**Guidelines 07/2020 on the concepts of controller and processor in the GDPR version 1.0**

**Response to consultation, 18 Oct 2020**

1. Thank you for the helpful and well-written paper (and for numbering paragraphs individually which is also helpful – this response follows the same style).
2. The clarification in para. 101 that processors are equally required to put in place Article 28-compliant contracts is particularly helpful, as is the detailed guidance regarding joint controllers.
3. Some comments/requests are below.

**Major issues – cloud services**

4. Generally, please could the EDPB take the opportunity to update and clarify guidance regarding the use of cloud services, which is now widespread and increasingly considered important by the EU, but taking full account of the standardized and commoditized nature of those services, as the EBA has done in its outsourcing guidelines. Particular comments follow.
5. Para. 28 – after "Even if the processor offers a service that is preliminary defined in a specific way," please consider adding "(for example, acloud service)"; and clarify how the references to controller ability to request changes and processor's inability to change "essential elements" would apply to a standardized, commoditized service that cannot be tailored or customized to meet different requests of different customers – rather, customer must choose to accept the service and changes, or not. This paragraph could also usefully cross-refer to fn. 24 in para. 63.
6. Para. 38 – "the detailed security measures which may be left to the processor to decide on" – cloud could be cited as an example of where this may be done
7. Para. 63 – surely this example of shared infrastructure could also be used in relation to the situation where a *processor*, such as a cloud provider, provides a platform/standardised infrastructure where cloud customers (its controllers) may decide how they wish to set up their use of the platform. That seems to be more common than a joint controller providing standard platforms for other joint controllers to use.
8. Para. 69 1st example – if the mother company hosting the database is a processor, even though it presumably determines the measures for securing the database (security measures were not discussed in that example), so too should be a cloud provider hosting customers' databases. Also, it does not seem realistic for a group of related companies that "They cannot access or use each other's data", although that would be the case for databases hosted (as processor) for different customers in the cloud.
9. Para. 80 – "The nature of the service will determine whether the processing activity amounts to processing of personal data on behalf of the controller within the meaning of the GDPR." Surely, this should be "the nature of the processing operation", not the nature of the service. With IaaS/PaaS or storage SaaS, the customer can use the service to process personal data (or not) as it chooses – the nature of the service there is such that it is use-agnostic. It is how the customer uses the service that matters. So in some cases the nature of the service will *not* determine whether there is processing of personal data on behalf of the controller.
10. Para. 80 – also this sentence suggests all cloud providers are controllers!: "In practice, where the provided service is not specifically targeted at processing personal data or where such processing does not constitute a key element of the service, the service provider may be in a position to independently determine the purposes and means of that processing which is required in order to provide the service. In that situation, the service provider is to be seen as a separate controller and not as a processor." Cloud providers are obviously controllers of any

personal data within the *account/registration data* of their customers, e.g. customer staff contact names/email addresses, but they are not necessarily controllers of the personal data uploaded to their services by controller customers. IaaS/PaaS and some SaaS services are not specifically targeted at processing personal data and such processing may not consitute a key element of the service. Please clarify that position here.

11. Para. 82 – please clarify how "be able to request changes" applies to standardized cloud services, where it is impossible for different customers to request different changes? If the controller does not like how a service is set up then it should not use the service in the first place.
12. Para. 82 – the example of cloud hosting is helpful, and the fact that the service is standardized, but it is unclear what is meant by "It must also make sure that their specific instructions on storage periods, deletion of data etc. are respected by the cloud service provider regardless of what is generally offered in the standardized service"? Cloud services are used in self-service fashion, with the customer's configuration and use of the service comprising its main "instructions" to the cloud provider. Customers choose how long they want to store data and will delete data directly as and when they wish to do so, so these are issues within the controller's direct control – how can they ensure these matters are "respected" by the provider?
13. Para. 109 – specifying level of security required – again in cloud the customer should review the security measures provided and decide if they are suitable or not, rather than trying to modify the provider's security arrangements.
14. Para. 111 – with cloud services, "instructions" are generally given through how the customer operates and uses the service.
15. Para. 113 – same point about "instructions" in cloud.
16. Para. 123 – again an obligation to obtain all controllers' approval to security measures before they can be changed does not work with cloud. As long as the processor has committed to maintaining certain minimum standards (i.e. the minimum *security objectives* referred to in para. 124), approval to processor security changes (which are often *improvements* or upgrades to their security) should not be required from every controller before the security changes can be made. Para. 123 should refer clearly to para. 124's security objectives and not require individual controller approvals of changes – large cloud providers have much better expertise regarding security measures than most controllers in any event, particularly SME customers.
17. Para. 125 – please confirm "actively indicates or flags" includes providing a sign-up form for notifications such as at https://pages.awscloud.com/sub-processors/.

