Response to the EDPB on its legitimate interests guidelines - November 2024

Google welcomes the opportunity to provide feedback to the European Data Protection Board on its *Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR*, as adopted on 8 October 2024 (the **Guidelines**). Our response contains some general observations on the Guidelines together with a number of specific points of interpretation that we would be grateful for the EDPB to consider. We hope these viewpoints are helpful.

At Google, we believe innovation and technological adoption stem from user and public trust and cannot come at the cost of user data protection rights. It is important to encourage the development and use of technologies which strengthen privacy protections for users whilst facilitating and promoting innovation in emerging fields. This innovation can enhance the experience of users online and accelerate public interest research.

The legitimate interests ground of Article 6(1)(f) GDPR plays an important role in facilitating this innovation and ensuring organisations can grow, change and develop whilst protecting the rights and freedoms of the individuals whose personal data they process. Google, like many large digital technology platforms, relies on the legitimate interests ground as its lawful basis for a number of the processing activities it carries out.

General feedback

Overall approach

Google welcomes the development of new guidance on this topic and fully supports a legitimate interests regime with the rights and freedoms of data subjects at its heart. In addition, Recital 4 makes it clear that the GDPR respects all fundamental rights and that the right to the protection of personal data should be balanced against such rights, in accordance with the principle of proportionality.

Overall, we feel that certain aspects of the Guidelines are not proportionate to the objective they seek to obtain and as a result could create a burden on organisations that goes beyond the GDPR requirements and the principle in Recital 4 of the GDPR. In particular, the Guidelines do not appear to take into account the different contexts in which processing takes place, and in turn the need to appropriately balance all relevant fundamental rights (including the right to freedom of expression and information, right to education, right to healthcare and the freedom to conduct a business). The result could have unintended consequences for organisations. For example, the Guidelines:

- suggest that broader societal and public interests cannot be taken into account when relying on the legitimate interests ground (paragraph 25, as discussed further below) which is inconsistent with the position in WP217 that '*[s]ome interests may be compelling and beneficial to society at large'. We* also assume this interpretation is not intended to capture the many projects pursued by organisations in the public interest, on a pro bono or similar basis, that are not linked to their core activities and are done wholly or predominantly in the wider public interest;

- suggest that only mitigating measures that *go beyond what is required* under the GDPR should be considered as part of the balancing test (paragraphs 34, 48 and 57, as discussed further below) - this feels counter-intuitive and disproportionate given how broad many of the requirements under the GDPR are, meaning arguably all measures implemented could be considered required under the GDPR;

- suggests that personal data must be treated as special category data *if it is possible* to infer sensitive information from the data processed, irrespective of any intention of actually doing so (paragraph 40) - this is difficult to reconcile with the EDPB Guidelines 03/2019 which suggest that CCTV footage showing someone wearing glasses or in a wheelchair is not considered special category data. Similarly, paragraph 54 of the Guidelines also references CCTV suggesting an organisation can, subject to satisfying the three-stage test, rely on the legitimate interests ground to implement CCTV. The ICO takes a more proportionate approach under the UK GDPR that the controller must intend to make an inference or to treat someone differently on the basis of inferred information, for the personal data to be treated as special category personal data;

- promote the level of granularity in transparency information that would be disproportionate and would make it difficult for organisations to provide meaningful transparency information - in particular, the Guidelines require organisations who are relying on legitimate interests to process personal data for the purpose of combating fraud, to "be specific about what type of fraud they are trying to prevent" and to include more than a generic reference in the privacy policy about that purpose (paragraphs 105 and 106) - this goes significantly beyond what is meant by a *specific legitimate interest* (referred to in the Transparency Guidelines). This approach would also have a disproportionate impact on areas of research and development where it is important that organisations have flexibility to find out what they don't already know meaning it may not be possible to be specific about the interest at a granular level - this in turn impacts organisations ability to innovate;

- require organisations to provide data subjects with information about the balancing test (paragraph 68, discussed further below) - this goes beyond the transparency and accountability provisions of the GDPR;

- require 'compelling legitimate interests' to be *essential* (paragraph 73, as discussed further below); and

- fail to provide a positive use case for the processing of children's personal data in accordance with the three-stage test (paragraphs 94 and 95, as discussed further below).

The nature of an interest (paragraph 17)

The Guidelines require an interest to be '*real and present'* and '*not speculative"*, for it to be *'present and effective at the date of the data processing and… not [to] be hypothetical at that date'* and to be *'precisely articulated'.*

WP217 (referenced in the Guidelines at paragraph 17, footnote 26), requires an interest to be *sufficiently clearly articulated*. The EDPB's decision to use the word '*precisely*' (whilst referencing the test in WP217) requires such specificity and exactment that it will be incredibly burdensome, if not unattainable, for organisations to comply with and it risks impacting innovation and research. The '*sufficiently clearly*' language in WP217 provides organisations with some flexibility, linked to the context, whilst ensuring interests are articulated in a way that enables them to be weighed against the rights and freedoms of individuals as part of the balancing test.

