Google welcomes the opportunity to provide feedback to the European Data Protection Board (EDPB) on its draft Recommendations 1/2026 on the Application for Approval and on the elements and principles to be found in Processor Binding Corporate Rules, as adopted on 15 January 2026 (the **Recommendations**). We summarise our key observations on the Recommendation below, which we would be grateful for the EDPB to consider.

Overall, we believe that too much of the Recommendations directly mirrors the Controller BCR requirements, and thereby fails to recognise the fundamental differences in the role and activities of a processor. We suggest that the Recommendations would benefit from being more tailored to the specific role played by a processor.

In terms of the differences between controllers and processors, we particularly note that:

1. In all but exceptional cases, a processor has no direct relationship with the data subject. Indeed, it is highly likely that the processor will be entirely invisible to the data subject. Articles 13 & 14 GDPR do not impose an obligation to inform data subjects about specific processors, and so processors generally operate 'behind the scenes'. We also think it is critical to keep in mind that processors have no means of communicating with data subjects; the reality is that the data subject's primary point of contact will always be the controller.

2. For a variety of data processing services, including cloud storage and infrastructure services – but also data analytics and other general purpose services – processors will have very little or even no visibility over the data they are processing, nor the identity of the data subjects. It is highly likely that a processor would not even be able to verify a data subject as an individual whose personal data they are processing.

3. A processor relying on P-BCRs may be contracting directly with the controller, but equally may be appointed as a further (sub)processor, potentially many levels down the chain. It is highly likely that a processor would not even be able to verify an individual or company as a data controller further up the chain, when the processor's customer is themselves a processor. Nor, when the processor's customer is themselves a processor, will that customer want to share *its* entire customer list (which compromises sensitive and valuable commercial information) with its processor.

4. The P-BCR requirements should be sufficiently flexible to allow for the (very common) situation where the BCR applicant is contracting with a

processor-customer, and so has no contract with the controller. The P-BCR requirements should therefore focus on rights granted to the *customer*, rather than necessarily the *controller*. For example, where a processor does not contract directly with the controller, it is inappropriate to require that "*the Controller shall have the right to enforce the BCR against the BCR member*". As a reminder, the processor in many cases will have no contract with the controller, no means of identifying the controller, nor any direct instructions from the controller. So, to require the BCR-P to bind the processor in relation to, and to be enforceable and auditable by, the controller will leave the processor with significant liability owed to an unknown entity the processor has not contracted with (multiplied across the many potential controllers involved), and also create significant security risks (by mandating that a third party not bound by any contract terms entered with the processor should be able to conduct an audit). Furthermore, this additional liability borne by the processor would either be uncapped (due to the lack of any contract between the processor and each controller) or, if subject to the liability cap agreed between the processor and the customer, will reduce the amount of that cap available to the customer. In either case, this would be manifestly unfair to (1) a processor whose contract terms with its customer (including the prices charged to that customer and liability caps agreed with that customer) will have been determined and agreed in the expectation that the contract would apply only between the processor and its customer, and/or (2) the customer, who will find that the amount of liability coverage it thought it had negotiated with the processor gets consumed by one or multiple third parties whom the customer does not control This is simply unworkable, and undermines commercial and contract freedom; the far better solution would be to leave enforcement and liability to follow the contractual chain.

5. Processor BCRs (unlike their Controller counterparts) form part of a business arrangement between two commercial parties (the processor and their customer). The obligations under the Processor BCRs must be seen in the context of the overall arrangement, which may already include commercial terms on termination, audit rights, liability etc., and is required to include the data processing terms mandated by Art. 28(3) of the GDPR. Thus, when the recommendations state "*The processing agreement entered into between the controller and the processor(s) should not be in contradiction with or lower the protection provided by the BCR-P*", they seem to lose sight of the fact that the processor's status as such begins with, and derives entirely from, the already-regulated processing agreement. It therefore does not seem appropriate to prioritize the BCR-P over that agreement.

In light of the above, we would like to see greater differentiation between the Controller and Processor BCR requirements, and consideration of the distinct role/ position of a Processor. Specifically:

- We are concerned that too many of the requirements in the Recommendations have been copied verbatim from the Controller Recommendations, for example s.2.1 on

the material scope of the BCRs[1]. As should be clear from the above, a number of processors will not be in a position to provide any meaningful information on the categories of personal data or the categories of data subjects.

- As noted above, processors will often have little or no visibility of the personal data (e.g. due to encryption controls), and will have very little context for the processing. Accordingly, the new 'Accuracy' principle is not appropriate. Processors cannot be expected to monitor the accuracy or up-to-date nature of the data they process; this is for the controller. In fact, very often controllers seek to limit any monitoring of their data by processors, and would not want their processors to undertake the additional (potentially wide-ranging) processing that would be involved in monitoring for accuracy / currency. We suggest this updated obligation be removed, and revert to the previous duty to act on the controller's instructions to update or correct data.

- It should be possible to create third party beneficiary rights for data subjects in the agreement between the processor and the customer, rather than under the mechanism that makes the P-BCRs internally binding (see section 1.3.1). Indeed, this would be more logical, since it is only because of the contract with the customer that the P-BCRs will apply in respect of a specific data subject (without the customer agreement, even if the P-BCRs are binding at a general level, they would not apply to any specific dataset). Furthermore, since the agreement between the processor and the customer must incorporate the P-BCRs, the P-BCRs will form *part of* that agreement. Consequently, it should be sufficient to set out the third party beneficiary rights in the P-BCRs only.

- In contrast to the Controller BCRs, the P-BCRs should be viewed primarily as a contractual instrument describing the roles and responsibilities of two commercial entities towards each other, i.e. the appointing controller/processor and the BCR applicant. Whilst it is important that the language of the P-BCRs can be understood by the BCR applicant's personnel who are implementing the P-BCRs, it is equally important that the language be allowed to meet contractual standards of certainty and completeness, using legal terminology suitable for an arrangement between two commercial parties.

- Relatedly, the Recommendations should permit P-BCRs to include common protections as between two commercial parties, e.g. obligations of confidentiality in respect of audits, and the ability to charge a reasonable fee when additional services are being provided. Similarly, processors should be able to include common protections when termination rights are exercised.

[1] Another example of this is in section 1.7, where it is suggested that the P-BCRs could be published on the Group intranet if the data subjects are exclusively employees; since an employer will always be a controller, this seems very unlikely to apply in a processor scenario. Likewise section 3.4, which states that DPOs cannot carry out a DPIAs (a solely controller obligation).

Unrelated to the specific role of a processor, we also make the following submissions in respect of the new Recommendations:

- We believe that the Recommendations adopt an overly rigid approach towards internal training (in both the BCRs themselves and the application form). It should be for each organisation to determine the appropriate training programme for their personnel, and this is not something that the DPA reviewers need to have input on (neither employee training nor employment law are their area of expertise). For example, it may not always be appropriate to "test" all employees on each occasion. Similarly, it should not be necessary to commit to specific training intervals in the P-BCRs, as this could vary over time and/or as between groups of employees. Instead, it should be sufficient to commit to "appropriate" training, which implies sufficient coverage, frequency and assurance.

- Also, on page 48, we would urge the deletion of additional, purely bureaucratic requirements such as the following: "*The BCR-P should also contain a commitment that where any safeguards in addition to those envisaged under the BCR-P should be put in place,* ***the Liable BCR member(s), and the relevant Privacy officer or Function will be informed and involved in such assessment***" [emphasis added]. The BCR-P already impose complex requirements about transfer impact assessments - we see no need for the BCR-P to effectively reach inside organizations to dictate how they should operate internally when completing those assessments.

- In today's modern world, there surely can be no need to require a physical address as a contact point. It is difficult and expensive to administer, and will only cause unnecessary delays (for example, physical post received by a data importer in a foreign jurisdiction would then have to be forwarded on to the appropriate contact point internally). An electronic communication contact point is far more efficient and secure, and gives the data subject greater confidence that their communication has been received.

- Where the Recommendations reflect a GDPR requirement, they should precisely mirror the language used in the GDPR and not go beyond or differ from that. By introducing new standards, the Recommendations create uncertainty, and also create a different regime between the data exporter and the data importer. For example, under the purpose limitation principle, importers must process personal data only for the "*specific, explicit and legitimate purposes of the transfer*", as set out in the processing agreement. The GDPR requirement is, of course, to only process the personal data on the "*documented instructions*" of the controller. This new test of 'specificity, explicitness and legitimacy' creates an inconsistency with the GDPR, and a difference between the obligations of the exporter and the importer.

- On p.51, paragraph (iii), the data importer must inform the data exporter if it is partially or completely prohibited from providing the information required. However, this should be subject to the requirements of local law, as many orders will equally prohibit the communication of their existence. This position would be consistent with Clause 15.1(c) of the Standard Contractual Clauses (where this obligation is drafted as "*Where permissible under the laws of the country of destination…*").

- Overall, we note that the table for requirements of the P-BCRs now fills 37 pages (an increase from 17 in WP257). We believe this is a result of substantially increasing the complexity of P-BCRs, and that this will have a direct, negative effect on both the extent of their use / adoption by organizations, and their ability to guarantee rights for data subjects. So many of the requirements are overly prescriptive, overly complex and overly long, potentially to the point of being unworkable. Particularly given that, during the application process, DPAs now seem to expect the BCR requirements to be met using the precise language of the requirements, it is vital that the Recommendations also exhibit the "clear, intelligible and transparent" approach required of the P-BCRs themselves.. We would therefore suggest the DPAs consider removing some of the new additions, thus simplifying the document overall. By way of some specific examples:

    - On page 49, a data exporter may be obliged to suspend a transfer "*as well as all transfers for which the same assessment and reasoning would lead to a similar result*". We believe this language should be deleted, as it is convoluted and unnecessary (the obligation to suspend already applies to *any* transfer or set of transfers). However it is not merely redundant: it could also result in duplication of efforts and create confusion as to what constitutes a "similar result".

    - On p.56, the Recommendations address how the term "applicable law" should be used. Specifying whether it refers to a national/local law is unnecessarily prescriptive and will only increase the complexity of the drafting. The BCR applicant will, when drafting the language, need to address the fact that several laws may be applicable; and that these may be regional, national, or international. "Applicable law" is a well-understood term used habitually in legal agreements, and therefore offers both the legal certainty and flexibility required.

    - On p.56, the requirement that GDPR provisions (and definitions) be quoted in full. This will add substantially to the length of the P-BCRs, and make them more difficult to read. By way of example, even the definition of "personal data" runs to 67 words; "processing" is 53 words; and "controller" is 64 words. We would add that the text of the GDPR, including all definitions, is readily available to anyone with access to the internet.