DIGITALEUROPE

16 JANUARY 2020

Response to EDPB consultation on Data Protection by Design and by Default

Executive summary

DIGITALEUROPE welcomes the European Data Protection Board's (EDPB) draft Guidelines on Data Protection by Design and by Default (DPbDD). We concur with the importance of DPbDD being incorporated from the early stages of planning a new data processing operation, and appreciate the EDPB's promotion of DPbDD as an asset that fosters compliance and trust.

We particularly appreciate the practical suggestions contained in the Board's document, such as the frequent inclusion of examples and the lists of 'key design and default elements,' which can provide a useful point of reference for a broad range of businesses. Amid the practical aspects discussed in the draft Guidelines, we also welcome the discussion of constructive design techniques, in particular those that can help support data subjects' comprehension of how their data may be processed.

In our response, we'd like to highlight areas where the final Guidelines could be improved to provide clearer and more workable recommendations for data controllers.

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

Table of contents

Understanding 'necessary'

DIGITALEUROPE welcomes the draft Guidelines' mention of data minimisation as a very important aspect of DPbDD. At the same time, as in our responses to previous consultations,[1] we'd like to call the Board's attention to the fact that necessity is not an absolute determination that merely depends on an abstract consideration of the purposes of processing.[2]

On the contrary, determining what data processing is necessary for a given purpose is highly contextual and must always be carried out with full regard to the broader context, as the Guidelines' paras 25-27 already suggest. As a result, it is often not possible to define *ex ante* and objectively what are the essential and non-essential types of data processing for broad categories of processing purposes.

For instance, two services processing personal data for ostensibly the same purpose may in reality function very differently or have very different features. They may as a consequence have to process very different types of personal data or process such data differently.

Necessary vs. consent

The example contained after para. 63 is an interesting one in relation to necessity. As currently drafted, the example stipulates that banks should retrieve data from public authorities for the purposes of managing loan applications only on the basis of consent.

However, banks have both a legal obligation and a legitimate interest to prevent unauthorised or fraudulent use of credits or situations where consumers might be unable to repay credits. For example, the Consumer Credit Directive requires creditors to assess a consumer's creditworthiness, where necessary, by consulting the relevant database if mandated by Member State law.[3]

This example also implies that a provider cannot process data for reasons of efficiency from the perspective of Art. 6(1)(b), but must always offer an alternative, less efficient process with associated legal basis. However, in this example, if it is materially more efficient to obtain the data directly from the

---

1 See, for example, DIGITALEUROPE's response to the EDPB public consultation on the draft Guidelines on performance of a contract for online services, available at https://www.digitaleurope.org/wp/wp-content/uploads/2019/05/DIGITALEUROPE-response-to-EDPB-public-consultation-on-draft-Guidelines-on-performance-of-a-contract-for-online-services.pdf, in particular pp. 7-8.

2 See, for example, the language at para. 63 of the draft Guidelines.

3 Art. 8, Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers and repealing Council Directive 87/102/EEC.

authorities, the bank should be able to consider this as reasonably necessary to perform the contract.[4] We suggest this be clarified, to make it clear that organisations should be free to choose processes which are inherently suited to their contract offering.

Understanding 'default'

By the same token, data protection by default does not mean that *all* settings/processing must be off by default, as seems to be suggested by paras 39-43. Any processing which is reasonably necessary to achieve the purpose in the specific context of a given product or service can still be enabled by default, and this must be judged by the controller in line with their lawful bases under Art. 6(1).

In particular, organisations should not be required to provide as default a lower-grade, stripped-back version of their product, without elements which are reasonably necessary to provide a quality service.

Relevance of the cost of implementation

Cost is a relevant factor in determining what measures are appropriate. The draft Guidelines currently only emphasise that controllers must factor in DPbDD as a business cost. However, the inclusion of cost in the GDPR's Arts 25 and 32 is a clear recognition that cost is a factor in assessing proportionality, and so should be taken into account when assessing what is required.

A controller is not required to buy the most expensive technology where this would be disproportionate to the risks – not only where it is not effective, as suggested by para. 24 of the draft Guidelines. The most expensive technology may, indeed, be more effective, but if it is disproportionate to the risk then the additional cost is unnecessary.

Storage limitation

The draft Guidelines' para. 52 should recognise the exception to the storage limitation principle where data will be retained for the purposes of archiving, scientific or historical research or statistical purposes, in accordance with Art. 89.

Where data is likely to be useful for future purposes, e.g. research, even if that need has not yet arisen, controllers should be allowed to keep the data in accordance with Art. 89, by applying safeguards such as pseudonymisation. We

[4] See again our response to the public consultation on the draft Guidelines on performance of a contract for online services.

also welcome the acknowledgment in para. 52 that anonymisation is a helpful alternative to deletion.[5]

The example under para. 77 requires immediate deletion of personal data when membership is terminated. The controller, however, may need to retain the personal data for a period after the membership, for example to protect themselves from complaints or legal claims, which should be acknowledged in the final Guidelines.

