4.5. Transfers to third countries and EU bodies

4.5.1. Background

[redacted]

On 21 March 2019, the Executive Director (ED) of Europol granted the first authorisation of transfers of personal data to a third country under Article 25(5) ER.[102] The legal basis used was Article 25(5)(c) ER, i.e. transfers necessary in individual cases for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal sanctions. The EDPS was notified of such authorization by letter of 22 March 2019.[103]

[redacted]

102 See **Annex 1** for additional information on the third country and context.

103 EDPS Case file 2019-0311.

On 22 March 2019, Europol ED granted a second authorization to transfer personal data to a third country under Article 25(5) ER.[104] The transfer was based on Article 25(5)(d) ER, i.e. the transfer is essential for the prevention of an immediate and serious threat to the public security of a MS or a third country. Europol notified the EDPS of such authorization by letter of 29 March 2019.[105]

In light of the above, the EDPS decided to inspect Europol's personal data exchanges practices with EU bodies and third countries.

4.5.2. Criteria

The following **provisions of the Europol Regulation** are of particular relevance in this context:

- Article 17(2) authorises Europol to process personal data from publicly available sources, including the internet and public data;
- Article 24 authorises Europol to transfer personal data to Union bodies;
- Article 25(5) and Article 25(6) provide for two types of derogation to the regime for the exchange of personal data between Europol and third parties, as well as international organisations as defined in Article 25(1);
- Article 26 regulates exchanges of personal data between Europol and private parties
- Article 38(6) ER assigns the responsibility for the legality of a transfer between Europol and a Union body to Europol;
- Article 28(1)(b) ER includes the principle of purpose limitation into the list of general data protection principles applicable to Europol.

The EDPS also took into consideration the following **Europol's internal documents**:

- Letter of 22 March 2019 of Europol to the EDPS informing of the authorization of a transfer of personal data to [*first third country mentioned in **Annex 1***];
- Letter of 29 March 2019 of Europol to the EDPS informing of the authorization of a transfer of personal data to [*second third country mentioned in **Annex 1***];;
- Request for an exceptional transfer of personal data under Article 25(5) ER for the transfer to [*second third country mentioned in **Annex 1***];[106];
- Request for an exceptional transfer of personal data under Article 25(5) ER for the transfer to [*first third country mentioned in **Annex 1***][107];
- Exceptional Transfer Procedure (Art. 25(5) ER)[108];
- Guide to Completion of Exceptional Transfer of personal data Request form[109].
- Update of the Cooperation Agreement between Australia and Europol of 10 November 2017[110] and subsequent exchange of emails.

104 See **Annex 1** for additional information on the third country and context.
105 EDPS case file 2019-0355.
106 EDOC#1035131.
107 EDOC number not provided.
108 EDOC#1036453v1.
109 EDOC#1018588v3.
110 EDOC#926844-v2.

Finally, the EDPS also took into consideration the following **EDPS documents**:

- [redacted]
- EDPS Opinion 3/2018 on online manipulation, 19 March 2018.

4.5.3. Actions and findings

The inspection team (team A) met with members of G24 Unit, with the Head of Unit of O1. The interviews were followed by hands-on demonstration with a senior analyst of O111. A member of the DPF unit was present throughout the on-site activities.

The EDPS checked during the hands-on demonstration:

- Process of acceptance/rejection of messages from third parties;
- Implementation of the Exceptional Transfers (Article 25(5)) Procedure
- All messages exchanged with [*first third country mentioned in **Annex 1***];and [*second third country mentioned in **Annex 1***] under the Article 25(5) ER authorisations;

[redacted]

All inspection activities are described in detail in the inspection minutes.[112] This section focuses on the most relevant inspection activities and in particular on activities which triggered findings and recommendations.

a) Exceptional Transfers (Article 25(5)) Procedure

The EDPS verified through interviews with G24 and the DPF and the review of the relevant documentation, the existence and the correct use of the procedure in place to request the use of the derogations contained in Article 25(5) ER to transfer personal data to third countries (the "Exceptional Transfers (Article 25(5)) Procedure").