It would also be helpful if the EDPB provided some additional context here as to what amounts to a *real and present* interest. Similarly, it would be helpful if the Guidelines could clarify that research and development activities can amount to *real and present* interests and is not speculative nor hypothetical even if the more precise outcome / aim of the processing is unknown at the point at which it commences.

General public interests and data subject benefits (paragraphs 25)

Google welcomes the acknowledgement that processing activities can have a positive impact on individuals and that the interests pursued by a specific controller or third party may also serve broader interests such as the interests of the wider community.

At Google, our services provide an even more important means for individuals to exercise fundamental rights including the right to freedom of expression and information. In this regard, European Courts, including the CJEU in its Tietosuojavaltuutettu case on the interpreting Directive 95/46/EC, have made clear that in order to take account of the importance of the right to freedom of expression in a democratic society, it is necessary to interpret notions relating to that freedom broadly and that account must be taken of the evolution and proliferation of methods of communication and the dissemination of information.

However, the Guidelines suggest that the interests of the wider community are only relevant where organisations rely on Article 6(1)(c) or (e) meaning that where a controller seeks to rely on the legitimate interests ground, it cannot consider the interests of the wider community (who are not considered third parties). Instead, the controller must demonstrate that such processing is done in pursuit of the controller's *own* legitimate interests or those of *specific* third parties (emphasis added). As noted above, this interpretation is inconsistent with WP217 (which is relied upon elsewhere in the Guidelines by the EDPB) and it doesn't account for the many projects pursued by organisations in the public interest, on a pro bono or similar basis. For example, many organisations across the EU were involved in data

sharing efforts in response to the COVID-19 pandemic, often for the benefit of society at large and supported by guidance of supervisory authorities.

By contrast, the UK Information Commissioner, in its guidance on legitimate interests under the UK GDPR makes it clear that legitimate interests *can* include broader societal benefits and public interest.

Google's view is that the reference to 'third parties' includes the interests of the wider community, as long as they can be reasonably defined and objectively articulated, and these interests can form a key part of a legitimate interests assessment in relevant cases. Organisations should be able to process personal data on the basis that such processing has a broader societal benefit (subject to the necessity and balancing tests). Many organisations engage in activities that have no connection with the broader mission/activity of the organisation but are otherwise done for broader societal benefits and it would be disappointing if the interests of society could not be considered.

Therefore the Guidelines provide the EDPB with a great opportunity to recognise the potential societal benefits of processing activities (particularly new and innovative uses of technology) and acknowledge that such societal benefits can be considered as part of a legitimate interests assessment. Importantly, this approach would:

- continue to protect the rights and freedoms of individuals - the legitimate interests ground involves a three stage test so controllers would continue to be required to assess those broader societal benefits against a necessity requirement and balance such benefits against the potential impact (positively and negatively) on an individual's rights and freedoms; and
- give significant confidence to all organisations developing or deploying new technologies that EU regulation does not pose a barrier to innovation and rather encourages innovation carried out in a safe and controlled manner.

Identifying mitigating measures (paragraph 34, 48 and 57)

As part of carrying out the balancing test, the Guidelines suggest only mitigating measures that go *beyond* what is required under the GDPR should be considered relevant as part of the balancing test. Given the breadth of many of the concepts covered by the GDPR including privacy-by-design and privacy-by-default, all measures could arguably fall within what is required by the GDPR so it seems counter-intuitive to say that those measures are not relevant to mitigate the risk to individuals.

We believe that a measure that affords a meaningful and positive difference to a data subject (which is required under the GDPR) should be considered a mitigating measure in the context of the balancing test, if not at step (iv) then in all cases at step (ii) of the test. This would be consistent with WP217 (p42) which acknowledges that mitigation measures implemented as part of the balancing test '*may already be compulsory under the Directive*'. The Guidelines seek to rely on WP217 (referenced in paragraph 57, footnote 65) but respectfully the position adopted by the EPDB is not, in our view, consistent with WP217.

A good example to illustrate this point is the implementation of privacy enhancing technologies (PETs) that drive responsible innovation, creates a safer ecosystem for internet

users and can benefit organisations in a number of sectors from R&D and public health to online advertising. Google uses a range of PETs as a measure to assist it in meeting its obligations under the GDPR, such as its obligations of data minimisation and privacy by design. During the COVID-19 pandemic, we worked to produce, aggregate, anonymise and share datasets on community movement that have helped public health officials and researchers to manage the spread of the pandemic.

