EUROPEAN DATA PROTECTION SUPERVISOR

EDPS OPINION ON TRANSFERS TO A THIRD COUNTRY RESULTING FROM THE USE OF A NEWSLETTER SERVICE BY ENISA

(Case 2020-1122)

1. INTRODUCTION

- This Opinion relates to the possible use of a derogation under Article 50 of Regulation (EU) 2018/1725[1] ('the Regulation') by the European Union Agency for Cybersecurity (ENISA) for transfers to a third country resulting from the use of a newsletter service to which interested parties can subscribe on ENISA's website.

- The EDPS issues this Opinion in accordance with Article 58(3)(c) of the Regulation.

2. BACKGROUND INFORMATION

By email of 16 November 2020, the DPO of ENISA consulted the EDPS on transfers to a third country (the United States of America, US) resulting from the use of a newsletter service to which interested parties can subscribe on ENISA's website *"based on consent"* and *"after being provided with very clear information (also on the risks related to the transfers)"*.

The service provider is based in the EU, but has sub-processors in the US and uses the European Commission´s Standard Contractual Clauses. *"The contract with the service provider will have the standard DG Budget clauses and an Annex with approved subcontractors, to whom transfers may take place (and the approved transfer tools)"*.

On 19 April 2021, the EDPS acknowledged receipt.

[1] *Regulation (EU) 2018/1725 of the European Parliament and the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ, L 295, 21.11.2018, pp. 39-98.*

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

3. LEGAL ANALYSIS AND RECOMMENDATIONS

The analysis and recommendations below relate mainly to the transfer-related question raised by ENISA and more specifically about the possibility for ENISA to make use of Article 50 derogations, regardless of the specificities of the contractual terms and conditions between ENISA and the newsletter service.

3.1. Lawfulness, informing data subjects and obtaining their consent

Before addressing the application of a possible derogation under Article 50 of the Regulation, ENISA needs to ensure the lawfulness of the processing (Article 5 of the Regulation), irrespective of any transfer.

As controller, ENISA will need a **ground for lawfulness** under Article 5 of the Regulation. Whilst situations in which certain outreach events (such as organising a conference) might be covered by Article 5(1)(a) of the Regulation (processing is *necessary* for the performance of a specific task carried out in the public interest), for standard outreach events including the **publication of newsletters** to subscribing members of the general public, as in the present case, ENISA will need to ensure valid consent of the data subjects concerned under **Article 5(1)(d) of the Regulation**[2].

ENISA as controller needs to ensure *inter alia* that data subjects are fully informed about the processing of their personal data resulting from the use of the newsletter service to which they subscribe on ENISA's website. The standard option to do this is by means a of **specific data protection statement**[3].

Where this is complemented with third party processing information (e.g. a link to a data protection statement of a service provider), the controller needs to ensure that the information remains easily accessible, understandable and transparent to ensure fair and transparent processing under Article 4(1)(a) of the Regulation[4].

Data subjects need to be fully **informed** – but, if their **consent** is needed as a legal basis for the processing under Article 5 of the Regulation (which is the case for external participants in an outreach event), they also need to be given the **genuine choice** to opt-in voluntarily.

---

[2] *See Report on the remote audit of information provided to data subjects when they sign up to newsletters and other subscriptions ("audit report"), p. 8.*

[3] *See audit report, pp. 5/6.*

[4] *See EDPS guidance on transparency requirements, including the need to avoid information overkill here: https://edps.europa.eu/sites/edp/files/publication/18-01-15_guidance_paper_arts_en_1.pdf.*

Indeed, consent must comply with the requirements of Article 3(15) of the Regulation - i.e. any freely given[5], specific[6], informed[7] and unambiguous indication of the data subject's wishes[8] - and should thus be given by a **clear affirmative act**, which indicates the data subject's acceptance of the proposed processing of his or her personal data, e.g. by ticking a box. Silence, pre-ticked boxes or inactivity therefore do not constitute consent (see recital 19 of the Regulation and the Court's ruling in *Planet49*, C-673/17, where the Court has established that valid consent cannot be obtained through pre-ticked boxes).

Recommendation: ENISA needs to provide comprehensive information of the subscribers under Articles 15-16 of the Regulation and to ensure their valid consent under Article 5(1)(d) of the Regulation, in line with the requirements of Article 3(15) of the Regulation and given by a clear affirmative act.

3.2. Disclosure by transmission including third country transfers

3.2.1. Context: ENISA's contractor as processor

In the case at hand, it is not ENISA directly transferring the above personal data, but transfers to a third country (the US) result from the use of a newsletter service provider located in the EU with US sub-processors to which interested parties subscribe on ENISA's website. This newsletter service provider processes the above personal data **on behalf of ENISA** in the sense of Article 3(12) of the Regulation.

- Under Article 29(1) of the Regulation, "*Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.*"

- Article 29(3) of the Regulation stipulates that "*Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller...*".

