16 January 2020

Comments by the Centre for Information Policy Leadership on the European Data Protection Board's
"Guidelines 4/2019 on Article 25 Data Protection by Design and By Default"

Adopted on 13 November 2019

On 13 November 2019, the European Data Protection Board (EDPB) adopted its Draft Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (Draft Guidelines or Guidelines).[1] The EDPB invited public comments on this document by 16 January 2020.

The Centre for Information Policy Leadership (CIPL)[2] welcomes the EDPB's initiative to further explore Data Protection by Design and by Default (DPbDD) under Article 25 of the GDPR and submits the comments below as input for the EDPB's final Guidelines (Final Guidelines).

1. General comments

CIPL highlights that DPbDD is modelled on the GDPR's overarching principles of organisational accountability and the risk-based approach. Organisational accountability and the risk-based approach should be further emphasised in the Final Guidelines as core drivers of efficient DPbDD to better assist controllers when implementing DPbDD in practice.

- **Organisational accountability**: Article 25(1) requires the controller to implement "appropriate technical and organisational measures" (TOMs) which are designed to implement the data protection principles of the GDPR for a given processing activity in an effective manner. In order to do so, on the basis of the risk posed by the processing, the controller must implement operational policies and procedures to turn data protection principles into actionable requirements that can be implemented at engineering level and integrate the "necessary safeguards into the processing." The controller must also train the relevant personnel accordingly and audit such policies and procedures' proper application. Bringing DPbDD to life is in fact just a subset – at the processing level - of implementing the overarching accountability principle of Article 24(1) of the GDPR.[3] Article 25(1) also requires DPbDD to apply "both at the time of the

[1] Draft Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, available at https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf.

[2] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 89 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[3] See CIPL white paper on "The Case for Accountability: How It Enables Effective Data Protection and Trust in the Digital Society", (23 July 2018), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf at pages 10 and 11.

determination of the means for processing and at the time of the processing itself" which requires applying DPbDD to the development and product lifecycle. This mandates continuous oversight and, if needed, an update of the measures to ensure they remain effective. This is similar to Article 24(1) of the GDPR, which also requires that the TOMs necessary to demonstrate that the processing is done in accordance with GDPR be "reviewed and updated where necessary". In practice, the controller has to put in place the necessary controls and procedures to ensure that DPbDD is an iterative rather than static process.

- **Risk-based approach**: Article 25(1) of the GDPR makes clear that the implementation of the DPbDD principle by the controller is not a "one-size-fits-all" exercise, but varies from one organisation to another and from one processing operation to another on the basis of (1) the state of the art, (2) the cost of implementation, (3) the nature, scope, context and purposes of the processing, and (4) the risks of varying likelihood and severity for rights and freedoms of individuals. The TOMs need to be calibrated to the risks of the processing, depending on the particular product, service or project. Consequently, depending on the risks and the factors listed in Article 25(1), organisations can better set priorities and allocate their resources more efficiently to enable more targeted mitigations of identified risks based on where there is the biggest risk to the organisation and to individuals.[4]

- **Accountability tools**: Article 25(3) of the GDPR provides that certifications may be used as an element to demonstrate compliance with the DPbDD (similar to how certifications may be used under Article 24(3) on accountability to demonstrate compliance with the obligations of the controller). As mentioned in the Guidelines, certifications have the benefit of enhancing trust in the digital world.[5] Certifications provide benefits not only to the controllers (or other organisation in the digital supply chain) when selecting technology providers but also to data subjects when choosing products and services. Unfortunately, 18 months after the GDPR went into effect, the regime surrounding GDPR certifications is still not in effect. While not specifically provided by article 25(3), the EDPB should also recognise that adoption of codes of conduct under article 40 could be used as a mechanism to demonstrate compliance with the requirements of article 25(1) and (2). As provided by article 40.1 and 40.2, codes of conduct are designed to specify the application of the GDPR by sector and in particular as regards the implementation of the data protection principles. CIPL underlines the importance of these accountability tools for organisations that look for pragmatic guidance when implementing DPbDD (and in particular SMEs) and for individuals when choosing products.

