\Orchestrating a brighter world NEC	**NEC Group Comments. Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. EDPB**

Page 4: **Executive Summary**

Data protection by design must be implemented both at the time of determining the means of processing and at the time of processing itself. It is at the time of determining the means of processing that controllers shall implement measures and safeguards designed to effectively implement the data protection principles. To ensure effective data protection at the time of processing, the controller must regularly review the effectiveness of the chosen measures and safeguards. The EDPB encourages early consideration of DPbDD when planning a new processing operation.

Comment: Does new processing operation refers to the practice of considering privacy requirements from the first stages of product and service design into data protection regulations?

Page 5: **Scope**

1. The Guidelines focus on controllers' implementation of Data Protection by Design and Default (hereinafter "DPbDD") based on the obligation in Article 25 of the GDPR. Other actors, such as processors and technology providers, who are not directly addressed in Article 25, may also find these Guidelines useful in creating GDPR-compliant products and services that enable controllers to fulfil their data protection obligations. Recital 78 of the GDPR points out that DPbDD should be taken into consideration in the context of public tenders. Despite all controllers having the duty to integrate DPbDD into their processing activities, this provision fosters the adoption of the principles, where public administrations should lead by example.

2. The requirement is for controllers to have data protection designed into and as a default setting in the processing of personal data. The core of the provision is to ensure effective data protection both by design and by default, which means that controllers must be able to demonstrate that they have in place the appropriate measures and safeguards in the processing to ensure that the data protection principles and the rights and freedoms of data subjects are effective.

Comment: Although it is the data controller who is responsible for fulfilling this obligation in light of Recital 78 and the Article 28 of the GDPR data protection by design also involves other participants in the processing of personal data, such as service providers, product and application developers or device manufacturers. The data controller must encourage them to "take into account the right to data protection when developing and designing such products, services and applications" in such a manner, that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subjects.

Does it mean that companies acting as Data Processors need to follow up the guidelines and not only as a recommendation coming from the EDPB?

Page 5: **Analysis of article 25**

6. DPbDD is a requirement for all controllers, independent of their size, including small local associations and multinational companies alike. The EDPB brings to the reader's attention

that the complexity of implementing DPbDD will vary based on the individual processing operation.

Comment: Although it is the data controller who is responsible for fulfilling this obligation in light of Recital 78 and the Article 28 of the GDPR, data protection by design also involves other participants in the processing of personal data, such as service providers, product and application developers or device manufacturers. The data controller must encourage them to "take into account the right to data protection when developing and designing such products, services and applications" and when they must engage another processor for data processing, they must 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 and ensure the protection of the rights of the data subject."

In brief, it is the data controller who, as part of their duties, must limit their selection of products and processors to those that can ensure the fulfilment of the GDPR requirements and is especially obliged by law to guarantee data protection by design and by default.

Does it mean that companies acting as Data Processors need to follow up the guidelines and not only as a recommendation coming from the EDPB? How can data processors comply with article 28 requirements if DPbDD are not part of data processors' obligations?

What about other actors such as joint controllers? Based on their respective responsibilities how can they determine and fulfil with this obligation?

Page 7: **Designed to implement the data protection principles in an effective manner and protecting data subjects' rights and freedoms**

Addressing effectiveness

16. Controllers must be able to demonstrate that they have implemented measures and safeguards to achieve the desired effect in terms of data protection. To do so, the controller may determine appropriate key performance indicators to demonstrate compliance. Key performance indicators may include metrics to demonstrate the effectiveness of the measures in question. Metrics may be quantitative, such as level of risk, reduction of complaints, reduction of response time when data subjects exercise their rights; or qualitative, such as evaluations of performance, use of grading scales, or expert assessments. Alternatively, controllers may provide the rationale behind their assessment of the effectiveness of the chosen measures and safeguards.

Comment:
We consider it necessary to establish a common criteria for key performance indicators to companies to assess their degree of compliance

State of art

18. The concept of "state of the art" is present in various EU acquis, e.g. environmental protection and product safety. In the GDPR, reference to the "state of the art" is made not only in Article 32, for security measures, but also in Article 25, thus extending this benchmark to all technical and organisational measures embedded in the processing.

Comment: state of art is a very subjective and ever changing term so any guidance needs to reflect this.