- According to Article 29(3)(a) of the Regulation, that contract or other legal act shall stipulate, in particular, that the processor "*processes the personal data only on*

[5] *See pp. 7-9 of the EDPB Guidelines 05/2020 on consent, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf for guidance on respective provisions of the GDPR.*
[6] *See pp. 13-15 of the EDPB Guidelines 05/2020 on consent.*
[7] *See pp. 15-18 of the EDPB Guidelines 05/2020 on consent.*
[8] *See pp. 18-20 of the EDPB Guidelines 05/2020 on consent.*

*documented **instructions from the controller**, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest*" (emphasis added).

Where third country transfers take place in the light of this assessment, the contract should notably specify the requirements for transfers to third countries, taking into account the provisions of Chapter V of the Regulation[9].

In the order of 5 October 2020 (Case 2020-0766), the EDPS has requested EUIs to take a strong precautionary approach concerning new processing operations carried out with appropriate safeguards and appropriate supplementary measures. The EDPS strongly encouraged EUIs to ensure that any new processing operations or new contracts with any service providers does not involve transfers of personal data to the United States. Given ENISA´s responsibility as controller, ENISA shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the Regulation and ensure the protection of the rights of the data subject in accordance with Article 29(1). ENISA should primarily **assess with the processor the availability of alternative newsletter solutions** not involving the transfer of personal data to sub-processors in the US.

In view of the scope of this consultation, the analysis will focus on ENISA's **instructions to its processor** with a view to comply with the **specific requirements** of Chapter V of the Regulation **on transfers**[10].

3.2.2. Additional legal ground for international transfers - Use of derogations

If and where transfers of personal data to a third country take place, these come under **Chapter V of the Regulation**. Under Article 46 of the Regulation, "*Any transfer* (…) *shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor* (…). *All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined*".

ENISA should instruct its processor as regards transfers (see above) and the latter should comply with the provisions of Chapter V, including on Article 50 where relevant[11].

---

[9] *See p. 34 (§116) of EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR (version 1.0 adopted on 2 September 2020), which applies mutatis mutandis to the Regulation: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf.*

[10] *For the other instructions to be provided by the controller, see Article 29 of the Regulation and pp. 29-39 (Part II.1) of EDPB Guidelines 07/2020 on the concepts of controller and processor.*

[11] *As expressly stated in Article 46 of the Regulation, transfers are "subject to the other provisions of the Regulation", i.e. specific provisions on transfers add to the 'standard' requirements for any processing, including general principles.*

Article 50 of the Regulation offers derogations for specific situations to allow for transfers to a third country or an international organisation in the absence of an adequacy decision or appropriate safeguards[12].

Against this background, the consultation underlying this Opinion expressly refers to transfers to the US resulting from the use of a newsletter service to which interested parties can subscribe on ENISA's website, raising the specific question of whether the consent derogation under Article 50(1)(a) could be applied.

The present Opinion thus focusses on this issue instead of covering all provisions in Chapter V of the Regulation.

According to **Article 50(1)(a) of the Regulation**, the transfer can take place if "... *the* ***data subject has explicitly consented to the proposed transfer****, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards.*"

- As already noted above[13], data subjects need to be fully **informed** that the processing of their personal data involves a transfer to a third country (or an international organisation). In the absence of an adequacy decision and appropriate safeguards, this must also include information on the **possible risks of such transfers for the data subject** resulting from the absence of an adequacy decision and appropriate safeguards[14].
  The *Schrems II* judgement[15] highlighted the limitations on the protection of personal data arising from the domestic law of the US on access and use of data transferred to the US and the lack of enforceable data subject rights.
  This aspect is indeed one of the risks that the data subjects should be informed about. Which risks exist for data subjects will depend on the specificities of the US based sub-processor chosen by ENISA's processor.

- **Explicit consent**: As already mentioned, according to Article 3(15) of the Regulation, any consent should be freely given (in the present case, we note in particular that data subjects still have the option to consult the newsletter directly on the website of ENISA), specific (see following point), informed (see previous point) and

[12] *See EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf*
[13] *See section 3.1. above.*
[14] *See pp. 7/8 (Section 2.1.3.) of the EDPG Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, noting in particular that "...information has to be given as to the possible risks for the data subject arising from the absence of adequate protection in the third country and the absence of appropriate safeguards. Such notice, which could be standardized, should include for example information that in the third country there might not be a supervisory authority and/or data processing principles and/or data subject rights might not be provided for in the third country." (p. 8).*
[15] *Judgement of the Court (Grand Chamber) of 16 July 2020 in case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems.*

unambiguous. On this last condition, Article 50(1)(a) is stricter as it requires "*explicit*" consent[16]. The Regulation requires explicit consent in situations where particular data protection risks may emerge, and so, a high individual level of control over personal data is required. Such particular risk appear in the context of international data transfers[17]. Consent should be given by a clear affirmative act, which indicates the data subject's acceptance of the proposed processing (transfer) of his or her personal data, e.g. by ticking a box[18]. Silence, pre-ticked boxes or inactivity therefore do not constitute consent (see above for further references). If participants are simply informed that e.g. "*by registering to the newsletter, the user agrees to the privacy terms and conditions of [the newsletter service provider]"* and there is no subsequent clear affirmative act by the participants to indicate their agreement with the transfers to the US referred to by these terms and conditions , valid consent on the transfer will not have been obtained.

