KONFEDERACJA LEWIATAN

KL/565/159/AM/2024

Polish Confederation Lewiatan position paper on the draft Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR (version 1.0) adopted on 8 October 2024 by the European Data Protection Board

1. Processing personal data for purposes of hypothetical establishment, exercise or defence of legal claims

In point 17 (page 9) of the Draft Guidelines the EPDB has stated that *An interest may be regarded as "legitimate" if the following cumulative criteria are met (…) The interest is real and present, and not speculative. As clarified by the CJEU, the legitimate interest must be present and effective at the date of the data processing and must not be hypothetical at that date.*

In our opinion despite the fact that, as a rule, the legitimate interest must be present and effective at the date of the data processing and must not be hypothetical at that date the following does not apply to data processing for the establishment, exercise or defence of legal claims. The EPDB should explicitly take the position in the *Guidelines* that basing such hypothetical processing on the premise of legitimate interest is permissible.

The issue of defending claims has been given special emphasis by the GDPR provisions, such as the following:

a) In the article 9 (2) (f) of the GDPR one of the prerequisites for allowing the processing of special categories of data is a situation when processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
b) Establishment, exercise or defence of legal claims by the controller prevents the possibility of invoking the right to be forgotten (article 17 (3) (e) of the GDPR), the right to restrict the processing (article 18 (2) of the GDPR), the right to object to processing of personal data (article 21 (1) *in fine* of the GDPR);
c) The enforcement of civil law claims is one of the basis for restriction of rights and freedoms of data subject by EU or Member State legislation as referred to in article 23 (1) (j) of the GDPR.
d) Establishment, exercise or defence of legal claims is one of the prerequisites to transfer personal data to the third countries or international organizations in the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules (article 49 (1) (e) of the GDPR).

What is more, as it is stated in the recital 4 of the GDPR *The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in (…) freedom to conduct a business, the right to an effective remedy and to a fair trial (…).*

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

Controllers are not in a position to predict when and what claims will be asserted by data subjects. Limiting the legitimate interest pursued by the controller only to claims currently being asserted puts the controller in a less favourable position than the rights holder exercising this right. This is because the controller in this situation would be obliged to delete all personal data processed for the purposes of defending or exercising any hypothetical claims.

The above leads to a situation in which controllers are deprived of a real possibility to defend themselves against claims or exercise thereof (both at the judicial and out-of-court stage) and thus to an imbalance between the right of persons to dispose of their rights and the legitimate interest of the controller. It should be emphasised that the obligation to delete personal data, entails the necessity to delete, *inter alia*, the history of the customer's transactions and any correspondence carried out, which deprives the controller of having any means of proof. This may violate the controller's freedom to conduct a business and indirectly leads to the infringement of right to an effective remedy and to a fair trial.

The above is of great importance for instance in the case of claims under Article 82 GDPR, according to which the controller, in the event of possible proceedings, is obliged to prove that it is in no way at fault for the event giving rise to the damage (Article 82(3) GDPR).

Mere access to personal data provided by the data subject e.g. in a filed lawsuit as a result of his/her claim will not be sufficient, as the controller will not have other information to refute the allegations made against it.

The above is also confirmed by the judgments of the Polish Voivodship Administrative Court in Warsaw (judgment of 10 November 2021 ref. II SA/Wa 868/21 and judgment of 31 March 2022 ref. II SA/Wa 3561/21).

Thus the EPDB, in order to clarify possible interpretative doubts should explicitly take the position that basing processing for the purposes of hypothetical establishment, exercise or defense of legal claims on the basis of legitimate interest is permissible.

2. **Contrary to the EPDB's view data controllers do not have legal obligation to provide the data subject with information about the conducted balancing test. The above obligation could be deemed as imposition of an administrative obligation, failure to comply with which may result in the imposition of an administrative penalty, not defined clearly in the GDPR.**

In point 68 (page 21) of the *Guidelines* the EPDB have stated that:

In any case, information to the data subjects should make it clear that they can obtain information on the balancing test upon request. This is essential to ensure effective transparency and to allow data subjects to dispel possible doubts as to whether the balancing test has been carried out fairly by the controller or assess whether they might have grounds to file a complaint with a supervisory authority.75 Such transparency obligation also follows from the accountability principle in Article 5(2) GDPR, which

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

requires the controller to be able to demonstrate compliance with each of the principles set out in Article 5(1) GDPR, including the lawfulness principle.

