ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Privacy Now: Developments in the European Union

Technology, Privacy, and eCommerce

In the past few months, there have been several key privacy developments. There have been adequacy decisions for the United Kingdom and the beginning of an adequacy decision for South Korea, the issuance of new Standard Contractual Clauses (SCCs), guidance published by the European Data Protection Board (EDPB) on international data transfers, and quite a bit of enforcement and activity around cookies and other online trackers.

Adequacy decisions

United Kingdom

On June 28, 2021, the European Commission announced it has approved two adequacy decisions for the United Kingdom: one for the General Data Protection Regulation (GDPR) and one for the European Law Enforcement Directive, which gets little attention.

June 30 was the deadline for a decision that would not complicate data transfer, so the decision was made just in time. With this hurdle out of the way, personal data can continue to flow freely from the European Union to the United Kingdom, without the need for additional safeguards or regulator approval.

There are some complications in that it is not a permanent decision; the European Commission has declared that it is concerned about the United Kingdom’s desire to welcome foreign investment to

develop data protection laws that are more flexible. Thus, the European Commission is prepared to revoke the adequacy decision if justified.

Action item: If you are operating in a European country, you need to appoint a UK representative under the UK GDPR, just like UK companies must appoint an EU representative under the GDPR. All other countries must appoint a representative in both the United Kingdom and the European Union if they do business there.

South Korea

South Korea has long been recognized as having perhaps the strictest privacy laws of any one country. That the European Commission is entertaining an adequacy decision for South Korea is not really surprising. On June 16, 2021, the European Commission initiated the process, which would also complement the EU-Republic of Korea Free Trade Agreement.

From here, the European Commission has sent its intention to the EDPB for its opinion, then to the committee comprising the members from the EU Member States. Once these steps are complete (a formality, but perhaps a persuasive one depending on the opinions), then the adequacy decision can be finalized. This process can take months.

Action item: Await the opinions from the EDPB and committee.

New Standard Contractual Clauses (SCC)

July 16, 2020 brought news from Europe that Schrems II not only invalidated the EU-US Privacy Shield, but that all transfers to third countries (those not in the European Union or Iceland, Norway, and Lichtenstein, altogether the European Economic Area (EEA)) must be evaluated on a case-by-case basis.

Most companies immediately switched to using SCCs, albeit not GDPR friendly, and maintained their certification to the EU-US Privacy Shield as the replacement remains in sight. However, now the European Commission has issued new SCCs — and the excitement and confusion begin.

On June 4, 2021, the European Commission issued new model clauses. The SCCs can be used as a legal basis to transfer personal data out of the EEA, under Article 46 GDPR on the basis of the appropriate safeguards.

There are two sets of SCCs:

1. Transfer SCCs intended to work between controllers and processors in four different arrangements, and
2. Processing Contract SCCs intended to serve as the required contractual requirements under Article 28.

Most companies transferring data out of the EEA already include the Article 28 contractual requirements in their data processing agreements or even the master services agreements. It is not required to use the new Processing Contract SCCs, but they are available.

The most confusing part to the new SCC decision is that if a company is directly subject to the GDPR

thorough Article 3(2) by offering goods and services directly to individuals in the EEA or monitoring their activity, then SCCs are not needed as a transfer mechanism at all.

This does not mean data must stay within the EEA; on the contrary, it means that data transfer may be simpler. In fact, not only are the Transfer SCCs not required, they also are not allowed. This is explicitly ruled out in Recital 7. Organizations that have been used to including SCCs in their contracts for decades may need to get used to this change, but when looking carefully at the text of the GDPR, it seems clear in hindsight. For more information on the scope of GDPR under Article 3, refer to the EDPB guidance.

The GDPR claims extraterritorial application. Thus, companies directly subject to the GDPR do not require a data transfer mechanism to force GDPR compliance. All transfer mechanisms in Chapter V GDPR, whether adequacy, SCCs, BCRs, or the derogations like consent and vital interest, are only intended to ensure that the level of data protection offered by the GDPR is not undermined. This is clearly stated in Article 44 GDPR.