**Other issues**

18. Para. 72 and 79 – there are many situations in practice where one company may act as a processor (e.g. providing a platform) for a controller, but where the controller also specifically permits the processor to use certain personal data for its own purposes as a controller. See for example Microsoft's July update to its Online Services Terms after the EDPS required it to change its terms to reflect its controller status for some processing operations (such as managing the overall security of its services for the benefit of itself and all its customers). Where a processor is *permitted* by a controller to become a controller itself for certain processing operations, the processor is *not* infringing the GDPR. These paragraphs should therefore be amended to clarify that a processor that becomes a controller does *not* always infringe the GDPR when it does so. There are situations involving processing outside the controller's lawful instructions, which involve an agreed controller-to-controller data sharing

(for those specific purposes) rather than an infringement of the GDPR or the controller's instructions.

19. Para. 81 – it is helpful that the guidance says incidental limited access by an IT consultant fixing a software bug does not make the consultant a processor, but could more guidance please be given on the circumstances when access is "too much"? Should the wording at the end of para. 81 (before the 1st example) "taking into account the nature, scope, context and purposes of processing as well as the potential risks for data subjects" be applied not just to considering whether or not to *entrust* processing to a particular service provider, but also to determining *whether* the service provider is to be considered a "processor" or not? Similarly for "occasionally come across" in para. 87 1st example.

20. Para. 91 – error, in "a processor must ensure that persons authorised to process the personal data have committed themselves to confidentiality (Article 28(3));". Article 28(3) specifies what the controller-processor contract should cover, it does not impose a direct statutory obligation on processors to ensure confidentiality obligations on the part of their staff. The reference should instead be to Article 29, which *does* impose a similar but different obligation directly on processors, and the wording changed accordingly.

21. Para. 93 – as with para. 91, there is no direct statutory obligation on processors to assist controllers, although this must be an obligation specified in their contract.

22. Para. 105 – the sentence starting "Also, the SCCs will generally be embedded…" could be moved to a new paragraph, because this is true not only of SCCs, but also of contracts referred to in para. 102 that are *not* in standard SCCs form. Please also clarify that, regarding Article 28 terms (whether in SCCs *or otherwise*), additional clauses are possible in relation to commercial terms e.g. reasonable fees/costs for providing assistance.

23. Para. 107 – please clarify that controllers' approval of updated standard data processing agreements (which are often amended by providers so as to be more beneficial to controllers) can be through continued use of the service after notification of the amended terms.

24. Para. 111 – last bullet point. Surely the obligations of the controller to be set out in the agreement must refer to the contractual obligations of the controller *to the processor*. There seems no sense or point in the *contract* stating what the obligations of the controller already are under the GDPR. The examples given of ensuring compliance and supervising processing are obligations under the GDPR, and perhaps rights of the controller in relation to the processing, but they are not obligations of the controller to the processor under their contract.

25. Para. 118 – please delete "before starting the processing", which seems to be wrong or misleading. The GDPR does not require the processor to inform the controller, before commencing the *processing relationship*, of laws in the processor's jurisdiction that might require the processor to process the data otherwise than in accordance with the controller's instructions. Only that the processor informs the controller (unless prohibited by law etc.) before conducting *any processing required under EU/Member State law that would contradict such instructions* (e.g. disclosing data to regulatory authorities, or retaining data after contract termination for tax or accounting reasons). The latter interpretation makes more sense and is more practicable than forcing all processors to provide legal advice to would-be controllers, pre-contract, on EU/Member State laws that might require the processor to act otherwise than as instructed; and of course new laws could be enacted in a Member State that might require disclosure or retention of controller data, surely processors should not be forced to provide "legislation tracking" services to controllers! Please reconsider the position here and redraft.

26. Para. 121 – it goes beyond what the GDPR requires to say that "details concerning the relationship" "must" be addressed under the confidentiality obligation. There are cases where a processor wants to publicise that it works for a particular named controller, and the controller has agreed to that.
27. Paras. 127-128 – these should take into account that, for self-service cloud involving the passive provision of IT resources, the controller can simply login and search for the relevant data to access/delete/correct etc. It does not need to require the processor to do anything.
28. Para. 130 – informing the processor of risks (here and elsewhere) is not appropriate in cloud. It should be for the controller to assess the risks and then decide if the service is adequate for the risks involved.
29. Para. 139 – the GDPR does not require the processor to notify the controller of any such laws or vice versa. This is just an exception allowing the processor to continue to store personal data if required by law even if, after termination, the controller wants the data to be deleted/returned.
30. Para. 140 – it is for the *controller* to decide how long it wants certain data to be retained by the processor during the term of the contract (and in cloud the controller can directly delete data itself), so it is unclear why the processor should provide any information on its data retention, because it should simply follow the controller's instructions in this regard?
31. Para. 142 – please clarify that the "immediately inform" requirement is a statutory obligation on the processor and does not have to be set out in their contract – there is a mistake in the GDPR's text introduced by the jurists/linguists (see the diagram tracing through the changes in the draft GDPR in this article and the Netherlands government's contribution to the 2-year review of the GDPR on p.51, in 3.8 point 3 of the consolidated Council document), and the words "With regard to point (h) of the first subparagraph" should be read as omitted given the legislative history.
32. Para. 146 – same comment as for paras. 72 and 79, above.
33. Para. 148 – the text "In both cases, the processor must obtain the controller's authorisation in writing before any personal data processing is entrusted to the sub-processor" should cross-refer to para. 153 where with general authorisation failure to object (within the relevant timeframe) can be interpreted as such "authorisation in writing".

**Other clarity/editing/formatting issues**

34. Para. 68 – in practice separate controllers are often referred to as "independent" controllers, although this is mentioned in para. 69 2nd example, it would be helpful to phrase it as "separate and independent controllers" in para. 68 and the 1st example of para. 69 too.
35. Para. 83 - please clarify "A recipient of personal data and a third party may well simultaneously be regarded as a controller or processor from other perspectives. For example, entities that are to be seen as recipients or third parties from one perspective, are controllers for the processing for which they determine the purpose and means." Does this mean, "A third party or recipient may also be a controller or processor of the personal data it receives even though it falls within the GDPR's definition of 'third party' or 'recipient'"? Or does it refer to subsequent processing of that personal data by the third party or recipient? Deleting the "perspectives" wording may be clearer as otherwise it's unclear what "other" perspectives or processing situations are meant.
36. Para. 86 – "an employee or a role highly comparable to that of employees, e.g. interim staff provided via a temporary employment agency" is helpful but this expansion could and should be moved to para. 76, and further expanded to mention temporary individual subcontractors

(not through an agency but self-employed) who are often engaged by controllers but should not be considered as "processors".

37. Para. 92 – in practice this process of checking sufficient guarantees is pre-contractual due diligence, and it would be helpful if the words "due diligence" were actually mentioned in this paragraph?
38. Para. 99 – please state that electronic signatures and electronic agreements are permissible.
39. Para. 103 – the link in footnote 39 does not work.
40. Para. 112 – could examples be given please of what other relevant information should be included in the contract please? Pre-contract information may usefully be provided without having to be included in the contract itself.
41. Generally, it would be most helpful if there could be clickable links to documents cited in the footnotes, e.g. footnote 42.
42. Para. 119 – very minor but the words "The contract must say that the processor needs to ensure that anyone it allows to process the personal data is committed to confidentiality" would be clearer if they read, "The contract must say that the processor *must* ensure that anyone it allows to process the personal data is committed to confidentiality".
43. Para. 120 – insert "the" before "processor".
44. Para. 126 – please cross refer from here to para. 157 which explains fully what "same" means.
45. Paras. 158-189 – structurally, it would be helpful if these paragraphs immediately followed the guidance on joint controllership to follow section 3 of part 1, rather than being at the end of the guidance.

Thank you.