

UNI Europa feedback on the EU Commission proposal on a framework for the free flow of non-personal data in the EU (2nd Data Package)

UNI Europa is the European sectoral trade union federation for private services workers – the backbone of economic and social life in Europe. We represent 7 million workers in 272 national trade unions in 50 European countries.

We cover workers from the following sectors: Commerce, Banking Insurance and Central Banks, Gaming, Graphical and Packaging, Hair and Beauty, Information and Communication Technology Services, Media, Entertainment and Arts, Postal Services and Logistics, Private Care and Social Insurance, Industrial Cleaning and Private Security, Professional Sport and Leisure, Professionals/Managers and Temporary Agency Workers.

1 General remarks

Whilst UNI Europa acknowledges the potentials and value of data, we find the 2nd Data Package problematic, unclear and ultimately obsolete on the following grounds:

- 1 Clear definitions to core concepts are lacking: for example, what is non-personal data, and what does the proposal mean by ‘data processing’?
- 2 It is all too clear from experts in the fields of data, data processing and algorithmic design that the very distinction between personal and non-personal data is more of a political issue than a technical one.
- 3 Computer science has shown that non-personal data can be linked and tracked back to individuals, and that de-identified data can be re-identified. Put differently, most data can be made personal depending on the identifiers and data sets used¹.
- 4 The line between PII (personal data) and non-PII (non-personal data) is not fixed but rather depends upon technological developments and new uses of technology.
- 5 Indeed, in 2010 already, the US Federal Trade Commission, the FTC, acknowledged “the blurring of the distinction between personally identifiable information and supposedly anonymous or de-identified information”².
- 6 Furthermore, taking into account the fact that, in practice, most data sets held by companies are ‘mixed’, i.e. they contain both personal and non-personal data, which cannot be easily separated, and that both the provisions of the General Data Protection Regulation (GDPR) and the 2nd Data Package, if adopted, would have to be applied, this EU legislative proposal will lead to an unnecessary compliance burden, adding complexity rather than removing it.
- 7 The 2nd data package allows for the possible undermining of the GDPR and a breach of fundamental rights.

¹<https://piwik.pro/blog/what-is-pii-personal-data/>,
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1909366

² <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf>

2 Recommendation

Thus, for legislative clarity and to avoid grey zones and insecurity, UNI Europa recommends:

- a) That the precautionary principle as detailed in Article 191 of the Treaty on the Functioning of the European Union is applied,
- b) That this legislative proposal is rejected and,
- c) That the provisions in the GDPR are applied to all forms of data.

3 Elaborative comments

For workers, the risk of a breach of fundamental rights could have a significant impact on their employment. As the 2nd data package proposal stands, data subjects have no rights should they suspect that their personal data are being transferred across borders under the 2nd data package. Whilst data subjects can use the provisions in the GDPR to test their suspicions, the mere fact that these rights do not explicitly exist in the 2nd data package is wrong. Given that the majority of corporate data is mixed, and given that the distinction between personal and non-personal data is questionable, the 2nd data package thus allows for the possible undermining of the GDPR and a breach of fundamental rights. Invisible electronic data collection and cross-border transfer must be avoided.

From the perspective of workers, privacy rights and protection in relation to data mined, used, handled and stored by companies, are crucial. To avoid future scenarios where management rely on (semi) automated decisions in their HR processes without the possibility for workers to gain insight into the datasets used, how they are used, and from where they are gathered, UNI Global Union, UNI Europa's global head office, has issued the [Ten Principles for Workers' Data Rights](#).

As provisioned in the GDPR, it is of utmost importance that workers are fully informed about data processes in the company and that they, in addition to the right to edit said data, have the crucial right of explanation in relation to data-informed managerial decisions (articles 13-15 and 22). This is particularly relevant in recruitment, promotion, disciplinary or dismissal HR processes. Although the de facto right of explanation in the GDPR is contested (see [here](#) for argumentation that it does not exist and [here](#) for argumentation that it does), UNI asserts that workers, as citizens, must have the opportunity for data insight as well as the right to object to being subject to decisions based on that data.

Data-informed managerial decisions concern and affect workers and have been used in ways that directly breaches, adversely affects or lowers the enjoyment of workers' rights (see Phoebe Moore (2017), Cathy O' Neil (2016)). Without the rights of insight, explanation and objection, there will be no check and balance on data sets used by management. This in turn could lead to a rise of non-ethical, immoral and discriminative HR processes.

Given that the free flow of data is possible if the GDPR provisions are followed, one of the reasons given to the necessity of the 2nd data package seems irrelevant. If companies want a free flow of data, all they need to do is follow the GDPR. This would precisely build the trust that the 2nd data package states is lacking and will increase transparency.

4 Concluding remarks

UNI Europa wishes to comment that we have been informed by relevant insiders that this legislative proposal is a step in the way to resolving outstanding issues in relation to

the free flow of data in international trade agreements. We note that in the WTO, the EU is pushing for new e-commerce rules, which amongst others, include the free flow of data (all types of data) and the removal of localisation requirements. Yet the EU is doing so without having the legal basis to do so as the contradictions between the free flow of data and the GDPR are, as of yet, unresolved. Why is the EU Commission trying to get other countries to commit to something they themselves cannot even legally commit to?

We also wish to raise that the USA is pushing for provisions in trade agreements that stipulate that it is the data protection regime in the country that hosts the servers on which data is stored that determines who can have access to the data stored. If agreed in an international agreement, this demand would undermine the GDPR.

Also, we would like to stress that the free flow of data by no means equals the free and equal access to data³. As it stands now, and without sound policies in place defining data ownership and data control, it is estimated that the Big 6 (Alibaba, Google, Amazon, Facebook, Microsoft and Apple) “own”, through their data brokers and supply chains, the vast majority of the world’s data. Given that the value of global data flows in 2014 was [2.8 trillion USD](#)⁴ and has undoubtedly risen since, we urge the EU Commission to expand on innovative solutions to data control versus data ownership. The Estonian system where citizens have extended possibilities to see who is accessing their personal data and what data they are accessing, and to control this access, seems highly inspirational and applicable not only to workers and the workplace, but to citizen empowerment in its entirety.

We would ask the Commission to rethink how the wealth created by data flows can be distributed, so it benefits the majority and not just the few. A possible avenue could be to explore the concept of “community data”: i.e. that the value added of a large amount of data generated by communities must be returned to the identifiable and relevant community, e.g. the workplace or the city/village. It is essential that the individuals/users/workers, who create most of the data, have explicit rights of access to, insight into, and use of that data.

Lastly, it is worth remembering that as of today, 50% of the world’s population still do not have access to the internet. In addition, half of the world’s countries⁵ do not have data protection laws in place and very few data protection laws specifically for workers exist in any country in the world. There is much that needs doing in order to bridge the digital divide, why these issues should be multilaterally addressed prior to further discussions in trade agreements and elsewhere on the flow of data.

A copy of this response has been sent to the IMCO and ITRE committees of the European Parliament.

³ <http://www.thefutureworldofwork.org/stories/uni-global/myths-of-the-free-flow-of-data/>

⁴ <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows>

⁵ https://www.wto.org/english/forums_e/business_e/3_4_Cecile_ppt.pdf