DIGITALEUROPE

20 NOVEMBER 2024

Legitimate interest: One of six legal bases to process personal data

Executive summary

We welcome the European Data Protection Board's (EDPB) draft Guidelines on legitimate interest, which are crucial given evolving case law on the topic.[1] The draft Guidelines are particularly relevant because legitimate interest is a key legal basis under the General Data Protection Regulation (GDPR) applicable to new and developing technologies.[2]

Legitimate interest is one of six equally valid legal bases under the GDPR, and is particularly relevant in scenarios where other legal bases, such as consent, are impractical or insufficient. This is notably the case when addressing issues such as cybersecurity, automated decision-making or fraud prevention. Furthermore, legitimate interest is often the only viable legal basis to process large datasets, whether to develop AI tools or to build data sharing ecosystems.[3]

Organisations require clarity and proportionality to apply legitimate interest effectively and responsibly. This paper outlines recommendations to avoid any complexities that would restrict legitimate interest's practical utility:

- To recognise that in some cases, such as with technologies that rely on wide datasets, legitimate interest can be the only available legal basis;
- With respect to the GDPR's risk-based approach, to note that the purpose for legitimate interest may evolve over time, without constantly being subject to full re-assessments;

[1] Draft Guidelines 1/2024.

[2] Regulation (EU) 2016/679.

[3] We have detailed the growing complexity of EU data rules in our flagship reports *Data transfers in the data strategy: Understanding myth and reality*, available at https://cdn.digitaleurope.org/uploads/2022/06/DIGITALEUROPE_Data-transfers-in-the-data-strategy_Understanding-myth-and-reality.pdf, and *The Single Market Love Story: 10 digital actions to save the 30-year marriage*, available at https://cdn.digitaleurope.org/uploads/2024/02/DIGITAL-EUROPE-THE-SINGLE-MARKET-LOVE-STORY-FINAL-WEB.pdf, as well as in our contribution to the GDPR review, *The GDPR six years in: From harmonisation to alignment*, available at https://cdn.digitaleurope.org/uploads/2024/02/The-GDPR-six-years-in-from-harmonisation-to-alignment.pdf.

DIGITALEUROPE
Rue de la Science, 37, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

- To avoid that the controller is required to go 'beyond what is strictly required' by the GDPR to use legitimate interest as a legal basis;
- To avoid additional burden placed on the controller in guidance on the use of legitimate interest for specific applications (inc. automated decision-making, security and fraud prevention).

Table of contents

One of six legal bases

We welcome the draft Guidelines' recognition that legitimate interest should not be treated as a 'last resort' for rare or unforeseen circumstances where other legal bases might not apply. Equally, it should not be automatically selected or unduly extended based on a misconception that it is less restrictive than other legal bases.

The introduction's emphasis on the equal application of all GDPR legal bases reinforces this balanced approach, which aligns with the principles outlined in the WP29 Opinion 06/2014. This earlier Opinion also highlighted the importance of legitimate interest in avoiding overreliance on other legal bases.

We also appreciate the EDPB's detailed explanation of the threefold test for assessing the validity of legitimate interest as a legal basis. Unlike other legal bases under Art. 6(1) GDPR, legitimate interest explicitly includes exceptions, arguably making it one of the most comprehensive and nuanced legal bases.

To ensure its effective application, the interplay of the GDPR provisions, relevant case law and the Guidelines should provide greater legal clarity, enabling organisations to fully and confidently utilise legitimate interest where appropriate.

Applying legitimate interest to evolving technologies

The draft Guidelines rightly emphasise that legitimate interest should not serve as an 'open door' for data processing without adequate safeguards.[4] For this reason, it is essential to fully acknowledge scenarios where legitimate interest is the only feasible option for controllers.

For example, in the context of AI models trained on datasets comprising billions of data points – often a mix of personal and non-personal data – obtaining individual consent is technically unfeasible. Recognising that legitimate interest is the only suitable legal basis aligns with para. 12 of the draft Guidelines, which notes that in some cases, the last two steps of the proposed balancing test may effectively merge.

We welcome the draft Guidelines' acknowledgment of further compatible processing pursuant to Art. 6(4) GDPR.[5] The draft Guidelines state that the compatibility assessment will 'in general' be relevant for further processing 'in the legitimate interest of a third party.' However, the final Guidelines should recognise that further compatible processing also pertains to the data controller itself.

---

[4] Para. 9 of the draft Guidelines.

[5] Para. 26, ibid.

The requirement to reassess the purpose in instances such as fraud detection may impose an excessive burden on controllers. In these cases, detailed information beyond the prevention of fraudulent behaviour may not provide significant value to the data subject, and could hinder the agility of fraud prevention measures.

Regarding the nature of data to be processed, instead of setting the standard to 'whether it is objectively possible to infer sensitive information,' the final Guidelines should adopt the threshold adopted by the Court of Justice of the EU (CJEU) of a 'certain degree of probability' for identifying special category data under Art. 9 GDPR.[6] This approach would ensure greater consistency and feasibility of the required legal standards.

Foresight in the balancing exercise

Technical feasibility should be a key consideration in transparency obligations, particularly given the volume of data and the methods available for retrieving the source of information. The documentation requirements outlined in para. 68 of the draft Guidelines exceed the scope of Arts 13 and 14 GDPR. These obligations should remain aligned with the GDPR provisions to ensure proportionality and feasibility for organisations.

When assessing the potential consequences of processing, some of the examples listed, such as the 'potential future decisions or actions by third parties that may be based on the personal data processed by the controller or the 'emotional impact,' may be difficult, if not impossible, for a processor to predict. The broader and more complex the dataset, the harder it becomes for the controller to foresee all possible outcomes.

Recital 47 GDPR already addresses the reasonable expectations of the data subject, and the final Guidelines should further recognise the inherent limitations in predicting all potential consequences. A best-effort approach, offering flexibility within the assessment, would be more practical and aligned with real-world processing scenarios.

Regarding mitigating measures and additional safeguards, these must be integrated into the balancing test itself, rather than imposing requirements that go beyond the GDPR. A consideration of mitigating measures and safeguards is quintessential to the balancing test itself. The suggestion in the draft Guidelines that 'going beyond what is strictly required under the GDPR may be seen as an additional safeguard' is therefore illogical, and would unduly restrict the correct use of legitimate interest.[7]

We welcome the draft Guidelines' acknowledgment that information can be provided in various formats, such as privacy statements and notices, to reduce

[6] Case C-21/23.

[7] Para. 62, ibid.

fatigue.[8] This flexibility is especially important given the extensive information required to support the balancing test.

To further assist organisations, particularly SMEs, the inclusion of templates or model questions for conducting the balancing exercise would be invaluable. Additionally, the final Guidelines would benefit from more positive examples demonstrating where legitimate interest can be appropriately applied, including the balancing measures contemplated as part of the balancing test. Similarly, detailed examples addressing the three-pronged test and the varying levels of transparency needed for different cases would provide much-needed clarity for legal practitioners and organisations alike.

Further guidance for specific applications

The EDPB introduces an additional set of criteria for the balancing test in the context of automated decision-making.[9] However, Art. 6(1)(f) applies uniformly across all technologies, as the GDPR is explicitly technology neutral. Additional blanket constraints on specific technologies must be avoided, as they would undermine the GDPR's existing provisions and neutrality.

The final Guidelines should reflect the current geopolitical and technological landscape regarding processing for security purposes, which has evolved significantly since the issuance of the WP29 guidance. The rise in the scale, rapidity and sophistication of cyber threats requires organisations to maintain flexibility in their responses.

Whilst the draft Guidelines rightly caution against 'excessive processing of personal data,' they should clearly state that addressing security threats, as a rule, constitutes a correct application of legitimate interest. The final Guidelines should fully reference Recital 49 GDPR by affirming unequivocally that ensuring network and information security 'constitutes a legitimate interest,' rather than stating it *may*. Furthermore, the final Guidelines would benefit from the inclusion of additional positive use cases for legitimate interest, complementing those previously outlined by the WP29.

We also encourage the EDPB to provide more specific guidance on the appropriate legal basis for situations where organisations must cooperate to address cybersecurity threats and ensure a secure ecosystem, even in the absence of a formal legal obligation. This would address a critical gap in the framework for collaborative security efforts.

In para. 102, the separation of fraud prevention from fraud detection appears artificial, as detection is an integral component of prevention. Greater clarity is needed regarding whether fraud prevention encompasses activities such as countering money laundering, money mule schemes, identity theft and other forms of fraudulent behaviour. Consent, in these contexts, would be

[8] Para 68, ibid.

[9] Para 82

inappropriate, particularly for individuals who have previously committed fraud against the controller or in scenarios involving automated trend and pattern analysis for fraud detection.

By addressing these points, the final Guidelines can better balance the protection of data subjects' rights with the operational realities of organisations navigating a changing security environment.

FOR MORE INFORMATION, PLEASE CONTACT:

Beatrice Ericson

Manager for Data Economy & Privacy

beatrice.ericson@digitaleurope.org / +32 490 44 35 66

Alberto Di Felice

Policy and Legal Counsel

alberto.difelice@digitaleurope.org / +32 471 99 34 25

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract, and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies. Our membership represents over 45,000 businesses that operate and invest in Europe. It includes 108 corporations that are global leaders in their field of activity, as well as 41 national trade associations from across Europe.

DIGITALEUROPE
Rue de la Science, 37, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20