- **Research:** Because DPbDD requires a mix of technology and design skills, CIPL believes that a multi-stakeholder research approach involving regulators, industry, civil society and academia would be needed to ensure that DPbDD solutions are designed and implemented effectively. Some initiatives have already started to bring together stakeholders from different backgrounds in order to help identifying innovative solutions for privacy challenges through design.[6] CIPL

[4] *Id*. at page 8.

[5] The EDPB should also acknowledge the important role of international standards such as ISO or IEEE on Privacy Engineering.

[6] See the Control and Transparency Labs at https://www.ttclabs.net - This cross-industry effort was initiated by Facebook in March 2018 to create innovative design solutions that put people in control of their privacy. To date, 25 workshops have gathered stakeholders from multiple disciplines to explore challenges, analyse real

recommends that the EDPB acknowledge the need for multi stakeholder research in the DPbDD field.

2. Specific comments

- **Paragraph 14 - Addressing effectiveness of the data protection principles.** The Draft Guidelines provide that "it is [ ] not enough to implement generic measures solely to implement DPbDD compliance; each implemented measure must have an actual effect"**.** CIPL underlines that depending on the processing at stake, the measures implemented by the organisation may be generic and apply to all processing (i.e. a global information security policy or a GDPR data subject rights procedure) or may be specific to a processing operation (i.e. a specific encryption measure for a processing operation involving sensitive personal data). There may also be a mix of generic and specific measures. This determination should be made by the controller in the context of its processing activities. The adoption of specific and dedicated measures are not necessarily mandated as long as the controller is able to demonstrate the effective implementation of the data protection principles at the processing level. CIPL recommends that paragraph 14 of the Guidelines be amended to better reflect this and be aligned with paragraph 15 that provides that "Article 25 does not oblige controllers to implement any prescribed technical and organizational measures or safeguards, as long as the chosen measures and safeguards are in fact appropriate at implementing data protection into the processing."

- **Paragraph 15 – Addressing effectiveness of the data protection principles**: The Draft Guidelines provide that the TOMs or safeguards should be "be able to be scaled up in accordance with any increase in risk of non-compliance with the principles." Scalability implies deployment of more of the same, or more granular or similar TOMs. CIPL underlines that a TOM may not be always scalable. In some instances, an organizational measure may need to be changed to a technical measure where there is increased risk of noncompliance with the principles. For instance, a server Central Processing Unit (CPU) technical design flaw cannot be fixed by "scaling up" but by implementing a technical software solution to mitigate security risks. Scaling a social media organization up with personnel to monitor inappropriate content in local languages may not be sufficient. In many cases, relying instead or additionally on technical solutions will be more practicable and effective to reach the desired objectives. In addition, scalability may not necessarily provide secure processing because safeguards that were "state of the art" at the time of risk assessment, may no longer be appropriate due to technological threat evolution. The scalability statement risks becoming a default term of data protection contracts, such as, "any and all TOMs must be able to be scaled up" which may be too rigid and not help achieve the purpose of effective implementation of the data protection principles. CIPL therefore recommends to replace the wording "be able to be scaled up" by "scalable when practical and appropriate and continue to properly implement data protection principles in an effective manner."

- **Paragraph 16 – Creation of Key Performance Indicators (KPIs) to demonstrate effectiveness**: The EDPB provides that controllers may determine appropriate KPIs for DPbDD (and that technology providers demonstrate the effectiveness of their measures to controllers through KPIs). In the IT

user behaviors, build common solutions and design user interface in areas such as Age Appropriate Design, Algorithmic Transparency or Designing for People with Low Digital Literacy.

industry, KPIs are additional commercial contract terms to address measurements that are not addressed in the contract and service level agreements or specifically stated as TOMs. With the EDPB statement, KPIs risk becoming contractual requirements that do not necessarily map to the time and resource necessary to implement the principles into the processing. Furthermore, KPIs may result in increased liabilities for processors where they fail to meet the desired result even where they have not negatively impacted the effective implementation of the data protection principles (for instance, failing to achieve a KPI on the reduction of response time to data subject requests does not mean data subject rights are not properly addressed within the one-month time limit). The demonstration of whether controllers (and as the case may be processors) have implemented the necessary measures and safeguards to achieve the desired DPbDD effects are determined by the specified TOMs and their on-going monitoring, review and assessment and not by the KPIs. CIPL therefore recommends that the EDPB replace the term KPIs with "risk-based approach" in the Final Guidelines.

