of sanctions, adds discretionary factors (under article 79 (2a) (e)) **and defines more precisely the conditions for sanctions to be applied. Nevertheless, the magnitude of potential fines is still very high and sanctions are applied in cases of non-major offences.**

Some scales having into account proportionality criteria, the harmed caused by the infringement, re-offence and the background cancelation should be introduced. Also, the percentages of companies' turnover to calculate the sanctions should be reduced and applied to the turnover in the country in which the offense is committed, not to the worldwide turnover. The supervisory authority should have the option of issuing a warning without imposing a penalty.

We trust that finally fixed penalties are applied evenly by data protection authorities of each Member State, as currently this lack of uniformity involves loss of competitiveness of enterprises in some states over others.

On collective redress, we would like to express our support for the Council position and reiterate our strong opposition to the introduction by the draft regulation of a European system of collective redress for infringement of the data protection Regulation, which might lead to a claim culture, driven by business models based on buying and exploiting legal claims. In particular, the referral by the Parliament to Art. 77 in Art 76.1 presents the risk of establishing a "class action" system.

We reject this proposal. The effect would be deterring innovation and creating additional costs for companies, with negative repercussions for consumers themselves.

In this context, we recommend following the general approach of the Council. Unlike the Commission proposal and the EP report, the Council does not require Member States to adopt one single collective redress system. This is in line with the 2013 Commission Recommendation on collective redress.

However, we do not support that the Council text stills allows for compensation for 'immaterial damage' (art. 77.1), maintaining the proposal from the Parliament. This might create issues in those national legal systems that do not recognise these types of damages.

13. DATA PROCESSING IN EMPLOYMENT CONTEXT (ART. 7.4, 82 AND 83)

(→ SUPPORT FOR COUNCIL AND EP TEXTS ON CONSENT IN EMPLOYMENT CONTEXT, SUPPORT FOR COUNCIL TEXT ON DATA PROCESSING IN EMPLOYMENT CONTEXT)

We strongly support the EP and Council position on consent in employment context. It should continue to be possible to use consent as a legal basis for data processing in employment context. This must be maintained during the trilogue discussions.

We also encourage the possibility to use collective agreements such as sectoral and works agreements as a basis for data processing. Art. 82 as proposed by the Council provides this possibility, besides giving the flexibility to Member States in employment context. It also states that collective agreements can provide for more specific rules on data protection in the employment context, taking into account certain variations which are necessary in order to give companies the flexibility they need. Recital 124 determines that works agreements are part of the broader expression "collective agreement". This is of major importance, since companies mainly conclude works agreements in order to handle data protection matters. We therefore support Council's approach on collective agreements.

Furthermore, regarding the processing of personal data for statistical purposes it is essential to ensure that labour market organisations can continue to conduct wage and labour costs statistics which play an important role in the collective bargaining system in some countries. Art. 83 as proposed by the Council and EP provides this possibility. Valid information on costs and gains concerning potential collective agreements is crucial for a rational and responsible dialogue between the social partners and play also an important role for governments.

14. PROCESSING OF PERSONAL DATA FOR HEALTH RELATED PURPOSES

Contrary to what approved in the EP report, we believe **that processing of personal data concerning health should not be subject to specific identified types of research**, but to different possible new future or different types of research. At the time of data collection it is not always possible to describe the future use of these data, including the reuse of medical records and records of diseases.

Regarding the processing of personal data concerning health which is necessary for historical, statistical or scientific research purposes, we believe that a general exception should be made to the requirement of consent for research when it serves a high public interest, if that research cannot possibly be carried out otherwise.

15. SECURITY BREACH NOTIFICATION

(→ SUPPORT FOR THE EP AND COUNCIL TEXTS, DEPENDING ON THE ISSUE)

Experience from other jurisdictions with breach reporting duties show that the threshold and time limit for reporting breaches can be difficult to comply with in practice, if not carefully drafted. Individuals could also become overly accustomed to receiving notices of breaches, which can undermine the importance/significance of these notices, thus undermining the purpose of having the requirement.

The Council's risked based approach set out in Article 31 is preferable and more proportionate, in terms of definition of the duty of a controller to report a breach, as only breaches that are likely to result in high risk for the individual have to be reported. However, the Parliament's position on timing i.e. the requirement to report an incident "without undue delay", after actual establishment of a breach is preferable. The Council's proposed time limit of 72 hours of becoming aware of a breach is too arbitrary and lacks clarity, as it does not specify whether the notification has to be made just on the basis of suspicion, rather than an actual breach.

16. E-PRIVACY DIRECTIVE (ART. 89)

(→SUPPORT FOR THE EP TEXT, SUBJECT TO CHANGES)

The Commission has announced a comprehensive review of the e-Privacy Directive 2002/58/EC, once the data protection Regulation is adopted. We believe that it is however important to already address the deletion of those articles of the e-Privacy Directive that would become redundant as they are already covered by provisions of the GDPR. This applies notably to the clauses on data breaches notifications (art. 4), on location data (art.9) and traffic data (art.6). As these articles should be considered as superseded by the GDPR, they should be explicitly deleted in order to avoid a double regulation regime. We therefore support the Parliament's position to delete Art. 4 and do propose to extend the deletion also to Art. 6 and 9 in Art. 89 of the GDPR on the relationship between the e-Privacy and the GDPR.

* * *