Articles + Publications | September 27, 2022

Deadline for New UK Contract Requirements for Personal Data Transfers Is Here (EU and California Deadlines Looming)!

WRITTEN BY

James Koenig | Molly S. DiRago | Brent T. Hoard | Ronald Raether, Jr. | James E. Schutz | Peter T. Wakiyama | Brandon Woods | Joel M. Lutz | Jonathan M. Ishee | Robyn W. Lin

Don't Hyperventilate. There are new United Kingdom (UK), European Union (EU), U.S., and global regulatory requirements that just went into effect or will be effective before or soon after year-end that will impact contracts addressing privacy and data protection, including but not limited to:

- New EU standard contractual clause (SCC) modules;
- New UK personal data transfer mechanisms;
- New enforcements and contractual requirements for service providers handling personal information in California (and other U.S. states); and
- Additional countries globally introducing their own forms of SCCs and personal data transfer mechanisms.

This alert will help you keep track of the deadlines and develop simple step-by-step, global, holistic approaches for implementing the new requirements in a timely and cost-effective manner to meet all of the 2022 and other subsequent deadlines.

Post-Brexit UK Data Transfer Contract Requirements Now in Effect and Required! If you're relying on the old versions of the EU SCCs to transfer personal data out of the UK, the deadline has passed. Specifically, for all new agreements after September 22, 2022, you can only use the new UK contract data transfer mechanisms. Existing agreements must be updated by March 21, 2024.

- **Two Options for UK Data Transfer Mechanisms.** After Brexit, the UK passed its own version of the EU's GDPR, as well as two mechanisms for transferring personal data out of the UK:
  - **Option 1: International Data Transfer Agreement (UK IDTA).** The UK IDTA is the UK version of the EU SCCs, and largely is a standalone data transfer mechanism for UK personal data compliance only.
  - **Option 2: The UK Addendum.** The UK International Data Transfer Addendum (UK Addendum) is a much more streamlined approach that gets attached as an additional addendum to a new EU SCC module and

covers both EU and UK compliance.

Other Notable Year-End or Soon-After Deadlines. In addition to the newly effective UK requirements, to keep data transfers flowing, companies should be aware of the following additional contractual obligations:

- **December 27, 2022 – EU SCC Four Modules.** For legacy agreements, these contracts must be updated by December 27, 2022. This includes two new modules related to transfers from an EU processor to non-EU sub-processors and non-EU controllers, as well as updates to the two existing modules.

- **Starting January 1, 2023 – US States, including the California Privacy Rights Act (CPRA).** CPRA comes into effect on January 1, 2023, and will require specific contract language for service providers, contractors, and other third parties. *See* our recent alert on CCPA enforcements. Additionally, other state laws coming into effect have contract requirements when data is shared between companies, including Virginia (January 1, 2023), Colorado (July 1, 2023), Connecticut (July 1, 2023), and Utah (December 31, 2023).

- **Other Countries Developing Similar SCCs.** These include Kingdom of Saudi Arabia, Egypt, China, and Brazil.

Five Emerging Best Practices to Act on Now to Keep the Data Flowing. Rather than rolling out updated contracts, master service agreements, and data processing addendums at the time of each new requirement, many companies are taking global, holistic approaches. The following are five emerging best practices used by other companies for implementing the new requirements in a cost-effective and timely manner to meet all deadlines in one coordinated set of initiatives:

1. **Identify Regulated and High-Risk Areas by Developing and Updating Data Inventory and Records of Processing.** The first step companies are taking to comply with the UK, EU, and other global data transfer requirements is to establish and maintain an inventory of the personal data that your company processes and to document (*e.g.,* through data mapping, records of processing, data inventory, and other procedures) how the personal data is transferred to/from vendors and third parties in/outside of the UK, EEA, or other regulated jurisdiction.

2. **Update DPAs and Existing Agreements for Multiple Law Changes Simultaneously With a Cost-Effective and Global Approach.** The second step companies are taking is to update form agreements/MSAs, existing contracts, and template data processing addendums (DPAs) to contemplate both the new privacy laws and updates to existing privacy laws. Instead of creating undue EU and UK-specific obligations and rolling out new templates and updates multiple times with every new law, many companies are taking a holistic approach and updating form agreements and DPAs designed also to comply with the California Privacy Rights Act (CPRA)/California Consumer Privacy Act (CCPA) and/or other pending, new, or updated privacy laws (*e.g.,* UK post-Brexit, Thailand, Brazil, Saudi Arabia, Egypt, New Zealand, Singapore, South Africa, or other jurisdictions).

    - **Implementation Tip: Develop Upstream and Downstream Forms of DPAs.** Many companies typically develop downstream DPA for when they entrust/share customer, consumer, and employee personal information with a vendor that incorporates many security, indemnification, and other provisions that go beyond what is required under the law. Increasingly, many companies that receive such data (*e.g.,* service providers and vendors) are developing lighter touch DPAs that stick to only the minimum requirements in the hopes to use their template with customers to avoid heightened obligations, risk, and exposure.

3. **Establish a Risk-Based Implementation Plan.** Given the potential for an overwhelming volume of legacy contracts that will have to be updated for UK, EU, U.S., and other laws, many companies are creating a phased, risk-based implementation plan to update legacy agreements. For example, high-risk, business critical agreements and/or agreements with significant EU and/or UK data flows or processing are done first, while other agreements/DPAs that use the old SCCs as the transfer mechanism are done next or, if lower risk or business impact, deferred to contract renewal.

    - **Implementation Tip: Define Secondary Use, Sharing, and Sale Rights.** Given the increasing use of data by service providers for analytics and/or other secondary uses, analyze the new versions of the SCCs and ensure that the appropriate version of the new SCCs is implemented (and also aligns with your data use, sharing, and sales position under CCPA/CPRA and other U.S. state laws).

4. **Create or Update Intra-Group Agreements.** Many companies have established intra-group agreements (IGAs) based on the old SCCs that govern a global company's customer and employee personal data transfers between affiliates involving EU, UK, and Swiss personal information around the world. While companies that implemented IGAs are updating them for the new EU SCC forms and the UK Addendum, other companies that previously did not have IGAs in place are increasingly implementing them as a global data transfer baseline to address EU, UK, and Swiss requirements, as well as other global requirements beyond just the EU, UK, and Switzerland.

5. **Train Internal Stakeholders.** To promote compliance and help close contract negotiations quicker and with consistency, many companies are training internal employees and contractors who may be impacted by the changes to personal data transfer practices and contractual obligations (*e.g.,* procurement, sales, legal) on the company's updated DPAs and the company's approach for cross-border and global data transfers. Many companies are also creating and/or updating prepared statements that can be issued to customers and data exporters to explain their DPA updates, as well as describing the company's approach to protecting EU, UK, and other personal data and dealing with law enforcement requests.

Questions. To learn more about the impact on your company and how to implement the new SCCs and/or the UK Addendum, please contact Jim Koenig, Joel Lutz, Robyn Lin, or any member of our Privacy + Cyber team.

RELATED INDUSTRIES + PRACTICES

- Health Care + Life Sciences
- Intellectual Property
- Privacy + Cyber