BCLP. Client Intelligent

Insights

UPDATED EU DATA TRANSFERS GUIDANCE

WHEN IS A TRANSFER NOT A "TRANSFER"? AND CAN YOU BE HELD RESPONSIBLE FOR PERSONAL DATA OVERSEAS EVEN WITHOUT A PRECEDING "TRANSFER"?

Mar 17, 2023

The updated guidelines (05/2021) from the European Data Protection Board ("**EDPB**") issued on 14 February 2023 (the "**New Guidelines**") look at the interplay of two fundamental, protective mechanisms contained in the EU GDPR. These are (a) extra-territorial ("long arm") application of the regulation (Article 3) and (b) restricting outbound transfers of personal data from the EU to inadequately protective third countries (Chapter V). The New Guidelines follow a public consultation and update the version adopted on 18 November 2021 (the "**Draft Guidelines**"), discussed in our alert. In this briefing we summarise the effect of the New Guidelines and comment on changes introduced since the Draft Guidelines.

As noted above, the EU GDPR has two main mechanisms for ensuring that personal data with a sufficient nexus to the EU is "protected". Fundamental to this is: what is meant by a "transfer"? The New Guidelines also describe safeguards, which need to be put in place where "EU" personal data is being processed outside the EEA even where there has been no "transfer".

THE THREE CRITERIA REQUIRED FOR A "TRANSFER"

The EDPB notes that the EU GDPR does not provide a legal definition for the notion of a "transfer to a third country or to an international organisation" and that relevant case law is limited. The three cumulative criteria below are provided as clarification of the EDPB's views (the criteria have not changed in substance since the previous version). As well as assisting controllers and processors, this clarification is also described as "important for the consistent interpretation and application of the GDPR by the supervisory authorities" – this is an interesting observation at a time where focus is being given to the increasing the effectiveness of pan-EU cooperation of the supervisory authorities under the cooperation and consistency mechanisms under Chapter VII of the EU GDPR.

The three transfer criteria are:

- A controller or processor is subject to the EU GDPR for the given processing; and

- This controller or processor ("exporter") discloses by transmission, or otherwise makes personal data, subject to this processing, available to another controller, joint controller or processor ("importer"); and
- The importer is in a third country, irrespective of whether or not this importer is subject to the EU GDPR for the given processing in accordance with Article 3, or is an international organisation".

TRANSMISSION OR OTHERWISE MAKING AVAILABLE – A BROAD CONCEPT

A transfer does not require transmission of personal data; it needs only for personal data to be "made available". Examples in the New Guidelines of personal data being "made available" to an importer in a third country include (i) creating an account; (ii) granting access rights to an existing account; (iii) confirming or accepting a request for remote access; (iv) embedding a hard-drive, or (v) submitting a password to a file. Interpreted literally, the New Guidelines indicate that facilitating access will be considered equivalent to disclosure even if access has not yet taken place or (query) does not take place.

REMOTE ACCESS

The EDPB confirms that remote access from a third country will be considered a transmission to/making available in such third country (even if it takes place only by means of displaying personal data on a screen, for example, in technical support situations, troubleshooting or for administration purposes) and/or storage in a cloud outside the EEA offered by a service provider.

TRANSFER AND NON-TRANSFER SCENARIOS FROM THE NEW GUIDELINES

In the table below we include some notable examples from the New Guidelines.

No.	Example (from New Guidelines)	Transfer?
1-3	An online consumer based in the European Union ("**EU**") provides their personal data *directly* to an online retailer based outside of the EU.	No
-	The sharing of personal data by an organisation located in the EU to a **branch** located outside of the EU (i.e. personal data is not being disclosed to a legally separate controller or processor).	No
6	Personal data of non-EU located individuals is sent "home" from a processor based in the EU, to the controller based outside of the EU.	Yes
8	An employee of an EU organisation on a business trip to a	No

	jurisdiction outside of the EU has access to personal data via their laptop.	
9	An Irish company, which is a subsidiary of a parent company in a third country, transfers personal data of its employees to be stored in the centralised HR database by the parent company in the third country.	Yes
11	Remote access by a third country processor to personal data stored in the EU, where the processor is acting on behalf of an EU controller.	Yes

SAFEGUARDS TO BE PROVIDED IF PERSONAL DATA IS PROCESSED OUTSIDE THE EEA BUT NO "TRANSFER" TAKES PLACE

Scenarios added to the New Guidelines underscore that controllers remain accountable for their processing activities **wherever** these take place, even if a "transfer" has not technically occurred.

