Guidelines 4/2019 on Article 25 Data Protection by Design and by Default – Response to Consultation

1. Overarching issues

1.1 Interpretation of Art.25(1)

1. In section 2.1.1 of the Guidelines headed “Controller’s obligation to implement appropriate technical and organisational measures and necessary safeguards into the processing”, para.7 states:
“The controller shall (1) implement appropriate technical and organisational measures which are designed to implement the data protection principles and (2) integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects.”

2. The English version of Art. 25(1), at least, could equally (or arguably better) be interpreted as:
“The controller shall ~~(1)~~ implement appropriate technical and organisational measures which are designed to: (1) implement the data protection principles effectively and (2) integrate the necessary safeguards into the processing, in order to meet the requirements of the GDPR and protect the rights of data subjects.”

3. In other words, it seems from the English version that the focus of Art.25(1) is on **designing technical and organisational measures** in such a way that they are **appropriate** to both **implement the principles effectively** and **integrate the necessary safeguards,** in each case in order to both meet the **GDPR’s requirements** (e.g. Art.32, not just the principles), and **protect data subject rights**. Perhaps the other language versions could shed more light on the intended meaning, but in my view the English language version reads better, from a sense perspective, as focusing on **appropriate measures** to implement the principles and integrate safeguards for compliance and rights protection, just as Art.32 focuses on the implementation of appropriate measures for security.

4. On that basis, measures are not separate from safeguards, but instead measures must include safeguards as well as implement principles.

5. Accordingly, I’d disagree with para.10 that “safeguards act as a second tier”. It seems to me that there’s no issue of first tier or second tier – for compliance and data subject rights protection, controllers must implement appropriate measures designed both to implement the principles effectively and to integrate safeguards. On this basis also, if my suggested interpretation is accepted, the second sentence of para.10 should be amended; in para. 11 “or safeguard” changed to “to integrate a necessary safeguard”; in para.16 “and safeguards” deleted; para.14 change “dedicated measures” to “appropriate measures designed” and “integrated” to “implemented measures designed to integrate” (or explain why measures have to be “dedicated”?); para.52 last sentence change “systematic” to “appropriate” or at least add “appropriate” after “systematic”.

1.2 Effectiveness vs. “designed for effectiveness”

6. Just as it is impossible to guarantee 100% security in practice, whatever technical and/or organisational measures are taken, equally it is impossible to guarantee 100% effective data protection in practice – that seems to be why Art.25 refers to “designed”, and “appropriate”, and is more in keeping with the risk-based approach previously endorsed by the Working Party.

7. Many paragraphs of the Guidelines are however phrased in quite absolute terms, regarding effectiveness rather than “designed” and “appropriate”. Such an approach implies that if a measure has in fact turned out to be ineffective, that would automatically treated be as an infringement of Art.25 (even though it was designed to be an appropriate measure in the circumstances, in light of the state of the art etc.). If that is the intended approach; if, no matter what measures controllers take, any and every data protection failure is always treated as an infringement of Art.25; then this might disincentivise some controllers from implementing genuinely appropriate measures properly designed to implement the principles and integrate safeguards.

8. If the interpretation focusing on “design” and “appropriateness” rather than 100% effectiveness is accepted, in para.8 “fit” should be “designed”; para. 14 add “Designing for” at the start; para.15 change “able” to “designed to be able”; para.78 change “shall both” to “shall require appropriate measures designed to both”; para.86 change “the effective implementation of the principles and the rights of data subjects into the processing” to “the implementation of measures that are appropriate to implement the principles effectively and integrate the necessary safeguards, in order to meet the requirements of the GDPR and protect the rights of data subjects”.

1.3 Interpretation of Art.5 principles

9. It is helpful to provide specific examples of how to design for implementation of principles, from para.61 onwards. However, many of the bullet points are preceded by “Key design and default elements may include”, whereas the bullet points use language like “shall” and “should”. Please clarify those bullet points are only examples of possible elements (which “may” suggests), and not mandatory.

