GUNDERSON DETTMER

Privacy Alert: Updates on Personal Data Transfers from the European Union and the United Kingdom

Insights
August 25, 2022

Under the European Union and United Kingdom General Data Protection Regulation (collectively, "GDPR"), companies that transfer personal data out of the European Economic Area ("EEA") or United Kingdom ("UK") to other countries must ensure appropriate safeguards are in place. Prior to 2020, many U.S. companies complied with this requirement by certifying to the EU-U.S. Privacy Shield. However, in July 2020, in a landmark decision referred to as "*Schrems II*," the Court of Justice of the European Union ("EU") invalidated the European Commission's adequacy decision for the EU-U.S. Privacy Shield, meaning that it could no longer be relied upon to meet the GDPR's data transfer requirement. Since the *Schrems II* ruling, companies that transfer personal data outside of the EEA and UK have been navigating a complicated and evolving set of requirements and guidelines from EEA and UK regulators, including two new sets of Standard Contractual Clauses ("SCCs"). This client alert recaps important developments regarding international transfers, including the status of negotiations around a successor to the EU-U.S. Privacy Shield, recent guidance from the European Data Protection Board ("EDPB") and the European Commission regarding international transfers, and the new UK SCCs. This client alert also outlines steps companies should take now to protect the transfer of personal data from the EEA and UK to certain other jurisdictions.

What is a "transfer"?

Under the GDPR, companies that transfer the personal data of individuals in the EEA or UK to the U.S. and other jurisdictions that lack an "adequacy" determination from the European Commission or the UK's Information Commissioner's Office ("ICO") must put in place appropriate safeguards to protect that data. While the GDPR does not explicitly define what qualifies as a "transfer" of personal data to a country outside the EEA or UK, guidance from the EDPB states that a transfer occurs when:

- a controller or a processor of personal data is subject to the GDPR for the given processing, *and*
- this controller or processor ("exporter") transmits or otherwise makes available the personal data to another controller, joint controller, or processor ("importer"); *and*
- the importer is in a third country or is an international organization.

If each of these criteria is met, the processing constitutes a "transfer" regardless of whether the importer is subject to the GDPR for the given processing. For example, a transfer occurs when a multinational company (the exporter) provides personal data of EEA or UK data subjects from its EEA or UK subsidiary (which is subject to the GDPR) to a vendor in the U.S. (the importer).

What is not considered a "transfer"?

Per guidance from the EDPB, there is no transfer when a data subject discloses personal data directly and of their own initiative to a company. This means, for example, that when consumer-facing companies in the U.S. collect and import personal data directly and voluntarily from EEA-based data subjects, there is no transfer, and therefore, the processing falls outside the scope of the EU SCCs. Note that personal data that is passively collected – for example, through analytics cookies – likely would not be considered directly or voluntarily provided by EEA-based data subjects and therefore would still constitute a transfer under the guidance.

Can we rely on the EU-U.S. Privacy Shield to cover transfers?

No. Previously, the EU-U.S. Privacy Shield was one compliance mechanism that companies relied upon to comply with the GDPR's data protection requirements when transferring personal data from the EU and Switzerland to the U.S. However, on July 16, 2020, the Court of Justice of the European Union ("CJEU") issued its landmark *Schrems II* decision, in which the CJEU invalidated the European Commission's adequacy decision for the EU-U.S. Privacy Shield. As a result, the EU-U.S. Privacy Shield no longer serves as a valid data transfer mechanism, and companies should

consider alternative personal data transfer mechanisms, such as SCCs. For more information about the *Schrems II* decision, please see our prior client alert here.

As discussed in more detail below, the legal landscape after the *Schrems II* decision has called into question the viability of personal data transfers from the EEA to the U.S. under the GDPR, leading many companies to advocate for a swift political resolution to stabilize trans-Atlantic commerce.

What do we know about Trans-Atlantic Data Privacy Framework (i.e. Privacy Shield 2.0)?

On March 25, 2022, after years of negotiation, the European Commission and the U.S. announced that they had "agreed in principle" on a new "Trans-Atlantic Data Privacy Framework" that would address the concerns raised in the *Schrems II* decision (the "Framework"). Although the agreement has yet to be finalized, the White House and European Commission have each issued statements that offer basic information regarding the Framework.[1],[2] Under this Framework, the U.S. has made an "unprecedented commitment" to implement reforms that will "strengthen the privacy and civil liberties protections applicable to U.S. signals intelligence activities."[3] In particular, the U.S. has agreed to:

1. Implement new rules and safeguards to ensure that U.S. signals surveillance activities (i.e. surveillance of communications) are "necessary and proportionate in the pursuit of defined national security objectives";

2. Establish a new two-level redress mechanism to investigate and resolve the complaints of EEA individuals, including a Data Protection Review Court comprising individuals chosen from outside the U.S. Government with independent and binding authority to adjudicate claims and direct remedial measures; and

3. Enhance its existing oversight of signals intelligence activities to ensure compliance with limitations on surveillance activities.

