The Consumer Voice in Europe

# BEUC COMMENTS ON THE EDPB GUIDELINES 4/2019 ON DATA PROTECTION BY DESIGN AND BY DEFAULT

**Contact: Ernani Cerasaro – digital@beuc.eu**

**BUREAU EUROPÉEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND**
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union

Ref: BEUC-X-2020-003 - 16/01/2020

## Why it matters for consumers

Today technology is a vehicle for consumers to articulate large parts of their lives. Digital services should assist them without undermining their individual rights. Unfortunately, consumers are frequently manipulated by tech tools weakening their autonomous agency and reducing their fundamental freedom of choice, via the exploitation of their personal data. It is key to ensure that products and services have data protection measures 'baked in' from the design stage and through their whole lifecycle. Data Protection by Design and by Default is necessary to ensure an effective protection of consumers in the digital space.

## General remarks

BEUC supports the interpretations and guidance given by the EDPB regarding DPbDD with some general remarks, and some more specific comments.

DPbDD are key concepts of effective consumer protection in the digital age when products and services become ever more opaque, complex and automated, which leads to a profound shift in the power balance between consumers and controllers. Consumers need to be able to trust that the basic protections are automatically present in the products and services they buy. At this stage, consumer organisations' product testing and other legal and technical analysis of products and services demonstrate that this is not the case.

Data subjects can be seriously threatened if a digital tool is not created in order to respect their fundamental rights to privacy and data protection during its whole lifecycle.

It is therefore key to have a systematic approach in interpreting, implementing and enforcing the DPbDD provisions of the GDPR, which takes into account all the various elements of the lifecycle of a product/service: including its design, its application, its use, the consequences of this use, up to its disposal.

The whole process is a chain of organizational, commercial and technical measures that potentially impact on consumers. Each of the single steps can have a significant impact on the consumers' wellbeing as the single decisions adopted by the controllers are not only affecting consumers' rights and freedoms but also their satisfaction.

Too often personal data protection depends on the assumption that consumers are fully aware of the processing activities, can read and understand long and complex privacy policies. "Dark patterns'' are also used to nudge consumers into accepting privacy intrusive practices. This, together with the omnipresence of digital technologies and data processing in all activities and aspects of our daily lives, is creating a situation where consumers are in an increasingly vulnerable position.

A correct implementation of DPbDD would bring numerous benefits for consumers: it would help to restore their freedom of choice; it would increase the level of awareness, being them able to rely on clearer and user-friendly information; it would increase the

level of trust towards companies and the market itself; it would potentially reduce power imbalances and information asymmetries; etc.

In other words, DPbDD are crucial to ensure effective consumer protection in the digital age and to help achieve a fair and healthy digital ecosystem.

For this reason, BEUC supports these guidelines, as they clarify the scale and the scope of DPbDD highlighting their systematic relevance and as well as their practical implications.

BEUC especially welcomes the approach by the Board in interpreting the legal requirements of DPbDD in the light of the general data protection principles (transparency; lawfulness; fairness; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality).

All this being said, BEUC has some specific comments that will hopefully be taken into account in the final version.

## The role of processors and technology providers

More clarity on the role and responsibility of actors other than the controller would have been appreciated. The scope and the structure of the guidelines may be further developed in this sense.

If, on the one hand, article 25 of the GDPR imposes obligations only on the controller, on the other hand, it should be highlighted that many of the elements (or KPIs) correctly identified by the Board are actually activities that the controller (especially if SMEs) outsources to processors, who possibly outsource to sub-processors.

As also pointed out by the EDPS in its Opinion, "A *serious* limitation of the obligations of Article 25 is that they apply only to impose an obligation on controllers and not to the developers of those products and technology used to process personal data"[1]. This is a major vacuum of the GDPR.

After all, also these guidelines underline that "Although not directly addressed in Article 25, processors and technology providers are also recognized as *key* enablers for DPbDD. They are in a position to identify the potential risks that the use of a system or service may entail and are more likely to be up to date on technological developments".

In addition to this, third parties who may possibly intervene in the product/service development - including manufacturers, product developers, application developers and service providers – are only mentioned in the recital 78 which does not place a requirement on them to comply with DPbDD, as this remains with the controller.

While BEUC recognizes that this is a legislative gap - which now BEUC hopes will be addressed, at least partly, in the framework of the "ePrivacy Regulation" - would have welcome a greater effort by the Board in giving guidance on this aspect.

It actually constitutes a key element for an effective application of the measures and safeguards described in the guidelines.

In particular, the list of almost seventy KPIs related to the general principles will certainly help in the correct establishment of processes that are more respectful of consumer

[1] EDPS Opinion 5/2018 - Preliminary Opinion on privacy by design.

rights, but only if explicitly highlighting that they may take place within complex contexts, building on multilevel relationships between various actors, including third parties.

