Position Paper

Response to EDPB draft guidelines on Article 25 Data Protection by Design and by Default

Our reference:	COB-DAT-20-001	Date:	14 January 2020
Referring to:	Guidelines 4/2019 on Article 25 Data Protection by Design and by Default		
Contact person:	Ana-María López-Chicheri Llorente, Policy Advisor, Conduct of Business	E-mail:	llorente@insuranceeurope.eu
Pages:	4	Transparency Register ID	33213703459-54

Introduction

Insurance Europe welcomes the European Data Protection Board's (EDPB) draft guidelines on Article 25, Data Protection by Design and by Default (DPbDD), under the General Data Protection Regulation (GDPR), and invites the EDPB to clarify the issues below to provide the necessary legal certainty to insurers.

- **General comments:**

  - **Unrealistic approach to DPbDD**: The draft guidelines focus on the implementation of DPbDD when starting a new data processing process, but do not cover the maintenance of DPbDD in the long-term. The EDPB should therefore include further guidance on how to maintain an adequate level of DPbDD when data processing activities are actually taking place and when real-life situations could put DPbDD at risk.

    The draft guidelines do not acknowledge the existence of IT legacy systems. IT systems were in place before the entry into force of the GDPR and, as a result, are unavoidable. This fact should be addressed in the final guidelines. Moreover, the guidelines should include advice on IT legacy management.

    Importantly, the draft guidelines must stress that a risk-based approach should be applied when implementing DPbDD. This would allow controllers to concentrate on the systems and applications that are used more regularly and to focus on those that may contain more risky aspects to the privacy of customers.

    Recommendation: The final guidelines should consider DPbDD throughout all stages of the life cycle of a business and not only at the time of implementation. Moreover, the final guidelines should advise on how to manage IT legacy systems from a DPbDD perspective and stress the need to take a risk-based approach when implementing DPbDD.

  - **Obligations for controllers but not for technology providers:** The draft guidelines acknowledge that Recital 78 of the GDPR recognises technology providers as key enablers of DPbDD. In this regard, some of the EDPB recommendations for DPbDD in pages 25-27 are directly

Insurance Europe aisbl
Rue Montoyer 51, B-1000 Brussels
Tel: +32 2 894 30 00 • Fax: +32 2 894 30 01
E-mail : info@insuranceeurope.eu
www.insuranceeurope.eu

addressed to technology providers. However, data controllers are the sole responsible subjects for compliance with DPbDD. This creates a situation of imbalance of power, where controllers are completely dependent on what technology providers offer and with no bargaining power to demand higher data protection standards for the products.

Recommendation: The final guidelines should propose, where possible within the scope of the GDPR, further stringent recommendations to ensure that technology providers make available products with an adequate level of data protection.

- **Comments on the chapter on data protection by design:**

  - **EDPB definition of "state of the art":** The EDPB notes in footnote 6 and pages 7-8 that "*state of the art" can be identified as the technology level of a service or technology product that exists in the market and is most effective in achieving the objectives identified"*. Moreover, the draft guidelines mention that "*neglecting to keep up to date with technological changes could therefore result in a lack of compliance with Article 25 GDPR*". Even if data controllers have the obligation to stay up-to-date with technological developments, that does not imply an obligation to always update their systems, with the consequent organisational and financial burdens. The above-mentioned statement and its economic implications go beyond the political agreement in Article 25 GDPR, where "state of the art" should be assessed together with other elements such as the cost of implementation.

    Recommendation: The EDPB should clarify that its interpretation of "state of the art" does not imply the obligation for controllers to constantly update their systems to the latest DPbDD technology.

  - **Cost of implementation**: The draft guidelines state in page 8 that the "*the controller shall plan for and expend the costs necessary for the effective implementation of all the principles*" and that "*incapacity to bear the costs is no excuse for non-compliance with the GDPR*". The EDPB's interpretation of the cost of implementation goes beyond the aim and spirit of the GDPR. Nowhere in the GDPR, is stated or implied, as the EDPB suggests, that data controllers shall expend excessive resources to achieve a marginally higher level of DPbDD. It is more likely, that the legislators' intention was to propose a proportionality test including all the elements mentioned in Article 25 GDPR – *taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing* (…). Therefore, these elements should not be assessed in isolation, but as a whole.

