Warsaw, 20/11/2024

Public consultation reference: 10/2024

ODO 24's input in EDPB's public consultations to Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR

adw. Radosław Radwan, r.radwan@odo24.pl

Executive Summary

- We recommend that the Guidelines provide more guidance on DPO's role in LIA;
- The role of DPO could be similar to the role of DPO in DPIA;
- We recommend that the LIA methodology is expanded and includes risk assessment methodology for objective balancing exercise;
- Such expansion could result in objective and repeatable results of LIA.

1. INTRODUCTION

We welcome EDPB's new guidelines on legitimate interest (hereinafter as the "Guidelines"). As a company providing consulting services in the field of information security and data protection, we help our clients assess legitimate interest (hereinafter as the "LIA") and we have published comprehensible web tool for conducting LIA: https://odo24.pl/kalkulator-test-rownowagi. The tool will be reviewed after the final adoption of the Guidelines.

As a company providing DPO outsourcing services we are highly interested in the current discussions regarding the position and tasks of DPO. In result we would like to firstly focus on our comments to the Guidelines on the role of DPO.

Secondly, we assign a lot of focus to risk assessment under GDPR. In our web tool we provide simplified risk assessment to assess the impact of the processing on rights, freedoms and interests of data subjects. In our view such assessment will provide objective information to the controller and allow to choose appropriate measures.

2. THE ROLE OF DPO IN LIA

In 2022 Polish SA took action to assess the controllers' and processors' compliance with regards to DPO's designation and position, including conflict of interests. In the same year EDPB selected this topic as the issue of 2024 Coordinated Enforcement Action. The reports resulting from Polish SA and EDPB activities stressed the need of further guidance regarding, *inter alia*, conflict of interest.

Conflict of interest can arise when DPO is entrusted in other tasks which could result in determination of means and purposes of processing on behalf of controller or processor[1].

After both reports were published Polish SA and stakeholders (e.g. DPO outsourcing companies) started broad discussion about the role of DPO. During this discussions DPO and consulting companies' associations: SABI - Stowarzyszenie Inspektorów Ochrony Danych and Związek Firm Ochrony Danych Osobowych (ZFODO) commissioned the preparation of an opinion from Professor Grzegorz Sibiga[2]

In the recent opinion, PUODO stated that DPO cannot document and record data breaches because "if the DPO independently performs the tasks assigned to the controller or acts on their behalf, they lose the ability to conduct an objective assessment. This leads to a conflict of interest. The GDPR prohibits such practices

[1] CJEU, *X-FAB Dresden,* C-453/21, par. 44

[2] G. Sibiga, Konflikt interesów w wykonywaniu funkcji inspektora ochrona danych i jego unikanie. Problemy zaistniałe w praktyce i sposoby ich rozwiązania, WWW: https://sabi.org.pl/wp-content/uploads/2024/04/Opinia_Konflikt-interesow-IOD_SABI_ZFODO.pdf [access: 15/11/2024]

(Article 38(6) of the GDPR)"[3]. Similar argumentation can be used to other duties commonly assigned by controllers to DPOs such as drafting policies and notices, conducting DPIAs, recording processing activities, risk assessment or legitimate interest assessment[4]. However, there are conflicting opinion among SAs which task results in conflict of interests, e.g. on one hand, some SAs claim ROPA cannot be maintained by DPO[5], some SAs claim DPO can keep records of processing activities up to date[6]. Same uncertainty applies to other tasks, e.g. role of DPO in LIA.

The Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR mention DPO in paragraph 12:

"The assessment should be made at the outset of the processing, with the involvement of the Data Protection Officer (DPO) (if designated), and should be documented by the controller in line with the accountability principle set out in Article 5(2) GDPR."

In the first part paragraph provides only for involvement of DPO at the earliest stages of conducting LIA, without mentioning his exact role in this assessment. The second part of the paragraph states that the obligation to document LIA lies on the controller.

From the second part of the sentence, it can be inferred that LIA is an obligation of the controller, similarly to DPIA or ROPA. In this regard, according to Polish SA's interpretation, the conflict of interest can arise when DPO is responsible for conducting and documenting LIA.

DPO could act in this assessment analogously to DPIA. According to opinion of prof. Sibiga, DPO can prepare DPIA on behalf of the controller under condition that DPO does not decide on measures such a security measures or mitigating measures during balancing rights and freedoms od data subject. Additionally, DPO cannot decide on

[3] Biuletyn UODO nr 10/10/2024, pp. 24

[4] EDPB, 2023 Coordinated Enforcement Action. Designation and Position of Data Protection Officers, adopted on 16 January 2024, pp. 25

[5] PUODO, Sprawozdanie krajowe polskiego organu nadzorczego, pp. 9

[6] CNIL, Practical Guide GDPR for Data Protection Officers, pp. 7

means and purposes of processing. Opinion states that DPO can fill the DPIA's checklists or prepare DPIA methodology[7].

