Comments on the draft Guidelines 01/2024 of the European Data Protection Board

This paper exclusively reflects the views of its author.

On 8 October 2024, the European Data Protection Board published its draft Guidelines 01/2024[1] *"on processing of personal data based on Article 6(1)(f) GDPR"* (hereinafter referred to as Draft Guidelines or Draft).

The Draft Guidelines were issued just four days after the judgement of the Court of Justice of the European Union in Case C-621/22 (hereinafter: Judgment),[2] and the said judgment was incorporated into the Draft, which is a laudable performance.

With the judgment and the Draft, the "fog" surrounding legitimate interest seems to be lifting, however, the Draft misses the opportunity to clarify some other important points.

1. Relationship with the old opinion

The Draft states that it *"build[s] upon and update[s] [emphasis added – Zs.B.] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC of the Article 29 Data Protection Working Party"*.[3] This will cause confusion in the practice and will oblige to decide on which elements of the old opinion are still "in force" and which are not. For the sake of legal clarity, the Draft should replace (and "repeal") the old opinion.

2. Statement of the obvious

In my view, which I have been saying since 2018, two things are necessary to apply the legal ground of "legitimate interest":

a) there must be a legal order in the light of which the legitimacy of the interest can be judged,
b) there must be a mechanism designed to judge on the legitimacy of the interest.

Normally, both exist in a country, but especially the mechanism mentioned in point b) might require further assessment.

Thanks to the Judgement, everybody can now know (and should accept[4]) that *"the concept of 'legitimate interest'… is not limited to interests enshrined in and determined by law"*, it is

[1] See at the following link https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf
[2] Judgment of the CJEU of 4 October 2024 in Case C-621/22 (*Koninklijke Nederlandse Lawn Tennisbond* vs. *Autoriteit Persoonsgegevens*), (ECLI:EU:C:2024:857), https://curia.europa.eu/juris/document/document.jsf?text=&docid=290688&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=4086618
[3] Paragraph 5 of the Draft
[4] Including the data protection supervisory authorities

enough if *"the alleged legitimate interest [is] lawful"*.[5] Interest has, therefore, only one attribute, "legitimate", or, in other words, "lawful". Precisely articulated" and/or "real and present"[6] are therefore not attributes of the interest– the Judgment did not impose such conditions. Such criteria might be examined in the 2nd step of the three-step assessment,[7] i.e. when the necessity of processing must be examined. So, the first condition mentioned above is in place.

The Draft fails to realise the second condition, at least it does not mention anything in this regard, although, from the perspective of the application of the 1st step of the three-step assessment, this issue is essential. The "interest" can, theoretically, cover any kind of real-life situations, but, due to the second subparagraph of Article 6(1) GDPR, mainly real-life situations between private parties (i.e. civil law situations) should be considered under the GDPR. However, considering the arguments of the CJEU in Case C-252/21,[8] it is not evident at all that data protection supervisory authorities can always assess the legitimacy of an interest, but other authorities, and—due to the nature of the relationship of the parties (the controller and the data subjects)—the courts can be authorised to make a judgment on the given interest, in accordance with the national legislation. The existence and the legitimacy of an interest, therefore, are preliminary questions for the data protection supervisory authorities. The procedural consequences of this should be examined by the Draft, including the kind of rights the data subject whose data would be disclosed to the requesting "third party" can exercise before disclosure.

3. Can law determine "legitimate interest"?

Briefly, not really. Member States or the Union may enact legal rules with regard to point (c) and (e) of Article 6(1) GDPR (i.e. "public task" and "legal obligation"[9]). In this regard, the general reasoning for the Hungarian draft GDPR-amendment act[10] clearly stated, theoretically rightly, that the provisions of those sectoral data processing laws which are based on legal grounds other than points (c) and (e) of Article 6 GDPR must be deregulated.[11] Therefore, the Draft Guidelines should also be revised in order to remove any examples that may be considered as law-determined "legitimate interests".

Even if we accept that the law might determine "legitimate interests", the next question is what should be balanced in that case? The essence of processing based on "legitimate

[5] Paragraph 40 of the Judgement and the decision

[6] See para. 17 of the Draft. It must be added that these categories are just playing with words, and cannot be considered as „objective" criteria, and, even the judgment of the CJEU in Case C-708/18 did not give clear guidance on how to interpret "real and present" interest. This leaves room for arbitrariness by the data protection authorities, taking into account that making a decision on a data processing activity based on Article 6(1)(f) GDPR is necessarily hypothetical since it is about the future. One can also argue against if "disclosure of data for purposes of transparency and accountability" (paragraph 23) is really "precisely articulated" and/or "real and present".

[7] See Draft, part II.

[8] Judgment of the CJEU of 4 July 2023 in Case C-252/21 (*Meta v. Bundeskartellamt*), (ECLI:EU:C:2023:537),

[9] See Article 6(2) and (3) GDPR.

[10] Published as Act XXXIV of 2019 on amendments to the laws necessary for the implementation of the European Union's data protection reform (In Hungarian: 2019. évi XXXIV. törvény az Európai Unió adatvédelmi reformjának végrehajtása érdekében szükséges törvénymódosításokról)

[11] See general reasoning for Act XXXIV of 2019 on amendments to the laws necessary for the implementation of the European Union's data protection reform

interest" is that the controller considers its own interests, the interests of the data subjects, and then it compares these two kinds of interests to decide which are stronger. In other words: the balancing of interests might favour the data subject as well. However, in case of law-determined "legitimate interest" (*"ex lege legitimate intertest"*), the controller can rely on the fact that (i) the legislator has already defined the interest, and that interest is lawful (1st step), and by doing so (ii) the legislator has already decided on the precedence of the controller's interest over those of the data subjects (3rd step), and, therefore, the only issue that might be done is to check whether the conditions of data processing meet the requirement of the necessity and proportionality principle (2nd step). The possibilities of the data protection supervisory authorities are also aligned with this, i.e. said authorities cannot question the existence and the legitimacy of the controller's interest, nor if that is overridden by the data subject's intertest. It must be seen, however, that some such "ex lege legitimate interests"[12] are *not an interest* but a *right* that is provided by law, and the given person can exercise this right without taking into account any interest of the other party, because the legislator made the "balance of interests" of the parties (be it contracting parties or parties between them the relationship originated from, for example, a damage) for this purpose.[13]

Last, but not least, the Draft failed to realise that some "legitimate interests" that the Draft Guidelines analyse are not "legitimate interests" but legal obligations or fall under other legal ground(s). For example, the Draft Guidelines state that *"Measures to ensure an appropriate level of network and information security may entail processing of personal data. Such processing activities may, in principle, be based on Article 6(1)(f) GDPR, provided that its conditions (including the necessity and balancing tests) are complied with. This was acknowledged – although indirectly – by the CJEU in Breyer,[14] as well as in Recital 49 GDPR, and in Recital 121 of Directive (EU) 2022/2555."*[15] However, one of the **legal obligations** of the controller directly stemming from Article 32 GDPR is to *"implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk"*, which includes the obligation "to ensure an appropriate level of network and information security". Further, processing of personal data for the protection of the rights of another natural or legal person or *for reasons of important public interest* of the Union or of a Member State[16] is not "legitimate interest" but either a legal obligation or exercising a public authority, i.e. it falls under point (c) or (e) of Article 6(1). Lastly, public bodies are generally obliged (while private entities or natural persons only in given cases) to *report alleged criminal acts* (or other infringements) to law enforcement authorities. Such obligation is, for sure, a legal obligation, not a "legitimate interest". Classifying such obligations as "legitimate interest" is a serious mistake in the Draft. The fact that the data processing in question is based on legal obligation does not exclude that the controller determines some elements of the data processing in accordance with Article 6(3) GDPR.

[12] Primarily the "establishment, exercise or defence of legal claims"

[13] See in detail in the article „Thoughts on the legal grounds of data processing in the GDPR" available at https://www.linkedin.com/pulse/thoughts-legal-grounds-processing-gdpr-zsolt-b%C3%A1rtfai-ll-d-ll-m/

[14] The reference to the Breyer-case seems to be thoughtless, because the referred statement (para. 60 of the Breyer-case) is about the cases under point 4 below (Legitimate interests pursued by public authorities), but the application of this statement of the Court is no longer possible since public bodies cannot refer to the legal ground of „legitimate interest" any longer.