    Recommendation: The EDPB should redraft the section on cost of implementation and propose a new chapter where all the aspects mentioned in Article 25 are analysed in the form of a proportionality test and follow a risk-based approach, and not in isolation as currently proposed in the draft guidelines. This approach would be in line with the spirit of the GDPR and in particular with the letter in Article 32 and recital 83[1]

[1] GDPR Recital 83: "*In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, **taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected**".*

- **Comments on chapter on implementing data protection principles in the processing of personal data using DPbDD**:

  - **Transparency**: the draft guidelines state in the example in page 14 that "*necessary information must be provided in the right context at the appropriate time*". And that "*generally a privacy policy on the website alone is not sufficient for the controller to meet the requirements of transparency*". The draft guidelines lack the reasoning that would justify such general statements, as it is indeed dependent on the context. Therefore, there is no reason to assume that the information, as presented in the example in page 14, is not provided in the right context and in the appropriate time.

    Recommendation: The EDPB should provide the explanations that are lacking in the above-mentioned statements to justify the conclusion reached in the example in page 14. In the absence of an explanation, the statement should be deleted.

  - **The balancing of interests in the section on lawfulness** (page 15): The draft guidelines state that where Article 6 (1) (f) – legitimate interest - is the legal basis used for the processing of data, the controller should disclose the assessment of the balancing of interests. The measure proposed by the EDPB goes beyond the requirements of the GDPR. Articles 13-15 GDPR clearly establish that, when processing data on the basis of legitimate interest, the controller shall simply disclose the information concerning the legitimate interests pursued. The draft guidelines also state that the controller must carry out an *objectively* weighted balancing of interest. The criteria of objectivity is not mentioned in Article 6 (1) (f) and so goes beyond the requirements of the GDPR.

    Recommendation: The final guidelines should be aligned with the GPDR with respect to the balancing of interests.

  - **Example on lawfulness** (pages 15-16): The draft guidelines state that when the controller uses Article 6 (1) (b) GDPR – performance of a contract – as the legal basis to process data, then all data must be collected directly from the data subject, and in the case where some data needs to be collected from a third party then the only appropriate legal basis to do so would be Article 6 (1) (a) GDPR – consent. The draft guidelines establish a principle which is not intended nor included in the GDPR, and that is to oblige controllers to always collect data directly from the data subject. This creates an uncertainty of the application of the legal bases included in the GDPR and risks diverging application.

    Recommendation: The example on pages 15-16 should be amended to be aligned with the principles established in the GDPR on the lawfulness of processing.

  - **Data subject's expectations in the section on fairness** (page 16): The draft guidelines state that "*processing should correspond to data subject's expectations*". In this regard, the final guidelines should clarify that data processing should correspond with the data subject's ***reasonable*** expectations, since unreasonable expectations should not be required to be fulfilled. In this regard, the Information Commissioner's Office (ICO) explains that fairness means that controllers "*should only handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them*"[2]. Moreover, the notion of reasonable expectations is stressed throughout the GDPR. For example, recitals 47 and 50 refer to "*reasonable expectations of data subjects based on their relationship with the controller*".

    Recommendation: The final guidelines should be aligned with the GDPR and clarify that data processing should correspond with the data subject's ***reasonable*** expectations.

[2] ICO website: Principle (a): Lawfulness, fairness and transparency.

- **Purpose limitation**: The draft guidelines state in page 18 that "*if any further processing is to take place, the controller must first make sure that this processing has purposes compatible with the original ones and design such processing accordingly*". In practice, it is common to have at the same time several legal grounds and legitimate purposes to process data. For example, customer data is collected to set up the customer relationship, to offer an insurance product and at the same time comply with anti-money laundering requirements. Additionally, other requirements in connection to legal obligations may appear afterwards. These additional requirements cannot be taken into account when designing the processing.

  Recommendation: The final guidelines should clarify that further processing of data should be allowed to comply with legal requirements.

- **Example 1 on accuracy** (pages 21-22): The example concerns the use of AI to profile customers applying for bank loans. In this example, the draft guidelines note that "*[the bank] will never rely solely on the AI to decide whether to grant loans*". This sentence should be edited to take into account the Guidelines on Automated individual decision-making and Profiling (page 23) which state that "*automated decision-making described in Article 22 (1) may also be necessary for pre-contractual processing*" and include an example where automated decision-making may be necessary in order to make a short list of possible candidates in the case where the business may find that it is not practically possible to identify fitting candidates, without first using fully automated means to sift out irrelevant applications.

  Recommendation: Example 1 on accuracy should be amended to be aligned with Article 22 GDPR and the Guidelines on Automated individual decision-making and Profiling.

- **Comments on the chapter on conclusions and recommendations:**

  - The draft guidelines recommend that controllers should be transparent to data subjects on how they assess and demonstrate effective DPbDD implementation (page 27). This recommendation goes beyond the requirements in the GDPR. It is also not apparent how this transparency should be complied with and it could even be a security issue to be too transparent.

    Recommendation: The recommendation on transparency of DPbDD implementation should be deleted.