cleura

27 January 2025

Cleura AB's comment on the public consultation of EDPB Guidelines 02/2024 on Article 48

Cleura takes this opportunity to comment on the public consultation version of the EDPB 02/2024 guidelines on Article 48 GDPR adopted on 2 December 2024 (the 'draft guidelines'). Specifically, this comment concerns para. 25-26 and 29-30 of the draft guidelines.

Background

Cleura is a European provider of cloud infrastructure services (IaaS) focused on security and compliance. This is a market where US hyperscalers are aggressively attempting to paint themselves as viable alternatives for processing personal data in full respect of EU law.

Cleura has noted numerous examples of abuse and lack of due process, also recently, in relation to different forms of US surveillance. **For example, in May 2023, it was revealed that the FBI had conducted more than 278 000 unauthorised searches of an intelligence database containing FISA 702 information.**[1]

Cleura has historically had data center regions outside the EU, including in the US, but relatively recently decided to discontinue those satellite regions to focus on its home market Europe. This has reduced Cleura's and our customers' exposure to third-country legal regimes, including those lacking with respect to fundamental rights.

Without a significant business presence in the US, it becomes more difficult for US authorities to attempt to pressure Cleura into giving access to data in violation of EU fundamental rights, even when Cleura processes those data entirely in the EU. **US authorities cannot target Cleura assets in the US and use them as leverage if such assets do not exist.**

US cloud service providers, on the other hand, boast rigorous compliance with requirements under US law to disclose personal data.

When the GDPR allows for disclosures of personal data

As a cloud service provider with Swedish roots, and data center regions and operational staff across the EU/EEA only, everyone at Cleura is acutely aware of their responsibilities under the GDPR to safeguard Cleura customers' data when Cleura provides cloud services.

In particular, as a processor of personal data under the GDPR, it is a crucial responsibility for Cleura to **only** process those data according to our controllers' instructions (typically our customers, or our customers' customers), unless required to do so under **EU law or EU/EEA member state law**. For example, this might be a disclosure demand from Swedish police, valid under Swedish law. In such a case Cleura will be loyal to the EU and member state legal order and

1 The Wall Street Journal, FBI Searched Jan. 6 Rioters and George Floyd Demonstrators in Spy Database and The Register, FBI abused spy law but only like 280,000 times in a year. The Register further reports that among those monitored were a US senator, a state senator and a state judge.

comply with the legal requirement. At the same time, this means Cleura does not disclose personal data in response to unilateral extraterritorial third-country demands.

This is entirely logical, as we would not expect our EU customers to comply with such third-country requirements either.

In fact, complying with the controller's instructions, except when otherwise required under EU or member state law, is an obligation on both controllers and processors explicitly mentioned in multiple places in the GDPR. **It is written into Article 28(3)(a). It is written into Article 29. It is written into Article 32(4).** And the legislator specifically describes and points out the problem with unilateral, extraterritorial third-country laws in **Recital 115**.

The fact that some cloud service providers are capable of complying with these requirements, while others are not, is a different matter.

As then-president of the CJEU, Judge Koen Lenaerts, pointed out in this context in 2015: "Europe must not be ashamed of its basic principles: The rule of law is not up for sale."[2]

Furthermore, the EU legislator has established a legal avenue which appears appropriate for enabling processors such as cloud service providers to legally disclose personal data to third-country authorities. **That legal avenue consists of international agreements between third countries and the EU or member states, as stipulated in Article 48 GDPR.** Such an international agreement could enable cloud service providers to point to a legal instrument under EU or member state law, allowing them to disclose data despite the default requirement to only process those data according to the controller's instructions.

However, such an agreement does not appear to exist between the EU and the US in the context of disclosures under US surveillance laws. An adequacy decision is not an international agreement. An agreement for e-evidence related to criminal investigations has been under negotiation but is yet to materialise. Crucially, no agreement exists enabling cloud service providers to disclose personal data under US intelligence gathering laws such as FISA 702. Those are the laws the CJEU found not clear and precise enough to enable sufficient protection against the risk of abuse.

Even the president of a big US cloud company has underlined the need for international agreements, saying "We also need a new generation of international agreements that define when and how governments will seek data stored within other countries' borders, starting with our European allies. The United States cannot build a stronger alliance of the world's democracies without clear international rules to protect the privacy of each other's data."[3]

It seems to us that if the EU legislator had intended for controllers and processors to be able to comply with unilateral demands under third-country laws to disclose personal data, the legislator wouldn't have repeatedly, explicitly and exclusively demanded that a requirement must be made under **EU law or EU/EEA member state law** to allow a processor to depart from its controller's instructions. This also appears consistent with the fact that the EU legislator put a spotlight on the problem with unilateral extraterritorial third-country laws in the GDPR's recitals, while pointing to international agreements as the way forward.