In the context of developing a new product, we consider carefully the GDPR principles, such as lawfulness, fairness and transparency. Although complying with the principles of data protection is a minimum requirement, this does not detract from Google's considered approach to the balancing test. More generally, to ensure compliance with the principles set out in GDPR, Google's products are developed from the outset with built-in protections to address data related risks, such as data leakage. This also includes the establishment of strong privacy safeguards and data minimisation techniques, as well as a conscious effort to ensure transparency around data practices.

The package of measures we implement at Google are designed to mitigate the risk to the data subjects. However, based upon the Guidelines, it could be argued that they are all required to meet the GDPR requirements meaning they would not be considered as part of the balancing test. This would be an unjust outcome and is counter-intuitive.

We would expect the EDPB to encourage mitigation measures to be implemented to protect the rights and freedoms of data subjects and that the implementation of these measures can be considered by controllers when weighing the risk to those data subjects. The approach set out in the Guidelines does not currently allow for this and, whilst we appreciate this is likely not the intention, it could incentivise some controllers to argue that many measures typically implemented to mitigate risk to individuals are in fact not *required* under the GDPR and are additional measures that can be implemented on a case-by-case basis only where necessary following an LIA.

Accountability - The DPO Role (paragraph 12)

The Guidelines suggest that a legitimate interests assessment should be made at the outset of processing with the involvement of the DPO (paragraph 12). This is quite a binary statement. Whilst the DPO retains responsibility for enabling compliance with the GDPR in an organisation and oversight of the work of their team, it may be impractical for large organisations to involve the DPO in every legitimate interests assessment. Rather, the role of the DPO in the process should be in proportion to the likely risks and the novel nature of the processing. It would be helpful if the EDPB could acknowledge this in the Guidelines and note that organisations may have a team of individuals who work together to assist the DPO in their role as contemplated in sections 3.1 and 3.2 of WP243 and more recently in the EDPB's report on the Designation and Position of Data Protection Officers.

Reasonable expectations (paragraphs 51-54)

We agree with the statement in the Guidelines that the reasonable expectations of the data subject play an important role in the balancing test. We would be grateful if the EDPB could acknowledge that the reasonable expectations of data subjects can change over time (for example, they would have undoubtedly changed since the WP217 was published).

Transparency (paragraph 68)

Google appreciates the importance of transparency and of informing data subjects of the situations where it relies on the legitimate interests ground as its lawful basis for processing, and setting out what those legitimate interests are in accordance with Article 13(1)(c)/(d) and Article 14(1)(c) and 14(2)(b) GDPR. In addition, Google also has processes in place to fulfil data subjects rights, including the right of access in accordance with Article 15 GDPR.

None of these legislative provisions require an organisation to provide a data subject with information about the balancing test, yet the Guidelines suggest that data subjects should be able to obtain information from a controller about the balancing test. The transparency and data subject rights provisions of the GDPR were carefully crafted as part of the legislative process. For example:

- the GDPR specifically requires data subjects to be provided details of legitimate interests relied upon where a controller seeks to rely on Article 6(1)(f);
- where an international transfer is subject to appropriate or suitable safeguards, the GDPR explicitly requires the data subject be informed of those safeguards and be given the right to access a copy;
- where processing is based upon the consent ground, individuals must be informed of the right to withdraw that consent; and
- where there is automated decision-making, a controller is required to provide data subjects with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing.

In addition, Article 35(9) provides a flexible mechanism for further engagement with a data subject in high-risk processing scenarios, whilst allowing organisations to protect their commercial interests and the security of processing operations. Conversely, there is no GDPR requirement to provide data subjects with details of the balancing test carried out and only a suggestion that this *can* be done in the EDPB's Transparency Guidelines. We respectfully suggest that the inclusion of this new requirement in the Guidelines is not consistent with, nor is it contemplated by, the GDPR and we would be grateful if it could be removed.

Compelling legitimate interests (paragraph 73)

In line with our general feedback on the Guidelines, the section on compelling legitimate interests again seeks to impose requirements that are excessive and disproportionate. The Guidelines suggests that, to invoke the legitimate interests ground under Article 21 GDPR, the ground should be *essential* to the controller or third party for it to be considered compelling. The Guidelines therefore effectively seek to change the requirement of "compelling legitimate interests" to "essential legitimate interests" which is disproportionate, not consistent with the language of the GDPR itself, and significantly restricts the ability of organisations to rely on this ground. We would be grateful if the EDPB could reconsider this point.

Children's personal data (paragraphs 94 and 95)

Google understands and appreciates that the processing of children's personal data comes with great responsibility with the best interests of the child requiring careful consideration as part of the balancing test, with appropriate safeguards implemented to protect those interests.

In line with our general feedback on the tone of the Guidelines, we recommend the Guidelines are revised to provide a positive use case for reliance on the legitimate interests ground to process children's data, subject to careful consideration and prioritisation of those interests as part of the three-part test. The onus should be on the controller to carry out that three-stage test and to take careful account of the impact on children's rights and interests; the Guidelines undermine that process as drafted.

November 2024