

Comments on the Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR

From: Dagital Legal, s.r.o, Privacy & Technology Law Firm, Bratislava
Date: 20th November 2024

Dear All,

We would like to take this opportunity to comment on the Board's Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR (the "**Guidelines**"). The concept of the legitimate interest and conducting the balancing exercise of legitimate interest assessment (the "**LIA**") is one of the most important concepts and obligations under the GDPR and also under ePrivacy rules. We pride ourselves to have conducted several hundreds of different of LIA scenarios in practice. We also pride ourselves to have developed and to continuously develop our own methodology and tools for LIAs. We feel Guidelines do not consider the established practice and do not provide relevant and practical examples. We have strong objections against several key points in the Guidelines. We strongly recommend considering these points when preparing the final version of the Guidelines:

1. To the first "**condition**" of the 3-stage test

We understand that the Guidelines follow-up on the recent CJEU judgement in case C-621/22 (*Koninklijke Nederlandse Lawn Tennisbond v Autoriteit Persoonsgegevens*) that followed-up on the previous CJEU judgement in case C-252/21 (*Meta Platforms Inc. v Bundeskartellamt*). In these cases, the CJEU confirmed the 3-stages of the LIA while referring to the first state or condition as: "*first, the pursuit of a legitimate interest by the data controller or by a third party.*"

We believe the Guidelines should put more emphasis on the wider aspect of legitimacy than on the distinction of whether the legitimate interest is pursued by the controller itself or a third party.

That distinction is important at various places and stages of the LIA but is hardly a separate condition that needs to be met. This is because the legitimate interest is always pursued by the controller or a third party. Also, is always relied upon as a legal basis only by the controller doing the balancing exercise. In addition, in most cases where also a third-party legitimate interest is invoked, it is simultaneously a legitimate interest of the controller. Very few controllers rely on the legitimate interest that is not pursued by them, but solely by a third party.¹ This should be more evident from the Guidelines.

We also feel this aspect and discretion of the controller as to whether to pursue the legitimate interest is lacking in the CJEU's case-law and believe the Guidelines should address this.

¹ We do not know of such situation where only 3rd party's legitimate interest is pursued. If such situation exists, we would welcome such example to be mentioned in the Guidelines.

In joined cases C-17/22 and C-18/22 the CJEU was dealing with preliminary question whether some processing could be carried out by the controller based on the legitimate interest pursued by a third party without realizing that such question was irrelevant. It was irrelevant because the controller in question did not decide to rely on such legitimate interest and did not pursue it. In fact, the controller has opposed such legitimate interest and did not want to conduct the processing. The unsurprising fact that it could invoke such legitimate interest does not change the controller's discretion to ultimately freely decide if to pursue it or not.

2. To the 2nd test (necessity)

We believe the necessity assessment put forward in Guidelines is too simplistic, narrow and might lead to enforcement backlash against anything based on the legitimate interest: *"...it should be ascertained whether the legitimate interests pursued cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental rights and freedoms of data subjects, also taking into account the principles enshrined in Article 5(1) GDPR. If such other means exist, the processing may not be based on Article 6(1)(f) GDPR."*

The problem we face every day is the never ending technological development. What used to be a department of human beings in corporations is now a big data algorithmic recommendation system. See fraud prevention in financial sector and how it evolved in last 10 years.

Guidelines are silent on what **less restrictive** means and what **reasonably achieved just as effectively** means. What is less restrictive, an algorithm or human? What do we consider in restrictiveness, the scope of data and amount of data subjects scanned by the system in a second or the human curiosity, biases and human errors that can happen on a much smaller data sample? Can reasonably just as effective be +/- 20 percent more/less effective or +/- 50 percent more/less effective? There is no methodology, and no examples used in the Guidelines to demonstrate the thinking we should employ here. The risk is that without expanding here, supervisory authorities will just adopt too restrictive approach.

Obviously, there needs to be more flexibility when analysing the necessity. We can put forward the best practice we employ. First, usually there is always an alternative that is less restrictive due to the technological development. We ask, how was this done in past and by doing so we usually identify a less restrictive alternative. For example, how was the property, life and health protected in front of the public buildings before CCTV systems? By guards or policemen standing there and monitoring the security. Was it less restrictive? Possibly yes. Was it as effective? No. Therefore, CCTV system is necessary despite having the army of guards around the country would be less restrictive to privacy of data subjects, but immensely more expensive and immensely less practical and effective. This simple example proves we need to consider and balance two categories:

- one is the weight, percentage or value of restrictiveness; and
- the other the weight, percentage or value of implementation costs, effectiveness and practicality.

Even if something is more restrictive and intrusive by 5 percent, it can be thousand of percents more effective, cheaper and practical and therefore can meet the necessity test. And the technological development usually meets this analogy. Therefore, it is the balance of these two that we should be considering, not just merely ask what is less restrictive out of similarly practical solutions. Therefore, we refer to the whole LIA as the balancing exercise because we balance opposite values in each and every step, not just in the 3rd test.

We believe the Guidelines should put more emphasis on weighting and measuring of the restrictiveness and effectiveness of the closest alternative solution in the 2nd test.

3. To the 3rd test (proportionality)

Section C starting on page 12 of the Guidelines is titled “Methodology” but there is no methodology in Section C explained, mentioned or described in any way. To say we need to “**strike a balance**” is not enough. Although we fully agree with the aspects mentioned paragraph 32, this list is not exhaustive at all² and simply “**identifying and describing**” these is not enough. There are existing decisions of the supervisory authorities where these simple and descriptive documents were not enough to comply with the principle of accountability. There must be some measuring, weighting, putting values to or counting of these two opposing sides to the measurement with quantifiable results. If these measurements are left for individual’s discretion – the legitimate interest will always override – practice the EDPB should oppose. Please bear in mind that the organization that seeks to pursue the legitimate interest is doing the assessment and therefore it has natural bias towards its own overriding result.

We do not believe there is a single correct methodology as there might be multiple different methodologies available. **However, we do believe that some fixed and common requirements of these methodologies need to be established by the Guidelines.** Otherwise, the risk is decreasing level of data protection compliance. It is simply not enough to identify and describe these four aspects and call this a methodology of conducting LIA.

In addition, there are no examples used for the 2nd and 3rd test. Why not to establish with examples what legitimate interests usually meet the two most important tests of the LIA?

4. To the relationship between the LIA and the DPIA

Guidelines put too much emphasis on assessing “impact” on the data subjects though reference to interests, fundamental rights and freedoms. The reference to interests, fundamental rights and freedoms is made in Article 6(1)(f) solely in relation to balancing, i.e. to assess if these interest, rights and freedoms override or if the legitimate interest overrides. In addition, Article 6(1)(f) refers only to interests, fundamental rights and freedoms, **which require protection of personal data.** It does not refer to general catalogue of the fundament rights and freedoms.

Legitimate interest is a legal basis. The LIA is an exercise that the controller undertakes to answer if the processing of personal data can be done legally. At no point the GDPR requires – in connection with the legitimate interest – to undertake any human rights impact assessment. LIA is not an impact assessment as such. That is the DPIA under Article 35. Guidelines mention “**impact to data subjects**” 36 times and by doing so, mix up the LIA with DPIA. This should be avoided.

We believe the Guidelines should focus more on how to balance interests, fundamental rights and freedoms of data subjects (which require protection of personal data) with the legitimate interest pursued rather than on assessing the impact on the data subjects’ fundamental rights and freedoms which is for the DPIA to cover.

5. To the relationship between legitimate interest and purpose of processing

Paragraph 14 of the Guidelines presents a view that the legitimate interest is wider and broader term than the purpose of processing:

² Rather, this list should be expanded by further general aspects but also left opened for controllers to introduce other case-by-case specific aspects to be considered.

“A “purpose” is the specific reason why the data are processed: the aim or intention of the data processing. An “interest”, on the other hand, is the broader stake or benefit that a controller or third party may have in engaging in a specific processing activity.”

We strongly disagree with such view and believe only these two options are possible under the GDPR:

- either the purpose of processing and legitimate interest have the same meaning and scope;³ or
- the purpose of processing is wider and broader term which can encompasses multiple different legitimate interests pursued towards the same unifying purpose.

The purpose is the broadest “building stone” of the data protection compliance which is supported by the fact that almost all basic principles under Article 5 refer to the purpose of processing and all information obligations under Article 13 and 14 must be construed around and provided separately for each purpose of processing. There is nothing higher or broader than purpose of the processing. Even the Guidelines confirm that on multiple occasions.

Likewise, there is no general objection under Article 21(1) against the whole purpose of processing.⁴ The objection relates only to the **processing** based on legitimate interest, including **profiling** based on legitimate interest. There might be more legal bases for the same purpose and some processing within the same purpose might be based on consent, contract or legal obligation. Therefore, processing and profiling are clearly more narrower terms than the whole purpose. If the objection (against the legitimate interest) is in fact only against partial processing operations, how could the legitimate interest be a broader term than the purpose? Clearly, Article 21 confirms the opposite.

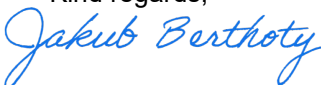
We believe the Guidelines should not confirm the legitimate interest is wider and broader term than the purpose of processing, because it simply isn't. One finds that when objecting to something based on legitimate interest.

6. To the relationship with ePrivacy directive

The paragraph 11 provides that the **“Guidelines are without prejudice to the ePrivacy directive”**. This is clearly not true. If the ePrivacy directive (or its national implementation) allows exemptions from consent, for most of the time, the legitimate interest is the only available legal basis.⁵ Then the Guidelines must be used and observed in the same way as the legitimate interest is applied on most of the cookies and similar technologies and unsolicited communications not based on consent.

We hope our comments will be useful for the Board when adopting the Guidelines. I/we hereby consent to the publication of personal data contained in this document.

Kind regards,



On behalf of **Digital Legal, s.r.o.**

Jakub Berthoty
attorney and director

³ This is the case of simple operations and can be seen e.g. in connection with CCTV systems, where the wording of purpose and legitimate interest is generally the same or very similar: *protecting the property, health and life*.

⁴ Obviously, objection against the direct marketing purposes is the only exemption. But the LIA on conducting call calls on non-clients and sending communication to existing clients will most definitely have a different result and outcome. Confirming the legitimate interest is narrower than the purpose.

⁵ Provided that personal data is processed and GDPR applies.