Disclosing Personal Data to Non-EU Authorities - GDPR Guidance Published

DECEMBER 18, 2024

Key Takeaways

- When faced with a third country authority request to disclose information including personal data, organisations subject to the GDPR have been attempting the difficult feat of simultaneously complying with the request and the GDPR, including its transfer requirements.
- The European Data Protection Board has published draft guidelines for controllers and processors within the European Economic Area designed to support an organisation in complying with the GDPR when faced with such a request.
- The guidelines address a two-step test to assess the legality of data transfers. This test involves: (1) assessing the legal basis for responding to the request, and (2) identifying a valid ground for transfer under Chapter V of the GDPR.
- A public consultation on the guidelines is open until 27 January 2025.

Background

On 3 December 2024, the European Data Protection Board ("**EDPB**") announced[1] the publication of Guidelines 02/2024 on Article 48 GDPR ("**Guidelines**")[2]. Interestingly, the Guidelines state that they only cover the situation where disclosure requests from public authorities outside the European Economic Area ("**EEA**") (i.e. third country authorities) are addressed to controllers or processors within the EEA and subject to the GDPR because of their EEA establishment. There is no further mention of how organisations not established in the EEA, but nevertheless subject to the GDPR, might deal with similar requests.

Organisations subject to the GDPR have often faced a conflict between simultaneously complying with transfer requests from third country authorities and GDPR requirements. The EDPB acknowledges that organisations receive requests to share personal data from a wide variety of public authorities, such as banking regulators, tax authorities, and law enforcement and national security authorities. The Guidelines aim to clarify and assist EEA-based organisations in handling direct requests from third country authorities for the disclosure of personal data.

Article 48

The Guidelines interpret Article 48 as providing that any official request from a third country authority requiring disclosure of personal data "*may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter".*

The first question is therefore whether there is an international agreement. However, this is not a necessity in order for an organisation to respond to a request, albeit in the absence of such an

international agreement a third country authority request would not be recognised or enforceable in EEA courts. The Guidelines make clear that, even absent such an agreement, organisations may in principle still respond to the request provided that the GDPR is complied with. Conversely, the Guidelines clarify that Article 48 does not provide a basis for disclosure in response to the request in and of itself.

Regardless of whether there is an applicable international agreement, where an organisation discloses personal data in response to a third country authority's request, this will constitute a transfer to a third country and that transfer must therefore comply with the GDPR's requirements. The Guidelines state that an EEA organisation must always apply a 'two-step test' for all personal data transfers to third countries.

First, there must be a legal basis for data processing under Article 6 of the GDPR. Second, there must be a valid ground for transfer under Chapter V of the GDPR. Additionally, organisations may need to comply with other requirements, such as national procedural rules or international agreements providing for cooperation with third country authorities.

Step 1: Legal Basis for Processing

All processing, including any disclosure, must have a valid legal basis under Article 6 of the GDPR.

- Legal obligation: The Guidelines start here given that Article 48 presupposes a court judgment or administrative decision from a third country requiring the disclosure of personal data. As indicated above, such requests are only enforceable if they are based on an international agreement. This scenario may create a legal obligation for the organisation, with non-compliance leading to legal consequences. Under these circumstances, Article 6(1)(c) GDPR provides a clear legal basis for processing personal data to meet this obligation.

If the organisation is not subject to a legal obligation stemming from an international agreement, other legal bases under Article 6 of the GDPR must be considered on a case-by-case basis.

- Consent: While consent (Article 6(1)(a) GDPR) could theoretically be used as a legal basis, the EDPB notes that it is generally inappropriate in these contexts, especially when the processing involves authoritative powers. This is because consent must be freely given, which is often not the case in situations involving such requests.
- Performance of a Contract: The EDPB discounts the performance of a contract (Article 6(1)(b) GDPR) as a lawful basis, as it requires the data subject to be a party to the contract, which would not be the case in the context of a third country authority request.
- Vital Interests: In specific cases, the EDPB acknowledges that the vital interests of the data subject (Article 6(1)(d) GDPR) could be relied upon, provided that any conditions set out in international law are met. The Guidelines specifically refer to requests related to abducted minors, where the transfer of personal data would be in their vital interests.
- Public Interest: If disclosure based on an international agreement is not mandatory but allowed under EU or Member State law, the organisation could rely on the public interest basis (Article 6(1)(e) GDPR). As an example, albeit in the context of transfer derogations rather than as a legal basis, the UK Information Commissioner's Office ("**UK ICO**") has previously concluded that SEC-regulated UK firms could transfer personal data to the SEC on the basis of public interest embedded in UK law.[3]
- Legitimate interests: The Guidelines state that legitimate interests (Article 6(1)(f) GDPR) might be a viable legal basis in exceptional circumstances. This basis requires a balancing test to ensure that the processing is necessary and does not override the data subject's rights and freedoms. The EDPB emphasises that private businesses cannot rely on this basis for the preventive collection and storage of personal data to prevent, detect, and prosecute criminal offences when this processing is unrelated to their own activities.

Step 2: Chapter V Transfer Ground

The Guidelines clarify that Article 48 GDPR is not itself a ground for transfer. Therefore, an organisation seeking to respond to a request must identify an applicable transfer ground under Chapter V of the GDPR.

The Guidelines do not go into detail on the options here, but Chapter V provides that transfers may be made on the basis of adequacy decisions, or appropriate safeguards such as standard contractual clauses or binding corporate rules. In the absence of either of these options, an organisation may be able to rely on a derogation, such as necessity for public interest or legal claims, but the Guidelines issue the reminder that derogations are to be interpreted restrictively and relate to occasional and non-repetitive processing.

However, the Guidelines do specifically call out that appropriate safeguards may be provided for by "*a legally binding and enforceable instrument between public authorities or bodies (i.e. an international agreement within the meaning of Article 48".*

Comment

The EDPB's final guidelines rarely deviate too substantively from their draft versions so, while these Guidelines are still subject to public consultation, the substance can be expected to remain the same. EEA-based private organisations who receive third country authority requests will appreciate the additional guidance and reminders issued by the EDPB, especially the Annex with a flowchart designed to help organisations determine if they can lawfully respond to disclosure requests from third country authorities. The Guidelines will provide particular assistance to organisations in the decision-making process for determining which legal basis to rely on under Article 6 of the GDPR and grounds for transfer under Chapter V, where this may have previously been unclear in such circumstances. Although EDPB Guidelines are no longer directly applicable to the UK regime, UK organisations may still find them valuable for aligning their practices with broader data protection standards. The EDPB has opened a public consultation inviting stakeholders to submit their comments on the Guidelines from 3 December 2024 until 27 January 2025[4].

Footnotes

[1] Available online at: https://www.edpb.europa.eu/news/news/2024/edpb-clarifies-rules-data-sharing-third-country-authorities-and-approves-eu-data_en

[2] Available online at: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-022024-article-48-gdpr_en

[3] The UK ICO intervened on behalf of UK firms whose SEC registration applications were suspended over the SEC's concerns that the GDPR would prevent such firms from supplying certain requested information. The UK ICO's letter to the SEC is available here.

[4] Interested parties can provide feedback using the EDPB's online form which is available online at: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/reply-form_en?node=8307

Related Professionals

PARTNER

Paul Kavanagh

London
+44 20 7184 7510

ASSOCIATE

Dylan Balbirnie

London
+44 20 7184 7639

ASSOCIATE

Anita Hodea

London
+44 20 7184 7428

ASSOCIATE

Madeleine White

London
+44 20 7184 7302

Related Services

Cyber, Privacy & AI
Intellectual Property