EDPS Opinion on the meaning of 'reasonable intervals' under Article 36(1) of the Europol Regulation

(Case 2021-0364)

1. INTRODUCTION

This Opinion relates to the meaning of 'reasonable intervals' by which individuals may submit Data Subject Access Requests (DSARs) under Article 36 of the Europol Regulation.

The EDPS issues this Opinion in accordance with Article 43(2)(d) of Regulation (EU) 2016/794[1] ('the Europol Regulation', or 'ER' abbreviated).

2. BACKGROUND INFORMATION

Under Article 36(1) ER, any data subject may ask Europol, 'at reasonable intervals', whether the organisation processes any personal data relating to him or her. Europol's Data Protection Function (DPF) receives an average of approximately 300 Data Subject Access Requests (DSARs) each year.[2] Among this number, Europol reports having recently received several repetitive requests, i.e. more than one request for access from the same data subject.

In the context of such repetitive DSARs, Europol's DPF consulted the EDPS on 31 March 2021 on the practical interpretation of the notion of 'reasonable intervals.' Europol asks what time period should elapse in order for the interval between repeat requests to be

1 Regulation 2016/794 of the European Parliament and the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.05.2016.

2 EDOC#1060458v5.

EUROPEAN DATA PROTECTION SUPERVISOR
Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.europa.eu
Website: edps.europa.eu
Tel.: 32 2-283 19 00 - Fax: 32 2-283 19 50

considered 'reasonable' and for a subsequent request to be treated as a new DSAR under Article 36 ER.

Europol makes specific reference to repetitive DSARs that result in a full hit in its systems. Where access requests result in a full hit, i.e. where a search establishes that personal data on the requester is being processed in Europol's systems, Europol is obliged to consult the Member State or provider of the data concerned, in accordance with Article 36(5) ER. Europol asks whether, in the case of a repetitive DSAR resulting in a full hit, where access has previously been refused under Article 36(6) ER, but where the interval between requests is considered reasonable, Europol should re-launch the entire consultation procedure with the Member States and the providers of the data concerned or whether it would be possible to rely on the previous assessment and respond in the same manner.

[redacted]

In preparing the following guidance, the EDPS consulted national data protection authorities via the European Data Protection Board (Borders, Travel and Law Enforcement Expert Subgroup).

3. LEGAL ANALYSIS

The right of an individual to access the personal data processed on him or her is a central tenet of the fundamental right to data protection, as enshrined in the EU Charter of Fundamental Rights (the Charter).[3] It enables individuals to verify the accuracy of their personal data and the lawfulness of the data processing carried out by controllers. It is also an essential instrument supporting the exercise of other data subject rights, allowing the individual to have his or her data rectified, erased or to object to their processing.[4] This is particularly salient under the framework of the Europol Regulation, where the

[3] Charter of Fundamental Rights of the European Union (2007/C 303/01), Article 8(2).
[4] Case C-553/07 *College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer* [2009] ECR I-3889, paras 51-52.

right to rectification or erasure under Article 37 ER is only triggered once the data subject has been granted access under Article 36 ER.[5] This legal pre-condition makes ensuring fair, coherent and proportionate procedures for the handling of DSARs under Article 36 ER critical and means that any limitation on the right of access should be interpreted narrowly.

Data protection legislation allows for controllers to refuse to act upon DSARs that are manifestly unfounded or excessive. This safeguard serves to limit the burden on controllers posed by potential cases of abuse, such as where a data subject files unreasonable and repetitious requests or where s/he abuses his or her right to access data by providing false or misleading information.[6]

Recital 63 GDPR[7] states that "*A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing*." The EU's Law Enforcement Directive (LED)[8] provides under Article 12(4) that: "*Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may.... refuse to act on the request*."

This safeguard is reproduced in the Europol Regulation (albeit under a narrower form), by Article 36(1):"*Any data subject shall have the right, at reasonable intervals, to obtain information on whether personal data relating to him or her are processed by Europol*". By implication, Europol reserves the right to refuse to act upon a DSAR when it receives a repeat request from the same individual within an unreasonably short time-frame.

[5] See EDPS Case 2021-0088.
[6] See the EU doctrine on abuse of rights, e.g. Case C-255/02 *Halifax and Others v. Commissioners for Custom & Excise* [2006] ECR I-1609), Opinion of AG Maduro, para 63.
[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016.
[8] Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016.

3.1. Defining a 'reasonable interval' under Article 36(1) ER

The Europol Regulation does not specify the parameters of an 'interval', nor the time period that should elapse between requests in order to qualify an interval as reasonable, neither does it provide criteria for making this assessment.