The EDPS considers that the overall procedure implements adequate controls to ensure that appropriate justification is provided for the use of Article 25(5) ER. The inspection activities have, however, shown that some aspects could be improved.

First, it is not clear to what extent the **final endorsement of the use of the derogations** contained in Article 25(5) ER covers the recommendations respectively made by G24 and by the DPF. In such case, the G24 and the DPF only act in their advisory capacity. The final endorsement does not specify whether the recommendations are followed or, in case they are not, the reasons why. In that case, the EDPS could however verify that the recommendations formulated by G24 and the DPF were followed in practice.

[redacted]

112 Inspection minutes, pp. 15-32.

Second, the oral procedure used to deal with urgent cases, such as the one that motivated the transfer of personal data to [redacted], have proven to be efficient and protecting the guarantees introduced by the regular procedure. However, this **urgent procedure** should be formalised in the document. The inspection activities showed that Europol is in the process of drafting a procedure to deal with "imminent danger cases", a specific procedure which differs from the procedure during "office hours". Yet, it is not clear from the documentation provided whether urgent cases refer to all cases that happen outside office hours or to cases where there is an imminent danger. In addition, the document provided does not include the **consultation of the DPF**, despite the DPF having been consulted in the case of transfers to India, which was presented as an example of an urgent case. This omission was not discussed during the interviews.

Finally, the procedure does not include an **obligation to regularly verify** whether the conditions for the use of Article 25(5) ER as defined in the original request form are still complied with, whenever the authorization covers several transfers. This would for instance be the case if the transfers become systematic, massive or structural or if the fundamental rights and freedoms of the data subject would override the public interest in the transfer where Article 25(5)(d) and Article 25(5)(e) ER are used as legal basis.

The EDPS thus **recommends** that Europol clarify in the Exceptional Transfers (Article 25(5)) Procedure: a) the scope of the endorsement by the ED, in particular whether such endorsement includes the recommendations of additional safeguards made by G24 and the DPF and the justification whenever recommendations are not followed, b) when each of the two processes will be followed. The EDPS also recommends that Europol include in all cases a request for advice to the DPF.

b) Channels used to share data with third countries under Article 25(5) ER

As Europol did not have any prior working arrangement or cooperation agreement signed with the third countries at stake[113], the transfer of the personal data had to be arranged through secure channels alternative to SIENA.

1) Transfers to [*first third country mentioned in Annex 1*]

Findings and conclusions are described in **Annex 1.**

2) Data sent to [*second third country mentioned in Annex 1*]

Findings and conclusions are described in **Annex 1.**

c) Processing of publicly available data: use of external service providers

The data shared under Article 25(5)(c) ER were obtained from public sources [*see **Annex 1***] monitored by an external service provider, under contract with Europol and part of the advisory network of CT. This private company is a reseller of publicly available information. They only share information with Europol when they identify relevant information. In that case, Europol could not further check the information because the chat had been closed at that time. Europol could only rely on the screenshots provided by the third party provider.

113 Name of the two third countries is mentioned in **Annex 1**.

Europol has an explicit and specific **legal basis**, under Article 17(2) ER, **to process information**, including personal data, **from publicly available sources**, including the internet and public data. This article does not exclude the possibility for Europol to subcontract this activity to a third party. The third party should however act as processor, i.e. on behalf of Europol. This means that this third party cannot participate to the determination of the purposes and means of such processing of personal data.

On the contrary, would the third party provider of publicly available information qualify as controller, such data processing activity would fall under Article 26 ER ("Exchange of personal data with private parties"). Under this article, Europol is expressly **forbidden to receive personal data directly from private parties**.[114] Such information should be transmitted by the national unit in accordance with national law, the contact point of a third country or an international organization with which Europol has concluded a cooperation agreement, or from an authority of a third country or an international organization which is the subject of an adequacy decision or part to an international agreement. In case it nevertheless does, Europol should either identify the national unit, the contact point or authority concerned, or if not possible, Europol must only process such data for the purpose of this identification.

It follows that, under Article 26 ER, Europol cannot process the data obtained from the third party provider for the purpose of their transfer to a third country. The only possible legal basis for the processing that motivated the transfer of personal data to India under Article 25(5)(c) ER is thus Article 17(2) ER.