However, whether Transfer SCCs needed or not, you must comply with the GDPR and be able to document that compliance through a GDPR Validation or Certification with a code of conduct like the EU Cloud Code of Conduct. You must assess all processors to ensure their compliance or status under the GDPR.

If you are a processor, communicate with all your controllers to make sure the status of GDPR subjectivity is addressed and documented. Assess all third countries where your data goes for surveillance activities. Implement safeguards to offset all of these risks:

- The data (e.g., the amount and type of data),
- The data subjects (e.g., the number, the types, the location), and
- The need for data transfers.

You may decide that there are no safeguards good enough to protect certain data in certain countries and you need to change your practices or cancel your contracts with applicable controllers. The EDPB guidance is thorough and provides case examples with lots of suggestions.

There is a transition period, which is helpful, as there was not one after the Shield was invalidated in 2020. Old SCCs are still valid to negotiate with new contracts until September 27, 2021, and those already in place are still valid until December 27, 2022. So, you have roughly 15-18 months to transition. During this time, you must assess processors and controllers, determine GDPR status, amend contracts, assess third countries, implement additional safeguards, and document everything.

For the Transfer SCCs, there are four modules that apply to transfers between controller-to-controller(C2C), controller-to-processor (C2P), processor-to-processor (P2P), and processor-to-controller (P2C). Determine which ones you need.

Note that the United Kingdom has issued its draft International Data Transfer Agreement, on August 11, which is in consultation mode at this time and will replace the SCCs. The draft includes a process to coordinate with EU SCCs and other nations which have similar requirements.

Action items:

- Determine if your processing activity is directly subject to the GDPR. It pertains to specific

activities not companies, so be aware that some of your activities may be subject and some may not be.

- Document your subjectivity to GDPR. Either you are or are not subject under Article 3(2). Stop negotiating with the old SCCs by September 27, 2021.
    - Transition all contracts with EEA to new Transfer SCCs (or none) by December 27, 2022.
    - Assess processors for contract transitions.
    - Assess controllers for contract transitions.
    - Make sure you are compliant with GDPR .
    - Be able to demonstrate your compliance via a third party (best route).

- Monitor the UK developments

Cookies

The use of cookies and other online trackers has recently become an even bigger topic of conversation. In particular, the French data protection authority Commission nationale de l'informatique et des liberté (CNIL) published their updated cookie implementation guidelines in 2020, effective this past March 31, 2021.

Right after the effective data, the CNIL issued a statement that about 100 organizations just received investigatory letters from them. But that is not all. In May 2021, noyb, an Austrian non-profit organization established by privacy activist Max Schrems publicly declared their goal to “end cookie banner terror” by notifying 10,000 companies that use cookie banners in a way that noyb believes to be non-compliant. Both the CNIL and noyb have provided the companies with one month to become compliant.

Some of the complaints seem easy to fix: Give users true options without making one option glaringly apparent in a big green button, whereas the other options are in six-point font hiding in a paragraph somewhere. This is an extreme example, but close to reality for some companies.

Furthermore, the Irish Council for Civil Liberties is fighting the advertising industry with multiple complaints against the Interactive Advertising Bureau (IAB) standards, including real-time bidding and companies claiming legitimate interest as a legal basis for cookies and trackers. Booth cases are currently with data protection authorities.

Action item: Review your cookies banners and change implementation to match the CNIL guidance. Ask your cookie compliance management company how to fix the errors.

Conclusion

Europe is moving fast with its updates and impacting countries in other regions. There is no doubt that more actions are on the way and counsel need to be aware of these activities and be prepared to guide their companies.

K Royal

Global Chief Privacy Officer

Crawford & Company

K Royal earned her JD from the Sandra Day O'Connor College of Law at Arizona State University. She also holds a PhD in Public Affairs from the University of Texas at Dallas.

Reach out to K about her column at @heartofprivacy on Twitter, or www.linkedin.com/in/kroyal/.