

KEEP EUROPE GROWING

24 September 2015

GDPR Redlines – the missing link between GDPR and DSM

Europe is home to some of the best connected and most innovation-driven economies in the world. In particular, Finland (2nd), Sweden (3rd), the Netherlands (4th) and the UK (8th) are the European digital peak performers on the 2015 World Economic Forum's (WEF) global technology benchmark.¹ With several Member States significantly lower in the ranking, the EU as a regional bloc would rank well behind the US, which comes in at 7th place. In an effort to create a true digital knowledge-based economy in the EU, the European Commission has launched the Digital Single Market (DSM) flagship strategy. This plan aims to promote Europe as “*a place that nurtures investment and entrepreneurship*”, where business flourish and can “*become global leaders in sectors of the future*”.²

An ambitious and successful DSM strategy that boosts Europe's economy must embrace the technological revolution brought about by ICTs including cloud computing, big data analytics and Internet of Things. Indeed, as recognized by the Commission, “*data has become a key asset for the economy and our societies similar to the classic categories of human and financial resources*”.³

The European Data Coalition (Coalition) stands for a Europe that both delivers effective data protection standards for citizens and creates an environment in which European based companies are encouraged to innovate and develop Europe's digital ecosystem. The success of the European digital peak-performers identified in the WEF's report – which both adhere to high EU standards of protection and deliver global digital top-performance – prove that under an appropriately balanced framework, these two aims can complement one another. With this in mind, the proposed Regulation on Data Protection (GDPR) was introduced with the laudable goal of updating data protection rules for the 21st century, reducing administrative burdens and harmonising the divergent approaches taken by the different Member States.

The Coalition believes that a progressive solution is within reach of the ongoing GDPR trilogue negotiations, provided the right balance between privacy and innovation is struck, the future GDPR must:

1. Create incentives and reduce administrative burdens in order to stimulate investment in data-driven innovation, making the EU the go-to market for product launches and new services;
2. Remove unnecessary costs due to fragmented national implementation of data protection rules through meaningful harmonisation;
3. Lay a secure and flexible foundation for open international data transfers that facilitates interaction with global partners;

¹ World Economic Forum, *Global Information Technology Report 2015*, available at <http://reports.weforum.org/global-information-technology-report-2015/>

² European Commission, *Digital Economy*, available at <https://ec.europa.eu/digital-agenda/en/digital-economy>

³ European Commission, *Making Big Data Work in Europe*, available at <http://ec.europa.eu/digital-agenda/en/big-data>

4. Maintain clear and separate roles and responsibilities between controllers and processors in the data processing value chain, avoiding replication of effort;
5. Provide a proportionate sanctions regime that punishes non-compliance but avoids draconian measures that would discourage investment in data-driven innovations.

Unfortunately, the current path taken by some GDPR trilogue negotiators threatens to undermine the five key criteria identified above. There is a risk that the GDPR will fail to build on the success already achieved in some Member States, preventing the EU from realising its DSM ambitions and substantially improving its digital performance. The threats of a failed GDPR to the DSM are as follows:

1. **Failure to create incentives for investment in data-driven innovations:** The GDPR instead maintains a negative position towards data processing combined with a tunnel-vision on perceived threats to privacy. It threatens to expand restrictions on data processing far beyond the 95-Directive, limiting the available legal bases for processing and hence the opportunity scope of data-driven innovations. Under the proposed restrictions:
 - I. **Consent** would be limited such that only *explicit* consent justifies data processing. This would create substantially increased costs for businesses, which would have to provide many separate consent clauses, without guaranteeing any increase in protection. Furthermore, such consent requirements may disproportionately impact SMEs who have neither a large customer base nor an established brand to draw customers in. This is an example where GDPR is not only failing to reduce administrative burdens but is also unduly increasing them.
 - II. The **legitimate interest** legal basis would be narrowed through the inclusion of a new, highly subjective “*reasonable expectations*” test as an additional requirement that risks sowing confusion among controllers concerning which interests they are able to claim as justification for processing. This will result in decreased investor confidence due to increased legal uncertainty, and consequently decreased levels of investments in data-driven businesses.
 - III. An overly constraining interpretation of **purpose limitation** would stifle the data-driven economy, which is dependent on the possibility of retaining data for re-use. Big data analytics attempts to draw connections and relationships between data that are unexpected and previously unknown. Its value is in its potential to uncover new correlations for new uses which benefit society. The disconnect between the proposed law and reality puts at significant risk the development of an EU data-driven economy, as aspired to in the EU’s DSM strategy.
 - IV. There is a failure to ensure that businesses can practically deal with the scope of the rules and failure to reduce unnecessary administrative burdens. This is exemplified by the lack of allowances within the **definition of personal data** for special cases such as business contacts and pseudonymised data. Data should only be considered personal if the controller is capable of identifying someone using it. If administrative burdens are not made proportionate, for example by reducing the obligations associated with the collection and use of pseudonymous data, the GDPR provides no incentive for businesses to offer services internationally from Europe. Instead, it will drive European entrepreneurs, European data-driven innovators and European-based data processing to third countries.
2. **Failure to deliver the necessary harmonisation for European industry:** Where the GDPR should have been strong, uniting the EU’s current divergent national systems

based on the 95/46 Directive, it is likely to falter. For instance, in the Council's version, the much needed "one-stop-shop" mechanism aimed at promoting consistent application of the GDPR throughout the EU would remain cumbersome and bureaucratic. Of particular concern are cross-border complaints for which a coordinated consultation of a large number of Data Protection Authorities (DPA) would be necessary. Moreover, to further the goal of legal certainty, it is crucial to establish guidance on what constitutes a "main establishment" in the context of identifying the lead DPA overseeing data processing activities.