10. If the bullet points are intended to be mandatory, then it would be more helpful and transparent on the part of the EDPB if it first issued separate consultations specifically on the relevant principles (where it has not already done so – I acknowledge it has e.g. for transparency), so that all have the opportunity to comment on any proposed mandatory elements, and finalise those guidelines before finalising the DPbDD guidelines. For example, in para.61, by “accessible to all”, is the EDPB saying that all website privacy notices must be accessible to the disabled/less able (e.g. to the blind)?

2. Detailed comments

11. Para.10 – “providing automatic and repeated information about what personal data is being stored” may lead to data subject “information fatigue”, so perhaps another example of a “necessary” safeguard may be better?

12. Para.11 – footnote 4 – thanks for clarifying that encryption is an example of pseudonymisation. I appreciate WP216 section 4 (which pre-dates the GDPR) classes hashing as an example of pseudonymisation, but does the EDPB definitely consider that it’s still pseudonymisation as defined in Art.4(5) “…without the use of additional information, provided that such additional information is kept separately…”? That phrase on additional information does not seem very apt to apply to hashing?

13. Para.12 – thank you for the useful clarification here. Should “rights” and “freedoms” be interpreted similarly in all the other provisions of the GDPR too?

14. Para.14 – please clarify/amend: “It is therefore not enough to implement generic measures solely to document DPbDD-compliance; each implemented measure must have an actual effect” - as measures to “document” compliance are of course clearly insufficient to meet Art.25’s requirements as those oblige implementation, not “documentation”, and also please explain why “generic” measures are not good enough if they are “appropriate” in a particular situation? What exactly is meant by “generic” here please?

15. Para.18 – is the EDPB specifically endorsing the document mentioned in fn.7 in relation to the meaning of “state of the art” throughout the GDPR, please clarify? (It just says “an example”,)

16. Para.24 – “Incapacity to bear the costs is no excuse for non-compliance with the GDPR” – what about SMEs? If one measure is “appropriate” and cheaper than another measure which may be “better” but is more expensive, shouldn’t controllers be permitted to use the cheaper measure as long as it is “appropriate”?

17. Para.27 – please give one or two examples of what are considered to be “inherent characteristics” of processing?

18. Para.30 – please specify which sections/paragraphs of WP248rev01 provide guidance on risk assessment? It provides guidance on when processing is “high risk”, but other than p.22 which calls out risks of illegitimate access, undesired modification, and disappearance of data, it’s not entirely clear to me where that document provides guidance on how to assess data protection risks and how to carry out a data protection impact assessment?

19. Para.34 – it may be helpful to add specifically here that "time of determination" includes the time of procuring software, hardware, systems and services as well as the time of implementing procured software, hardware and systems and integrating/connecting any existing software, hardware and/or systems with service providers' services.

20. Para.40 – this could also mention systems and services. Also, the hyperlinks in this para. ("software application" etc) have not been highlighted in blue and it would be helpful if they, and any other unhighlighted links, were in blue.

21. Para.41 – should "enabled" be "processed" here, for clarity? Also, last sentence – or alternatively, don't use such software at all!

22. Para.42 – please explain why values should be "universal to all instances"? In some cases wouldn't one set of values for one set of instances and another set of values for another set of instances be permissible?

23. Para.43 – this could mention that allocating access must include not only to whom access is allocated for which sets of personal data, but also what type of access and its extent (e.g. edit rights, or view-only).

24. Para.44 – is this the EDPB's interpretation of "appropriate" in Art.25 i.e. "suitable, adequate, relevant and limited to achieve the intended purpose"? If so, this could be moved to much earlier (and explain that "intended purpose" means "intended purpose of processing" as presumably that's what's meant)? Also, please clarify if this is the EDPB's interpretation of "appropriate" elsewhere in the GDPR too e.g. Art.32? For security purposes (and indeed data protection), "limited" may not always be best as security measures that exceed what's needed for the intended purpose should surely not be discouraged.

25. Para.46 fn.10 – for accuracy and completeness, update the title of that document, and also add an additional reference to the https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf document.