Both paras 52 and 77 suggest that deletion should be automated. However, while deletion can be automated, it is not possible nor desirable for all controllers to implement in all cases. In some cases, it might be more appropriate for deletion to be at the election of the user rather than automated. The final Guidelines should hence clarify that automatic deletion is one design option, but not a requirement.

Lastly, we would welcome clarification of the meaning of the bullet point on data flows contained in para. 77.

Key design principles and elements

Accessibility of personal data

Para. 54 of the draft Guidelines fails to articulate the relationship with national legislation reconciling data protection with the protection of freedom of expression and information (Art. 85), simply stating that Art. 25(2) applies 'irrespective of' them. We urge the EDPB to expand on and clarify this relationship in the final Guidelines.

Accessibility of data protection information

As highlighted by the Article 29 Working Party's Guidelines on transparency,[6] it may not always be feasible for the privacy policy to be just one click away. A layered approach might be more appropriate in a digital context, ensuring that the most relevant information is made available to users at the most pertinent time when they interact with a product, with the ability to access more detailed information via further links if need be. This is especially true for smart or IoT

[5] The draft Guidelines rightly note that the state of the art is constantly evolving. As a result, in light of the constant evolution of anonymisation techniques and of research on re-identification, it is not realistic to require that the controller reach full certainty that data cannot be re-identified, as suggested for example in the fifth bullet point under para. 77. While this is undoubtedly the goal every time a controller anonymises data, the final Guidelines should make it clear that this involves a risk assessment and risk minimisation exercise, rather than requiring full certainty, which might discourage controllers from attempting anonymisation altogether.

[6] wp260rev.01.

devices, which have more limited user interfaces and pose novel design challenges.

Fairness

The draft Guidelines characterise personalisation or proprietary technologies as potentially unfair from a data protection perspective in that they may lock in users. While DIGITALEUROPE fully agrees that consumers should not be locked in to any one service, we do not believe this should be relevant when assessing the fairness of data processing, which should instead focus on whether the data processing at hand is in conformity with the intended purpose. The GDPR does addresses 'lock in' problems but does so, correctly, under Art. 20 on data portability.

We would also like to suggest a reconsideration of Example 1 under para. 65, which seems to target very specific service providers and does so in an unnecessarily pejorative way. This example ultimately aims to illustrate the importance of accurately representing the ramifications of each choice to the data subject, and we find that a more neutral example could be more useful.

Finally, under para. 65 the bullet points on 'expectation' and 'non-discrimination' could be further clarified by referring to the data subject's '*reasonable* expectations' for the former and to the need for the controller not to '*unfairly* discriminate against data subjects' for the latter.

Supporting compliance by controllers

The draft Guidelines' conclusions (para. 86) state that technology providers should support controllers in complying with DPbDD. Similarly, the example under para. 67 states that a provider's product should 'flag which kind of processing activities using personal data [are] not in line with the legitimate purposes of the controller.'

We would like to point out that – irrespective of the general obligations contingent on processors and unlike, for instance, Art. 32 – the GDPR's Art. 28 does not specifically call out Art. 25 as one of the provisions that processors should assist controllers with. This is justified by the nature of DPbDD, which involves determinations and choices that are at the core of a controller's responsibility.

Linked to this, and as an example of the repercussions of such a recommendation, requiring technology providers to notify controllers of any change in the 'state of the art'[7] has the potential to expose providers to legal risks, as the implication is that the provider is responsible for a DPbDD

[7] Fourth recommendation under para. 86, p. 26 of the draft Guidelines.

assessment which in reality falls on the controller. As such, we are concerned with the EDPB's recommendation that controllers should delegate such responsibility to processors by way of contractual requirements.

Artificial intelligence

Example 1 under para. 74 stipulates that banks should 'never rely solely on the AI to decide whether to grant loans.' Consistent to our response to the Article 29 Working Party's draft Guidelines on automated individual decision-making and profiling,[8] we respectfully disagree with the EDPB's underlying argument that Art. 22 implies an outright prohibition on automated decision-making. Instead, Art. 22 establishes a right for data subjects to exercise.

In addition, the last bullet point under para. 65 refers to 'fair algorithms,' requiring information to be provided in relation to automated decision-making. This bullet appear to us to be related to transparency more than fairness; we hence suggest moving it to the transparency section.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

Senior Policy Manager for Infrastructure, Privacy and Security

alberto.difelice@digitaleurope.org / +32 471 99 34 25

[8] Available at https://www.digitaleurope.org/wp/wp-content/uploads/2019/01/20171128_DIGITALEUROPE%20response%20to%20WP29%20guidelines%20on%20profiling.pdf. See in particular p. 3.

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Airbus, Amazon, AMD, Apple, Arçelik, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Epson, Ericsson, Facebook, Fujitsu, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, MasterCard, METRO, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, Visa, VMware, Xerox.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK