Opinion on ***"Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR Version 1.0"*** from the EDPB adopted on 8 October 2024

1. **Our Feedback on Section I (**Introduction**)**

We believe that the introduction of the Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR Version 1.0 (**"Guidelines"**) provides a clear and concise overview of the purpose, scope, and importance of the Guidelines. It effectively sets the stage for the detailed guidance provided in the subsequent sections. We do not have any specific feedback or concerns regarding the introduction.

2. **Our Feedback on Section II (**Elements to Be Taken into Account When Assessing the Applicability of Article 6(1)(F) GDPR as a Legal Basis**)**

a. Conditions for Pursuing a Legitimate Interest

The initial sections of the Guidelines provide a comprehensive and structured explanation of the legal basis for legitimate interest under **Article 6(1)(f) of the GDPR**. The Guidelines clearly outline the three cumulative conditions that must be met—pursuit of a legitimate interest, necessity, and the balancing test. However, while the foundation of the Guidelines is clear, some sections could benefit from further clarification, particularly in areas where vagueness might lead to interpretive challenges for businesses.

The Guidelines define a legitimate interest as needing to be lawful, clearly articulated, and "real and present" rather than speculative [cite: 17].

- **Need for Positive Examples to Demonstrate Legitimate Interest**

Pages 8-9 include an example for each criterion [cite: 18]. However, the Guidelines primarily focus on negative examples where legitimate interest cannot be relied upon. While these examples clarify the limitations of legitimate interest, they do not provide sufficient guidance on situations where it can be legitimately relied upon.

To enhance the effectiveness of the Guidelines for businesses, we recommend that the EDPB include examples of scenarios where data controllers can successfully rely on legitimate interest by meeting three conditions at the same time.

- **Commercial Interest as a Lawful Legitimate Interest Should Be Elevated**

The Court of Justice of the European Union (CJEU) has recently ruled[1] that commercial interests can qualify as legitimate interests, which is highly relevant for the business

[1] Judgement CJEU 4 October 2024, C-621/22 (Koninklijke Nederlandse Lawn Tennisbond v Autoriteit Persoonsgegevens)

community. The reference to commercial interest is currently included in the footnotes related to the lawful nature of interests [cite: 17], stating that "legitimate interest is not limited to those enshrined in law, but it requires that the interest be lawful."

Given the importance of this ruling for businesses, we believe it should be elevated to the main body of the Guidelines. We believe that it should be given greater visibility and further explanation within the main body of the Guidelines, particularly in the section discussing the conditions that can qualify as legitimate. Commercial interests are central to many businesses, especially those operating in competitive, data-driven sectors such as e-commerce, fintech, and digital services.

b. Clarifications Needed on the Analysis of the Necessity of the Processing to Pursue the Legitimate Interest

The Guidelines state that processing is necessary if the legitimate interests "*cannot reasonably be achieved just as effectively by other means less restrictive of data subject rights.*" [cite: 29] However, the terms "reasonably" and "just as effectively" may be open to interpretation for businesses and lead to inconsistent applications of the necessity test and uncertainty when relying on legitimate interest. Moreover, while the Guidelines briefly mention that demonstrating necessity for third-party interests can be more challenging [cite: 30], it doesn't provide sufficient guidance on how to assess necessity in such cases.

We believe that the Guidelines should offer more specific criteria for assessing "reasonableness" and "effectiveness" when evaluating alternative means. Also, the EDPB should include practical examples demonstrating how the necessity test applies in various situations, including those involving third-party interests.

c. Methodology for the Balancing Exercise

- **Confliction and Redundancy Possibility on the Application of Article 9(2) and Article 6(1)(f) GDPR Together**

In [cite: 40], Section 2.1 of the Guidelines, footnote 47 states that “It should be reiterated that meeting the conditions laid down in Article 9(2) GDPR does not automatically fulfill the conditions of Article 6(1)(f) GDPR. If this legal basis for processing is to be used, the controller must satisfy the requirements of both GDPR provisions when processing special categories of personal data.”

This interpretation suggests that controllers processing special categories of personal data must satisfy both Article 9(2) and Article 6(1)(f) GDPR requirements if invoking legitimate interest as a legal basis. However, we find this dual requirement redundant and potentially conflicting.

Article 9 GDPR specifically governs special categories of personal data and is intended to afford heightened protections to individuals due to the sensitivity and risks associated with these data types, such as health information, racial or ethnic origin, or biometric data. The high

threshold required under Article 9 provisions sets a lex specialist, meaning these specific conditions are intended to override more general rules when addressing special data categories. Therefore, meeting Article 9(2) criteria alone should sufficiently demonstrate that the processing is lawful, thus eliminating the need to invoke additional justification under Article 6(1)(f).

By requiring Article 6(1)(f) compliance even in cases meeting Article 9(2), the Guidelines introduce potential ambiguity for controllers in distinguishing the application of these provisions. This dual requirement creates a redundancy, as Article 9(2) standards already provide robust justification that arguably supersedes the balancing exercise of legitimate interest.

In cases where both Article 6(1) and Article 9(2) could apply, Article 9(2) conditions would inherently demand higher protection, making a balancing test redundant. For instance, processing necessary to protect the vital interests of the data subject or another person is deemed lawful under Article 6(1)(d); however, under Article 9(2)(c), additional safeguards are mandated, such as the data subject's inability to provide consent. This exemplifies that Article 9's specific criteria sufficiently ensure protection without needing supplementary validation through legitimate interest.

Subjectivity in "Broader Emotional Impacts" Evaluation in Further Consequences of the Processing

In Section 2.3, [cite: 46], while addressing the potential consequences of processing, the Guidelines reference *"broader emotional impacts resulting from a data subject losing control over personal information."* However, even though the Guidelines do reference potential "broader emotional impacts", it does not explicitly define the specific types of emotional harm, or the criteria for evaluating those harms. Therefore, we believe this terminology introduces excessive subjectivity into the legitimate interest assessment and warrants further clarification.

Emotional responses to data loss or misuse can vary significantly based on individual sensitivities, cultural backgrounds, and the specific context of the processing. Without objective criteria for measuring or evaluating such impacts, controllers are left with little guidance on how to incorporate them into the balancing test.

To address this ambiguity, we recommend the EDPB provide a more precise definition of "broader emotional impacts" by outlining specific types of emotional harm that may be relevant in the context of data processing, and offer guidance on how to evaluate the severity and relevance of these emotional impacts in the legitimate interest assessment to promote greater consistency and objectivity in applying the balancing test. If developing objective criteria proves challenging, we would like EDPB to consider removing "broader emotional impacts" as a factor in the legitimate interest assessment in order to ensure objectivity and consistency.

- **Prioritizing Clarity in Communication Over Documentation in Data Subject Information for "Reasonable Expectations"**

In Section 3, Reasonable Expectations of the Data Subject, particularly in cite [53], the Guidelines emphasize that *"reasonable expectations do not necessarily depend on the information provided to data subjects."* It further states that while failure to provide information can lead to data subjects being surprised by certain processing activities, merely fulfilling the information obligations outlined in Articles 12, 13, and 14 GDPR does not automatically mean that data subjects can reasonably expect a given processing.

While we agree that fulfilling the informational obligations under Articles 12, 13, and 14 of the GDPR does not automatically establish reasonable expectations, we believe that this approach may overlook a crucial aspect: the *accessibility* and *comprehensibility* of the information provided.

We argue that it may be more difficult for consumers to recognise relevant contractual provisions relating to data processing or to fully understand contractual provisions with heavy legal language[2] than privacy policies or notices with clear and clean language, particularly given that contractual provisions may be embedded in lengthy documents, making it less likely that the consumer will review them thoroughly. Therefore, relying on such provisions to establish reasonable expectations may be insufficient, especially for individuals without legal expertise, that is to say, an "average" data subject.

In contrast, clear and concise privacy policies or notices, written in plain language and readily available to data subjects, can have a significant role in shaping reasonable expectations. When data subjects are provided with easily understandable information about how their data will be processed, they are more likely to have realistic expectations and less likely to be unduly surprised by the processing.

We recommend that the EDPB considers prioritizing clear access to information over the documentation on this point. EDPB might also suggest that, in certain cases, going beyond standard privacy policies may be necessary to align with reasonable expectations. While a simple privacy policy may not be sufficient, we believe that providing clear, accessible communication regarding data processing practices beyond what is legally mandated in Articles 12, 13, and 14 could create reasonable expectations of data subjects and improve transparency. For example, documentation and demonstration of the relevant processing, maybe even visually, could properly widen the expectations of the data subject.

- **Exemptions to Average Consumer Criterion in "Reasonable Expectations" Could Also Include Qualifications and Experience of Targeted Data Subject Groups**

In Section 3, "Reasonable Expectations of the Data Subject," the Guidelines provide examples of contextual elements to consider when assessing reasonable expectations. However, we believe these examples could be expanded to include more specific professional contexts.

In the part where the Guidelines discuss characteristics such as the data subject's age, status as a public figure, and professional position, we believe that the EDPB should explicitly include

[2] Referencing footnote [61], where the following is indicated: *"it should be noted that contractual provisions regarding personal data may have a bearing on the reasonable expectations of data subjects"*

a reference to the *professional qualifications and experience of the targeted data subject group(s)*.

This is because some personal qualifications would alter the reasonable expectations of data subjects. We acknowledge the fact that it is difficult for the data controller to assess reasonable expections when it targets a large group of data subjects having different backgrounds, some services target specific data subject groups, which would have different expectations than an “average” data subject.

For example, a marketing professional using an e-commerce website providing tools for marketing and sales might reasonably expect that their data will be used to tailor advertisements or offers in line with their browsing or purchasing behavior.

Thus, we recommend that the EDPB incorporates "professional qualifications and experience of the targeted data subject group(s)" as an additional criterion into the list of contextual elements under [cite: 54] to enhance the clarity and comprehensiveness of the Guidelines.

- **Mitigating Circumstances Should be Structured More**

Lastly, in Section 4, *Finalising the Balancing Test*, the Guidelines address that the controller may consider introducing mitigating measures, which differ from the measures that the controller is legally required to adopt anyway to ensure compliance with the GDPR, to limit the impact of the processing on data subjects, in view of achieving a fair balance between the rights, freedoms, and interests involved. [cite: 56] It states that mitigating measures must go beyond what is already necessary to comply with these legal obligations under the GDPR. [cite: 57] Although it is a great measure for the data controller to manage the balancing and tilt it in the favor of both itself and the data subject, it is not sufficiently clear how to determine when a measure truly goes beyond those obligations, especially in the context of data security. If a data security measure is technically strong, should it be considered a mitigating measure in the balancing test, or if there are other mitigation methods rather than providing additional safeguards, what are they? All the examples given are providing data subject more flexibility in using their rights. If that is the main criterion or one criterion, it should be clarified. Moreover, we assess that the weight of the mitigating circumstances, in other words, what would happen when there are mitigating circumstances but other legitimate interest criterion is missing are unclear. For example, if the data controller allows the data subject to exercise the right to object without any of the limitations in Article 21 GDPR but the processing is beyond its reasonable expectations, would it be sufficient to assess that there is a legitimate interest?

Furthermore, the Guidelines leave some ambiguity regarding the procedural requirements following the adoption of mitigating measures. After implementing such measures, controllers are instructed to re-conduct the balancing test. But it is unclear whether implementing mitigating measures necessitates conducting a complete legitimate interest assessment, or just an assessment as to whether the circumstances are sufficiently mitigating to eliminate the facts affecting the balancing [cite: 58].

To address these concerns, we recommend that EDPB provides clearer guidance on the difference between basic measures and mitigating measures that go beyond the GDPR; clarify

the amount of weight the mitigating circumstances have over other legitimate interest criteria; explicitly state whether implementing mitigating measures requires a complete or partial reassessment of the legitimate interest.

3. **Our Feedback on Section III** (Relationship Between Article 6(1)(F) and Data Subject Rights)

In this section in the Guidelines, EDPB outlines the relationship between legitimate interests under Article 6(1)(f) GDPR and the rights of data subjects. It emphasizes the mandatory nature of data subject rights, how these rights should be interpreted when legitimate interest are pursued and the obligations of data controllers to clearly communicate the legitimate interests they pursue as part of their transparency requirements.

a. "Compelling Legitimate Grounds" Criterion Should be More Widely Assessed and Further Evaluated

When a data subject exercises their right to object, the controller may only continue processing if they can demonstrate "compelling legitimate grounds" that override the interests, rights, and freedoms of the data subject. According to the Guidelines, this criterion implies that only essential, overriding interests of the controller, or third-party beneficiaries of the processing, may meet this standard. For example, the Guidelines describe "compelling" grounds as those necessary to prevent immediate serious harm or severe penalties to the controller [cite: 73].

While we understand the importance of a high threshold for overriding interests, we suggest that the Guidelines consider allowing more flexibility in interpreting "compelling legitimate grounds" to better address the diverse operational contexts in which data processing often occurs. Specifically, when legitimate interest processing is integral to an organization's operations, requiring an extreme threshold may inadvertently create challenges not only for the controller but potentially for the data subjects themselves.

Example:

Consider a data controller utilizing cloud services as a cost-effective solution compared to owning dedicated hardware. The legal basis for these transfers is legitimate interest. If a data subject objects to the use of this cloud provider (e.g., due to perceived risks associated with the provider), ceasing this processing activity might necessitate a complete halt of services for the data subject or an impractical shift to a different provider solely for one individual. This change could pose undue financial or operational burdens on the controller, potentially affecting service continuity and data security.

This example illustrates how halting, restricting, or re-routing data processing for legitimate interest may cause unintended service disruptions or broader negative impacts on both the data subject and the controller. In light of these practical realities, we recommend that the "compelling legitimate grounds" threshold incorporate a degree of flexibility in cases where:

- The processing is a **significant or essential part** of the controller's core operations,

- The processing is **closely tied to other lawful processing activities**, where ceasing one activity may obstruct other necessary processes based on different legal bases,
- Complying with the objection would **cause tangible harm to the data subject** due to service disruptions or decreased data security,
- Complying with the objection would create **disproportionate consequences relative to the intended outcome**, such as halting multiple related processes.

4. **Our Feedback on Section IV** (Contextual Application of Article 6(1)(F) GDPR)

Section IV of the Guidelines offers context-specific guidance on applying legitimate interest in various situations, such as processing children's data, fraud prevention, direct marketing, and information security.

a. Processing of Children's Data

While Section IV appropriately highlights the importance of children's best interests, it falls short in providing the practical guidance necessary for businesses to effectively implement these principles. However, the statement "While this does not mean that there will never be a situation in which the interests of the child can be overridden, it does mean that the interests of children as data subjects should have high priority and will very often outweigh the interests of the controller or third parties" raises concerns due to its vagueness and lack of practical guidance. [cite: 94]

The EDPB's emphasis on prioritizing these interests is commendable, but without concrete examples and specific criteria, businesses are left with a subjective interpretation of "best interests," potentially leading to inconsistent applications and hindering the development of child-friendly online services.

We believe that businesses need clear illustrations of how to balance children's best interests with legitimate business needs in areas like age-appropriate design, online safety tools, and educational platforms. It would be more helpful if the EDPB provided **real-world scenarios** where the balancing test might allow for legitimate interest to prevail, perhaps in cases of public safety or minimal data processing with strong safeguards.

b. Processing by public authorities

While the section concerning the application of Article 6(1)(f) GDPR by public authorities clearly states that public authorities cannot rely on legitimate interest as a legal basis when processing data in the performance of their specific tasks, it leaves open the possibility for reliance on Article 6(1)(f) GDPR in "exceptional and limited cases", however, it does not provide concrete examples of what constitutes "exceptional and limited cases".

To ensure clarity and consistency in the application of the GDPR, we recommend that the EDPB provides more detailed guidance to public authorities on when they can rely on legitimate interest to offer clear and objective criteria for determining the types of activities

that fall outside the scope of "public tasks" and provide specific examples of permissible uses of Article 6(1)(f) for public authorities.

c. Processing for direct marketing purposes

The Guidelines touch upon the interplay between the GDPR and the ePrivacy Directive but could provide more detailed guidance on their relationship, particularly concerning the use of cookies and online tracking for marketing purposes. The widespread use of cookies in today's digital environment, where every website and application utilizes some form of tracking or analytics, raises critical questions about their compliance under GDPR.

The Guidelines state that Article 5(3) ePrivacy Directive requires consent for the use of tracking techniques, such as storing cookies or gaining access to information in the terminal equipment of the user, and when these techniques are used in the context of direct marketing activities. It also highlights the need to respect these consent requirements when cookies are used for direct marketing. [cite: 115]

However, given the large-scale nature of personal data processing through cookies, we believe that further clarification is necessary on how these types of cookies can fit within the legitimate interest framework. The interaction between legitimate interest and the consent requirements under the ePrivacy Directive remains a complex issue. Specifically, the recent CJEU ruling that recognized *purely commercial interest* as a legitimate interest, could impact the use of cookies, particularly non-essential first-party cookies that go beyond necessary operational use. For example, cookies used for purposes like market research, or advanced performance optimization may not be strictly necessary for the functioning of a website but are often essential for improving user experience or conducting legitimate business analysis. The Guidelines do not provide sufficient clarity on how such cookies might fit into the legitimate interest framework under Article 6(1)(f) GDPR, especially in light of the recent CJEU case law.

We recommend that the EDPB provides clearer guidelines on how legitimate interest can be applied to first-party cookies beyond those that are strictly necessary for website operation. Specifically, the EDPB should clarify whether commercial legitimate interest could apply to first-party cookies beyond those strictly necessary for website operation in light of the CJEU's ruling. We recommend that the EDPB provides more detailed guidance on the application of legitimate interest to first-party and third-party cookies. Specifically, it should clarify whether commercial legitimate interest could apply to first-party cookies that are not strictly necessary for website operation, such as those used for analytics, user experience optimization, and marketing research, especially in light of the CJEU's recognition of commercial interest as a legitimate interest.

d. Processing for the purpose of ensuring network and information security

In this section, the EDPB outlines the possibility of using Article 6(1)(f) GDPR as a legal basis for processing personal data to ensure network and information security. It emphasizes that the necessity and balancing tests must be carefully applied and references previous CJEU rulings,

including *Breyer* and *Meta v. Bundeskartellamt*, which highlight the importance of assessing whether less intrusive means could achieve the same security objectives.

While we appreciate the comprehensive overview provided in this section, we believe there is room for significant improvement in terms of clarity and practical guidance.

The Guidelines mention that the "objective of security cannot justify excessive processing of personal data" but do not provide clear criteria for determining what constitutes "excessive processing". [cite: 127] It mentions that the WP29 stressed in previous Opinions the risks inherent in certain security solutions (including firewalls, anti-virus and antispam), as they may lead to the large scale deployment of deep packet inspection and other kinds of intrusive analysis of communication content and meta data, which may have a significant impact on the outcome of the balancing test. However, it doesn't offer detailed guidance on the conditions for legitimate use of specific security measures, such as intrusion detection systems, firewalls, or anti-malware software.

This ambiguity may leave room for subjective interpretations and may lead to inconsistent application of the legitimate interest assessment. We recommend that the EDPB expands this section by providing more specific examples, clearer criteria for assessing "excessive" processing, and practical guidance on balancing security needs with data protection obligations.

Additional Comments:

Along with these, we believe it is also important for Section IV “Contextual Application of Article 6(1)(F) GDPR” to address the processing of personal data based on legitimate interest in the developing, training, and using **artificial intelligence (AI) models**. Indeed, including them in such guidance could facilitate the harmonization of perspectives across different data protection authorities, establish a framework for balancing tests specific to AI systems, and provide direction for ongoing AI advancements in compliance with both the GDPR and the AI Act.