

EDPS comments on the draft internal rules concerning restrictions of certain rights of data subjects in relation to processing of personal data in the framework of the functioning of the European Defence Agency

1. Introduction

- These comments refer to the draft internal rules of the European Defence Agency (EDA) concerning restrictions of certain rights of data subjects in relation to processing of personal data in the framework of the functioning of EDA (hereinafter ‘the draft internal rules’). Our comments refer to the document submitted on 2 September 2019.
- We provide these comments in accordance with Article 41(2) of Regulation (EU) 2018/1725 (hereinafter ‘the Regulation’)¹.

2. General comments

- The EDPS welcomes that an obligation was included in the draft rules to document the application of restrictions and the reasons to apply them. We note in particular that EDA will perform a **necessity and proportionality test** whenever it considers a restriction of data subjects’ rights in practice. The EDPS recalls that this test should be repeated in the context of the **periodic review of applied restrictions**, following an assessment of whether the factual and legal reasons for a restriction still apply.
- Concerning the **information to be provided to data subjects** regarding restrictions, the EDPS notes that EDA will publish data protection notices, privacy statements² and/or records on its website and intranet informing all data subjects of the potential restrictions of their rights related to personal data processing.
- The draft internal rules will serve as EDA’s legal basis to impose restrictions under Article 25 of the Regulation, in the absence of a legal act adopted on the basis of the Treaties. As these restrictions seek to temporarily render unavailable rights that lie at the heart of the right to data protection, such as the right to information and the right to erasure, **their legal basis should be well defined**. Therefore, the EDPS would ask EDA:
 - a) in respect of points (i)-(k) of the first paragraph of Article 5³, to further clarify these activities for which EDA would need to restrict data subject rights, including a mention of the legal acts on the basis of which EDA performs them; and
 - b) to clearly link each of the specific activities it performs or expects to perform, with the respective ground(s) for restriction listed in Article 3 on which EDA would rely.

¹ OJ L 295, 21.11.2018, p. 39.

² The EDPS would like to point out that ‘data protection notices’ and ‘privacy statements’ are terms that are interchangeably used to refer to the same type of document. In this sense, the EDPS recommends removing ‘privacy statements’ from this list, as data protection notice more clearly points to the right of data protection as such.

³ We note that the list of points of Article 5(1) is also repeated in the first paragraphs of Articles 6 to 8. In line with our comment b) we would recommend instead to move them to Article 3 so that they can be linked to their respective grounds for restriction. Consequently, this repetition could be removed.

- The EDPS is aware that EDA's draft internal rules are closely aligned with those developed earlier by other EU institutions, bodies and agencies. However, in light of our experience in reviewing such rules we believe it is in the interest of the data subject to address certain drafting aspects below. The EDPS welcomes any further contribution to **the clarity and precision** of the text prior to adoption. The EDPS trusts that EDA will fully review the text in line with the EDPS' recommendations, including as regards its clarity, precision and numbering, prior to the adoption of the internal rules.

3. EDPS recommendations

- **Recommendation no. 1:** The draft internal rules contain a number of overlaps between the Recitals and Articles (more specifically, Recital 6 and Article 2(2); Recital 8 and Article 1(2)); Recital 15 and Article 4). The EDPS recommends avoiding such overlaps and ensuring that recitals and operative provisions fulfil their proper functions. In this sense, the operative provisions should define the subject matter and scope of the rules and create binding rights and obligations. Their language should make clear that they are binding (e.g. through use of "shall" rather than "is"). Recitals should act as a statement of the reasons for adopting the operative provisions that sets them in context.
- **Recommendation no. 2:** Article 25(2) of the Regulation makes separate reference to the requirement to include in the internal rules (d) "the safeguards to prevent abuse or unlawful access or transfer" and (e) "the specification of the controller or categories of controllers". In order to reflect this separation and for the sake of clarity, the EDPS suggests creating in the internal rules two separate articles: one concerning "safeguards" and one regarding "the controller".
- **Recommendation no. 3:** In accordance with Article 25(2)(d) the safeguards to be put in place should aim to "prevent abuse or unlawful access or transfer" and not to "avoid data breaches, leakages or unauthorised disclosure", as mentioned in Article 2(1) of the draft internal rules. The EDPS recommends that the terminology used in the draft internal rules, namely in Article 2(1), be aligned with the wording of the Regulation.
- **Recommendation no. 4:** The EDPS recommends clarifying certain aspects included in the draft internal rules in order to avoid ambiguities. More specifically, it is recommended to clarify the meaning of: "Replacing users is strictly prohibited" and "databases" (Article 2(1)c).
- **Recommendation no. 5:** Article 5 of the draft internal rules contains on the one hand provisions concerning restrictions to the 'right to be informed' as such (Articles 15 and 16 of the Regulation, included in the draft internal rules in e.g. paragraph 1) and, on the other hand, provisions on what information should be provided to data subjects regarding restrictions in general (e.g. unnumbered paragraph following paragraph 1). For the paragraphs containing information generally applicable to all restrictions, the EDPS recommends either moving them to Article 3 or to a separate Article.
- **Recommendation no. 6:** The EDPS welcomes the fact that, in accordance with Recital 15 and Article 4, the Data Protection Officer (DPO) will be informed of each restriction of the data subject's rights when it is applied, when it has been lifted or when it is being revised. The EDPS recommends that the internal rules provide for the actual

involvement of the DPO throughout the procedure – instead of the DPO merely being informed when a restriction is applied or reviewed – and for that involvement to be documented.

- **Recommendation no. 7:** In relation to the necessity principle, the EDPS underlines that **restrictions should be temporary and lifted when their causes no longer apply**. The EDPS takes note that, while Article 5 and 6 provide for a 6-month review cycle regarding restrictions of the right to information and the right of access of the data subject, Article 7 only contains a cross-reference to the registration requirement of Article 6. To avoid any confusion, the EDPS recommends EDA to include a central review provision, which would apply to all restrictions it imposes.
- **Recommendation no. 8:** Article 9 provides for entry into force of the decision on the day following its publication in the *Official Journal*. We note that this represents a departure from standard practice that is justified only in exceptional cases of urgency. The reasons justifying it are also usually documented in a recital. **We recommend checking whether urgent entry into force is necessary**. If it is, we recommend inserting an explanatory recital.

Brussels, 15 January 2020.