26. Para.50 – minor but for clarity change "less" to "smaller amounts" (as "less" might otherwise refer to the detail, not the amount). After "collected", add "or retained"? And it might be helpful here to cross-refer to para.71 example 1 as an excellent example of this.

27. Para.52 – second sentence please expand on or delete "in an accountable way", as the sentence already refers to "objectively justifiable and demonstrable" so what does "in an accountable way" mean if not that? Third sentence please expand on "relevant contextual elements"? (or specifically refer to WP216 for that). N.14 could repeat the link that's in n.14 for ease of access. Please clarify "For both deletion and anonymization process, the controller shall limit the retention period to what is strictly necessary" – because deletion/anonymisation are ways of limiting the retention period. Perhaps it should be rephrased as "The controller shall limit the retention period to what is strictly necessary and then delete or anonymize"? Last sentence add "or anonymization" before "embedded".

28. Para.55 – "Either way, the extent of the public accessibility of the personal data should be made transparent to the data subject at the time of "intervention", which is the moment for the data subject's intervention." – please explain or amend to clarify. Surely the extent of public accessibility should be made transparent to data subjects before making the data publicly accessible, rather than at the time of data subject intervention? If data subjects are not informed before the data is made public, and then after that they intervene, it's too late for them – the data is already public and could have been obtained by others easily. Data subjects should be given the opportunity to intervene before their personal data is made publicly accessible.

29. Para.56 – the issue is far more important and broader than just being one of robots.txt. Please expand to cite examples of personal data being available on the Internet without any authentication e.g. in France the CNIL's SERGIC and Active Assurances fines. Personal data should not be left open to the Internet without appropriate authentication or encryption, regardless of whether the controller includes an appropriate robots.txt file or not. Similarly, if a controller decides to publish personal data on a website, it must carefully consider how much data to publish and whether/which types of personal data to redact first (i.e. don't publish that data at all!) from the perspectives of legal basis, data minimisation etc, rather than simply publishing everything online, again regardless of whether or not it uses robots.txt - e.g. the DZPN fine in Poland. Please expand on what's meant by "it is also vital that the controllers

responsible for the search engines respect these protocols, although they aren’t binding” – why, on what basis, etc?

30. Para.57 – for clarity “a separate” should be “their own”. Their own legal basis could be the same one as the website publisher’s, e.g. legitimate interests.

31. Para.58 – for completeness, before “tenders” add “procurement of software, hardware, systems and/or services”, as not all procurement will involve tenders but procurement must still be with an eye to Art.25.

32. Para.61 – “machine readable languages” is not clear, please clarify/expand - presumably this should be “machine readable formats” not languages, as data subjects may prefer text to JSON! Also in what way would use of machine readable formats facilitate and automate readability and clarity for data subjects? It might facilitate automated analysis and comparsion of privacy notices, but not readability for data subjects? In addition, pleae change “beyond the textual” to “as well as the textual” as different data subjects have different preferences as to how they want to get information – if a website provides privacy information only in video but not textual form, that can nudge people like me not to view it, as personally I much prefer to scan quickly through paragraphs of text than to use up time having to play a sequential video all the way through!

33. Para.61 example - please see previous para. re. the reference to “video clips” – as long as it’s in addition to text, not instead of text, that would be fine. Shouldn’t “internal web-pages” be “public-facing web-pages” i.e. not intranet but website? “For example, when asking the data subject to enter personal data the controller informs the data subject of how the personal data will be processed and why that personal data is necessary for the processing” – surely this shouldn’t be necessary where the purpose is obvoius, e.g. address details needed to deliver physical goods, payment details to take payment for an order?

34. Para.63 – “Differentiation” – please explain what’s meant by “The controller shall differentiate…” – fn.19 refers to 2/2019, but that document doesn’t use the term “differentiate”? Differentiate when, how, to whom etc? Consent withdrawal – should add, “Where consent is the legal basis” (as with the next bullet point on balancing); and “processing” should be “controller” as withdrawal may involve a different processing operation than the initial collection. On “the controller should disclose their assessment of the balancing of interests” – why is this needed for lawfulness, which is the topic of this example, rather than for transparency; and indeed for transparency WP260 rev.01 itself states “As a matter of best practice, the controller can also provide the data subject with the information from the balancing test…” and does not require this disclosure, cf. “should” in this bullet point. “Cessation” – at the end of the sentence, for accuracy, add “unless it is for a compatible purpose”. Default configurations – this bullet point is unclear, what does legal basis have to do with configurations exactly and how, please expand? Allocation of responsibility – this is already required by Art.26, in what way is it a design or default element for Art.25 purposes, shouldn’t this bullet point be deleted to avoid confusion?

