COMMENT/POLICY BRIEF

Response to public consultation on EDPB Guidelines 02/2024 on article 48

Safespring wishes to thank the EDPB for this opportunity to comment on the public consultation version of the EDPB 02/2024 guidelines on Article 48 GDPR (the 'draft guidelines'). In the following, we will limit our comments to the texts proposed for para. 25-26 and 29-30 of the guidelines.

In summary, we do not agree that GDPR Art 6.1.f is an appropriate legal basis for disclosure of Europeans' personal data to foreign intelligence agencies for reasons detailed below. We also do not agree that GDPR Art 48 is not a ground for transfer of personal data. We do not agree that GDPR Art. 46.2.a contains language equivalent to GDPR Art. 48. Instead, GDPR Art. 46.2.a points to the necessity of a legally binding instruments between states or international organisations. We will provide greater detail in this argument below.

Background

Safespring is a Scandinavian provider of cloud services specialised in the academic and public sectors. We provide storage, compute and back-up services based on open source software to a range of Nordic and European clients including the European Commission. Since 2017, we operate out of the Swedish and Norwegian markets with a pan-European staff.

In this capacity, we are well placed to understand the increasing concerns of public and academic institutions to maintain solid operational, legal and technical security. In the past decade, customers of cloud services are becoming more aware of risks to their data and demanding increasing attention of service providers to both organisational and technical security measures. We believe this is in line with the ambitions of the European legislators as expressed in the General Data Protection Regulation (GDPR), the Network and

Safespring AB
Rättarvägen 3, 169 68 Solna
www.safespring.com

Tel: +46 (0)8-551 073 70
info@safespring.com

Information Security Directives (NIS and NIS2) as well as the Cyber Resilience Act (CRA) and Digital Operational Resilience Act (DORA), among others.

In particular, customers are increasingly asking Safespring not only for technical guarantees but also for legal guarantees. They want to maintain jurisdictional and legal control over their data assets, and have any access, collection or disclosure requirements operational only in jurisdictions where they themselves have legal rights. Our customers also feel that this is a responsibility - moral as well as legal - with respect to data subjects, and as a service provider we agree with this.

GDPR rules on data disclosure

In the following section, we will detail our view on when the GDPR allows for disclosures of personal data. Operating out of Sweden and Norway with security-sensitive customers in the EU/EEA area, we are acutely aware of our and our customers' obligations under the GDPR, and it is something that we train and make our staff highly aware of while we develop and provide services.

Safespring acts as a data processor under the legal framework of the GDPR. As such, we can only process data according to controllers' instructions. These instructions become binding on us either through a direct interaction with a customer, or through an indirect relationship between our customers and their customers. **The only possibility we have of processing personal data beyond these instructions must come from EU law or EU/EEA member state law.**

A Swedish or Norwegian public authority may, for instance, direct a demand at Safespring to disclose data and in this case Safespring would comply with this demand. However, Safespring cannot disclosure personal data in response to unilateral demands from third-countries.

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, for instance, mentioned in

- GDPR Art. 28.3.a,
- GDPR Art 29,
- GDPR Art. 32.4, and
- the legislator notes the problem with unilateral, extraterritorial third-country laws in Recital 115.

There is a mechanism to enabe processors such as cloud service providers to legally disclose personal data to third-country authorities. This mechanism is contained in GDPR Art. 48 and consists in "international agreements between third countries and the EU or member states".

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.**[1] An agreement for e-evidence related to criminal investigations is under negotiation but is not yet in place. No agreement enabling cloud service providers to disclose personal data under US intelligence gathering laws such as FISA 702 is known.

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. That this requirements complicates the legal situation for cloud service providers based in third countries is beside the point. As CJEU Chief 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]

Comments on para. 25-26 in draft guidelines

When a processor – for instance Safespring – is required to disclose personal data to comply with a legal obligation, we become a controller for the processing of locating and disclosing the data. All controllers need a legal basis under GDPR Art. 6 to process personal data. In this situation the GDPR has one legal basis which fits perfectly: Art. 6.1.c, used when processing is necessary for compliance with a legal obligation to which the controller is subject. GDPR Art. 6.3 requires this legal obligation to be laid down by EU law or member state law.

However, in para. 25-26 of the draft guidelines, the EDPB considers the possibility for companies to rely on **GDPR Art. 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*".

It is critical to point out that GDPR Art. 6.1.f does not explicitly require the controller to have a legal obligation laid down by EU or member state law.

The conclusions of the EDPB in this regard are surprising, not in the least because EDPB's own 1/2024 Article 6(1)(f) version 1.0 guidelines, 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.*" The EPBD, in guidelines 1/2024, also observes that "*[i]n any event, a legitimate interest may not be invoked with the **aim or effect** of circumventing legal requirements.*" (Safespring's emphasis).