It goes without saying that it is not the EDPB's place to precede the established process necessary to enter into such international agreements, with the associated opportunity for citizens to engage in debate and hold their politicians to account.

2 The Wall Street Journal, European Court Chief Defends Decision to Strike Down Data-Transfer Agreement.
3 Brad Smith, The Washington Post, The Secret Gag Orders Must Stop.

Legal basis for disclosures of personal data to national authorities

With that established, we can turn to the legal question we are commenting on in para. 25-26 of the EDPB's draft guidelines.

When a processor – such as a cloud service provider – is required to disclose personal data to comply with a legal obligation, the provider becomes a controller for its processing when locating and disclosing the data. All controllers need a legal basis under Article 6 GDPR to process personal data. In this situation the GDPR has one legal basis which fits perfectly: Article 6(1)(c), used when **processing is necessary for compliance with a legal obligation to which the controller is subject**. Furthermore, Article 6(3) GDPR requires this legal obligation to be laid down by **EU law or member state law**. This is entirely in line with previously mentioned GDPR provisions which uphold the same requirement when a cloud service provider deviates from its controller's instructions, such as to disclose personal data to national authorities.

However, in para. 25-26 of the draft guidelines, the EDPB considers the possibility for companies to rely on **Article 6(1)(f), a legitimate interest assessment**, as a legal basis for transfers or disclosures to third country authorities. The draft guidelines state that the EDPB "**assumes** that [this] **may** be possible … in **exceptional** circumstances" and that "**a controller**, in some cases, may have a **legitimate interest** to comply with a **request to disclose personal data** to a third country authority" (Cleura's emphasis).

It is critical to point out that Article 6(1)(f) **does not** explicitly require the controller to have a legal obligation laid down by **EU or member state law** to process (e.g. disclose) personal data, while Article 6(1)(c) **does** have a specific requirement to this effect through Article 6(3).

Cleura here notes the EDPB's own 1/2024 Article 6(1)(f) version 1.0 guidelines, which state that the legal basis of legitimate interest should not be "unduly extended to circumvent **specific legal requirements** or because it would be considered as **less constraining than the other legal bases in Article 6(1) GDPR**." and that "In any event, a legitimate interest may not be invoked with the **aim or effect** of circumventing legal requirements." (Cleura's emphasis).

Cleura further notes that the 02/2024 draft guidelines state that a controller may have a legitimate interest to comply with a "request" to disclose personal data. It is unclear if the EDPB therefore considers Article 6(1)(f) to only be potentially usable in response to *requests*, but not *requirements*, to disclose personal data. However, we also note that the first sentence of para. 25 of the draft guidelines uses more general wording. We therefore assume that the EDPB considers it possible to, at least in some cases, rely on Article 6(1)(f) in response to *requirements* under third-country laws to disclose personal data.

To justify its view in the draft guidelines, the EDPB references CJEU case C-252/21 (Meta Platforms Inc and Others v Bundeskartellamt), para. 124 and 132. However, para. 124 of that case in essence states that **a company's (controller's) objective of sharing information** with law-enforcement agencies to prevent, detect and prosecute criminal offences, **is not capable, in principle**, of constituting a legitimate interest pursued **by the company (controller)** under **Article 6(1)(f)** GDPR.

In para. 124, the CJEU says that this objective can conversely justify processing by a company where this is "objectively necessary for compliance with a legal obligation" to which that company is subject. This is the case when a company is required under law to disclose personal data. The legal basis of Article 6(1)(c) **thus appears to fit perfectly in these situations,** also when a cloud service provider is required to disclose personal data to national authorities.

In para. 132 of case C-252/21, the CJEU in essence notes that it will be for the referring court to, **inter alia**, inquire whether the company at issue in the case is under a legal obligation to collect

and store personal data with a view to being able to share those data with national authorities. This part must be read against the background of the circumstances at issue in the case and the CJEU's conclusion in para. 124 that Article 6(1)(c) was the proper legal basis, whereas Article 6(1)(f) was not.

Again, this was because a company's (controller's) **objective** of sharing information with law-enforcement agencies to prevent, detect and prosecute criminal offences, **was deemed not capable, in principle**, of constituting a legitimate interest pursued **by the company (controller)** under Article 6(1)(f) GDPR.