In light of the above, Europol must **verify the contract with the external service provider** of publicly available information in order to make sure that the personal data processing activities performed by the external service provider do not exceed the tasks of a processor. In particular, Europol should ensure that the external service provider acts on behalf of Europol and does not participate to the determination of purpose and means of the processing of such personal data activities.

In addition, the EDPS would like to point out that **monitoring social media users** is a personal data processing activity that creates high risks for individuals' rights and freedoms. It involves uses of personal data that go against or beyond individuals' reasonable expectations. Such uses often relate to personal data being used beyond their initial purpose, their initial context and in ways individuals could not reasonably anticipate.[115] The EDPS has already stressed that the surveillance of social media platforms by companies and government has a chilling effect on individuals' ability and willingness to express themselves and form relationships freely, including in the civic spheres essential to the health of democracy.[116] The use of such tools must not only be grounded on an explicit legal basis but also be surrounded by strong safeguards for the protection of individuals' rights and freedoms and strictly comply with the applicable data protection framework.

The EDPS thus **recommends** that Europol **scrutinize its social media monitoring practices** in order to identify the risks to data subjects' rights and freedoms and to ensure that such data

114 Art. 26(1) ER.

115 EDPS Opinion of 30 September 2019 on the formal consultation on EASO's social media monitoring report (case 2018-1083), p.3.

116 EDPS Opinion on online manipulation, [illegible] March 2018, p.3.

processing activities are surrounded by strong safeguards and that they strictly comply with the data protection framework.

d) Transfers to EU bodies

[redacted]

[redacted]

[redacted]

4.5.4. Conclusion and recommendations

In the light of the inspection's findings, the EDPS formulates recommendations as regards the Exceptional Transfers (Article 25(5)) Procedure), the channels used to share data with third countries under Article 25(5), compliance with Article 23(6) ER (undertaking by the recipient), the processing of publicly available information, compliance with purpose limitation principle in the context of transfers to EU bodies and the change of purposes of given datasets during their processing at Europol.

Therefore, the EDPS makes the following recommendations:

No	Content
[redacted]	Clarify in the Exceptional Transfers (Article 25(5)) Procedure: - the **scope of the endorsement by the ED**, in particular whether such endorsement includes the recommendations of additional safeguards made by G24 and the DPF and the justification whenever recommendations are not followed; - When the **procedure** "during office hours" and "imminent danger cases" have to be followed.
[redacted]	23.1. Include in the Exceptional Transfers (Article 25(5)) Procedure a **request for advice to the DPF** in all cases where Article 25(5) ER is to be used. This procedure involves the use of a derogation to data protection safeguards established for the regulation of transfers to third countries and international organisations. The

[redacted]

No	Content
	independent advice of the DPF in those cases is thus of paramount importance to ensure compliance with the data protection safeguards contained in the ER. 23.2. **Consult the DPF** on all Exceptional Transfers under Article 25(5) ER.
[redacted]	24.1. Include in the Exceptional Transfers (Article 25(5)) Procedure **regular reviews** to verify that the original conditions which gave rise to the authorisation are still complied with. Such regular reviews should avoid for instance situations where the evolution of the case create risks that the transfers will become systematic, massive or structural or that the fundamental rights and freedoms of data subjects will override the public interest in the transfer.
[redacted]	[*See **Annex 1***].
[redacted]	[*See **Annex 1***].
[redacted]	[*See **Annex 1***].
[redacted]	Europol must verify the **contract with the external service provider of publicly available information** in order to make sure that the personal data processing activities performed by the external service provider do not exceed the tasks of a **processor**. In particular, Europol should ensure that the external service provider acts on behalf of Europol and does not participate to the determination of purpose and means of the processing of such personal data activities.
[redacted]	Taking into account that **monitoring social media** is a personal data processing activity that creates high risks for individual rights and freedoms, as it involves the use of personal data that go against or beyond individuals' reasonable expectations, the EDPS recommends that Europol scrutinize its social media monitoring practices in order to identify the risks to data subjects' rights and freedom, to ensure that such data processing activities are surrounded by strong safeguards and strictly comply with the data protection framework.
[redacted]	