The opinion writer cannot agree with this interpretation of the EPDB for the following reasons:

a) The EPDB's interpretation is broadening and goes well beyond the literal interpretation of the GDPR and thus violates the principle of legality

The information obligations of controllers towards data subjects are fully described in Articles 13 and 14 of the GDPR. These provisions do not require the controller to provide the data subject with information about the balancing test process it has carried out, but only to provide him/her with the information on legitimate interest that is pursued by the controller or the third party.

Pursuant to article 84 (5) of the GDPR the violation of the articles 13 and 14 of the GDPR might be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. The abovementioned provisions leave no room for doubt in interpretation and, as provisions imposing administrative sanctions, they should be interpreted strictly, according to their literal interpretation.

The imperative to interpret strictly the provisions imposing penalties stems directly from the concepts of legalism and the rule of law, on which, according to Article 2 of the Treaty on European Union the functioning of the EU is based.

Pursuant to information available at the European Commision website, (https://www.consilium.europa.eu/en/policies/rule-of-law/) (DOA: 18.10.2024) *Rule of law is one of the EU's founding values, and essential to its very functioning. It is fundamental for the application of EU law, protects citizens and establishes the conditions for a well-functioning single market.* The Commision further states that *Under the rule of law, all public powers must always act within the constraints set out by law.*

The principle of legality was expressly mentioned in Article 2 (2) of Regulation 2988/1995: *No administrative penalty may be imposed unless a Community act prior to the irregularity has made provision for i.'* In accordance with European law doctrine the principle of legality certainly applies to penalties in EU law (de Moor-van Vugt, A. (2012). *Administrative sanctions in EU law. Review of European Administrative Law*, 5(1), 5-41. http://www.uitgeverijparis.nl/online/pdf/6123.pdf). What is more, the principle of legality has been confirmed by the CJEU jurisprudence, e.g. in the Könicke case, the Court emphasised that '*penalty, even of a non-criminal nature, cannot be imposed unless it rests on a clear and unambiguous legal basis'*(Judgment of the Court (Fifth of 25 September 1984.Karl Könecke GmbH & Co. KG, Fleischwarenfabrik, v Bundesanstalt für landwirtschaftliche Marktordnung**)**

In view of the above:

1) The EPDB (and ultimately Member States' data protection authorities) may not require controllers, without a clear and unambiguous basis in the relevant European Union act, to fulfil

additional information obligations towards data subjects, not clearly specified in the provisions of the GDPR.

2) In the absence of the proposed amendment of the *Guidelines*, national data protection authorities would still not be able to impose administrative penalties on controllers for failing to provide data subjects with information on the results of the balancing test carried out.

b) <u>The accountability principle does not relate to the obligation to demonstrate compliance to data subjects, but to data protection authorities</u>

Pursuant to article 5(2) of the GDPR *The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1* (i.e. each of the principles set out in Article 5(1) GDPR). The EPDB, in its proposed *Guidelines*, emphasized that the need to make available to the data subject the information on the outcome of the balancing test is due to the aforementioned accountability principle. However, one may not agree with such a statement. Controller's obligation derived from the accountability principle is directed towards the relevant data protection authorities, not data subjects.

Indeed, the data subject may not require the controller to inspect its internal documentation, such as record of processing activities or carry out a security audit of the processing of personal data. Should the data subject have doubts as to whether his or her data are being processed lawfully, he or she may address the competent data protection authority, which, in the course of the inspection, has the power to require the controller to provide any information, including the results of the balancing test. Pursuant to the article 5 (2) in connection with article 82 (3) of the GDPR a data subject would only be able to request from a controller a copy of a balancing test carried out to the extent that this would be necessary to prove the preconditions for the controller's liability for damages occurred as a result of infringement of the GDPR (Article 82(1) of the GDPR). However, according to CJEU case law, the mere fact that there has been a breach of the GDPR by the controller does not mean that the data subject is entitled to claim compensation (CJEU Judgment of 14 December 2023, C-340/21, *VB v Natsionalna agentsia za prihodite*).

In view of the above, it cannot be deemed that the principle of accountability relates to the controller's obligation to give a data subject information on the result of the balancing test, and the EPDB's understanding of this principle provided by the draft *Guidelines* constitutes an impermissible *contra legem* interpretation of the GDPR's provisions.

c) <u>Disclosure without a clear legal basis of the results of the equivalence tests constitutes a violation of trade secrets</u>

The internal documentation related to compliance with the law and the methods of conducting the balancing test are the intellectual property of the controller companies and are subject to the protection of know-how and trade secrets under the national legislation implementing the Directive of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

Therefore, disclosing without a clear legal basis of the results of the equivalence tests constitutes a breach of controller's trade secrets.