3.1.1. The parameters of an interval under Article 36 ER

The procedure for submitting a DSAR under the ER excludes the possibility for data subjects to submit requests directly to Europol. Rather, according to Article 36(3) ER, data subjects must first send their request to the authority appointed for that purpose in the Member State of his or her choice which forwards the request to Europol. The provision stipulates that that authority shall refer the request to Europol within one month of receipt, although in practice this deadline is not always respected and the transmission of requests can encounter delays. Once Europol receives a DSAR from the national authority, it must reply within a deadline of 3 months, in accordance with Article 36(4).

Any consideration of the notion of reasonable intervals for repeat requests under the ER should therefore take into account the timeframes for handling DSAR under the applicable legislation, which may take up to 4 months, or longer if subject to delays. An interval should therefore be calculated from the date on which a data subject receives a reply from Europol and the date on which s/he submits a new (repeat) request.

3.1.2. Defining an interval as 'reasonable'

Under the GDPR and the LED, when deciding if a request is manifestly unfounded or excessive, the controller must consider requests on a case-by-case basis, in the context in which they are made. The controller must be able to demonstrate to the individual why it considers that the request is manifestly unfounded or excessive.[9]

The EDPS recalls that a refusal to process an access request constitutes a limitation on the rights of the data subject. In accordance with Article 52(1) of the Charter, limitations

[9] Article 12(5) of the GDPR and Article 12(4) of the LED state that: "*The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.*"

may be made only if they are necessary and proportionate and must respect the essence of the rights and freedoms enshrined in the Charter.[10] A case-by-case appraisal should allow for such a proportionality assessment.[11]

Further, Europol is subject, as a public body, to the European Ombudsman's European Code of Good Administrative Behaviour, which states that "*any decision reaching the conclusion that correspondence sent by a citizen is improper, for example because it is repetitive, abusive and/or pointless, must be based on an individual and substantive assessment of a citizen's correspondence*."[12]

It follows therefore that when establishing whether the threshold of a reasonable interval has been exceeded, Europol should take into account the context and circumstances in which an individual request is made and should not rely on a single, blanket policy or pre-defined time limit.

Europol may, however, decide to define a threshold (for instance, a 3 month interval) in order to 'flag' DSARs which may potentially be qualified as unreasonably repetitious. Those flagged DSARs, which fall below the threshold, should then be subject to a more detailed case-by-case assessment.

When carrying out the assessment to determine if a reasonable interval has elapsed, the primary consideration should be the fact or probability that **circumstances surrounding the data processing have altered since the last request**.

An alteration may relate to a deletion of the data. It may be occasioned by a previous 'no hit' becoming a 'hit' due to previously non-searchable data having been extracted and included as an entity in Europol's systems. An alteration may also occur if access

[10] See also Recital 46 of the LED which states that *"[any] restriction of the rights of the data subject must comply with the Charter and with the ECHR, as interpreted in the case-law of the Court of Justice and by the European Court of Human Rights respectively, and in particular respect the essence of those rights and freedoms."*

[11] In its case law, the CJEU has acknowledged that a controller's duties as regards DSARs can represent an excessive and disproportionate burden and that the obligation has to strike a fair balance between the rights of individuals and the burden placed on controllers. See for instance: Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12992 where the CJEU acknowledged that a controller's obligations are "many and significant" and held that proportionality had to be taken into account when applying sanctions. See also Case C-553/07 *College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer* [2009] ECR I-3889.

[12] European Ombudsman, *The European Code of Good Administrative Behaviour*, 2002: https://www.ombudsman.europa.eu/en/publication/en/3510.

has previously been refused on the basis of a legal ground justifying the application of a restriction under Article 36(6) and the validity of that legal ground has since elapsed.

This latter consideration is particularly important given that there is no procedure established under the Europol Regulation to systematically and periodically review the application of an exemption under Article 36(6)[13], even though the four legal grounds which justify applying such an exemption can be temporary in nature. For instance, a refusal to disclose data on the ground that it is necessary to guarantee that a national investigation will not be jeopardised (Article 36(6)(c)) will in many cases cease to apply once the investigation in question is closed. An individual previously classified as a suspect of a serious crime and denied access under Article 36(6)(b), may in the meantime have been cleared of suspicion.