[1] Safespring in either case argues that the recent moves by the new US administration to reduce the size and viability of PCLOB (https://www.nytimes.com/2025/01/22/us/trump-privacy-civil-liberties-oversight-board.html) calls into question the viability of the adequacy decision currently in force.

[2] https://www.wsj.com/articles/european-court-chief-defends-decision-to-strike-down-data-transfer-agreement-1444768419

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 GDPR Art. 6.1.f to only be potentially usable in response to *requests*, but not *requirements*, to disclose personal data.

This distinction is important since in the first case, where the EDPB would consider that only heeding to requests is permissible under the legal basis of legitimate interest, a data processor could formulate its terms and conditions in such a way that it becomes clear to the data controller that the processor reserves the right to respond to requests from third-country authorities under terms determined by those authorities and the processor. In the second case, the EDPB would justify forced action against a processor by a third-country authority that therefore would not have to be disclosed beforehand to the controller, and could not therefore be included in the controller's risk management program.

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 controller's objective of sharing information** with law-enforcement agencies to prevent, detect and prosecute criminal offences, **is not capable** of constituting a legitimate interest pursued by the controller under GDPR **Art. 6.1.f.**

The CJEU in the same paragraph instead points to disclosures needing to be "objectively necessary for compliance with a legal obligation to which that operator is subject." This is the case when a company is required under law to disclose personal data. The legal basis of GDPR Art. 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 notes that it will be for the referring court to 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 GDPR Art. 6.1.c was the proper legal basis, while GDPR Art. 6.1.f was not.**

In spite of this clear argument by the Court, the EDPB seems to imply that a company can disclose personal data under GDPR Art. 6.1.f for the objective of sharing information with law enforcement agencies to prevent, detect and prosecute criminal offences, but perhaps not to collect or retain those data.

Companies, whether controllers or processores, can collect or store different personal data with the objective of sharing information with national authorities, including law enforcement authorities. Data may be processed specifically for this objective, or data which is processed for a different objective may be capable of being made available to such national authorities under a new objective. What para. 124 of case C-252/21 seems to state, is that the objective of sharing information with national authorities, is not capable of being a legitimate interest pursued by a private company under GDPR Art. 6.1.f. In the same

paragraph, the Court notes that the assessment of this objective is unrelated to the economic and financial activity of the private company at issue in the case.

Surprisingly, the EPBD instead concludes that it is only the objective of specifically collecting data for the purpose of disclosing it to law enforcement authorities that could be covered by this ruling. 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.

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.

Para. 25-26 of the draft guidelines should be revised to reflect the CJEU's position, discarding GDPR Art. 6.1.f as a legal basis when third-country authorities require a company such as a cloud service provider to disclose personal data. The GDPR legal basis contained in Art. 6.1.c should instead be used when processing is necessary for compliance with a legal obligation to which the controller is subject. This means GDPR Art. 6.3 applies as well, upholding the requirement that the legal obligation must be laid down by EU law or member state law.

Para 29-30 of the draft guidelines

GDPR Art. 48 reads as follows:

> *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 Safespring's view, the literal text of GDPR Art. 48 does appear to be a ground for transfer when there is an international agreement, such as an Mutual Legal Assistance Treaty (MLAT), in force between the third country and the Union or Member State. That GDPR Art. 48 also references other grounds for transfer does not detract from this obligation. 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.

However, para 29 of the draft guidelines reads:

> Unlike the other provisions of Chapter V, Article 48 is not a ground for transfer[.]

Safespring does not agree with or understand this conclusion given the literal text of GDPR Art. 48.

The EDPB goes on in para 30 to state:

> 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[.]

Safespring does not understand how the "legally binding and enforceable instrument between public authorities or bodies" could be considered equivalent to "an international agreement, such as a MLAT, in force between the requesting third country and the Union or a Member State". The GDPR uses clearly different terminology in GDPR Art. 46.2.a compared to GDPR Art. 48, which reasonably means the legislator intended to refer to different things in those articles.

Concluding remarks

The draft guidelines do not correctly interpret the GDPR, and misconstrue its provisions in a manner which circumvents crucial GDPR protections against third-country extraterritorial legislation. Safespring therefore urges the EDPB to reconsider its position.

It can be pointed out that today, the vast majority 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 (FISA 702, CLOUD Act, and others). 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.[3] The claims might in particular not cover metadata created or collected by the cloud service providers themselves. There is also no way of knowing if the published figures are correct.

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.

Safespring urges the EDPB to reconsider this position. Now more than ever, it is necessary for Europe not to be ashamed of its legal principles or the primacy of its own law. Digital sovereignty and self-determination requires all aspects of the European legal system to work in favour of Europeans, and aligning the guidelines with existing legal texts and jurisprudence would contribute to this goal.