35. Para.63 example – “Initially, this personal data is necessary in order to take steps at the request of the data subject prior to entering into a contract” – but why should tax data be considered necessary to take such steps prior to a loan management service, I’d have thought it was not necessary for that purpose? Generally there could be better examples as not many systems currently exist (or are trusted by users, even if access if temporary!) that would allow one controller to access electronically only limited set of personal data from another controller. Maybe try an open banking example? On “specific set of information” – add that this set that can be collected directly must be under the control and choice of the data subject, including as to type and extent/scope (e.g. time period) of their data, and not either controller!

36. Para.65 – Expectation – presumably should be “reasonable” expectations. Non-discrimination – this formulation is very broad, e.g. if a bank doesn’t want to lend large amounts to low-income people is that “discrimination”? Truthful – what does “provide account for what they do” mean here, to whom, how etc., is this meant to refer to the general accountability principle or something else, if the latter please expand/explain what exactly? Human intervention – what does “qualified” mean here, “expert”, or is it about authority to change machine decisions? Fair algorithms – this refers to analysis/predictions but Rec.71 (cited in the footnote, 22) is on automated decision-making, which is different?

37. Para.65 Example 1 – why should this example be limited to search engines processing user-generated data, why not other types of controller?

38. Para.67 – Specificity - "The purposes must be specific to the processing and make it explicitly clear why personal data is being processed" – this wording is different from Art.5(1)(b) "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes", i.e. "processing must be for specified purposes" is not the same thing as "purposes must be specific to the processing". It would be better to use the wording of Art.5 here. Limit further processing – how is "should not connect datasets" related to purpose limitation? If datasets are being processed for the same purposes, why should they not be connected? Technical limitations of reuse – too restrictive just to mention technical limitations, just crypto (as opposed to access controls), and just technical limitations as opposed to e.g. contractual limitations on reuse, internal policies/procedures etc.

39. Para.67 example – "the controller assesses whether the new marketing purpose and the targeted advertisement purpose are within the contractual purposes" – should that not be "original or compatible", rather than "contractual"?

40. Para.69 – please clarify/expand on what is meant by "They should verify whether technology, processes or procedures exist that could make the need to process personal data obsolete". Surely it's not just an issue of tech, processes or procedures, but more broadly can the relevant purpose be achieved without having to process personal data, irrespective of technology etc?

41. Para.71 – Necessity - please give examples of "personal data element". Data flow – why should "entry points for data collection" be minimised, shouldn't data subjects be allowed to choose between different multi-channel ways of providing personal data? State of the art – instead of "available and suitable", cross-refer to previous discussion on state of the art (and move "available and suitable" to the previous discussion)?

42. Para.71 example 1 – this is an excellent example, and should ideally be expanded as too many websites currently also require age if not date of birth, often gender, sometimes mother's maiden name (!). And date of birth etc. can be used for identity theft, fraud etc.

43. Para.71 example 3 – why must keys be frequently rotated, isn't the main point that they should be stored and managed securely?

44. Para.74 – Measurably accurate – please explain/expand on the reference to false positives/negatives, how is this relevant to many situations, is this bullet point about automated decision-making, if so add "where they influence automated decision-making". Verification - please give examples of the nature of the data e.g. special category? Accumulated errors – as with any errors this must be qualifed for accuracy having regard to the purposes, and "must" mitigate may not have to apply in situations where the data may be accurate enough for the purposes whatever the supply chain length or their errors. Access – please explain why data subjects "should be given an overview", does this add anything to the requirements of Arts.12-15; also "easy access" is fine but the access must also be secure and not just obtainable e.g. by citing name and date of birth (1&1 fine, Germany) – access must not be too "easy"! Continued accuracy – again accuracy must be with regard to the purposes (Art.5), 100% accuracy always may not be essential in all processing situations. Data design – what does "legal criteria" mean here please, can this be explained/expanded?

