Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

CIPL Response to the European Data Protection Board's Public Consultation on Draft Guidelines 02/2024 on Article 48 GDPR

Centre for Information Policy Leadership (CIPL)

24 January 2025

CIPL Response to the European Data Protection Board's Public Consultation on Draft Guidelines 02/2024 on Article 48 GDPR

The Centre for Information Policy Leadership (CIPL)[1] appreciates the opportunity to comment on the European Data Protection Board (EDPB) Draft Guidelines 2/2024 on official requests from a third country authority under Article 48 of the GDPR. CIPL commends the EDPB's efforts to enhance regulatory clarity and foster consistent application of data protection principles across the EEA.

The Guidelines provide a number of helpful clarifications regarding the scope and interpretation of Article 48 for private entities to whom requests qualified under Article 48 may be addressed.

CIPL appreciates the reminder that Article 48 itself does not constitute a legal basis and reconfirmation of the two-step test required for any transfer of personal data to third countries:

- Ensuring a legal basis under Article 6 and adherence to the principles of Article 5 GDPR, and
- Compliance with Chapter V, consistent with the EDPB's previous positions.

CIPL has identified several areas below where additional practical guidance would be welcome.

1. Scope

The EDPB provides helpful clarification regarding the intended scope of Article 48, namely a wide interpretation of the type and purpose of a request which would qualify under Article 48. However, the EDPB then concludes that the modalities of Article 48 "encompass[es] every possible way in which a controller or processor in the EU could make personal data accessible to a third country authority". This narrow interpretation does not reflect the reality of organisations operating internationally.

Requests for data disclosure will not necessarily be sent to the EU based organisation but to the parent or affiliate in the country of the requesting authority. In some circumstances controllers may provide data on a voluntary basis in response to a non-binding request (paragraph 14 of the Guidelines appears to consider this, while Article 48 GDPR wording refers to "requiring" and "enforceable". The Guidelines should more clearly reflect that transfers are not limited to circumstances of Article 48 GDPR.

2. Controller-Processor Responsibilities

CIPL agrees with the EDPB's explicit assertion that the controller is the responsible party for compliance with Article 6 GDPR. However, requests may often be directed at processors and either

[1] The Centre for Information Policy Leadership (CIPL) is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 85+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices to ensure the responsible and beneficial use of data in the modern information age. CIPL's work facilitates constructive engagement between business leaders, data governance and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at https://www.informationpolicycentre.com/. Nothing in this document should be construed as representing the views of any individual CIPL member company or of the law firm Hunton Andrews Kurth LLP. This document is not designed to be and should not be taken as legal advice.

incidentally or purposefully include the controller's data in their scope.[2] CIPL would, therefore, welcome more practical guidance and examples on the allocation of responsibilities of controllers and processors for compliance with the GDPR. For instance, the responsibility to comply with the 'two-step test' will likely fall into the controller's obligations, regardless of whether the request was initially directed to the processor.

3. Lawful Basis under Article 6 GDPR

CIPL appreciates the EDPB's efforts to provide further guidance regarding Article 6 in the context of requests from third country authorities.

We particularly welcome the acknowledgement that controllers can rely on legitimate interest under Article 6(1)f GDPR in response to such requests. However, the guidance limits reliance on legitimate interest to "exceptional circumstances" without further clarification. This undue restriction is not supported by the GDPR or recent jurisprudence.

CIPL urges the EDPB not to restrict the legitimate interest beyond the three conditions outlined in Guidelines 1/2024:

- the pursuit of a legitimate interest by the controller or by a third party;
- the need to process personal data for the purposes of the legitimate interest(s) pursued; and
- the interests or fundamental freedoms and rights of the concerned data subjects do not take precedence over the legitimate interest(s) of the controller or of a third party.

CIPL furthermore encourages the EDPB to provide examples of when a third party interest could be considered legitimate in this context.

4. Interaction with Chapter V GDPR

The Guidance confirms that Article 48 must be read in conjunction with Article 44 and emphasises that other grounds may be relied upon in the absence of an international agreement. The Guidelines would overall benefit from more in depth considerations and practical examples regarding the interaction of Article 48 and the transfer mechanisms available in Chapter V GDPR.

5. Adequacy or Appropriate Safeguards

CIPL encourages the EDPB to provide further clarity and especially practical examples regarding the extent to which adequacy findings (Article 45 GDPR) or appropriate safeguards in accordance with Article 46 (2) can be relied on for responses to requests falling under Article 48 GDPR. Where requests from an authority in an adequate country, the responding organisation can rely on the adequacy decision in such a case. Similarly, where an organisation relies on safeguards in accordance with Article

[2] See ANNEX. Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence, p. 3.

46(2) GDPR for the transfer to a third country, practical examples of the potential need for additional safeguards in line with EDPB Guidelines 2/2020 would be helpful, particularly to smaller organisations.

6. Derogations of Article 49 GDPR

CIPL strongly disagrees with the Guidelines assertion that derogations under Article 49 would only find application under the limited conditions where no international agreement exists or an existing agreement does not entail sufficient safeguards. This is not supported by the wording "without prejudice to other grounds for transfer" in Article 48 GDPR. As the European Commission also provides in their amicus curiae in Microsoft v. US, where "none of the grounds in Article 45 to 47 apply a transfer to a third country thus could proceed" where it qualifies under Article 49, outside of Article 48.[3]

CIPL welcomes the EDPB's explicit mention of both the public interest[4] and defence of legal claims[5] derogations of Article 49 GDPR in this context. However, we believe this guidance would provide an opportunity for more in-depth and practical guidance on potentially appropriate derogations for requests from a third country authority.

As the EDPB acknowledged, requests from third country authorities can take a number of forms and have varied purposes, including for example access by foreign authorities to data of their own citizens located in the EEA they may be entitled to or access to data held by regulated entities as part of oversight function in the third country to which the organisation may be subject.[6]

Additionally, organisations may receive requests from third country authorities for in situations of emergency to protect vital interest in accordance with Article 49(1)f.

Further practical guidance regarding the application of the derogations under Article 49 GDPR in circumstances where organisations are subject to GDPR and foreign law will support legal certainty.

[3] Brief of the European Commission on behalf of the European Union as amicus curiae in support of neither party in the matter of a warrant to search a certain email account controlled and maintained by Microsoft Corporation v. United States of America.
[4] Article 49(1)(d) GDPR
[5] Article 49(1)(e) GDPR.
[6] For example, access to books and records that may contain personal data in scope of the GDPR by the US Securities and Exchange Commission held by EEA domiciled organisations listed on a US exchange. The ICO had occasion to provide an in-depth analysis for such cases under the UK GDPR: Securities and Exchange Commission transfer analysis. https://ico.org.uk/media/for-organisations/documents/2619110/sec-letter-20200911.pdf.