Despite this, the EDPB appears to suggest that a company can **disclose** personal data just fine under Article 6(1)(f) GDPR for this objective, **but not collect or retain those data**.

It would appear helpful to point out that companies can perform different types of processing, **all with the objective of sharing information with national authorities**.

For example, personal data might be *collected* with a view of being able to share those data with national authorities. Personal data previously collected (even without a view of being able to share those data with national authorities) might be *stored* with a view of being able to share those data with national authorities. **And, importantly, personal data previously collected or stored (even without a view of being able to share those data with national authorities) might be *shared* with national authorities. In all three examples,** personal data are **processed** with the **objective** of sharing information with national authorities.

Para. 124 of case C-252/21 in essence states that the **objective** of sharing information with national authorities, **is in principle an objective not capable of being a legitimate interest pursued by a private company under Article 6(1)(f)**.

The CJEU notes in particular that this objective is **unrelated to the economic and financial activity of the private company at issue in the case**.

In its draft guidelines however, the EDPB restricts its interpretation of the above-mentioned case to mean, in essence, that the objective which cannot be pursued by a private company is **only** the *collection and storing* of personal data with a view of being able to share those data with national authorities. On the other hand, the EDPB considers that *sharing* those data can apparently be a company's legitimate interest, even while the *collection and storing* cannot. **The EDPB thereby excludes the actual sharing of personal data with national authorities from the objective of sharing information with national authorities.**

The EDPB does not explain how it arrives at this illogical conclusion. The conclusion appears to go against a plain-text reading of the CJEU's judgment in case C-252/21 where the CJEU specifically mentions that the **objective** relating to the sharing of information with law-enforcement agencies is in principle not capable of being a legitimate interest pursued by a private operator such as the one in that case.

The EDPB's conclusion is especially unconvincing because the CJEU's reasoning points out that the objective of sharing information with law enforcement agencies is unrelated to the private company's economic and financial activity. The EDPB does not explain why it only considers a private company's *collection and storage* of personal data in this context as *unrelated* to the company's economic and financial activity, while the company's actual *sharing* of personal data with national authorities is apparently *related* to the company's economic and financial activity.

It can be pointed out that today, the lion's share of Europeans' communications and digital behaviour, and vast amounts of metadata, including location data, are processed by a few US cloud providers who are all subject to the same mandatory US surveillance legislation.

This processing can include creating and collecting large amounts of personal data, and storing those data for long periods of time, on behalf of customers or for the provider's own purposes, even without being ordered to do so by national authorities. Under those circumstances, a person would not necessarily enjoy significantly better protection just because third-country authorities cannot require a cloud provider to collect or retain their data (which is likely to be collected and stored anyway), while the same authorities can compel disclosures of those data.

The draft guidelines proceed to touch on the elements of a legitimate interest assessment, and state that "**the outcome of the balancing test determines** whether the legal basis of legitimate interest may be relied upon for **the processing**." (Cleura's emphasis). **The processing** here refers to the **transfer or disclosure** of personal data to the authorities, or in other words, a private company's sharing of information with third-country authorities.

It should be recalled that before a controller can perform a balancing test, it must establish whether a valid, legitimate interest is pursued. This is all the more important because if balancing tests in these situations were allowed they would happen in secret. **A cloud service provider required to disclose personal data under an intelligence gathering law is likely to receive little to no information about the circumstances behind a disclosure requirement, and even less about the possible consequences for and interests of the person concerned.** At the same time, the provider may find itself pressured to arrive at a result in favour of disclosing the data, with an at best assumed but unverified trust in the national authorities in one hand and a looming fine in the other.

Para. 25-26 of the draft guidelines should be revised to reflect the CJEU's position, discarding Article 6(1)(f) as a legal basis when third-country authorities require a company such as a cloud service provider to disclose personal data.

As mentioned, in situations where a cloud service provider receives a disclosure demand for personal data, the GDPR has one legal basis which fits perfectly: Article 6(1)(c), used when **processing is necessary for compliance with a legal obligation to which the controller is subject**. This means Article 6(3) GDPR applies as well, upholding the requirement that the legal obligation must be laid down by EU law or member state law.

This is entirely in line with previously mentioned GDPR provisions which uphold the same requirement in the context of disclosures to national authorities.

Article 48 is a ground for transfer under Chapter V GDPR

We will now comment on para. 29-30 of the draft guidelines.

Para 29 reads as follows (Cleura's emphasis):

> **Unlike the other provisions of Chapter V, Article 48 is not a ground for transfer.** The provision itself contains no data protection safeguards but clarifies that decisions or judgments from third country authorities cannot be recognised or enforced in the EU/EEA unless an international agreement provides for this. **Therefore, before responding to a request from a third country authority falling under Article 48, the controller or processor in the EU/EEA must identify an applicable ground for the transfer elsewhere in Chapter V.**

We will also quote Article 48 in its entirety (Cleura's emphasis):

> *Transfers or disclosures not authorised by Union law*
> Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose 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.

In Cleura's view, Article 48 **does** appear to be a ground for transfer, contrary to what the draft guidelines claim. Article 48 references **other** grounds for transfer pursuant to Chapter V, implying that Article 48 itself is also a ground for transfer. Specifically, this ground for transfer can be used when there is an international agreement, such as a Mutual Legal Assistance Treaty (MLAT), in place between the third country and the EU or a member state. It seems to us that appropriate safeguards, enforceable data subject rights and effective legal remedies could to the extent necessary be provided through the international agreement required by Article 48. A controller or processor could then refer to this to perform the transfer.

Para 30 reads as follows (Cleura's emphasis, citation omitted):

> According to Article 46(2)(a) 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**. Such agreements are concluded by states and traditionally allow for cooperation between public authorities, but may also provide for direct cooperation between private entities and public authorities. (…)

In Cleura's view, Article 46(2)(a) **does not** appear to give an example of an international agreement under Article 48, contrary to what the draft guidelines claim. The appropriate safeguard in Article 46(2)(a) is "a legally binding and enforceable instrument **between public authorities or bodies**" (Cleura's emphasis). That is something different than an international agreement between **a third country** on the one hand and **the EU or a member state** on the other, as Article 48 requires. The GDPR uses clearly different terminology in Article 46(2)(a) compared to Article 48, indicating the legislator intended those articles to refer to different things.

Concluding remarks

The draft guidelines do not correctly interpret the GDPR, presumably by misunderstanding its provisions, in a manner which circumvents crucial GDPR protections against third-country extraterritorial legislation. Cleura therefore urges the EDPB to revise the draft guidelines.

Today, the lion's share of Europeans' communications and digital behaviour, and vast amounts of metadata, including location data, are processed by a few US cloud providers who are all subject to the same mandatory US surveillance legislation (such as FISA 702). This processing can include creating and collecting large amounts of personal data, and storing those data for long periods of time, on behalf of customers or for the providers' own purposes, even without being ordered to do so by national authorities.

Some cloud service providers claim that they have received relatively few disclosure demands from US authorities, at least on the basis of certain legal provisions, categories of requests, customer segments, services, or data types. Such claims may, for example, mention the number of disclosures of "customer data" or "content data" for a customer segment. However, these claims do not necessarily cover metadata, which can potentially be as sensitive as the contents of

communications.[4] The claims might in particular not cover metadata created or collected by the cloud service providers themselves.

All the terms of US cloud service providers that we have reviewed, in effect give the US legal system priority over the EU legal system. US cloud service providers present this as self-evident, that they, as US companies, must naturally comply with disclosure requirements under the US legal system. **US cloud providers thus expect it to be equally self-evident that their customers in the EU must give up the sovereignty of their own legal system in favour of the US legal system.**

The EDPB's interpretation of the GDPR in the draft guidelines unfortunately aligns with this view. It goes beyond the EU legislator's intent as well as a plain-text reading of the GDPR and CJEU case law. If adopted as a final version, the guidelines would promote a legal interpretation which undercuts the sovereignty of EU law and is likely to embolden the US government and US cloud providers in the view that it is entirely acceptable to the EU that vast amounts of personal data are within reach of US surveillance.

The EDPB would do this at a time when protection against the risk of abuse by an unfettered executive branch, and upholding the rule of law, appear as relevant as they have ever been in relation to Europeans' personal data since the fall of the Berlin wall.

Sincerely,

Arman Borghem
Regulatory and Compliance Advisor
Cleura AB

arman.borghem@cleura.com
+46 76 103 64 68

4 Depending on the nature of the cloud service, metadata could include information about when a person has used a service, from which approximate locations (through the IP address), with whom communication has taken place and how often, etc. Thus, more than just content data can be sensitive. The CJEU has noted that *"traffic and location data may reveal information on a significant number of aspects of the private life of the persons concerned, including sensitive information such as sexual orientation, political opinions, religious, philosophical, societal or other beliefs and state of health, given that such data moreover enjoys special protection under EU law. Taken as a whole, that data may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them. In particular, that data provides the means of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications"* (joined cases C-511/18, C-512/18 and C-520/18 La Quadrature du Net, p. 117, Cleura's emphasis).