45. Para.74 example 1 – shouldn't "legal access" be "a legal basis"? (If it's public they will have access.)

46. Para.74 example 2 – presumably "employee" should be "client".

47. Para.77 - Effectiveness of anonymization/deletion – "make sure" and "not possible" are very absolute, this should cross refer to the helpful and more detailed WP216 instead. Data flow – why should the use of temporary storage be limited, as long as any temporary storage is promptly and securely deleted/anonymised?

48. Para.77 example – delete "and correct" as the example is about storage limitation, not accuracy.

49. Para.78 – why are confidentiality, integrity and availability said to "strengthen data processing resilience"? Resilience is separate, and e.g. separately mentioned in Art.32(1)(b). Also, please expand on "in a seamless manner", what is meant by "seamless" here – easily? Quickly? Etc.

50. Para.80 – Access management – also mention extent of privileges etc., not just who can have access, and shouldn't "authorized personnel" be "personnel who need to have access to certain personal data"? Backups/logs – not only should there be audit trails, and event monitoring, but

logs etc. should actually be reviewed regularly and alerts/unusual matters acted upon promptly as necessary and appropriate. Maintenance and development – “software” is narrow, should be expanded to include “hardware, systems, services” etc.

51. Para.80 example – aren’t the measures mentioned (network segregation, access controls) also important for the medical database, not just the server containing extracts? Or in the example is the medical database supposed to be controlled by a third party? “This security measure will ensure that all users have access on a need to know basis and with the appropriate access level” should be “The controller will ensure that users have access only on a need to know…” as the sentence immediately follows one about reporting, which is not logical – reporting/alerts do not control access, it’s how access is allocated that achieves this. “Handling the incident” and “prevent future such data breach incidents” both seem to be out of place in an example about upfront measures? Missing “it” before “undertakes”.

52. Para.86 – “Such a certification may provide an added value to a controller when choosing between different processing systems from technology providers” – Art.42 only provides for certification of processing operations of controllers/processors e.g. Art.42(1), Art.42(6), (7). Is the EDPB stating its view that technology providers’ applications, software, systems can be certified under Art.42? Or is it the case that “good” (e.g. secure) software/hardware/systems will assist controllers to get their processing operations certified? (as per the sentence “Controllers, on the other hand, should not choose providers who do not propose systems enabling the controller to comply with Article 25…”). Also in the sentence quoted, “systems” should be expanded to “software, hardware, services or systems”. “Controllers should include this requirement as a contractual clause to make sure they are kept up to date” seems very absolute – if a service provider is contractually required to keep systems etc up to date and secure, why should it also be required to notify controllers of changes, particularly SMEs who may not understand the changes? The phrases “developing a solution” and “development of a solution” are quite limiting and should be broadned, as controllers may sometimes be directly purchasing hardware, software and/or systems, and not necessarily engaging technology providers to develop solutions for them. “The EDPB recommends controllers to require that technology providers demonstrate accountability on how they have complied with DPbDD” – strictly Art.25 requires compliance by controllers, not tech providers, so this should be changed to “The EDPB recommends controllers to require that technology providers demonstrate how their software, hardware, systems and/or services will enable the controller to comply with DPbDD”. The EDPB “encourages associations or bodies preparing codes of conduct in accordance with Article 40 to also incorporate DPbDD” – it is odd that Art.25(3) refers to certifications but not codes, even though Art.40(2)(h) itself refers to Art.25, and this seems to be an inadvertent oversight in the drafting of Art.25; it would be helpful if the EDPB specifically stated that it considers (although this is implied by that sentence) that SAs will accept codes on DPbDD under Art.40(2)(h) as being within Art.25(3) i.e. adherence to such a code may be used as an element to demonstrate compliance with Art.25.