European Data Protection Board Issues Guidance about International Data Transfers

Date : July 9, 2021

Introduction

The European Data Protection Board (EDPB) recently finalised and published its guidance on international data transfers entitled “Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data” (“Recommendations”). This article looks at this development in brief.

What’s this all about?

Under General Data Protection Regulation (GDPR) international data transfers can only be made in certain ways and subject to various conditions. These include country Adequacy Decisions (the EU recently issued ones for the UK, which we’ve written about here https://www.corderycompliance.com/eu-dpa-decisions-approved/), Binding Corporate Rules, and, probably the most relied on mechanism, Standard/Model Contract Clauses (SCCs - the EU recently issued new ones, which we’ve written about here https://www.corderycompliance.com/eu-new-sccs-for-idts/).

The European Court’s summer 2020 Schrems ruling (which we’ve written about here https://www.corderycompliance.com/ecj-rules-scc-valid-not-ps/) upheld SCCs but stated that data controllers data or processors, acting as exporters, are responsible for verifying, on a case-by-case basis and, where appropriate, in collaboration with the importer in the third country, if the law or practice of the third country impinges on the effectiveness of the appropriate safeguards (for data transfers) contained in GDPR. In these cases the European Court left open the possibility for data exporters to implement supplementary measures to fill in gaps in protection, but did not specify what these measures could be.

The EDPB has adopted its Recommendations in order to help data exporters with the complex task of assessing third countries and identifying appropriate supplementary measures where needed. The Recommendations provide exporters with a series of steps to follow, potential sources of information, and some examples of supplementary measures that could be put in place.

Some GDPR special terms are used in this note which are defined in our glossary at www.bit.ly/gdprwords.

What are the highlights of the Recommendations?

The Recommendations are set out in six steps, which in summary form are as follows:

- **Step One:** Know your transfers. Being aware of where personal data goes is necessary to ensure that it is afforded an essentially equivalent level of protection wherever it is processed. Also verify that the data transferred is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- **Step Two:** Verify the transfer tool the transfer relies on (amongst those listed in GDPR). If the European Commission has already declared the country, region or sector to which the data is to be transferred to as adequate, no further steps are needed. In the absence of an Adequacy Decision, determine which one of the transfer tools listed in GDPR can be relied on. GDPR also provides for some derogations if certain conditions are met;
- **Step Three:** Do due diligence. Assess if there is anything in the law and/or practices in the third country that may impinge on the effectiveness of the appropriate safeguards of the transfer tools intended to be rely upon, in the context of the specific transfer. The assessment should focus first and foremost on third country legislation that is relevant to the transfer in question. Examining also the practices of the third country’s public authorities will allow for verification if the safeguards contained in the transfer tool can

ensure, in practice, the effective protection of the personal data transferred. Examining these practices will be especially relevant where: (i) legislation in the third country formally meeting EU standards is manifestly not applied/complied with in practice; (ii) there are practices incompatible with the commitments of the transfer tool where relevant legislation in the third country is lacking; and, (iii) the transferred data and/or importer fall or might fall within the scope of problematic legislation (i.e. impinging on the transfer tool's contractual guarantee of an essentially equivalent level of protection and not meeting EU standards on fundamental rights, necessity and proportionality). In the first two situations, either the transfer will need to be suspended, or implement adequate supplementary measures in order to proceed with the transfer. In the abovementioned third situation, in light of uncertainties surrounding the potential application of problematic legislation to the transfer, it may be necessary to: suspend the transfer; implement supplementary measures to proceed with it; or, alternatively, proceed with the transfer without implementing supplementary measures if it can be considered, demonstrated and documented that there is no reason to believe that relevant and problematic legislation will be interpreted and/or applied in practice so as to cover the transferred data and importer. Document all of the above thoroughly. A data protection regulator and/or judicial authorities may request such documentation and hold the organisation accountable for any decision it takes;