3. **Failure to lay a secure and flexible foundation for open international data transfers that facilitates interaction with global markets:** The proposal instead introduces two unreasonable demands that together will greatly hamper the ability of European businesses in this sector to operate in an international context:
 - I. The exception allowing "non-bulk, non-frequent, temporal" transfers (article 44.1.h) on the grounds of "legitimate interest" may be discarded. If this is done, vital flexibility allowing for business-to-business outsourcing and catering to industrial internet data processing needs will disappear;
 - II. Article 43a on data disclosure requests from third countries would create extraterritorial conflicts of law for European companies operating inside and outside the EU. This would leave companies in impossible situations and moreover provides no meaningful legal protection for citizens.

4. **Failure to maintain clear and separate roles and responsibilities for controllers and processors in the data processing value chain:** Processors will instead be held liable for circumstances outside their sphere of control and influence, raising significantly the transaction costs of doing business. A joint liability regime will lead to processors duplicating the controller's privacy processing assessment for parts of the processing outside the processors' own assignment. This is both unnecessary and costly.

5. **Failure to provide a proportionate sanctions regime.** The proposed regulation suggests basing penalties on global turnover, including revenues that are entirely unrelated to data processing. The resulting penalties, without clear codified sanctions guidelines, could be completely disproportionate to the extent of the data processing, and the extent of any potential non-compliance that actually occurs. This will diminish incentives for data-driven innovation for global companies as well as discouraging "old-economy" companies from digitising and modernising. These substantially increased sanction levels must be seen in combination with the proposed joint liability provision, which will significantly increase outsourcing costs as processors will be faced with unacceptable levels of risk. This will cripple the EU outsourcing market and result in decreased levels of controller specialisation (as they will have to rely on in-house IT services) and ultimately a loss of competitiveness.

Conclusions

If we are to achieve EU-wide digital peak-performance, the digital economy that underpins the DSM must be allowed to flourish. As the digital economy is all about data and data-driven innovation, it is crucial that the soon-to-be-finalised GDPR **avoids the risks and pitfalls identified in this document and a progressive solution is found.**

A progressive GDPR is within our reach, trilogue stakeholders have the necessary knowledge and capacity to avoid the risks identified herein. **However, if the trilogue**

negotiations fail to avoid the dangers described above, the red lines for a progressive GDPR will be crossed, and Europe will have to bear the consequences of a failed GDPR.

European industry, SMEs and startups will be faced with unbearable disadvantages and will be unable to contribute to the political objectives of an ambitious DSM. The implementation of a failed regulation would undermine European businesses' efforts to realise the Juncker-Commission's DSM objectives.

A failed GDPR would establish an enormous disconnect in Europe from the requirements of a modern, advanced digital knowledge economy, putting at significant risk the development of a data-driven innovation economy, as aspired to in the DSM strategy. **It therefore comes down to a straight choice between an ambitious DSM and a failed GDPR.**

Let's make the right choice and assure a bright future for Europe's digital economy. There is still time in the ongoing trilogues to avoid the five GDPR failures listed above – let's make sure these redlines are not crossed.



Rene Summer
Coalition Spokesperson

ABOUT THE COALITION

Our Coalition is made up of nineteen European companies, from SMEs to Global Multinationals and non-profit organisations operating in a variety of sectors on a national, regional and global scale. With an aggregate turnover (2013) of over € 158 billion and some 752,000 employees worldwide, our footprint allows us to bring growth, progress and jobs to the EU's economy. Our membership includes...

- ... a global leader in power and automation solutions...*
- ... the leading Central and Eastern European e-commerce company...*
- ... a productivity solutions provider of compressors, vacuum solutions, construction and mining equipment...*
- ... a non-profit organisation dedicated to collecting money to prevent and combat child cancer diseases...*
- ... a global leader in household appliances...*
- ... two providers of communications technology and services...*
- ... a designer, engineer, manufacturer and distributor of outdoor power products...*
- ... an investment company...*
- ... a SME provider of online marketing through search engine marketing, conversion and lead generation...*
- ... an e-commerce company providing payment services for online storefronts...*
- ... an engineering group in tooling, materials technology, mining and construction ...*
- ... an enterprise software corporation...*
- ... a global provider of heavy trucks and buses, engines and services...*
- ... a provider of assured, secure cloud services to the UK public sector...*
- ... a global provider of renewable solutions in packaging, biomaterials, wood and paper...*
- ... the leading university in technology and digital arts programmes...*
- ... a provider of business software and services to more than 340 000 business in the Nordics...*
- ... a producer and distributor of trucks, buses and construction equipment...*
- ... the leading company in advanced mobile services...*

Our businesses are profoundly different but deeply united by the need for clear roles and responsibilities, open cross-border data flows, balanced codified sanction guide lines, effective one stop shop and absence of overly prescriptive rules as fundamental conditions for long-term growth, competitiveness and prosperity, for both us and the economies in which we operate.

For further information please visit us www.europeandatacoalition.eu or contact us at info@europeandatacoalition.eu