3) **Providing detailed description concerning data processing purposes of processing relating to specific kinds of combating fraud would cause 'information fatigue' and violate the transparency principles of Article 12 (1) GDPR**

The EPDB in its draft Guidelines (nb 106, page 29) have stated the following: *The EDPB recalls that any processing of personal data must comply with the principles set forth in Article 5(1) GDPR and that any failure to comply with these principles has the consequence that the respective processing may not take place. The principle of purpose limitation laid down in Article 5(1)(b) GDPR requires that data shall be only collected for specified, explicit and legitimate purposes. It should therefore be noted that a generic reference to the purpose of "combating fraud" to define the legitimate interest, for example in the privacy policy, is not sufficient to meet the transparency and documentation obligations under the GDPR.*

In the view of the opinion writer, providing too much detail on the purposes of the processing would lead to information fatigue, as the processing may concern the fight against different types of fraud, under different circumstances, which may change with the development of technology and cyber-attack techniques used by criminals. Furthermore, providing too much information to the data subject will not meet the requirements of Article 12(1) GDPR, i.e. providing all information to the data subject in a *concise, transparent, intelligible and easily accessible form, using clear and plain language.*

In practice, many controllers process the same personal data to prevent fraud of all kinds, such as for example smishing, vishing, phishing, identity theft, financial fraud, sale of counterfeit goods etc. Providing detailed information on every action a controller performs in order to combat would lead to a significant increase in length of privacy policies, resulting in them not being concise or transparent.

The draft opinion is very strict on processing for fraud purposes, which is unfortunate and we disagree with EDPB's stance. Fraud detection and prevention should be seen as beneficiary, almost an inherent element of the service. Section 100 of the opinion gives an interpretation of recital 47 that is even narrower than what the recital actually says.

4) **EPDB should expressly state that that consent for direct marketing granted under the ePrivacy Directive can also be interpreted as consent within the meaning of Article 6(1)(a) of the GDPR and that two consents do not need to be collected to carry out the direct marketing action.**

In the opinion of Polish Data Protection Authority and jurisprudence of Polish Supreme Administrative Court (case of 20 April 2021, III OSK 161/21 - judgment given on the basis of the previously applicable directive 95/46/WE) giving consent to the processing of personal data for the purposes of direct marketing does not mean that it is possible for any marketing content to be directed to the individual by e.g. email or telephone and *vice versa* – giving consent on direct marketing should not be regarded as a consent for data processing. Pursuant to the abovementioned court ruling in order to ensure that

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

data subject can be contacted via other channels, controller needs to obtain separate consents from the person concerned for (i) processing of his/her data, (ii) sending him/her direct marketing.

However, this approach may lead to an absurd situation where someone consents to be contacted by e.g. telephone, but does not consent to the processing of their personal data for marketing purposes. In practice, therefore, many controllers collected marketing consents on the basis of the ePrivacy Directive and based the processing of personal data on a legitimate interest basis.

The EPDB has implicitly recognized that user's single consent to receive direct marketing and the processing of personal data on the basis of article 6 (1) (a) of the GDPR is permissible. The above opinion is also similar to the view of the British Data Protection Authority, ICO described in its *Direct marketing code of practice* (https://ico.org.uk/media/about-the-ico/consultations/2616882/direct-marketing-code-draft-guidance.pdf) *Generally speaking the two lawful bases most likely to be applicable to your direct marketing purposes are consent and legitimate interests. However if PECR requires consent then in practice consent will be your lawful basis under the GDPR. If you intend to process special category data for direct marketing purposes it is likely that the only Article 9 condition available to you will be 'explicit consent'.*

The opinion writer therefore calls the EPDB for explicitly stating in the *Guidelines* that that consent for direct marketing granted under the ePrivacy Directive can also be interpreted as consent within the meaning of Article 6(1)(a) of the GDPR and that two consents do not need to be collected to carry out the direct marketing action.

4A) **Clarification on personalized advertising and direct marketing**

We note that par 109 of the guidelines suggests that personalized advertising may be considered direct marketing. We believe that such an assumption may be unwarranted and risky, especially in the context of existing CJEU case law. We suggest that the EDPB refrain from making such claims without clear support in CJEU rulings.