The risks associated with processing personal data in a given third country must still be accounted for by the responsible controller in determining what measures to take in order to ensure compliance with the EU GDPR (for instance, in respect of security and, where required under Article 35 EU GDPR, completing data protection impact assessments). In fact, the controller or processor should "pay particular attention to the legal frameworks of the third country that may have an impact on its ability to respect the GDPR". In certain cases, a controller might conclude that significant security measures are necessary, or even that the risk of government access / surveillance is so high that the processing cannot be conducted lawfully in that jurisdiction. The New Guidelines suggest that specific measures may be needed, such as preventing employees from taking their work laptops to high-risk countries.

CAN PROCESSORS SUBJECT TO THIRD PARTY LEGISLATION PROVIDE SUFFICIENT GUARANTEES?

Under Article 28(1) of the EU GDPR, controllers must only use processors that can provide sufficient guarantees that technical and organisational measures are taken to ensure compliance with the EU GDPR. The New Guidelines consider the scenario of an EU based controller that engages an EU based processor which is also subject to third country legislation. In such cases, controllers are directed to consider the likelihood of the processor receiving government access requests under that third country legislation (on the basis that compliance with those requests could result in a transfer of personal data).

When assessing whether a processor can provide sufficient guarantees, controllers should not only consider expertise and resources, but also "reliability" (which may be in doubt if the processor is subject to third country legislation that will prevent it from fulfilling its EU GDPR obligations as a processor). The EDPB also directs controllers to consider whether using such processors could

undermine the controller's responsibility for ensuring the lawfulness of processing and respect for the principles of integrity and confidentiality, since both could be hindered by the prospect of government access requests.

If a processor that is subject to third country legislation then complies with a government access request, in violation of the controller's documented instructions, the processor will become an independent controller in respect of that processing (in accordance with Article 28(10) of the EU GDPR).

TRANSPARENCY OBLIGATIONS

The New Guidelines state that when a controller intends to process personal data outside of the EEA (in circumstances where no "transfer" takes place), this information "should as a rule be provided to individuals as part of the controller's transparency obligations". It is unclear what lengths the EDPB is expecting organisations to go to in practice, e.g. in the case of employees making international business trips, is the EDPB expecting all potential destination countries to be included in the organisation's privacy policies? This would appear impracticable.

A NEW SET OF STANDARD CONTRACTUAL CLAUSES: TRANSFERS TO IMPORTERS SUBJECT TO THE EU GDPR

As the European Commission has confirmed in relation to the standard contractual clauses for transfers to third countries issued in June 2021 (the "**SCCs**"), the SCCs cannot be used where the recipient in a third country is **already subject to the EU GDPR.** The European Commission confirmed in its FAQs last year that it was developing a new set of standard clauses for that situation and the EDPB takes this opportunity to encourage the completion of such clauses.

CONCLUSION

The New Guidelines increase the clarity on what qualifies as a transfer under the EU GDPR. However, they also increase uncertainty in other respects.

What steps will organisations be expected to take where they are responsible for processing taking place in a third country where no "transfer" has occurred (and therefore the protection built in to Chapter V does not apply)? To what extent does the risk assessment, implicit in the New Guidelines for such non-transfer processing, overlap with more familiar post-Schrems II Transfer Impact Assessments? In terms of transparency, will EU supervisory authorities expect organisations to account for possible third country destinations visited by their employees on business trips? What constitutes "sufficient guarantees" from a processor in circumstances where the processor could find itself subject to subpoenas or other information requests from third country governments?

In view of these unresolved areas, it will be important to monitor closely the developing practice and enforcement by the individual EU member states' supervisory authorities. The EDPB has also

stated it will assess the need for additional guidance to be issued on safeguards in relation to processing in third countries. If you would like to discuss any of the matters covered by this note, please contact the authors or any member of our Data Privacy & Security Team.

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Geraldine Scali

London

geraldine.scali@bclplaw.com
+44 (0) 20 3400 4483