Considering Guidelines on Data Protection Officers ('DPOs')[8] and afore mentioned Opinion, the role of DPO in LIA could consist of tasks such as:

- Advice on carrying or not a LIA
- Preparation of LIA methodology, templates and checklists
- Training on conducting LIA
- Recommendation on mitigation measures
- Assessing the correctness of LIA and its results
- Filling prepared LIA templates with gathered information and requesting information from employees or processors

3. PRIVACY RISK ASSESSMENT IN LIA

LIA is "a type of light-touch risk assessment based on the specific context and circumstances of the processing"[9], GDPR provides additionally for risk-based approach. Risk assessment is a tool for choosing the means of achieving compliance with GDPR requirements.

Risk assessment can be useful in LIA. We can assess the risks (impact) on rights and freedoms of data subject objectively with the same methodology during every iteration of the balancing test.

The risk assessment could be used during the third part of LIA (3rd step of LIA methodology proposed by the Guidelines). By identification of interest, fundamental rights and freedoms we can further identify harms (negative consequences) for data subjects. The context and data subjects' expectations can be helpful to assess the likelihood of the risk source. The nature of processing provide insight into assessing

[7] G. Sibiga, Konflikt interesów… pp. 32-33

[8] Article 29 Data Protection Working Party, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, pp. 17

[9] ICO, A guide to lawful basis, WWW: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/legitimate-interests/ [access: 15/11/2024]

severity of the harm (negative consequences). The final impact of the processing should be determined as combination of likelihood and severity.

After the risk assessment with previous parts of LIA is conducted the controller can decide on further actions, such as mitigating measures or starting the processing.

Our web tool for LIA currently provides simplified risk assessment template which aims at helping controllers to choose appropriate safeguards and assess the impact of processing:

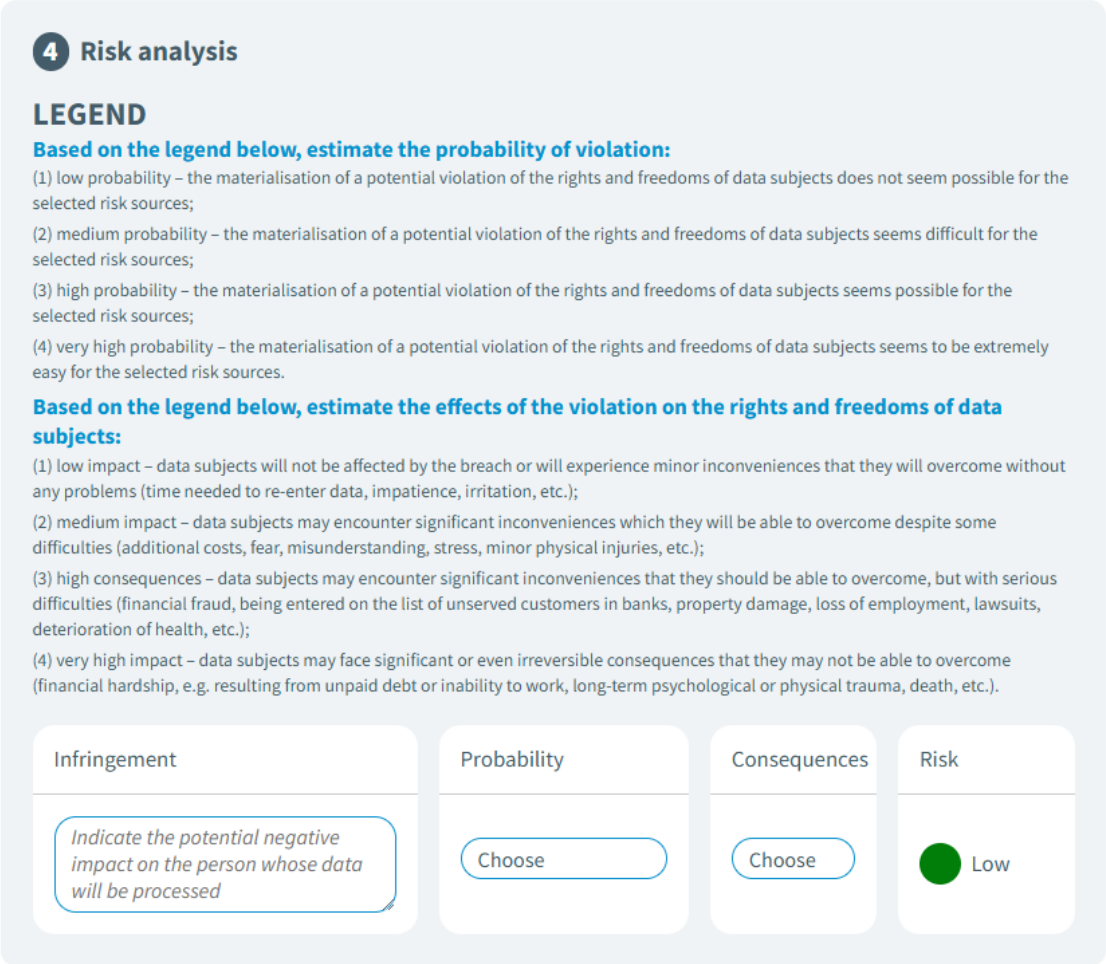


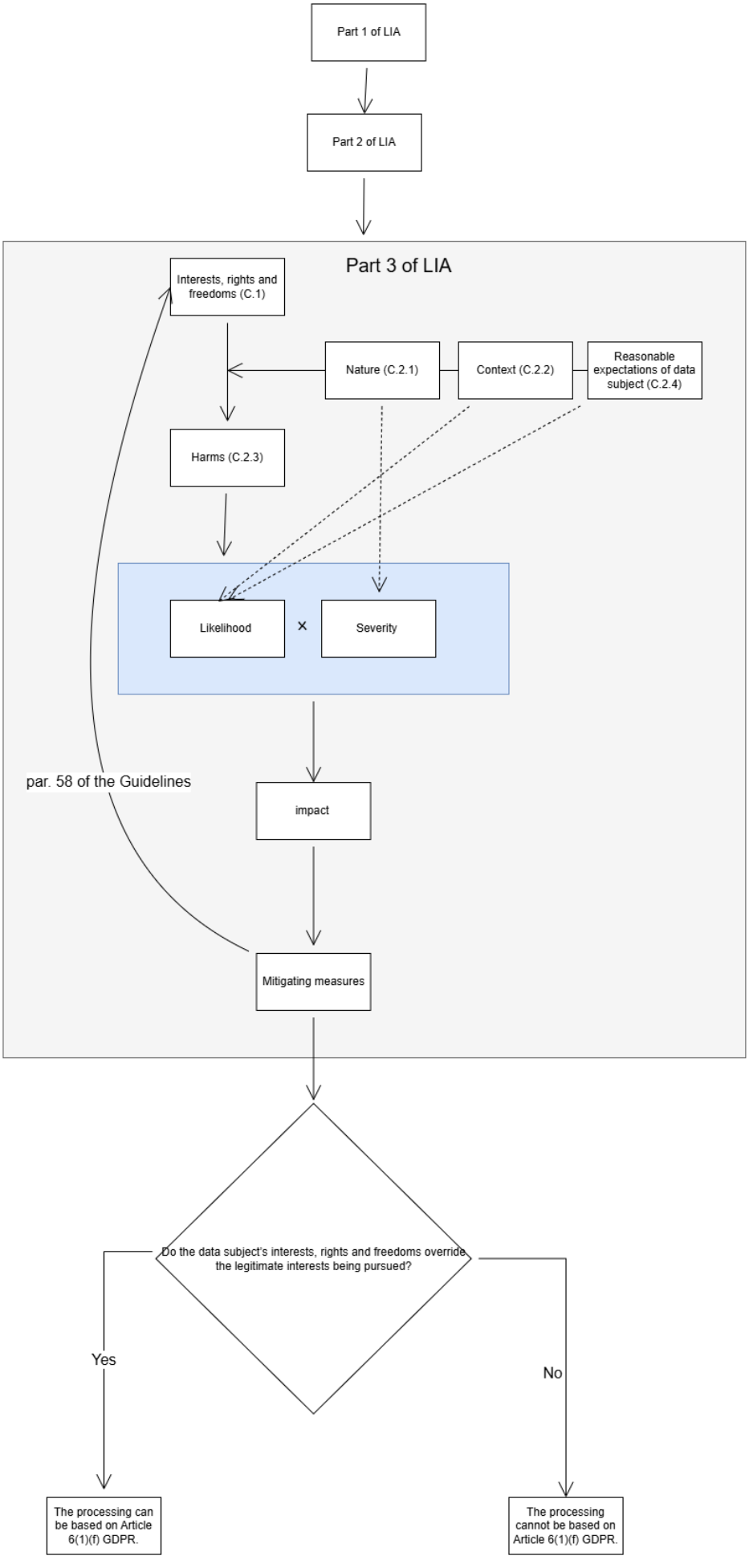
Figure 1 4th part of ODO 24's LIA tool: https://odo24.pl/kalkulator-test-rownowagi

More detailed approach could include identification of risk source, impacted interests, rights and freedoms, likelihood, severity and impact, e.g.:

Risk source (event)	**Interests, right and**	**Harms**	**Likelihood**	**Severity**	**Impact**

	freedoms concerned				
e.g. CCTV surveillance in a shop covering changing rooms	e.g. Privacy, data protection, dignity, consumer interests	e.g. Frustration, Chilling effects, feeling of being surveilled, dignity loss	4	2	8 (medium risk)

Such methodology integrated into LIA could be visualized by the following diagram:


Part 1 of LIA
Part 2 of LIA
Part 3 of LIA
Interests, rights and freedoms (C.1)
Nature (C.2.1)
Context (C.2.2)
Reasonable expectations of data subject (C.2.4)
Harms (C.2.3)
Likelihood
×
Severity
par. 58 of the Guidelines
impact
Mitigating measures
Do the data subject's interests, rights and freedoms override the legitimate interests being pursued?
Yes
No
The processing can be based on Article 6(1)(f) GDPR.
The processing cannot be based on Article 6(1)(f) GDPR.