5 Important Privacy Updates You Can’t Ignore in 2022

Technology, Privacy, and eCommerce

Cheat Sheet

- **EU privacy updates.** Recent General Data Protection Regulation requirements include adopting new Standard Contractual Clauses (SCCs) and completing a risk assessment prior to certain transfers.
- **UK Privacy updates.** The International Data Transfer Agreement, the UK version of the SCCs, along with the UK-SCC addendum to the EU SCCs, is currently pending before the UK Parliament and are expected to become effective on March 21 unless the Parliament objects.
- **US privacy updates.** The California Privacy Rights Act of 2020 will amend and replace many provisions of the California Consumer Privacy Act starting on Jan. 1, 2023.
- **New US state privacy laws**. The Virginia Consumer Data Protection Act and the Colorado Privacy Act will go into effect on Jan. 1, 2023.

Data privacy law isn't just for designated privacy practitioners anymore. This year, lawyers across all disciplines should familiarize themselves with emerging data privacy statutes and legislative updates that will take effect in the next 12 to 24 months. In particular, in-house counsel focused on intellectual property, transactions, employment, compliance, and general corporate matters are likely to encounter questions related to cybersecurity and privacy.

We've identified five key privacy updates that all attorneys should review and understand. These include updates to the General Data Protection Regulation (GDPR) in the European Union and United Kingdom, amendments to California privacy legislation in the United States, and new US state

privacy laws in Virginia and Colorado.

GDPR Updates in the European Union

Last year was a whirlwind for many reasons, so you may have missed updates to Europe's GDPR. In July 2020, the Court of Justice of the European Union ruled in the *Schrems II* decision that the EU-US Privacy Shield is no longer a lawful basis for transferring personal data between the United States and the European Union.

Although *Schrems II* was decided nearly two years ago, we occasionally come across contracts and privacy policies that were drafted or executed prior to July 2020 that rely on the outdated Privacy Shield framework as the sole basis of transfer (usually because they were signed with a multi-year initial term and the parties haven't revisited the contract yet). These contracts certainly need to be updated as soon as possible, but *Schrems II* left open the question of *how* they need to be updated. If the Privacy Shield is out, what is an acceptable basis of transferring personal data between the United States and European Union?

> If the Privacy Shield is out, what is an acceptable basis of transferring personal data between the United States and European Union?

New Standard Contractual Clauses

Nearly a year after *Schrems II,* the European Commission published its June 2021 Implementing Decision to adopt new Standard Contractual Clauses (SCCs) as lawful basis of transfer. Although this provided an answer for companies that previously relied on the Privacy Shield, it created a new challenge for companies that relied on an older version of the SCCs.

The June 2021 decision identified two key deadlines for updating old contracts:

The first deadline already passed on Sept. 27, 2021. After this date, all new contracts involving processing of EU personal data *must* use the new SCCs instead of the old ones. This applies both to entirely new business relationships *and* to new processing activities established in the course of an existing business relationship.

For example, if you executed a master Software as a Service (SaaS) agreement in January 2021 with the old SCCs, but you intend to expand the SaaS features to process new categories of personal data under a statement of work in January 2022, that statement of work must include the *new* SCCs.

The second deadline is scheduled for Dec. 27, 2022. This is the deadline for migrating all of your contracts that currently use the old SCCs to the new SCCs, regardless of whether the processing activities have changed. The European Commission has provided four different versions or "modules" of the new SCCs:

1. Transfer controller to controller,
2. Transfer controller to processor,
3. Transfer processor to processor, and
4. Transfer processor to controller.

Carefully consider which module to use based on the respective roles of the parties. Note that, in addition to adopting new SCCs, the June 2021 Implementing Decision introduced additional requirements, including completion of a risk assessment prior to certain transfers. Companies should review these requirements in connection with updating their existing agreements and data management practices.

New guidance on supplementary data protection measures

However, it's important to remember that the SCCs do not operate in a vacuum. Merely *executing* the appropriate form of the SCCs does not guarantee GDPR compliance if EU personal data is transferred to a country whose laws and practices do not offer EU-equivalent safeguards for the data. As discussed in the *Schrems II* decision, the United States may be one such country because:

- Public authorities and governmental agencies are not bound by SCCs executed by private data importers, and
- Those same authorities or agencies may be able to access EU personal data received by US-based importers through means that circumvent the safeguards required by the SCCs.

To address the issue of supplemental safeguards, on June 18, 2021, the European Data Protection Board (EDPB) adopted a second version of its extensive recommendations on how data exporters should evaluate and implement supplemental data protection measures when transferring data to restricted countries.

> Counsel should work closely with their internal IT personnel to ensure awareness of the EDPB's recommendations and that the company is actively working toward implementing adequate supplemental measures.