- **Specific**: The principle of purpose limitation implies that consent given regarding transfers for subscription purposes on the occasion of a previous subscription will not automatically cover the purpose of other / future outreach activities by ENISA[19]. Where ENISA controls the collection of personal data for newsletter subscription purposes, the EDPS would thus urge caution regarding subsequent use for the purpose of other outreach activities without a documented unambiguous consent from the data subjects in question[20].

- **Documented**: Such consent needs to be documented[21] by ENISA inviting members of the public to subscribe to their newsletter[22]. Article 7(1) of the Regulation stipulates that *"Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data."*

- **Withdrawal**[23]: Under Article 7(3) of the Regulation, *"The data subject shall have the right to withdraw his or her consent at any time. ...Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent."*
  Data subjects need to be told about the possibility to withdraw their consent in the data protection statement (Articles 15 (2)(c) / 16 (2)(c) of the Regulation)[24].

---

[16] See pp. 20/21 of the EDPB Guidelines 05/2020 on consent: "Explicit consent is required in certain situations where serious data protection risk emerge, hence, where a high level of individual control over personal data is deemed appropriate. Under the GDPR, explicit consent plays a role in Article 9 GDPR on the processing of special categories of data, the provisions on data transfers to third countries or international organisations in the absence of adequate safeguards in Article 49 GDPR".
[17] See p. 6 (Section 2.1.1.) of the EDPG Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679.
[18] See Example 17 on p. 21 of the EDPB Guidelines 05/2020 on consent.
[19] See pp. 13-15 of the EDPB Guidelines 05/2020 on consent.
[20] See audit report, p. 13.
[21] See pp. 22/23 of the EDPB Guidelines 05/2020 on consent.
[22] See audit report, pp. 13/14.
[23] See pp. 23-25 of the EDPB Guidelines 05/2020 on consent.
[24] See audit report, p. 14.

In principle, once consent has been withdrawn, it needs to be ensured that the data is deleted unless it can be processed on another legal ground. In case there may be difficulties to enforce contractual terms in practice in the third country, data subjects will need to be informed explicitly about this risk due to the absence of appropriate safeguards.

- **Double consent**: Explicit consent on transfer is different and adds up to the consent on the processing in general under Article 5(1)(d) of the Regulation.

Recommendations: In view of the above, ENISA needs to ensure that prior to the transfer (i.e. *before* subscribers to the newsletter provide their personal data involved in the subscription on ENISA´s website):

- Subscribers receive specific information about the transfer of their personal data to a US based sub-processor with a view to obtaining ENISA´s newsletter. The information must include information on the possible risks of such transfers for them due to the absence of an adequacy decision and appropriate safeguards;
- Subscribers consent explicitly on the transfer of their data to the US-based sub-processor with a view to obtaining ENISA´s newsletter, in addition to the consent on the processing in general.
- Information and consent on the transfer can be provided and obtained at the same time as the information and consent on the processing in general, as long as the former remains specific.
- Depending on the practicalities of the subscription process and the involvement of the processor in the whole process, ENISA could either provide specific information and obtain explicit consent on the transfer together with the general information and consent, or instruct its processor to do it under Article 29(3) of the Regulation (on top of the other instructions, ENISA may impose on its processor as to the transfer).

4. CONCLUSION

- As controller, ENISA needs to ensure the **lawfulness** of the processing operation under Article 5 of the Regulation.
  In this context ENISA needs to ensure valid **consent** of the data subjects under Article 5(1)(d) of the Regulation, in line with the requirements of Article 3(15) of the Regulation and given by a clear affirmative act.

- Given ENISA´s responsibility as controller, ENISA shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the Regulation and ensure the protection of the rights of the data subject in accordance with Article 29(1). ENISA should primarily **assess with the processor the**

availability of newsletter publishing solutions not involving the transfer of personal data to the US.

- If and when the data processing involves the transfer of personal data, ENISA also needs to comply with the additional requirements laid down in Chapter V of the Regulation. Prior to the transfer (i.e. before newsletter subscribers provide their personal data), ENISA needs to ensure that subscribers receive **specific information about the transfer** of their personal data to a US-based sub-processor with a view to subscribing to ENISA´s newsletter. The information must include information on the **possible risks of such transfers** for them due to the absence of an adequacy decision and appropriate safeguards.

- In addition, prior to the transfer, ENISA needs to ensure that participants **consent explicitly to the transfer** of their data to the US-based sub-processor with a view to subscribing to ENISA´s newsletter, in addition to the consent on the processing in general.

In light of the accountability principle, the EDPS expects ENISA to implement the above recommendations accordingly and has decided to **close the case**.

Done at Brussels on 27 July 2021

Wojciech Rafał WIEWIÓROWSKI
(e-signed)