# Navigating data protection laws: using European clauses as the foundation for U.S. agreements

**By Dorothy R. Auth, Esq., Howard Wizenfeld, Esq., and Andrew J. Harris, Esq., Cadwalader, Wickersham & Taft LLP**

**APRIL 18, 2023**

## Introduction: the hidden cost of data

In today's information-based economy, businesses increasingly find themselves transferring data containing personal information to or from vendors. As laws are enacted to control how a business can use personal data, such uses create liability for a business.

Damages for failure to properly protect personal data can be high: In 2022 alone, U.S. civil settlements exceeded $1 billion; a jury in a notable U.S. state case, *Rogers v. BNSF Railway Co*., awarded $428 million in damages, and European regulators issued an aggregate of over $1.7 billion in fines. Given this potential liability, businesses are well-advised to establish data privacy policies that assure protection commensurate with data privacy laws and to craft third-party agreements reflecting these policies.

In the United States, a patchwork of laws at the state and federal level regulate personal data privacy. Current laws are limited either to activities in a particular state or to a particular industry. Because current U.S. law is quickly changing and varies from state to state, it may be prudent to comply with the strictest data privacy provisions so that your business is compliant regardless of how it grows.

Currently, Europe's General Data Protection Regulation (GDPR) is one of the most comprehensive and strict data privacy laws worldwide. In addition to GDPR's robust set of data privacy regulations, the EU has drafted a set of contractual clauses (known as "Standard Contractual Clauses" or "SCCs"), which the European Commission (in its official decision implementing the SCCs) deemed to be in compliance with GDPR's contractual requirements.

This article explores the potential benefits of using the GDPR and its accompanying SCCs as the guiding foundational principles on which to develop data protection agreements in the U.S.

## GDPR SCCs provide a clear framework for companies to build upon

For many companies, the SCCs offer an attractive proposition: having one set of provisions for use in data privacy agreements which a company can use across jurisdictions. The GDPR neatly lays out its core principles: Articles 12-23 enumerate the rights of persons who provide personal data ("data subjects") (*e.g.*, to access, rectify, erase, object and restrict processing); Articles 24-43 specify the responsibilities of the parties using such personal data; and the accompanying SCCs offer standard provisions for use in data processing agreements.

As an additional resource, the EU's GDPR regulating authority, called the European Data Protection Board (EDPB), frequently issues guidance on GDPR requirements. Together, this substantial body of resources and law provides a foundation for complying with data privacy requirements.

*Because current U.S. law is quickly changing and varies from state to state, it may be prudent to comply with the strictest data privacy provisions so that your business is compliant regardless of how it grows.*

In GDPR parlance, businesses handling personal data are classified as either "controllers" or "processors," depending on their responsibilities and obligations in handling the data. As defined in Article 24, controllers determine the purposes and means of processing, whereas under Article 28, processors solely act on behalf and per the instructions of a controller. Once an entity determines whether it qualifies as a controller or processor in a specific transaction, determining its responsibilities is straightforward.

Importantly, the controller has primary accountability to comply with the regulations, *e.g.*, (i) to respond to data subject requests under Article 15; and (ii) to report a data breach under Article 33. In terms of liability, while both the controller and processor are jointly liable to the data subject, the controller faces far more scrutiny from regulators. As enumerated in Article 26, joint controllers may exist when both businesses in a data transfer exert decisive influence or jointly determine the means of data collection with a partner.

The SCCs use a modular approach based upon these "controller" and "processor" designations. In particular, there are four modules representing the four possible configurations in a two-party data transfer agreement (*i.e.*, Controller to Controller, Controller to Processor, Processor to Processor, and Processor to Controller). Once the contracting entities have determined their status, the corresponding module is selected for the data processing agreement.

Each module must be used in its entirety in the agreement, making the clauses easy to use. However, additional provisions which strengthen data protection (*e.g.*, technical and operational measures, such as encryption) may also be inserted.

## Changes to SCCs needed to comply with U.S. laws

Companies that need to comply with the specific privacy laws of multiple U.S. states can use the SCCs as a foundational template to create a standard data privacy agreement. Companies need not operate in Europe to incorporate the SCCs into their standard agreements – the SCCs can instead be used as a starting point and be further modified to address the nuanced differences between the GDPR and U.S. state laws, making a U.S.-only company ready to expand into Europe and other parts of the world.

*For many companies, the SCCs offer an attractive proposition: having one set of provisions for use in data privacy agreements which a company can use across jurisdictions.*

Although much of GDPR's requirements are also found in current U.S. data privacy laws, the rights and responsibilities created under GDPR differ in some respects. To achieve compliance under the applicable U.S. state laws, a business can simply adjust a specific SCC clause instead of drafting a completely new data privacy agreement.

For example, like the GDPR, the U.S. federal law protecting personal data in the financial industry, the Gramm-Leach-Bliley Act (GLBA), mandates safeguarding customers' nonpublic personal information. But, unlike the GDPR, the GLBA *also* requires financial institutions to provide customers with annual notices and opt-outs. Such notices and opt-outs can be added to a business's SCC-based data privacy agreement.

Another law specific to the financial industry is New York's Department of Financial Services (NYDFS) data privacy and cybersecurity regulations, which also overlaps with GDPR, but further requires robust cybersecurity plans and policies (including disaster recovery). This additional NYDFS requirement can also be layered into the SCC-based agreement.

Besides federal regulations, several U.S. states have enacted their own laws regulating use of personal data. The most prominent is the California Consumer Privacy Act (CCPA) which protects the personal information of California residents acting as consumers with businesses in California.

These protections were expanded through the California Privacy Rights Act (CPRA), which amended the CCPA and became effective Jan. 1, 2023. Today, the CCPA provides consumers with many of the same rights provided in GDPR (*e.g.*, the right to correct, right to delete, the right to access) and similarly delineates responsibilities based upon the controller and processor roles (using designations of "business" and "service provider," respectively).

Because the GDPR generally takes a more expansive view of data protection, many of the CCPA provisions are already encompassed in the GDPR: *e.g.*, (i) GDPR's broad definition of "data subjects" as compared to CCPA's restriction to "consumers"; (ii) GDPR's inclusion of *any* business which processes personal data of data subjects, compared to CCPA's limited application to for-profit businesses in California with specific characteristics; and (iii) GDPR's inclusion of any personally identifiable information compared to CCPA's express exclusion of medical information, financial information, and personal information covered by other laws.

However, the CCPA varies from GDPR in certain aspects, *e.g.*, under the CCPA, consumers who provide personal information are assumed to have consented to its use. Businesses must therefore provide consumers with the right to opt out of the sale or sharing of this information. In contrast, the GDPR generally prohibits a business from using customer personal information without the customer's explicit (opt-in) consent.

Also, the two regimes differ in their approach to collecting the data of children: Section 1798.120 of the CCPA requires businesses to only seek parental consent for the *sale* of such data whereas Recital 38 of the GDPR requires controllers to seek consent for *processing* such data.

The SCCs can thus be leveraged to address the nuanced differences between the two regimes. For most such differences, the SCC-provided Appendix can be used to list particular additional obligations between the parties as between the GDPR and CCPA. While a company may need to further modify its standard data privacy agreement as other states enact their own privacy laws (e.g., Colorado, Connecticut, Virginia, Utah and most recently Iowa), the SCCs provide a strong foundational template.

Using the SCCs as the foundational template to create a standard data privacy agreement is a strong first step in preparing a company for its eventual growth. As a company grows from a local, to a national, and even international business, these templates allow for quick, targeted modifications to include local nuances in data privacy laws, resulting in compliant data privacy contracts regardless of the jurisdiction.

## About the authors



**Dorothy R. Auth** (L) is an intellectual property partner in **Cadwalader, Wickersham & Taft**'s New York office who regularly advises her clients on complex intellectual property issues in both transaction and litigation contexts. She also advises clients regarding compliance with data protection regulations and negotiates and drafts data transfer agreements. She has a doctorate in biochemistry and can be reached at dorothy.auth@cwt.com. **Howard Wizenfeld** (C) is an intellectual property special counsel in the firm's New York office who focuses his practice in the area of intellectual property and data protection law. He regularly advises clients on compliance with data protection regulations and negotiates and drafts master services agreements and data protection agreements to be in compliance with these data protection regulations. He holds a bachelor's degree in electrical engineering and can be reached at howard.wizenfeld@cwt.com. **Andrew J. Harris** (R) is a law clerk in the firm's intellectual property group in New York. He can be reached at andrew.harris@cwt.com.

**This article was first published on Reuters Legal News and Westlaw Today on April 18, 2023.**