What is the status of the Framework?

At this time, a finalized Framework is not available, and companies should continue to rely on existing compliance mechanisms like the EU and UK SCCs (where appropriate) for data transfers, as discussed further below. While there is no precise timeline currently for the new Framework, European Commissioner for Justice Didier Reynders stated that "this process could be finalized by the end of [2022]."[4] Still, despite the excitement over these developments, potential legal challenges to the Framework's validity loom, including the threat of legal action from the privacy activist

who initiated the *Schrems II* lawsuit, Max Schrems. We will continue to monitor these developments and will keep our clients updated.

What are the new EU SCCs?

For business-to-business transfers, the most viable option after the *Schrems II* decision typically has been to rely on SCCs. Transfers from the EEA should be conducted pursuant to new EU SCCs issued by the European Commission on June 4, 2021, subject to certain exceptions. For more information about the new EU SCCs, including the deadline for implementing the new SCCs, please see our prior client alert.

Are other data transfer mechanisms available now for companies wishing to export or import EU or UK personal data?

As before, companies can rely on "derogations" under Article 49 of the GDPR for the transfer of personal data if they are applicable. Derogations include transfers pursuant to the explicit consent of the data subject and transfers necessary to perform a contract between the data subject and the controller. However, as a practical matter, few companies rely on these derogations because the EDPB views derogations as "exceptions" that should only be used where none of the other data transfer mechanisms are available, and not for routine or large-scale transfers. Additionally, obtaining a data subject's explicit consent to the data transfer – which is one type of derogation under Article 49 – can be challenging given the high bar for consent to be considered valid under the GDPR.

Can the new EU SCCs be used for transfers from the UK?

The UK left the EU on January 31, 2020, with the Brexit transition period expiring December 31st the same year. As a result, the UK data protection regulator (the ICO) does not recognize the new EU SCCs as a valid compliance mechanism for ex-UK data transfers. However, on March 21, 2022, the UK's new equivalent of the SCCs came into force. The UK SCCs come in two forms – the International Data Transfer Agreement ("IDTA") and the International Data Transfer Addendum to the new EU SCCs ("UK Addendum").

What are the IDTA and the UK Addendum?

The **IDTA** is a standalone agreement that operates as the UK's version of the new EU SCCs. It comprises four parts: Part 1 ("Tables," which the parties should complete with details of the transfer), Part 2 ("Extra Protection Clauses"), Part 3 ("Commercial Clauses"), and Part 4 ("Mandatory Clauses"). The IDTA is substantively comparable

to the new EU SCCs, including with respect to the obligation to prepare a Data Transfer Impact Assessment (referred to as a "Transfer Risk Assessment" in the IDTA).

The **UK Addendum** incorporates and amends the new EU SCCs to make them workable for personal data transfers out of the UK (for example, to account for UK data protection laws, including the UK GDPR and the Data Protection Act 2018). In other words, the UK Addendum acts as an add-on to the new EU SCCs. As with the IDTA, parties to the UK Addendum will need to complete certain sections with details regarding the transfer.

Which UK personal data transfer mechanism should we use?

Companies with personal data transfers subject to both the EU GDPR and UK data protection laws will likely elect to use the UK Addendum because this approach would obviate the need to execute two separate standard contractual clauses (i.e. the IDTA and EU SCCs). Rather, the company would instead be able to rely on the new EU SCCs and append the UK Addendum (which has the effect of modifying the EU SCCs for UK transfers). This approach will be particularly appealing to companies that have already executed the new EU SCCs.

Is there a grace period to implement the UK data transfer mechanisms?

Yes. As was the case with the new EU SCCs, companies have a grace period to implement the new UK personal data transfer mechanisms. Companies that enter into the old EU SCCs (which are still valid for ex-UK transfers) **between now and September 20, 2022**, can continue to rely on the old EU SCCs until **March 21, 2024** (unless the processing activities have changed). After **September 21, 2022**, companies must use the IDTA or the UK Addendum for any new data transfers. Any existing transfers that rely on the old EU SCCs must, in any event, be transitioned to the IDTA or the UK Addendum by March 21, 2024. ***Please contact your Gunderson Dettmer attorney to obtain an updated form Data Processing Agreement which incorporates the UK Addendum***.

What is a Data Transfer Impact Assessment and why do we need to perform one?

While Article 46 of the GDPR and the *Schrems II* ruling (along with subsequent EDPB guidance) already required an evaluation of the facts and circumstances surrounding a transfer of personal data to a third country, the new EU SCCs expressly require that a data exporter conduct a Data Transfer Impact Assessment ("DTIA") to evaluate and document the risks and impact of the transfer, including, among other things, the

transmission channels used, intended onward transfers, types of data and recipients, the purpose of processing, and location of the data storage. The new EU SCCs also require that data importers make certain commitments, including to notify the exporter if it believes that it has become subject to laws or practices that are not in line with the EU SCCs, or if it receives a legally binding request from a public authority for data transferred pursuant to the EU SCCs (with some exceptions where such notification is not legally permitted). ***Gunderson Dettmer's Privacy Group can help with the Data Transfer Impact Assessments required to facilitate your cross-border data transfers.***

What risks do we need to be specifically aware of if we use Google Font, Google Analytics, or Stripe?

