EDPB consultation on legitimate interests guidance – Amazon Response

Amazon appreciates the opportunity to submit comments to the EDPB on the draft Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR ("draft Guidelines"). Amazon is an organisation that processes personal data in a variety of scenarios. Robust privacy and security practices are essential to earning and maintaining the trust of our customers and others whose data we process.

We welcome new guidelines on the legitimate interests legal basis. Guidance is important to ensure that both controllers and data subjects have clarity on the expectations of data protection supervisory authorities when interpreting and applying the GDPR.

Our comments and feedback focus on two main areas where we consider that the draft Guidelines could be strengthened:

- **Ensuring controllers retain the ability to undertake a case-by-case assessment:** Consistent with CJEU case law, the draft Guidelines state several times that the legitimate interests assessment requires a case-by-case analysis of the particular facts in question. However, the draft Guidelines also include a number of definitive statements about elements of the legitimate interests assessment, and identify a range of general scenarios in which the legal basis is unavailable, that would reduce this flexibility. As just one example, the draft Guidelines state that, regardless of context, certain broad categories of data should always be considered inherently "more private" and thus more likely to have a "negative impact" on data subjects (para. 40, third bullet). Unless data has a special status under the GDPR, guidance should not establish a presumption that processing such data negatively impacts data subjects.

  We encourage the EDPB to avoid making generalised statements that restrict controllers' ability to assess their specific facts. Removing this element of discretion could effectively prohibit certain processing activities, regardless of the interests advanced or the protections in place. This approach would run counter to the case-by-case analysis that the legitimate interest test clearly contemplates.

- **Providing guidance that focuses not only on what can't be done, but also on what can:** As noted above, the draft Guidelines include a range of scenarios where legitimate interests would be unavailable. In order to help controllers understand more clearly how to assess when they can rely on Article 6(1)(f), it would be helpful for the EDPB to include more positive examples of steps that controllers can take to enhance their ability to rely on legitimate interests—for example, how a controller can evidence that the processing is within the reasonable expectations of data subjects or that the controller has implemented sufficient safeguards.

In addition to these general points, we have the following specific feedback:

Impact of compliance with GDPR on the balancing exercise

The draft Guidelines state that a controller's compliance with the GDPR cannot be taken into account as part of the legitimate interests balancing exercise (*see, e.g.,* paras 34, 48, 57, 62 and final sentence of 68). It is unclear why this is the case, given that the very purpose of the GDPR's data processing principles and its substantive obligations is to safeguard the privacy rights and interests of data subjects. Facilitating rights, being transparent, implementing strong security measures, and complying with data minimization and other core principles all reduce potential negative impacts on data subjects and should be factored into the balancing test. For example, if a controller allows a

data subject to easily opt out of a given processing operation, this meaningfully minimizes the impact of the processing—it is unclear why this fact shouldn't be considered.

Ignoring those measures that a controller has adopted to comply with the GDPR also raises the question of exactly what safeguards *are* sufficient to rely on legitimate interests. Most GDPR compliance requirements are not prescriptive, making it difficult to establish what "going beyond" GDPR compliance entails. Ruling out consideration of GDPR-mandated safeguards also leaves controllers subject to unknown and untested standards that different Member State supervisory authorities are likely to apply in different ways. If the EDPB adopts this position in its final guidelines, controllers will need additional guidance on what mitigating measures they need to deploy in order to rely on legitimate interests. The EDPB refers in footnote 65 to the original Working Party 29 ("WP29") Opinion 06/2014 for "further examples of possible mitigating measures," but as the EDPB acknowledges in paragraph 34 of the draft Guidelines, many of these mitigating measures are now legal obligations for controllers.

- We encourage the EDPB to explicitly recognise that measures adopted in compliance with the GDPR can mitigate negative effects of processing, and that these measures should be taken into account in the balancing test—and to amend statements to the contrary in the Guidelines accordingly.

