

Memorandum

Privacy Law Update: New EU/U.S. Data Agreement and Utah Law

April 14, 2022

It has been a busy spring for privacy and cybersecurity law. In recent weeks, the United States and European Commission (“EC”) agreed to replace the Privacy Shield to allow trans-Atlantic data transfers under the EU General Data Protection Regulation (“GDPR”), and Utah passed its own privacy statute. These developments come close on the heels of the new Cyber Incident Reporting for Critical Infrastructure Act,¹ which will require prompt federal-level reporting of cybersecurity breaches and ransomware payments, and the Securities and Exchange Commission’s new proposed rules to enhance and standardize disclosures of cybersecurity breaches.²

This memorandum offers important practice tips with respect to the new EU/U.S. agreement and Utah law.³

Trans-Atlantic Data Transfers

On March 25, 2022, the U.S. and EC agreed in principle to a Trans-Atlantic Data Privacy Framework (the “Framework”) that will permit EU-to-U.S. data transfers under the GDPR. The GDPR generally permits transfer of EU residents’ personal data outside the EU only if it is (i) subject to safeguards such as Standard Contractual Clauses (“SCCs”) or binding corporate rules or (ii) made to a country with EU-approved data protections, which previously included the U.S. under the Privacy Shield.

Practice Tip: U.S. businesses will likely want to rely on the Framework for EU-U.S. data transfers, to avoid the obligations of using recently-revised SCC forms, which include performing data impact assessments. After the Biden Administration adopts the Framework via executive order, businesses may use it by self-certifying their adherence to the Privacy Shield Principles through the U.S. Department of Commerce. This was accomplished by a website registration process under the Privacy Shield and its predecessor, the Safe Harbor.

History: The Privacy Shield was invalidated in July 2020 by the European Court of Justice (“ECJ”), due to objections to U.S. surveillance practices for personal data. According to a joint U.S.-EC statement, the U.S. will introduce “new safeguards to ensure that [U.S.] signals surveillance activities are necessary and proportionate in the pursuit of defined national security objectives” and “establish a two-level independent redress mechanism” for

¹ See Simpson Thacher, [Newly Enacted Federal Cybersecurity Disclosure Statute Will Significantly Expand Data Breach and Ransomware Reporting Obligations](#).

² See Simpson Thacher, [SEC Proposes Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure Rules](#).

³ This memorandum provides only a high-level summary of these laws and developments. For a more detailed discussion, please consult one of the authors of this memorandum.

Europeans “with binding authority to direct remedial measures.” The mechanism will include a Data Protection Review Court consisting of non-U.S. Government personnel that will hear complaints about U.S. intelligence practices. Alternative dispute resolution will remain available for complaints against Framework participants.

After the invalidation of the Privacy Shield, U.S. businesses have mainly relied on SCCs to make GDPR-compliant EU-U.S. data transfers. This has involved complicated implementation—businesses relying on SCCs had to conduct privacy impact assessments to accompany data transfers, and there are recent requirements to use updated SCC forms.⁴ As such, many U.S. companies hope to rely on the new Framework.

The Utah Consumer Privacy Act

On March 24, 2022, Utah Governor Spencer Cox signed the Utah Consumer Privacy Act (“UCPA”), making Utah the fourth U.S. state to approve comprehensive consumer privacy legislation. The UCPA becomes effective on December 31, 2023.

Practice Tip: The UCPA is generally less restrictive than other recent state privacy laws. Therefore, if your organization’s nationwide data processing activities already comply with the California Consumer Privacy Act and are prepared to comply with the new Colorado and Virginia laws, there is little else to do to comply with the UCPA, other than posting a Utah-specific privacy notice on your website.

Scope: The UCPA applies to controllers—persons doing business in Utah that decide the purposes and methods of data processing—and processors—persons processing personal data on behalf of a controller. Similar to laws in California, Virginia, and Colorado, the Utah law covers organizations that (i) conduct business in Utah or target products to Utah consumers, (ii) have at least \$25 million in annual revenue, and (iii) either (a) control or process the personal data of 100,000 or more Utah consumers in a calendar year or (b) derive over 50% of their gross revenues from personal data sales and control or process the personal data of at least 25,000 Utah consumers.

Exemptions: The UCPA does not apply to (i) employee data, (ii) de-identified, aggregated, and publicly available data, (iii) information regulated under various federal laws, including HIPAA, GLBA, FCRA, and FERPA, or (iv) certain entities, including nonprofits, government entities and contractors, and air carriers. Various uses of data are also exempt, including internal activities directed to development or repair or reasonably aligned with the consumer’s expectations, based on a pre-existing relationship with the controller.

Consumer Rights: Utah consumers are granted four non-waivable rights: (i) the right to confirm whether a controller is processing their personal data and to access such data, (ii) the right to delete data that they provided to a controller, (iii) the right to obtain a copy of such data, and (iv) the right to opt out of processing for targeted advertising or sales of their data. The “sale” definition is narrower than the one for California—it must involve monetary consideration—and has several exceptions, including transfers that are consistent with a consumer’s

⁴ See Simpson Thacher, [Privacy Law Update: Colorado, California, New York, GDPR and the Supreme Court](#).

reasonable expectations. Sales also do not include transfers of personal data as part of a merger or sale of a business.

Obligations: Controllers may not process sensitive data unless consumers have clear notice and an opportunity to opt out. Sensitive data includes genetic, biometric, or geolocation data, most information revealing racial or ethnic origin, religious beliefs, sexual orientation, citizenship or immigration status, or medical information. Further, controllers must (i) post accessible and clear UCPA-compliant privacy policies, (ii) maintain appropriate physical data security practices, and (iii) have certain protective language in their contracts with processors.

Enforcement: The Utah Attorney General has exclusive enforcement authority and may recover actual damages and up to \$7,500 per violation. The UCPA requires a 30-day notice and cure period before enforcement.

For further information regarding this memorandum, please contact one of the following authors:

NEW YORK CITY

Lori E. Lesser
+1-212-455-3393
llesser@stblaw.com

Jessica N. Cohen
+1-212-455-7736
jessica.cohen@stblaw.com

Nicholas S. Goldin
+1-212-455-3685
ngoldin@stblaw.com

Bobbie Burrows
+1-212-455-2333
bobbie.burrows@stblaw.com

Shanice D. Hinckson
+1-212-455-2113
shanice.hinckson@stblaw.com

Melanie D. Jolson
+1-212-455-3346
melanie.jolson@stblaw.com

Jonathan S. Kaplan
+1-212-455-3028
jonathan.kaplan@stblaw.com

Jacob Lundqvist
+1-212-455-3348
jacob.lundqvist@stblaw.com

Kate E. Mirino
+1-212-455-2055
kate.mirino@stblaw.com

Alysha J. Sekhon
+1-212-455-3762
alysha.sekhon@stblaw.com

Taylor Sutton*
+1-212-455-2232
taylor.sutton@stblaw.com
*Not Yet Admitted

LONDON

Owen Lysak
+44-(0)20-7275-6179
owen.lysak@stblaw.com

Tyler B. Robinson
+44-(0)20-7275-6118
trobinson@stblaw.com

Luqman Meedin
+44-(0)20-7275-6121
luqman.meedin@stblaw.com

PALO ALTO

Harrison J. (Buzz) Frahn
+1-650-251-5065
hfrahn@stblaw.com

The contents of this publication are for informational purposes only. Neither this publication nor the lawyers who authored it are rendering legal or other professional advice or opinions on specific facts or matters, nor does the distribution of this publication to any person constitute the establishment of an attorney-client relationship. Simpson Thacher & Bartlett LLP assumes no liability in connection with the use of this publication. Please contact your relationship partner if we can be of assistance regarding these important developments. The names and office locations of all of our partners, as well as our recent memoranda, can be obtained from our website, www.simpsonthacher.com.