- **Step Four:** Identify and adopt supplementary measures that are necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence. This step is only necessary if the assessment reveals that the third country legislation and/or practices impinge on the effectiveness of the particular GDPR transfer tool being or intended to be relied on in the context of the transfer. The Recommendations contain a non-exhaustive list of examples of supplementary measures with some of the conditions they would require to be effective. Some supplementary measures may be effective in some countries, but not necessarily in others. In those cases where no supplementary measure is suitable, the transfer must be avoided, suspended or terminated to avoid compromising the level of protection of the personal data. Document all of this thoroughly;
- **Step Five:** Take any formal procedural steps as required under the supplementary measure(s), as regards the GDPR transfer tool being relied upon. The Recommendations specify some of these formalities; and,
- **Step Six:** Re-evaluate at appropriate intervals the level of protection afforded to the personal data transferred to third countries and monitor if there have been or there will be any developments that may affect it.

What about Brexit?

Following Brexit the UK is no longer part of the EU so the Recommendations will not apply to data transfers from the UK to elsewhere; we've written and made films about Brexit and data protection here https://www.corderycompliance.com/brexit-uk-vs-eu-gdpr-faqs/ and here https://www.corderycompliance.com/dt-after-brexit/ and here https://www.corderycompliance.com/dp-after-brexit/.

The UK's ICO has previously issued guidance about data transfers post Brexit (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/) but whether it chooses to adapt its guidance or adopt new other guidance in light of the EDPB's Recommendations remains to be seen.

The UK will however be adopting its own set of SCCs in due course and is expected to publish draft SCCs this month, which will then be subject to a public consultation.

What about enforcement?

Enforcement of the data transfer rules is a hot topic at the moment particularly with the announcement not so long ago that German data protection regulators had agreed on a questionnaire based approach as a prelude to enforcement (which we've written about here https://bit.ly/gerenforce). There has also been activity in other countries including a suspension of data transfers to Cloudflare despite SCCs being in place (which we've written about here https://bit.ly/schremsport). Data transfer is one of our 5 key themes of the first 5 years of GDPR enforcement. You can find out more about this and watch our film here https://bit.ly/GDPR5film.

What are the takeaways?

Key considerations include the following:

1. It is more than likely that the most appropriate data transfer tool that many will be using is SCCs. The EU has new SCCs and a lot of work will be required to put these in place. We've written about these including detailed takeaways about what to consider as regards putting them in place, which can be found here https://www.corderycompliance.com/eu-new-sccs-for-idts/;
2. Doing the due diligence piece will probably be the biggest part of the work. This can be made easier by e.g. preparing questionnaires for the intended data importers to complete. Also consider doing due diligence on the data importer;
3. Other documentation may also need to be reviewed, e.g. external and internal privacy policies; and,
4. Make sure that everything is documented, especially for accountability purposes.

More information

Cordery's GDPR Navigator includes resources to help deal with data protection compliance. It includes a monthly call to keep up-to-date with GDPR changes across the EU. GDPR Navigator also includes films, template and written guides on topics including:

- Accountability and Audit
- Geographical reach
- Data Controller or Data Processor – what do these terms mean and which are you?
- Fine determination – work out what the consequences of a breach might be
- Appointing processors – how to reduce your risk
- One-stop-shop – determine who your regulator will be
- Binding Corporate Rules
- The security provisions of GDPR

For information about our Cordery GDPR Navigator tool please see
http://www.corderycompliance.com/solutions/cordery-gdpr-navigator/

We report about data protection issues here:
https://www.corderycompliance.com/category/data-protection-privacy/.

The European Data Protection Board guidance can be found here: https://edpb.europa.eu/our-work-tools/documents/our-documents_en.

For more about GDPR please also see our GDPR FAQs which can be found here:
http://www.corderycompliance.com/eu-data-protection-regulation-faqs-3/ and our Data Protection Glossary which can be found here: http://www.corderycompliance.com/?s=glossary.

For more information please contact Jonathan Armstrong or André Bywater who are lawyers with Cordery in London where their focus is on compliance issues.

Jonathan Armstrong, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH
Office: +44 (0)207 075 1784
Jonathan.armstrong@corderycompliance.com

André Bywater, Cordery, Lexis House, 30 Farringd
Street, London, EC4A 4HH
Office: +44 (0)207 075 1785
Andre.bywater@corderycompliance.com