Transparency and reasonable expectations

The draft Guidelines state that "[r]easonable expectations do not necessarily depend on the information provided to data subjects" (paragraph 53) and that "the mere fulfilment of the information obligations set out in Articles 12, 13 and 14 GDPR is not sufficient in itself to consider that the data subjects can reasonably expect a given processing." We encourage the EDPB to reconsider these statements: when a controller provides clear and prominent information to data subjects about how their data will be processed, that necessarily is relevant to determining what data subjects can reasonably expect. This fact does not change simply because the disclosures are required under the GDPR.

We also do not think it follows that reasonable expectations cannot be shaped by "what is considered common practice in certain sectors," as the draft Guidelines suggest. Where certain processing activities are common practice and generally well understood in a given context, this clearly is relevant to whether they are within the average data subject's reasonable expectations.

The above interpretations are also consistent with recital 47 GDPR, which provides that the "context of the collection of the personal data" is a relevant consideration when assessing data subjects' reasonable expectations.

- We recommend clarifying in paragraph 53 that although information that a controller provides to data subjects may not always guarantee data subjects' reasonable expectations, it is an important factor in the balancing exercise.
- Similarly, where certain processing activities are common practice in a sector, the Guidelines should recognise that this is potentially relevant to considering data subjects' reasonable expectations.

Methodology for the balancing exercise

Finally, we recommend that the EDPB addresses the following aspects in the draft Guidelines on how to conduct the legitimate interests test:

1. *Legitimate interests*

Paragraph 32 of the draft Guidelines, which sets out the methodology for the legitimate interests balancing exercise, does not refer to assessing the strength of the legitimate interest being pursued. This is an omission which would produce unbalanced results. Where interests that controllers pursue are particularly important—such as interests that advance community or public interest goals, are recognised in EU or Member State law, align with fundamental rights, or are in pursuit of EU economic goals—that fact would have no bearing in determining whether the controller's interests are outweighed by the data subject's rights and freedoms.

- We encourage the EDPB to revise the draft Guidelines to explain that as part of the balancing test, controllers should take into account the strength of the legitimate interest being pursued. This approach would also be consistent with WP29 Opinion 06/2014.

2. *Necessity*

When weighing the necessity of processing (step 2 of the assessment), the draft Guidelines state that "in practice, it is generally easier for a controller to demonstrate the necessity of the processing to pursue its own legitimate interests than to pursue the interests of a third party, and that latter kind of processing is generally less expected by the data subjects" (para 30). Rather than making a definitive statement along these lines, the Guidelines should encourage controller to consider the necessity of the processing activity on a case-by-case basis, including when relying on third parties' interests. We also encourage the EDPB to remove the presumption that reliance on third-party interests is generally less expected by data subjects—again, the facts of the specific processing scenario should be determinative. Indeed, there may be many scenarios in which processing that advances the interests of a third party is expected by a data subject (for example, in circumstances where parties share data to advance the wider community's interests in promoting health and safety).

- We encourage the EDPB to either remove or amend the statements relating to: (a) the ability of a controller to demonstrate the necessity of the processing when relying on the interests of a third party, and (b) the idea that reliance on third-party interests is generally less expected by data subjects. Instead, the draft Guidelines should make it clear that determining whether processing is necessary requires a case-by-case assessment of the facts of the processing.

3. *Impact of the processing*

Paragraph 39 of the draft Guidelines, which addresses the potential impact of the processing activity on data subjects, omits two key considerations: the *likelihood* of a potential impact arising in practice and its *severity*. Considering the likelihood and severity of an impact as part of the balancing exercise is important to ensure appropriate weight is given to a potential negative impact of processing. If, for example, a negative impact is highly unlikely to occur in practice or may be only minimal in its severity (or, by contrast, is very likely to occur and/or be significant in its severity), this is relevant to determining whether the controller's interests are overridden by data subjects' rights and freedoms. The omission of this point in the draft Guidelines also departs from the approach taken in the WP29 Opinion 06/2014.

- We ask the EDPB to update the guidance in paragraph 39 to make clear that controllers should consider the impact of the processing on data subjects, the likelihood of those impacts occurring in practice, and the potential severity of those impacts, if they were to occur.