The only means available for an individual who has previously been refused access under Article 36(6) to know that an exemption has been lifted, and to obtain access to their data in this context, is to submit a repeat request, and to have Europol consult the national authority or data provider concerned as to whether the circumstances justifying as exemption continue to apply. It is in this manner that data subject rights serve as an instrument to ensure the lawful processing of data, for instance by prompting Europol to delete data in its systems that are no longer relevant, or to correct personal data that are outdated or inaccurate.[14] Any refusal to process a DSAR on the basis of an unreasonable interval between requests should therefore be able to demonstrate that the likelihood of such an alteration in the circumstances of the processing is low.

The number of prior requests and the intent or rationale of the requestor, namely **evidence that there is a malicious, disruptive or time-wasting intent** on the part of the data subject, may also be taken into consideration as part of the case-by-case assessment.
Gauging such abusive cases (in which a data subject makes a request for the right of access with the sole intent of causing disruption or harm to the controller) may be based

[13] In its guidance on Article 25 of the Regulation 2018/1725 and internal rules restricting data subjects rights, the EDPS recommends EUIs to include in their internal rules on restricting data subject's rights under Article 25 the obligation to conduct periodic reviews every 6 months of the application of restrictions and to lift those restrictions as soon as the circumstances that justify them no longer apply. See EDPS, *Guidance on Article 25 of the Regulation 2018/1725 and internal rules restricting data subjects rights*, 24.06.2020:
https://edps.europa.eu/data-protection/our-work/publications/guidelines/guidance-art-25-regulation-20181725_en
[14] See, for instance, EDPS Case 2020-0908.

on the fact that an individual has explicitly stated that s/he intends to cause disruption and nothing else or if the individual is systematically sending repeated requests to Europol as part of a campaign, e.g. once a month, with the intention and effect of causing disruption.

However, the mere fact that an individual is engaged in a long-running dispute with Europol over the potential processing of his or her data, uses improper or impolite language or fails to provide reasons for multiple requests may not be sufficient to arrive at the conclusion that repetitive requests fall into this category.

The EDPS recalls that any assessment that results in a refusal to process a DSAR on the grounds that the interval between requests is unreasonable must be properly documented. The controller must be able to demonstrate to the data subject (and later to the EDPS if necessary) why it considers the request to be excessive. Those reasons should be set out in the reply to the data subject in accordance with Article 36(7).

3.2. Repetitive DSARs resulting in full hits and the consultation requirement under Article 36(5) ER

Europol asks whether a repetitive request, submitted by the data subject after a period of time considered as a reasonable interval, should trigger the launch of the consultation procedure with the Member States and the providers of the data concerned under Article 36(5) or whether it would be possible that Europol relies on the assessment previously made and responds in the same manner.

Article 36(5) of the Europol Regulation stipulates that: *"Europol shall consult the competent authorities of the Member States... and the provider of the data concerned, on a decision to be taken."* It follows that each DSAR which meets the qualification of having been submitted at a 'reasonable interval' should be treated as a new access request under Article 36(1) and must be subject to the full procedure of checks and to the obligation to consult the national authority and data provider concerned.
The EDPS recognises that handling a DSAR that results in a full hit in Europol's systems implies a greater investment of time and resources. However, treating the repeat access request as a new DSAR, including consulting the national competent authority or provider of the data concerned, does not preclude that the process is made more efficient, by

building upon the information, assessments and exchanges made in the context of the previous DSAR. In this context, consultation of the national authority or data provider may consist of a straightforward request to confirm that the circumstances justifying an exemption continue to apply (or otherwise, as the case may be).

4. CONCLUSION

The notion of what constitutes a 'reasonable interval' under Article 36(1) ER should be determined by Europol relying on a case-by-case assessment that ensures that any limitation to the fundamental rights of the individual is necessary and proportionate and respects the essence of the rights and freedoms enshrined in the Charter. This individual and substantive assessment should take into account the contextual factors surrounding the submission of the DSAR and in particular (the likelihood of) any alteration in the circumstances with regard to the processing of the personal data concerned.

Any assessment that results in a refusal to process a DSAR on the grounds that the interval between requests is unreasonable must be properly documented, and set out in writing to the data subject, in accordance with Article 36(7). The reply should clarify to the data subject that the present refusal to process the request does not prohibit his or her submission of a DSAR at a later date.

With regard to the handling of repeat DSARs submitted within a reasonable interval and concerning a full hit, the EDPS confirms that Europol must follow the full procedure set out in Article 36(5), comprising the consultation of the national authority and provider of the data concerned.

Done at Brussels, 13 July 2021

Wojciech Rafał WIEWIÓROWSKI
(e-signed)