- **Paragraph 25 – Cost of implementation:** The Draft Guidelines provide that the controller "must manage the costs to be able to effectively implement all of the principles" and that "effective implementation of principles must not necessarily lead to higher costs." CIPL underlines that controllers cannot necessarily directly manage or control the cost for the desired effective implementation of the principles of processing, in particular when selecting processors' standardized IT products, services and solutions (e.g. Cloud). The controller selects them according to market price set by processors. While controllers may be able to negotiate the overall price of the IT products, services and solutions, they cannot manage the costs related to the effective implementation of the principles directly. CIPL recommends to amend the Guidelines accordingly to replace "must manage" by "shall endeavor to manage directly or indirectly the costs" and "must not" by "may not."

- **Paragraphs 60 and 61 – Transparency**: CIPL welcomes the Guidelines' acknowledgement that multi-layered and contextual information are key design and default elements. With regards more specifically to the contextual requirement, the Guidelines provide that "[i]nformation shall be provided at the relevant time." CIPL underlines that the on-boarding experience of the user may not be the most relevant timing to provide information to the individual. Information may be more relevant and better-understood if provided to the individual at a later stage. Therefore, CIPL recommends that the EDPB clarify that the obligation of the controller to be "clear and open from the start" in the first sentence of paragraph 60 does not necessarily require that information be provided at the on-boarding stage if it can be provided in a more relevant manner at a later stage. The Guidelines also state that information must be provided "in the appropriate form." CIPL underlines that this requires a prior assessment of who will be using the service to take into account different users, ages, cultures and languages. For global products or services, this may be challenging to anticipate at the product definition level and may be better defined at a later stage depending on the specific context. CIPL recommends that the Final Guidelines clearly indicate that key design and default elements of transparency have to be assessed on a case-by-case basis depending on the context.

- **Example in paragraph 61 – Transparency**: The example provides details on what transparency means for a privacy notice. As such, it seems to overlap with the Article 29 Working Party Guidelines on transparency under Regulation 2016/679. To ensure coherence of information and ease of use by organisations, CIPL recommends that the Guidelines only refer to these pre-existing

guidelines. In addition, this example provides that the data subject is always only one click away from the information. CIPL underlines that it may be challenging to apply the requirement to have the privacy policy just a click away in smart devices or IoT devices contexts, which have more limited user interfaces and pose novel design challenges. Oftentimes, menus, including privacy policies, are accessible in the upper-left or upper-right corner of the screen. While this process is simple and intuitively understood by data subjects, it can often involve more than one click. The EDPB should make clearer that this specific example may not be applicable and relevant in all situations and that what is appropriate from a product design perspective must be assessed on a case-by-case basis.

- **Paragraph 65 – Fairness Key Design and Default Elements – Consumer Choice:** The Guidelines provide that the controller should not "lock in" their users by using features such as personalization of the goods and services preventing individuals from changing controllers, which may not be fair. CIPL believes that this statement does not accurately reflect the reality of the online market where personalization is intrinsically part of the services and a key feature expected by customers to navigate different offers and make their choice freely. Personalized content generally improves the quality of service while also fostering competition and innovation. CIPL recommends that the EDPB remove the statement that personalisation of goods and services creates lock-in situations.

- **Paragraph 65 - Fairness Key Design and Default Elements – Human Intervention**: The Guidelines provide that the controller must incorporate *qualified* human intervention to uncover biases that machines may create in relation to the right not to be subject to automated decision-making (ADM). CIPL wishes to underline that as per article 22.3 this would be applicable only where ADM that produces a legal or similarly significant effect is necessary for entering into or performing a contract, or is based on explicit consent. Also, in practice, compliance with the fairness principle of the GDPR in the ADM context can take other forms than "*qualified* human intervention." Organisations have been developing tools – such as fairness or algorithmic assessment tools – and processes to specifically address this point. Therefore, CIPL recommends that the Guidelines indicate that "*qualified* human intervention to uncover biases" is just one requirement as part of article 22.3, but that but that other means are acceptable to implement fairness as part of the DPbDD principle.

- **Paragraph 65 – Fairness Key Design and Default Elements – Fair Algorithm:** The Draft Guidelines provide that information "shall be provided to data subjects about the processing of personal data based on algorithms that analyse or make predictions about them, such as work performance, economic situation, health, personal preferences, reliability or behaviour, location or movements." CIPL believes that the statement "Information shall be provided" is quite vague, and does not help a product designer, data scientist or engineer determine what level of information is required to share with individuals. CIPL would therefore welcome confirmation from the EDPB that "information" in this paragraph shall be understood as information to be provided under article 13 of the GDPR.

- **Paragraph 65 - Fairness Key Design and Default Elements – Example 1:** The example considers that to implement the fairness principle in an online processing environment, the controller must implement the least invasive default options and the choice for further processing must be presented in a manner that does not deter the data subject from abstaining from sharing their

data. CIPL agrees that controllers should not make it difficult for individuals to decline sharing personal data or to adjust their privacy settings. With regards to the notion of "deterrence" used in this example, CIPL would suggest, however, that the key criterion should be rather that of accurately representing the ramifications of each choice to the data subject. The current example relies on what can be considered as positive or negative aspects of sharing or declining to share personal data, which may be very subjective. CIPL suggests instead that the Final Guidelines stress the importance to present these choices clearly together with a description of the impact of each choice (whether it is positive or negative).

- **Paragraphs 83 and 84 – Enforcement**: CIPL recommends that the Guidelines expressly provide that, depending on the facts of the case, the effective implementation of DPbDD may be considered as a mitigating factor as part of the application of Article 83 of the GDPR, especially in cases where implementation of DPbDD has led to mitigating the effect, scope, extent or duration of the damage.

- **Paragraph 86 – Technology providers:** The EDPB provides that technology providers should seek to support controllers in complying with DPbDD. Controllers, on the other hand, should not choose providers which do not propose systems enabling the controller to comply with Article 25, because controllers will be held accountable for the lack of implementation thereof. The EDPB further indicates that technology providers should play an active role in ensuring that the criteria for the "state of the art" is met, and notify controllers of any changes to the "state of the art" that may affect the effectiveness of the measures in place. Controllers should include this requirement as a contractual clause to make sure they are kept up to date. Technology providers should also consider cost efficiency during the development of a product or solution while controllers should demand that their technology providers be transparent and demonstrate the costs of developing the solution. CIPL believes that several of these statements go beyond GDPR and could be far reaching:

    - The notion of "technology provider" is very broad and may not fall under the remit of data protection law in all situations, especially where such technology provider only provides a product or service but does not in this context receive, process, store or access any of the personal data held by the controller. In such cases, the technology provider would not fall under the qualification of either a "controller" or "processor" under the GDPR and would therefore not be subject to any of its obligations. It would, therefore, be very challenging for controllers to impose any data protection related contractual obligation on a technology provider that is not subject to the GDPR. This may complicate contractual negotiations between controllers and technology providers rather than simplify discussions. In addition, where such a technology provider is also a processor under the GDPR, Article 28 already provides for a strict contractual framework with high sanctions in cases of non-compliance for both parties. CIPL recommends, therefore, that the EDPB amend the Guidelines to replace the notion of "technology provider" with "controller" or "processor" and refer to Article 28 of the GDPR when relevant.

    - CIPL recognises that although not specifically mentioned under Article 25 of the GDPR, processors have to be compliant with DPbDD as Article 28(1) of the GDPR requires controllers to "use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will

meet the requirements of this Regulation". Therefore, it is in the processors' interest to implement DPbDD to strengthen their reputation in the ecosystem and make them a trusted business partner. It also provides them with a competitive edge vis-à-vis other processors and minimises risks of contractual non-compliance and liabilities.

- On the obligation for technology providers to support controllers in complying with DPbDD and the EDPB's statement in paragraph 85 that technology providers and processors "are in a position to identify the potential risks that the use of a system or service may entail", CIPL underlines that the technology provider may not have access to all the information on the intended use of the product or service by the controller. Therefore, this obligation to support the controller must be limited to the information that is available to the technology provider (see Article 28(3)(f) on the obligation of the processor to assist the controller in ensuing compliance with Articles 32 to 36 "taking into account the nature of the processing and the information available to the processor").

- The obligation for technology providers to notify controllers of any changes to the "state of the art" that may affect the effectiveness of the measures in place and to include a contractual requirement to notify controllers of any changes to the state of the art appears to be far reaching in a B-to-B context between professionals. CIPL also believes that this goes beyond the wording of the GDPR that already regulates the contractual relationship of the controller and the processor. Beyond the provisions of Article 28, the parties should remain free to negotiate relevant contractual terms. Subject to applicable law, technology providers should remain free to decide on how to communicate on the update or their products (while also possibly agreeing contractually to inform some of their clients depending on the specific context).

- The requirement for the technology provider to disclose the cost of developing the DPbDD solution is too far-reaching as price structure is often confidential strategic information and any organisation will be very reluctant to disclose it (even in a contractual context with strong confidentiality obligations). Any disclosure of information related to price can also be extremely sensitive and may lead to competition issues especially in the context of tenders.

- Putting the burden on controllers and processors during the contractual negotiation phase (by mandating controllers to negotiate potentially challenging contractual provisions with their processors such as notifying them of any changes to the "state of the art" or demanding transparency on the cost of DPbDD) may not be the most efficient way to increase trust and accelerate DPbDD approaches. In addition, the Guidelines seem to overlook the new liability regime of the GDPR for processors, which now recognises that all parties involved in the processing of an individual's personal data in the ecosystem have some level of responsibility and accountability to ensure those rights and freedoms are protected. As a result, processors have their own direct obligations to individuals and regulators and will be concerned about managing this direct statutory liability risk in addition to any liability that the controller may try to impose contractually.[7] CIPL believes that having certified products and services from a DPbDD perspective that could easily

[7] *Supra* note 3 at page 16.

drive controller and processor choices would be much more efficient and less time consuming (see general comments in Section 1).

Summary of CIPL Recommendations

- Make a clear link between DPbDD and organizational accountability and the risk-based approach as cornerstones of efficient GDPR implementation.
- Facilitate the development of DPbDD certifications to guide organizations and increase trust.
- Recognize the importance of Codes of Conduct in specifying DPbDD by sector.
- Acknowledge the need for multi stakeholder research in the DPbDD field.
- Adopt a more flexible interpretation of "scalability" in the DPbDD context to only apply "when practical" and to cover the "on-going proper implementation of the data protection principles in an effective manner."
- Replace the notion of key performance indicators with "risk-based approach."
- Clarify that the transparency key design and default elements and examples must be assessed on a case-by-case basis based on each processing context.
- Acknowledge that controllers cannot always "manage" the cost of implementation of the data protection principles.
- Remove the statement that personalisation of goods and services creates lock-in situations.
- Indicate that "*qualified* human intervention to uncover biases" is just one requirement as part of article 22.3, but that but that other means are acceptable to implement fairness as part of the DPbDD principle.
- Confirm that "information" to be provided to data subjects about processing of personal data based on algorithms that analyse or make predictions shall be understood as information covered by article 13 of the GDPR.
- Recognize that implementation of the fairness principle should include presenting choices to individuals as well as information about the impacts and consequences of their choices.
- Expressly provide that, depending on the facts of the case, the effective implementation of DPbDD may be considered as a mitigating factor in enforcement cases.
- Replace the notion of "technology provider" with that of "controller" or "processor".

- Provide that the obligation for the processor to support the controller must be limited to the information that is available to the processor.

- Remove the obligation for technology providers to notify controllers of any changes to the "state of the art."

- Remove the requirement to include in contractual terms the obligation for the processor to disclose the cost of developing the DPbDD solution.

CIPL is grateful for the opportunity to provide recommendations in the context of the European Data Protection Board's Draft Guidelines on Data Protection by Design and by Default. If you would like to discuss any of these recommendations or require additional information, please contact Bojana Bellamy, bbellamy@huntonAK.com, Markus Heyder, mheyder@huntonAK.com, Nathalie Laneret, nlaneret@huntonAK.com, Sam Grogan, sgrogan@huntonAK.com, Matthew Starr, mstarr@huntonAK.com or Giovanna Carloni, gcarloni@huntonAK.com.