Article 1(2) of those recommendations summarizes the central requirement that:

> An essentially equivalent level of protection to that guaranteed within the EU must accompany the data when it travels to third countries outside the EEA to ensure that the level of protection guaranteed by the GDPR is not undermined, both during and after the transfer.

The EDPB goes on to provide a roadmap of how parties can apply this principle of data accountability in practice through a six-step inquiry:

1. Understand the mechanics and implications of your data transfer mechanisms;
2. Determine whether your transfer mechanism is adequate under GDPR pursuant to an existing adequacy decision or whether supplemental measures are required by law;
3. Assess whether the laws or practices of the country to which data is exported undermine the effectiveness of the transfer mechanism or SCC safeguards;
4. Identify and adopt any supplementary measures that are necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence;
5. Take any formal procedural steps required to officially adopt your proposed supplementary measures; and
6. Periodically re-evaluate and amend your supplementary measures as needed to adjust to changing data privacy landscape.

Counsel should work closely with their internal IT personnel to ensure awareness of the EDPB's recommendations and that the company is actively working toward implementing adequate supplemental measures.

GDPR Updates in the United Kingdom

Notably, the European Commission's June 2021 Implementing Decision requiring new SCCs only applies to EU member states. Following Brexit and the expiration of the UK-EU transition period, the United Kingdom is no longer an EU member state subject to the jurisdiction. What does this mean for GDPR compliance and data transfers when the data subject is located in the United Kingdom?

In late 2021, the UK Information Commissioner's Office (ICO) proposed and solicited public commentary on its own version of new SCCs, called the International Data Transfer Agreement, for use when the only personal information being processed pertains to UK residents. In addition, the ICO proposed a short UK Addendum that parties could add as an exhibit to the new EU SCCs, if the parties will process personal data of both EU and UK residents simultaneously.

Both documents were presented before the UK Parliament on Feb. 2, 2022, but as of Feb. 9, 2022, the UK Parliament had not provided a formal response either objecting to those documents or adopting them. These are expected to become effective on March 21unless the Parliament objects.

> During the interim period, US companies that control or process personal data pertaining to both UK and EU residents will need to include both sets of SCCs included in their contracts.

The United Kingdom has also not adopted the European Union's new SCCs. Until the UK Parliament provides formal guidance on the proposed UK SCC substitutes (which is expected in March 2022), US companies controlling or processing UK personal data may continue to rely on old SCCs when transferring UK personal data to the United States.

This means that, during the interim period, US companies that control or process personal data pertaining to both UK and EU residents will need to include both sets of SCCs included in their contracts. Assuming the UK Parliament adopts the new proposed UK SCCs without objection, those documents are expected to become effective in late March 2022.

As a reminder, given GDPR's (and its UK-analog's) extraterritorial application, many US-based companies will need to comply with the foregoing updated requirements if those companies process personal data of individuals located in the European Union (or United Kingdom, as applicable) in connection with (offering goods or services to individuals located in the European Union (or United Kingdom) or monitoring the individual's behavior within the European Union (or United Kingdom).

Privacy updates in the United States

Updated California privacy law

Businesses have been grappling with the California Consumer Privacy Act (CCPA) since it became effective on Jan. 1, 2020. However, even more challenges have been looming on the horizon since Californians voted "yes" on the Proposition 24 ballot initiative in November 2020. As a result, a *new* California privacy law, the California Privacy Rights Act of 2020 (CPRA) will amend and replace many

provisions of the CCPA **starting on Jan. 1, 2023**.

The CPRA also created a new California agency, the California Privacy Protection Agency, which must adopt additional regulations related to CPRA implementation by July 1, 2022.

In addition to creating a dedicated privacy protection agency, CPRA deviates from CCPA most significantly in the following ways:

- CPRA creates a new category of sensitive personal information that is subject to heightened security and processing requirements. Sensitive personal information includes (but is not limited to) a person's government identification numbers, precise geographic location, genetic data, racial or ethnic origin, and information about a person's sexual information.

- CPRA offers data subjects several more rights than the CCPA provides. Those rights include the right to correct inaccurate personal information and the right to restrict processing of sensitive personal information.

- CPRA increases one of the jurisdictional thresholds from 50,000 devices, households, or residents to 100,000 households or residents (omitting a reference to devices).

- CPRA requires some businesses to undergo annual cybersecurity audits and report annual risk assessments.

- CPRA includes new provisions to address automated processing and profiling activities.

- CPRA introduces new defined terms to distinguish between "selling" and "sharing" personal data and to clarify differences between "service providers" and "contractors."

- CPRA eliminates the B2B or employee exemption. Subject to limited exceptions, CPRA regulates all personal information, regardless of whether that information is collected for household, employment or business purposes.

Businesses that are currently subject to CCPA, or that will otherwise become subject to CPRA next year, should re-evaluate their data management practices to determine if any disclosures of personal data constitute "sharing," and whether disclosures are made to other "businesses," "service providers," "contractors," or "third parties," as each term is defined by CPRA.

New Virginia privacy law

In March 2021, Virginia became the second state to pass comprehensive, state-level privacy legislation when it enacted the Virginia Consumer Data Protection Act (Virginia Act). The Virginia Act becomes effective on **Jan. 1, 2023**.

The Virginia Act applies, with some exceptions, to companies that conduct business in Virginia or produce products or services targeted to Virginia residents *and* who meet at least one of the following criteria:

- During a calendar year, control or process personal data of at least 100,000 Virginia consumers; or
- Control or process personal data of at least 25,000 Virginia consumers and derive over 50

percent of gross revenue from the sale of such personal data.

The Virginia Act grants broad rights to Virginia consumers and generally requires that companies subject to the Act:

- Implement robust safeguards to protect personal data;
- Provide a clear privacy notice to consumers;
- Only disclose personal data to processors pursuant to a written agreement;
- Conduct data protection assessments (but only if the company engages in certain enumerated processing activities); and
- Implement at least some safeguards for de-identified or pseudonymized data. Notably, the Virginia Act does not grant consumers a private right of action, but each violation of the Act carries a fine of US$7,500.

New Colorado privacy law

Shortly after the Virginia Act passed, Colorado passed the Colorado Privacy Act, which will become effective on **Jan. 1, 2023**. The Colorado Privacy Act applies, with some exceptions, to businesses that conduct business in Colorado or produce products or services targeted to Colorado residents *and* who meet at least one of the following criteria:

- During a calendar year, control or process personal data or at least 100,000 Colorado consumers; or
- Control or process personal data of at least 25,000 Colorado consumers and derive revenue (or receive a discount on the price of goods or services) from the sale of such personal data.

The Colorado Privacy Act contains many familiar features reflected in other privacy legislation, including granting rights to data subjects, requiring notice and consent to processing, implementing security measures, and providing limited opt-out rights. The Colorado legislature is expected to provide additional guidance on its Privacy Act implementation, so businesses should remain flexible in their implementation strategy this year.

One additional quirk of the Colorado Privacy Act is that it does not include a blanked exemption for nonprofit entities.

Conclusion: Lawyers are the first line of defense

One challenge posed by this mosaic of data privacy legislation is that compliance with one statute rarely satisfies all requirements of another. This requires in-house counsel to stay updated on regulatory nuances and understand their companies' management practices with more specificity.

In particular, in-house counsel and compliance lawyers should evaluate how their companies collect, use, and disclose personally identifiable information (PII) and determine whether updates are required to internal or public-facing privacy policies, incident response procedures, data mapping functionality, storage or retention policies, or contract templates to account for updates in data privacy legislation.

One challenge posed by this mosaic of data privacy legislation is that compliance with one statute rarely satisfies all requirements of another.

Similarly, lawyers who regularly review, draft and negotiate commercial contracts should be able to identify:

- Whether the contract involves the sale, exchange, processing or transmission of PII;
- What type of PII is at issue;
- Whether the PII is regulated by any international, federal or state-based privacy laws; and
- Whether those privacy laws require updates to the contract at hand.

The field of privacy law will continue to change, as demonstrated by recent efforts to propose a federal privacy statute in the United States. Current state-based regulations will also continue to evolve, and new states may propose their own comparable statutes.

Although privacy-specific lawyers should be consulted when needed, other types of lawyers should become familiar enough with privacy concepts to serve as the first line of defense in spotting issues and risks affecting clients in other practice areas.

Deb Horwitz

Senior Director of Global Compliance and Privacy Operations

Merz Aesthetics

Deb Horwitz is the senior director of global compliance and privacy operations at Merz Aesthetics. She is a Certified Information Privacy Professional (Europe) who regularly advises on enterprise-level compliance and privacy strategy.

Will Cannon

Partner

Parker Poe

Will Cannon co-leads Parker Poe’s Technology Industry Team, whose services include helping clients negotiate hundreds of sophisticated technology contracts every year. Cannon handles contract negotiations and safeguards clients’ intellectual property rights.

Tiffany Burba

Attorney

Parker Poe

Tiffany Burba is an attorney on Parker Poe’s Technology Industry Team. Burba negotiates and drafts contracts involving cloud software, data sharing, cybersecurity consulting, and other areas at the intersection of intellectual property and technology.