In response to over 100 complaints lodged by Max Schrems' non-profit privacy group – *noyb* – several European data protection authorities published decisions regarding the use of Google Analytics, Google Font, and/or Stripe cookies. Generally, these decisions have found that the cookie providers lacked adequate supplementary measures to satisfy GDPR requirements around transfers of data to the U.S. Pursuant to these decisions, cookies are considered personal data and transfers of such data can only take place if they are protected by supplementary measures that ensure an essentially equivalent level of protection for the personal data transferred.

Companies using any of these or similar services will need to explore compliance options. It may be possible for companies to rely on so-called GDPR "derogations" such as explicit individual consent or necessity for the performance of the contract. However, these derogations should be considered prudently and some data protection authorities have cautioned that derogations may not be appropriate in the context of cookie services. The EDPB has also cautioned that "the derogations must be interpreted restrictively so that the exception does not become the rule" and that, as a general matter, they should not be used for routine transfers.

On March 16, 2022, Google announced that it is sunsetting its previous analytics solutions, Universal Analytics and Universal Analytics 360, on July 1, 2023, and October 1, 2023, respectively. These solutions will be replaced by a new cross-platform analytics solution, Google Analytics 4. Per Google, "Google Analytics 4 is designed with privacy at its core to provide a better experience for both our customers and their users. It helps businesses meet evolving needs and user expectations, with more comprehensive and granular controls for data collection and usage." Of note, Google Analytics 4 will no longer store IP addresses, seemingly in an effort to address the concerns expressed recently by EU regulators.

What else should companies do now?

Companies that act as exporters or importers of personal data subject to the GDPR should evaluate whether the data transfers comply with the latest requirements and guidance from EU and UK regulators. Companies, particularly U.S.-based service providers that will be importing data from the EEA or UK, will need to develop a plan to meet the obligations imposed by the new EU SCCs, UK Addendum, and IDTA and a strategy to efficiently integrate those updates into their global privacy compliance program. Consumer-facing companies, on the other hand, that are not established in the EEA or UK should evaluate how they collect and import data directly from EEA- and UK-based data subjects as those transfers fall outside the scope of the SCCs, the UK Addendum, and the IDTA.

How can GD help?

Developments regarding data transfers from the EEA and UK require a detailed analysis of the measures in place to ensure the security of transferred data and updates to existing data processing agreements, including the implementation of the new EU and UK SCCs. For assistance with that process, or if you have any questions regarding this client alert, please reach out to your Gunderson Dettmer attorney or contact one of our data privacy experts:

Anna Westfelt (650) 463-5367 awestfelt@gunder.com

Cecilia Jeong (646) 490-9094 cjeong@gunder.com

Frida Alim (415) 801-4921 falim@gunder.com

James Gately (617) 648-9313 jgately@gunder.com

Brian Hall (415) 801-4898 bhall@gunder.com

---

[1] https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087
[2] https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/
[3] https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087
[4] https://iapp.org/news/a/officials-thrilled-with-eu-us-data-flows-agreement-work-continues-on-finalization/

Related People

Anna C. Westfelt
PARTNER
P +1 650 463 5367

P +1 [illegible]

Frida Alim
ASSOCIATE
P +1 415 801 4921

James W. Gately
ASSOCIATE
P +1 617 648 9313

Cameron Jahansouz
ASSOCIATE
P +1 650 463 5468

Cecilia Jeong
ASSOCIATE
P +1 646 490 9094

Related Services

Data Privacy

Featured Insights

CLIENT NEWS

Brazilian Carbon Capture Company Mombak Announces $30M Financing

CLIENT NEWS

Africa B2B OmniRetail Announces $20M Financing

CLIENT NEWS

Glacier Announces Series A Financing to Expand Robot Recycling Fleet

CLIENT NEWS

Dataminr Announces $100M Investment Led by Fortress Investment Group

CLIENT NEWS

[illegible]

Omnidian Announces $87M Series C for Renewable Energy Performance

INSIGHTS

Splitting the Pie: How Savvy Founders Divide Ownership and Navigate Other Founder Equity Decisions

CLIENT NEWS

Chainguard Announces $356 Million Series D Led by Kleiner Perkins and IVP

INSIGHTS

Client Insight: California AI Transparency Act

INSIGHTS

Client Insight: Prepare for BE-10 Benchmark Survey of US Direct Investment Abroad

INSIGHTS

Tech Brew Interviews Aaron Rubin in “Where the legal battle stands around copyright and AI training”

CLIENT NEWS

Latin America Fintech Belvo Announces $15M Funding

INSIGHTS

Legal 500 Country Comparative Guides 2025: Venture Capital (Singapore)