[15] Paragraph 126 of the Draft.

[16] Article 18(2) GDPR, cited in para. 89 of the Draft

4. Legitimate interests pursued by public authorities

The second subparagraph of Article 6(1) GDPR reads as follows: *"Point (f) of the first subparagraph* [i.e. the legitimate interest] *shall not apply to processing carried out by public authorities in the performance of their tasks."*

The Draft acknowledges that this provision *"do[es] not prevent from relying, in exceptional and limited cases, on Article 6(1)(f) GDPR when the processing is not linked to or does not relate to the performance of their specific tasks or the exercise of their prerogatives as public authorities, but concerns, where permitted by the national legal system, other activities that are lawfully carried out."*

Beyond this, the Draft does not deal with this issue, although it would deserve more attention. In modern states, respective public authorities operate some core databases (e.g. civil registry, registry of vehicles etc.). This is their core task, including that these public authorities provide information from these databases (otherwise there is no point in these centralised databases). Although I am not aware of the concrete legal rules of each country, but I hardly believe that a person could not request personal data from these core databases if his/her/its request is fully justified (e.g. the requester wants to get to know the address of a person against whom he/she/it wants to put forward a legal claim). To provide such information to individual requesters is *in* the tasks of these public authorities, such activity cannot be considered as "not linked to their specific tasks". **Therefore, given public authorities *do* apply Article 6(1)(f) GDPR in favour of "third parties" and their legitimate interests, as their core task.** The poor quality of the text of the GDPR is not the fault of the EDPB, but the Draft should take realities into account.

5. Other issues

a) Although the Draft, by referring to an opinion of Advocate General Szpunar, states that *"the GDPR does not establish any hierarchy between the different legal bases laid down in Article 6(1)"*,[17] from the Judgement one can conclude the opposite, since the Judgement states that *"In the absence of such consent, [emphasis added – Zs.B.] or where that consent is not freely given, specific, informed and unambiguous, … such processing is nevertheless justified where it meets one of the requirements of necessity mentioned in points (b) to (f) of the first subparagraph of Article 6(1)"* of GDPR.[18] The Draft should clarify this.

b) There seems to be an inconsistency between the statement in footnote 61 and the second paragraph of Example 5 (reasonable expectation of data subjects based on contractual provisions).

c) While the Draft rightly cites that *"the specific legitimate interest(s) pursued must be precisely identified and communicated to the data subject in accordance with Article 13(1)(d) and 14(2)(b) GDPR"*, in the paragraph the Draft extends beyond the GDPR (i.e. "creates" law instead of "interpreting") when its states that *"information to the data subjects should make*

[17] Paragraph 1 of the Draft
[18] See footnote 9 in the Draft.

it clear that they can obtain information on the balancing test upon request".[19] Nothing in the GDPR (even Article 15) supports the latter statement, i.e. the data subjects don't have such rights, and the controllers don't have such obligations.[20]

d) Neither the GDPR, nor the Draft take reality into account when it comes to the assessment of fraud prevention. Now it is a general practice (based on legal requirements) that the payments (including international payments) are performed "immediately" (i.e. within seconds). On the other hand, however, financial institutions are also obliged to operate fraud prevention solutions which requires automated decision-making. If such fraud prevention solutions were based on "legitimate interest" (as the Draft suggests[21]), there would not be proper legal grounds for those solutions.

* * *

In sum, the Draft Guidelines, although they provide guidance in some cases, they are seemingly unable to cope with the complexity of real-life cases to which the rules of the GDPR should be applied. It may result in guidance that cannot be used in practice and will create more uncertainty than it could probably solve.

Lastly, the EDPB should consider not number their drafts (just when they are adopted after public consultation), since, in case of change in the drafts, it is difficult to follow which version we are talking about in a given case.

Zsolt Bártfai

[19] See paragraphs 67 and 68 of the Draft.

[20] Obliging controllers to do so by the data protection subpervisory authorities seems to be ultra vires. See for example the decision of the Hungarian DPA (NAIH/2019/2402 határozat), which also stated that the balancing test cannot be business secret. This latter statement is particularly worrying, since a good balancing test *does* contain business secrets.

[21] See point 3 of Part IV of the Darft.