The mere fact that a controller may be held liable for processors' activities is sometimes an insufficient solace for the consumer/user when the damage has already occurred. Some of the material and immaterial damages arising as a result of the non-compliance with DPbDD may due to the deficiencies of parties who are not necessarily controllers.

An example on integrity and confidentiality may be found in these guidelines – page 24 – regarding the access and mitigation of a "possible damage from malware". Assuming that the segregation is done by a processor under the instructions of the controller, what would be the level and the extent of the liability for both processor and controller if a damage occurs?

Moreover, this would be an important clarification given the new regime of the GDPR, where the processor is held liable for the damage caused by processing "only where it has not complied with obligations of this Regulation *specifically directed to processors* or where it has acted outside or contrary to lawful instructions of the controller" (art. 82).

On this last aspect, the guidelines could develop a more detailed interpretation, describing in a more explicit way the levels of the single responsibilities related to the respect of DPbDD.

For example, a meaningful interpretation of the transparency principle not only requires that the data subject receives clear, complete and updated information about the content of processing activities, but also about the parties *who* take part in it, when and which are the consequences.

The various examples and lists of KPIs in Section 3 could be further developed adding references to the role of the developers/processors which are now limited to the final part on recommendations (par. 86).

In conclusion, it is key to highlight that DPbDD are particularly important also to fill the gap and imbalances attributable to consumers' lack of awareness and understanding of *who* may access their information and *how* they may use it.

## State of the art and standards

BEUC welcomes the interpretation and the guidance provided by the Board in par. 18-21, where the state of the art has been defined as "a dynamic concept that cannot be statically defined at a fixed point in time, but must be assessed continuously in the context of technological progress".

In this regard, BEUC supports the interpretation given by the Board on the obligation for controllers to be aware and stay up to date on technological advances in order to secure an effective implementation of DPbDD.

Controllers should be aware of the existence of best practices and standards, which are a useful tool for complying with the law and respect data subject rights.

However, we would suggest to slightly modify the reference to standards in par. 22.

If in a certain field there are established practices, this should not imply that those who access (or are part of) that market, should feel obliged to take them into account.

Sometimes, it happens that consolidated practices are harmful to the people concerned and it is precisely the freedom of the players who do not consider these practices adequate enabling to develop more sustainable systems. Furthermore, this also implies the risk of increasing the level of influence of dominant players who have had the opportunity to impose their own standards.

We would therefore suggest rephrasing the sentence in the following manner: "Existing standards and certifications may play a role in indicating the current "state of the art" within a field. Where such standards exist *and provide for a high level of protection for the data subject in compliance with - or beyond - legal requirements,* controllers should take these into account in the design and implementation of data protection measures".

## Consumer choice and power balance

BEUC welcomes the references to the need to ensure consumer choice (e.g. avoiding the "lock in" effect) and to the power balance, in par. 65. However, they can be further developed.

With regards to the first, an explicit reference to data portability in practice could clarify the practical consequences of the lack of choice for the users. A reference, or an example, on the so called "dark patterns" would help as they constitute a usual practice to circumvent DPbDD.

Dark patterns are well-established user interfaces forcing unconscious users to do things they don't want and would not consent to if they were properly informed.

In 2018 our Norwegian member Forbrukerrådet, published two reports that analysed dark patterns. The first one - "Deceived by Design" - examines a sample of settings in Facebook, Google and Windows 10, and shows how default settings and techniques and features of interface design are used to nudge users towards privacy intrusive options. The second report - "Every step you Take" - shows that Google uses various tricks and practices to ensure users enable location tracking features and does not give them straightforward information about what this effectively entails. Based on this second report, BEUC launched a coordinated enforcement action against Google for breaching the GDPR.

With regard to the second, it is worth nothing that DPbDD are core protection tools against the inherent imbalance in the typical relationship between the controller and the data subject, particularly in digital markets where consumers have no possibility to understand by themselves the complexity of the data processing with regards to products and services they use. BEUC suggests rephrasing it in this way: "*Power balance must be a key objective of the controller-data subject relationship. Power imbalances shall be avoided. When this is not possible, they should be mitigated"*.

BEUC also suggests making a stand-alone point focusing on the obligation that controllers and technology providers do not transfer the risks of the enterprise to data subjects. Further clarification would be needed in particularly regarding what is meant by "the risk of the enterprise'' in this context.

## Enforcement

BEUC also takes this chance to underline the importance and the urgency of an effective enforcement of the Article 25 and its related provisions.

-END-

*This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2014-2020).*