5) Comments to Chapter II. ELEMENTS TO BE TAKEN INTO ACCOUNT WHEN ASSESSING THE APPLICABLITY OF ARTICLE 6(1)(F) GDPR AS A LEGAL BASIS, point 4. Finalising the balancing test

In this regard, a revision of the adopted position is called for as it contradicts the literal interpretation of the provisions of GDPR.

In our opinion, to the extent that the guidelines indicate that additional measures, interfering with the content of the data subjects' rights under GDPR, should be applied in certain cases, the guidelines contradict the literal wording of GDPR.

GDPR clearly indicates, in which situations it is permissible to apply the premise of legitimate interest pursued by the controller or by a third party; at the same time, there is no requirement in GDPR to apply additional measures when applying the aforementioned premise as a legal basis for processing

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

of personal data, including, in particular, measures that would directly interfere with the content of the rights of data subjects under GDPR.

At the same time, in our opinion, interference with the content of data subjects' rights under GDPR, taking place due to the aforementioned needs, could lead to misinterpretation or understanding of the modified rights by data subjects, also in the future. It would be difficult for data subjects in the aforementioned situations to assess, and for controllers to accordingly explain to data subjects in which cases and why data subjects are entitled to a broader range of rights than the standard rights under GDPR, when personal data is processed on the premise of legitimate interest of the controller or a third party.

In view of the above, it is suggested that it should not be implied from the wording of the guidelines that it is desirable in any case to apply additional measures interfering with the content of the rights of personal data subjects.

6) More positive examples of the application of the legitimate interest

The draft opinion is quite negatively formulated, i.e. all the examples – except only for example 4 (section on 3rd party impact) – are about use case where legitimate interest cannot be invoked, or where the balancing measures are not sufficient. I think it is fair to say that legal practitioners need not only negative examples but also some positive examples (of "allowed" practices), in order to be able to reasonably manage their compliance. Other examples of this approach are sections 41 and 47 which point the need to do more when processing "more sensitive" data or when doing "more intrusive" processing, but nothing is said about "less sensitive" data or "less intrusive" processing.

7) Protection of minors

The draft opinion takes also a strict stance on the processing of data belonging to minors, with sections 95 and 95 seemingly suggesting that commercial interests cannot be invoked, which seems more restrictive than recent CJEU caselaw (judgment of 4 October re the Dutch tennis association).

8) AI training data

The big elephant in the room is of course AI training data – not mentioned at all in the draft opinion. We consider that qualitative AI training requires a huge amounts of data, and that it is legitimate to use also EU data for this purpose, not only out of commercial interests, but also for broad societal benefits, such as advancing AI innovation for all users, easing access to information access, improving AI's quality (more diversity of data e.g. local languages, cultures, etc) and accessibility (data subjects can interact in their own language), also to avoid EU users are excluded or benefit less from global AI innovation.

9) Analysis of the necessity of the processing to pursue the legitimate interests

Distinction between own interest and third-party interest. We note that the guidelines in par. 30 indicate that proving the necessity of processing in the controller's own interest is simpler than in the

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

case of a third-party interest. We suggest that the EDPB explicitly recognize the importance of third-party interests, especially in new areas such as artificial intelligence, which may require a flexible approach to third-party interests.

10) The nature of the data to be processed

Introduction of "probability" as a risk element. EDPB should include the probability factor as part of the risk assessment, which has been overlooked despite being a key aspect of CJEU case law. We recommend that par 40 of the guidelines include a probability assessment, especially when inferring sensitive information from processed data.

11) Further consequences of the processing

Application of objective assessment and simplification of requirements. We encourage simplification of assessments so that controllers do not have to analyze the interests of each person in detail, especially when it is impractical to do so. par 47 of the guidelines suggests taking into account specific circumstances for more intrusive processing - we recommend that the EOD clarify that an objective assessment may be sufficient.

12) Recognition of legitimate expectations in the context of market practices and information.

We are concerned that par 52 limits the recognition of "legitimate expectations" to only the context of specific processing. We suggest that the guidelines also consider common market practices and key information contained in privacy policies that better reflect users' actual expectations.

13) Including legal compliance as a significant factor in the balance test.

Point 57 of the guidelines restricts the consideration of legal compliance as a mitigating factor in the balance analysis. We propose that compliance with legal requirements be recognized as an important element in the balance of interests analysis.

14) Lowering the threshold for the controller's "overriding" interests.

Point 73 indicates that legitimate interests must be "substantial" for the controller, which may be challenging in practice, especially in the context of new technology development. We suggest that the EDPB lower this threshold, recognizing that processing may be justified when it is beneficial for the controller.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy