Skadden

Privacy & Cybersecurity Update

Connecticut Becomes Fifth State To Adopt Comprehensive Privacy Law

Connecticut has become the fifth state to enact a comprehensive privacy law, further complicating the compliance efforts of businesses that collect or process personal data in the United States.

On May 10, 2022, Connecticut Gov. Ned Lamont signed the Connecticut Data Privacy Act[1] (CTDPA), becoming the fifth state to enact a comprehensive data privacy law following similar laws passed in California, Colorado, Utah and Virginia. The CTDPA will become effective on July 1, 2023, the same day as the Colorado Privacy Act (CPA). The new California Privacy Rights Act (CPRA) that will replace the California Consumer Privacy Act (CCPA) and the Virginia Consumer Data Protection Act (VCDPA) each go into effect on January 1, 2023, while the Utah Consumer Privacy Act (UCPA) goes into effect on December 31, 2023. Impacted companies should devote resources in 2022 to prepare for these significant changes to the U.S. privacy landscape.

Which Businesses Are Covered?

The Connecticut law follows a similar approach to the other four states' privacy laws regarding limiting coverage to larger organizations that operate or collect data of residents in that state. The CTDPA applies to all entities that conduct business in Connecticut and those that conduct business outside of the state but offer products and services to Connecticut residents, in each case if in the previous calendar year they: (1) controlled or processed personal data of not less than 100,000 consumers during a calendar year, excluding personal data controlled or processed solely for the purpose of completing payment transactions, or (2) controlled or processed personal data of not less than 25,000 consumers and derived more than 25% of their gross revenue from the sale of personal data.

This means that each of the five states apply a different test for companies to apply. For example, under the CPRA, companies that collect California consumers' personal data must comply with the legislation if: (1) in the previous calendar year, the company had a gross revenue of over $25 million; (2) the company annually buys, sells or shares personal information of 100,000 or more consumers or households; or (3) the company derives 50% or more of its annual revenue from the sale or sharing of personal information of California consumers.

[1] See the Connecticut Data Privacy Act statute language.

Exemptions

The CTDPA includes carve-outs for certain entities and information, similar to the laws in the other four states. For example, the law does not apply to state entities, nonprofit corporations, higher education institutions, national securities associations registered under the Securities Exchange Act of 1934, financial institutions or data subject to the Gramm-Leach-Bliley Act, covered entities and business associates governed under the Social Security Act. It additionally exempts certain information governed by certain federal laws, including, but not limited to, the Health Insurance Portability and Accountability Act, Fair Credit Reporting Act, the Driver's Privacy Protection Act, the Family Education Rights and Privacy Act, and Farm Credit Act.

Which Consumers Are Covered?

A consumer under the CTDPA is defined as "an individual who is a resident of the state [of Connecticut]" acting in an individual context not applying for employment or related to commercial, employment or government, or any of the like. Following the regulations of Colorado, Utah and Virginia, the CTDPA excludes in its definition of consumer any "individual acting in an employment or commercial context." The employment and commercial exception, which originated in California as a "temporary" exclusion, is a critical exception to these state privacy laws, since without this exception coverage would extend to every company. Notably, the EU General Data Protection Regulation (GDPR) does not include such an exception.

What Information Is Protected by the CTDPA?

The CTDPA defines "personal data" as "any information that is linked or reasonably linkable to an identified or an identifiable individual." This definition is almost identical to legislation in Colorado, Utah and Virginia, while the California CCPA and CPRA also both include information linkable to households.

Exemptions

Similar to the four other states, Connecticut's definition of personal data under the CTDPA excludes "de-identifiable data and publicly available information." "De-identifiable data" under the CTDPA is defined as "data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual." The CTDPA outlines similar measures as the four other states for a controller who possesses de-identifiable information. If a controller possesses de-identifiable data, they must: (1) take reasonable measures to ensure the data cannot be associated with an individual, (2) commit to processing the data in a de-identifiable manner and (3) contractually obligate any recipient of such data to comply with the CTDPA (presumably, to the extent applicable).

"Publicly available information" is defined as "information that (1) is lawfully made available through federal, state or municipal government records or widely distributed media, and (2) a controller has a reasonable basis to believe a consumer has lawfully made available to the general public." This language follows the formulation adopted by the other four states.

In line with these other states, the CTDPA states that certain consumer rights do not apply to "pseudonymous data" (*i.e.*, personal data that is not attributable to a specific individual without the use of additional information) as long as the controller can demonstrate that information necessary to identify the consumer is kept separately from the pseudonymous data and is subject to effective technical and organizational controls that prevent the controller from accessing such information.

Controllers and Processors

The CTDPA utilizes the categories of "controllers" and "processors" to describe obligations for businesses, mirroring the approach of the EU's GDPR and the privacy laws of Colorado, Utah and Virginia. A controller is defined as "an individual who, or legal entity that, alone or jointly with others determines the purpose and means of processing personal data," whereas a processor is any "an individual who, or legal entity that, processes personal data on behalf of a controller." The majority of the obligations created by the CTDPA are aimed at controllers rather than processors, with the CCPA and CPRA making similar distinctions between businesses and service providers.

Consumers Rights

Similar to the regulation in the four other states, the CTDPA provides consumers a series of data privacy rights, including the rights to (1) opt out, (2) confirm and access the personal data the controller is processing, (3) correct inaccuracies, (4) data portability and (5) delete personal data. Consumers may exercise such rights by submitting a request to a controller specifying the right the consumer intends to exercise, to which the controller must respond within 45 days. A controller may extend the initial 45-day period by an additional 45 days if reasonably necessary due to the complexity of the request or the volume of the requests received by the controller. The controller must inform the consumer of the extension in the initial 45-day period, including the reason for the extension. The CTDPA also allows for businesses to charge consumers a reasonable fee after the first request if the requests from a consumer are manifestly unfounded, excessive or repetitive during the same 12-month period.

Right To Opt Out

Consumers have the right to opt out of the processing of their personal data for purposes of (1) targeted advertising, (2) the

sale of personal data or (3) profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer. A consumer can exercise the right to opt out by submitting a request to the controller via the means described in the controller's privacy notice. As in California and Colorado, the CTDPA enables consumers to assign an authorized agent to act on the consumer's behalf to opt out of the processing of such consumer's personal data.

Similar to Colorado, Utah and Virginia, "targeted advertising" under the CTDPA is defined as "displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated Internet web sites or online applications to predict such consumer's preferences or interests." California's CPRA defines targeted advertising similarly under the name "cross-context behavioral advertising." All four of the other states afford consumers the right to opt out of receiving such advertisements.

"Sale of personal data" is defined by the CTDPA as "the exchange of personal data for monetary or other valuable consideration by the controller to a third party." This definition is in line with the approach adopted by California and Colorado, which considers a "sale" to have occurred for nonmonetary consideration. This contrasts with the approaches taken in Utah and Virginia, which limit "sales" to exchanges for monetary consideration. As with the exceptions to the "sale" definition under the privacy laws of other states, the definition expressly excludes various transfers, including the transfer of personal data as part of a merger, acquisition, bankruptcy or other transaction. Similar to Utah, Virginia and Colorado, also exempt are transfers to affiliates of the controller, though the definitions of "affiliate" differ among the statutes.

"Profiling" is defined as "any form of automated processing performed on personal data to evaluate, analyze or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location or movements." The CTDPA's opt-out right is expressly limited to instances where the profiling is in furtherance of automated decision-making. The opt-out right for profiling under the Colorado and Virginia laws are similarly worded, although they are not expressly limited in this way. Utah does not provide for any sort of opt-out right from profiling, whereas California's CPRA expressly contemplates the regulator issuing regulations governing opt-out rights regarding the use of automated decision-making technology, including with respect to profiling — although any such regulations have yet to be issued.

When the CTDPA takes effect on July 1, 2023, controllers are required to provide "clear and conspicuous links" on the controller's website to enable consumers or their agents to opt out of targeted advertising or the sale of the consumer's personal data. As of January 1, 2025, controllers also will be required to allow consumers to opt out of these uses of personal data through the transmission of an "opt-out preference signal, " which is similar to Colorado's requirement that controllers recognize such opt-out signals starting on July 1, 2024.

Right To Confirm and Access

Consumers have the right to "[c]onfirm whether or not a controller is processing the consumer's personal data and access such personal data, unless such confirmation or access would require the controller to reveal a trade secret." This right is present in some form in the laws of the other four states.

Right to Correction

Consumers have the right to "correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data." This right is in line with the privacy laws of the CPRA in California, as well as the laws in Colorado and Virginia, although the Utah law does not provide this right.

Right to Deletion

Consumers have the right to "delete personal data provided by, or obtained about, the consumer." This inclusion closely tracks the language adopted by Virginia, which allows consumers to require that the controller delete all personal data that a controller possesses about the consumer despite how the information was obtained. The statutory language describing this right in the CTDPA differs from that of Colorado, Utah and California — each of which also affords some form of deletion right. The formulation in Colorado's law is very broad, affording consumers "the right to delete personal data concerning the consumer." California and Utah only require deletion of personal data "collected from" or "provided by" the consumer, respectively, though as we noted in our March 2022 *Privacy & Cybersecurity Update*, the California attorney general released an opinion taking the view that internally generated inferences also are subject to this deletion right. The practical effects of these differences likely will not be fully understood until the states' respective regulators provide guidance regarding the exact scope of this right.

Right to Data Portability

The CTDPA affords consumers the right to "obtain a copy of the consumer's personal data processed by the controller, in a portable and, to the extent technically feasible, readily usable

format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means, provided such controller shall not be required to reveal any trade secret." Similar to the Colorado law, this right is broadly worded to include all of a consumer's personal data, regardless of its source. The data portability right under the Virginia and Utah laws is worded more narrowly to only apply to personal data "that the consumer previously provided to the controller," whereas the CCPA and CPRA in California do not include this right at all.

Obligations Imposed on Controllers

The CTDPA provides guidance on how businesses can collect and use consumers' personal data, poses limitations on personal data usage and requires businesses to implement specific security and transparency measures regarding personal data.

Limits on Collection and Use

The CTDPA limits a controller to the collection of personal data that is "adequate, relevant and reasonably necessary in relation to the purposes for which the data is processed, as disclosed to the consumer." Data may not be processed for purposes that are not reasonably necessary nor compatible with the disclosed purposes for which the personal information is processed, as was disclosed to the consumer, without the consumer's prior consent. The "disclosure" requirement suggests that businesses will need to specify how they plan to use personal data before they do so. This language is identical to that of the VCDPA.

Duty of Transparency and Purpose Specification

A controller must provide consumers with a reasonably accessible, clear and meaningful privacy notice that includes: (1) the categories of personal data processed; (2) the purpose for processing personal data; (3) how consumers may exercise their consumer rights; (4) the categories of personal data that the controller shares with third parties, if any; (5) the categories of third parties, if any, with which the controller shares personal data; and (6) an active email address or other online mechanism that the consumer may use to contact the controller.

Technical Safeguards and Transparency Measures

A controller must establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data that is appropriate to the volume and nature of the personal data at issue.

Duty of Nondiscrimination

A controller may not discriminate against a consumer for exercising any of the consumer rights, including by denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services to the consumer.

Duty Regarding Sensitive Data

A controller cannot process sensitive data concerning a consumer without obtaining the consumer's consent. With respect to processing sensitive data concerning a known child, the controller must process such data in accordance with COPPA. This legislation is similar to the requirements of the CPA and VCDPA, both of which also require consumer consent for such processing.

"Sensitive data" under the CTDPA is defined as "personal data that includes (1) data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation or citizenship or immigration status; (2) the processing of genetic or biometric data for the purpose of uniquely identifying an individual; (3) personal data collected from a known child; or (4) precise geolocation data."

Data Protection Assessments

Similar to California, Colorado and Virginia, the CTDPA requires data controllers to conduct and document a data protection assessment for each processing activity that "presents a heightened risk of harm to a consumer." These activities include (1) processing personal data for the purposes of targeted advertising; (2) the sale of personal data; (3) the processing of personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of injury to consumers; and (4) the processing of sensitive data.

Data Processors

Under the CTDPA, processors must adhere to the instructions of the controller and assist the controller to meet its obligations under the CTDPA. The law requires a contract to govern the relationship between the controller and processor that states the data processing procedures and protections, instructions for processing data, nature and purpose of processing, type of data subject to processing, duration of processing, and the rights and obligations of both parties. Processors may engage subcontractors pursuant to written contracts that require the subcontractor to meet the obligations of the processor with respect to the personal data. Aligning with Colorado, the CTDPA first requires that the processor provide the controller an opportunity to object before engaging any such subcontractor.

Enforcement

The CTDPA does not provide consumers with a private right to action for violations of the law, as violations can only be enforced by the Connecticut attorney general. This approach is aligned with the privacy laws in Colorado, Utah and Virginia.

Prior to initiating any action for a violation, the attorney general must issue a notice of violation to the controller if it is determined that that a cure is possible. Upon receiving such notice, the controller has 60 days to cure the alleged violation. This is the same cure period as the Colorado CPA, but longer than the 30-day cure period in California, Utah and Virginia. However, this cure period becomes optional on December 31, 2024. Violations of the CTDPA, including failing to cure a violation within the CTDPA notice period, are considered a deceptive trade practice under Connecticut's Unfair and Deceptive Acts and Practices statute, which results in civil penalties of up to $5,000 per willful violation.

The penalties imposed under the CTDPA are roughly in line with those other states. California's CPRA imposes a civil penalty of $2,500 for each violation or $7,500 for each intentional violation, while Utah's UCPA enforces actual damages to the consumer and up to $7,500 per violation in civil penalties. Similarly, Virginia's CDPA law imposes civil penalties of up to $7,500 for each violation. Colorado's CPA does not specify the penalty amounts, but civil penalties could be up to $20,000 for each violation with a maximum penalty of $500,000 for any related series of violations.

The CTDPA also requires the state's General Assembly to convene a task force to study topics concerning data privacy, including (1) information sharing among health care providers and social care providers, (2) algorithmic decision-making and the reduction of bias with respect thereto and (3) ways to verify the age of a child who creates social media account.

Key Takeaways

Even though there are many similarities between the CTDPA and the other four states' laws, there are many substantive differences that companies subject to some or all of these laws will need to reconcile as they implement and maintain a unified privacy compliance program. Companies also will need to determine whether to adopt a unified approach by applying the highest standards and best practices across operations in all jurisdictions — such that a single policy addresses all of these state requirements — or if a more individualized, state-by-state approach is preferable. Companies seeking to establish a unified approach should be aware that there are a number of state-specific requirements that may make this challenging. Such challenges are likely to only increase for the foreseeable future, as more and more states adopt their own version of these data privacy laws.

What remains to be seen is whether the continuing adoption of this patchwork of state-specific privacy laws puts pressure on Congress to develop a federal privacy law that preempts these state laws, in whole or in part. While such a federal law would seem a logical outcome, Congress has failed to even establish a federal data breach notification law despite the fact that each state has its own notification law.

Return to Table of Contents

Better Cybercrime Metrics Act Signed Into Law

On May 6, 2022, President Joe Biden signed the Better Cybercrime Metrics Act[2] (BCMA) into law, enacting the legislation originally proposed by a bipartisan group of lawmakers in response to increasing public concern about cybercrime and the lack of comprehensive cybercrime data and monitoring in the United States.

The BCMA requires the Department of Justice and law enforcement agencies to compile detailed cybercrime statistics and develop a taxonomy to help contextualize and sort cybercrime data. The act consists of four parts:

- **Cybercrime Taxonomy.** The National Academy of Sciences is authorized to create a taxonomy for cybercrime incidents in consultation with various stakeholders, such as federal, state and local law enforcement agencies, cybercrime experts and business leaders.
- **Cybercrime Reporting.** The attorney general is required to establish a category in the National Incident-based Reporting System for the collection of cybercrime and cyber-enabled crime reports from federal, state and local officials. The attorney general also is directed to incorporate recommendations from taxonomy mentioned previously.
- **National Crime Victimization Survey.** The DOJ's Bureau of Justice Statistics and the Census Bureau are directed to include questions related to cybercrime and cyber-enabled crime as part of its annual National Crime Victimization Survey.
- **GAO Study on Cybercrime Metrics.** The comptroller of the United States is required to assess and report the effectiveness of reporting mechanisms for cybercrime in the United States and identify disparities in reported data vis-à-vis other types of crime.

[2] Pub.L. 117-116.

Key Takeaways

The new taxonomy that will be created by the National Academy of Sciences may improve data collection on cybercrimes, thereby assisting relevant stakeholders in performing risk assessments with respect to certain categories of cybercrimes. The taxonomy is expected to be an important step in defining cybercrime metrics and providing recommendations to the DOJ and other authorities.

Return to Table of Contents

New York Enacts Law Requiring Notice to Employees Regarding Electronic Monitoring

On May 7, 2022, an amendment to the New York Civil Rights Law (NYCRL) went into effect, requiring that employers provide notice to employees regarding electronic monitoring of certain forms of communication.

Covered Employers and Employees

Employers that monitor their employees' electronic communications typically disclose such practices through employee handbooks or internal privacy policies. A new amendment to the NYCRL mandates that all employers (regardless of size) in New York state provide written notice to new employees upon their hiring if the employer monitors or plans to monitor or intercept their telephone communications, email communications or internet usage. The amendment also requires that new employees acknowledge receipt of the notice.

Under the amendment, employers are not required to obtain express acknowledgments from existing employees. Employers are, however, required to post a notice in a "conspicuous place which is readily available for viewing" by existing employees subject to electronic monitoring. "Conspicuous place" is not defined under the statute, but given that similar language has been adopted in other states — such as the California Online Privacy Protection Act's requirement that website privacy policies be "conspicuously posted," and in Connecticut's electronic monitoring law, which includes identical language — employers may want to consult the regulatory guidance from such states. For example, employers might consider the use of capitalized letters or the importance of font size when posting the notice of electronic monitoring policy on an intranet site or other place where employees can easily access and review the policy.

Of note, the amendment does not address whether any individuals hired by New York employers who are permitted to work remotely out of state are entitled to receive such notice. In the absence of such guidance, New York employers may opt to provide the notice to such employees out of an abundance of caution.

Electronic Monitoring Under the Amendment

The amendment states, in relevant part, "an employee shall be advised that any and all telephone conversations or transmissions, electronic mail or transmissions, or internet access or usage by an employee by any electronic device or system, including but not limited to the use of a computer, telephone, wire, radio or electromagnetic, photoelectronic or photo-optical systems may be subject to monitoring at any and all times and by any lawful means."

However, the amendment does not apply to processes that are: (1) designed to manage the type or volume of incoming or outgoing email, telephone voicemail or internet usage; (2) not targeted to monitor or intercept the activities of a particular individual; and (3) are performed solely for the purpose of computer system maintenance and/or protection.

Penalties for Violations

There is no private right of action available to employees for violations of the amendment. Instead, the Office of the New York State Attorney General is tasked with enforcing the amendment, and employers who are found to be in violation will be subject to fines of up to $500 for a first offense, $1,000 for a second offense and $3,000 for each subsequent offense.

Comparison to Electronic Monitoring Laws of Other States

The New York law is similar to laws passed in Connecticut and Delaware, with a few notable differences.

Connecticut's law requires employers to provide prior written notice to employees about electronic monitoring, and employers must post its notice of electronic monitoring practices in a conspicuous location. However, the Connecticut law does not require acknowledgment of receipt of the policy by new hires. Moreover, the law broadly defines electronic monitoring to include all information "on an employer's premises concerning employees' activities or communications by any means other than direct observation." Connecticut additionally permits employers to conduct electronic monitoring without providing prior notice if it reasonably believes that employees are violating the law, the legal rights of the employer or other employees, or creating a hostile workplace environment — an exception not present in the New York amendment. An employer in violation of Connecticut's law is subject to civil penalties, enforced by the state's labor commissioner, ranging from $500 to $3,000.

Delaware's state law shares many similarities with the New York amendment. However, Delaware explicitly defines notice as either: (1) daily notice when the employee accesses employer-provided systems or internet, or (2) a one-time written or electronic notice to the employee and an employee acknowledgment of receipt of notice. An employer in violation of the Delaware law is subject to a $100 civil penalty for each violation.

Key Takeaways

While New York is the latest state to enact such a law, trends across the country indicate that legislatures are introducing regulations that require employers to provide notice to employees regarding whether and how their data is being collected and used. For example, earlier this year, California Assembly Member Ash Kalra introduced the Workplace Technology Accountability Act (Assembly Bill 1651), which would require, among other things, employers to inform employees of how the employer collects and uses employee data before engaging in such conduct. These are in addition to the more general trend of states, including California, Colorado, Connecticut, Utah and Virginia, having adopted omnibus data privacy laws.

Moving forward, New York-based employers should ensure they provide all new hires with a stand-alone copy of their policy explaining their intent to engage in electronic monitoring of employees, and additionally collect written or electronic acknowledgment of receipt of the notice by all new hires. New York-based employers also may want to consider implementing this practice for all new hires, regardless of the employee's physical location. Additionally, such employers should ensure that a stand-alone copy of the policy is posted in a conspicuous place and made readily accessible for all employees.

Return to Table of Contents

FTC Adopts Policy Statement on 'Edtech' and COPPA

In a new policy statement adopted on May 19, 2022, the Federal Trade Commission (FTC) stated that children should not have to needlessly surrender their privacy rights in order to do schoolwork and participate in remote learning.[3] Moreover, the FTC will closely scrutinize compliance by providers of education technology (edtech) with the Children's Online Privacy Protection Act (COPPA).

Background

COPPA was enacted by Congress in 1998 to protect the privacy of children under the age of 13, which granted the FTC the authority to enforce the legislation and promulgate a related rule (COPPA Rule) that supplemented it. Since the enactment of COPPA, the FTC has viewed the protection of children's privacy as one of its key priorities.

Concerns about data collection in school settings are particularly acute. Technology use in the classroom has grown substantially in recent years, especially during the early months of the COVID-19 pandemic when many schools were forced to close down and switch to remote learning. On the other hand, the edtech industry is dominated by business models that collect and monetize customers' personal information, which can raise serious concerns about children's privacy, which the FTC's statement sought to address.

FTC's Focus

In the statement, the FTC underscored that edtech providers must fully comply with all of the provisions of COPPA and the COPPA Rule, and that such providers will be subject to the FTC's scrutiny. In particular, the FTC identified the following four areas of focus:

- **Prohibition Against Mandatory Collection.** COPPA-covered companies must not condition participation in any activity on a child disclosing information beyond what is reasonably necessary for the child to participate in that activity. For example, if email communication with a student is not needed for a particular activity, an edtech service provider cannot require students to provide email addresses in order to participate in such activity.
- **Use Prohibitions.** COPPA-covered companies are strictly limited in how they can use personal information they collect from children. For example, operators of edtech services that collect personal information pursuant to school authorization may use such information only to provide the requested service.
- **Retention Prohibitions.** Companies must not retain personal information collected from a child longer than reasonably necessary to fulfill the purpose for which it was collected. The statement specifically deems the retention of children's data for speculative future potential uses as unreasonable.
- **Security Requirements.** Companies must have procedures to maintain the confidentiality, security and integrity of children's personal information. The statement notes that even absent a breach, a lack of reasonable security constitutes a violation of the COPPA Rule — potentially signaling a more proactive enforcement posture from the FTC in the future.

[3] See May 19, 2022 FTC release, "Policy Statement of the Federal Trade Commission on Education Technology and the Children's Online Privacy Protection Act."

In releasing the statement, Samuel Levine, director of the FTC's Bureau of Consumer Protection, noted that "students must be able to do their schoolwork without surveillance by companies looking to harvest their data to pad their bottom line," and "[p]arents should not have to choose between their children's privacy and their participation in the digital classroom."

Key Takeaways

With the increase in use of edtech in public education, the FTC may be signaling a renewed interest in COPPA compliance and enforcement. Edtech providers and other COPPA-covered businesses should review the FTC's statement and ensure compliance with the COPPA Rule, while paying particular attention to the collection, use, retention and protection of children's personal information.

Return to Table of Contents

Queen's Speech Confirms Planned Overhaul of UK Data Protection Regime

On May 10, 2022 the U.K. government formally announced its intentions to proceed with reforms to the U.K.'s data protection regime through the introduction of a new Data Reform Bill. The announcement was made in the Queen's Speech, which sets out the government's yearly policy and legislative agenda for the new parliamentary session. While the precise content of the bill has not yet been confirmed, the Queen's Speech noted the government's view that "the UK General Data Protection Regulation and Data Protection Act 2018 are highly complex and prescriptive pieces of legislation … [that] encourage excessive paperwork, and create burdens on businesses with little benefit to citizens." It is therefore expected that the bill, once announced, will underscore the government's intention to implement a regulatory regime that departs significantly from the current U.K. GDPR. The bill is expected to be presented in the summer of 2022, at which point it will begin its lengthy and uncertain passage through Parliament.

Background

Reforms to the U.K.'s data protection regime have been anticipated since September 2021, when the Department for Digital, Culture, Media and Sport (DCMS) published a new consultation entitled "Data: a new direction,"[4] which included various proposals to reduce the burdens on U.K. businesses, including:

- **Removal of the requirement to keep records of data processing activities.** While the U.K. GDPR currently requires controllers to maintain records containing a number of mandatory categories of information (*e.g.*, for purposes of data processing and retention periods for each category of data), the consultation recommends introducing greater flexibility for the form and content of these records.
- **Removal of the requirement to appoint a data protection officer (DPO).** At present, the U.K. GDPR mandates that businesses conducting certain high-risk forms of processing (*e.g.*, processing of special category data on a large scale) must designate a DPO with "expert knowledge of data protection law and practices" and register their details with the Information Commissioner's Office (ICO). The consultation includes a proposal to instead allow businesses to internally designate an individual to oversee their data protection compliance programs.
- **Changes to the regime on data subject rights requests.** In response to a perceived high administrative burden on businesses, the consultation has set out a number of proposed changes to the current rules on data subject rights requests, including the introduction of a cost ceiling (*i.e.*, a limit to the amount of costs a business must incur when responding to a data subject rights request) and a reduction in the threshold that must be reached before a business can refuse to respond to a request (currently the request must be "manifestly unfounded").
- **Removal of the requirement to carry out data protection impact assessments (DPIAs).** Under the current regime, businesses must conduct a DPIA before any large-scale processing of special category personal data is undertaken. The consultation includes a proposal to allow businesses to adopt an approach that reflects their specific organizational circumstances.
- **Changes to the data breach reporting threshold.** While businesses must currently report any breach unless that breach is "unlikely" to result in a risk to the data subjects' rights, the consultation proposes that this threshold be amended so that reports need only be made if the risk is "material."

The consultation closed in November 2021 and with the results expected in the coming weeks and the draft bill to follow this summer. While it is clear that the reforms are intended to reduce administrative burdens on businesses and organizations, the

[4] For further details, please see our September 2021 *Privacy & Cybersecurity Update* article, titled "UK Government Launches Public Consultation in Planned GDPR Reform."

Queen's Speech was unequivocal in stating that this would not come at the cost of the rights of individuals. Indeed, the government has stated that the bill will still ensure that "UK citizens' personal data is protected to a gold standard" and that the new "culture of data protection" will be "outcomes-focused." Once presented before Parliament, the bill will have an uncertain future as its passage through the legislative process will see months of review and debate, and also may be rejected without being passed into law.

Key Takeaways

The reforms to the current data protection regime are expected to afford some level of flexibility to U.K. businesses, allowing for the implementation of data protection compliance programs and requirements over time. The U.K. government estimates that the bill will generate over £1 billion of savings in the 10 years following its introduction. The reforms are expected to be particularly significant to new businesses, small and medium-sized enterprises, and technology start-ups that may lack the resources to keep up with the regulatory obligations currently imposed by the U.K. GDPR.

For others, however, considerable resources have already been invested regarding the implementation of detailed data protection compliance frameworks, with many businesses having taken on additional skilled personnel to manage and administer these programs. In addition, for businesses that operate in both the U.K. and Europe (or who have customers in both territories), the bill may introduce unwelcome legislative divergence and increase the complexity of current compliance measures.

Finally, in the event that the bill introduces significant changes to the U.K.'s current regime, and those changes are tantamount to an erosion of individual rights, this may prompt the EU to review or even revoke the U.K.'s adequacy decision. This would mean that, much like current transfers of data from the U.K./EU to the U.S., transfers of data from the EU to the U.K. would need to be protected with additional safeguards (including contractual protections) that may further increase the administrative expense of trade between EU- and U.K.-based businesses.

Global organizations should carefully monitor developments regarding the U.K.'s data protection reforms to ensure that they are prepared in advance to respond to the changes, and we will provide updates on the status of the bill as further details emerge.

Return to Table of Contents

UK Information Commissioner's Office Publishes Updates to Data Anonymization Guidance

On March 7, 2022, the ICO published the latest chapter of its ongoing guidance on operational and organizational requirements for data protection law-compliant data anonymization (including personal data). This is the fourth draft chapter of ICO guidance on this topic, with more anticipated to come. The ICO is seeking views on all chapters until September 16, 2022, and, once finalized, the consolidated guidance will provide valuable insight into how the ICO will assess businesses' compliance with data protection laws. The newly released Chapter 4 is particularly useful to businesses, as it details a number of practical proposals for handling and safeguarding anonymized data.

Background

Anonymization allows businesses to exploit the potential of the data they control in a data-compliant way (*e.g.*, research, development, data analytics and big data). The GDPR and U.K. GDPR do *not* apply to data that is (1) truly anonymous (*i.e.*, where it is impossible to identify the data subject from that data) or (2) effectively anonymous (*i.e.*, where identification of the data subject is unlikely as the identifiability risk is sufficiently remote). However, the GDPR and U.K. GDPR *does* apply where a data subject is directly identifiable, indirectly identifiable or likely to be identifiable (as the identifiability risk is insufficiently remote), or where the data is pseudonymized (*i.e.*, where the data subject is no longer directly or indirectly identifiable without the use of additional information that is kept separate from the pseudonymized data). As such, businesses that intend to engage in commercialization or other processing of anonymized data of U.K. data subjects (on lawful grounds for purposes that will be made transparent to data subjects) are encouraged to put in place robust accountability and governance measures in line with GDPR/U.K. GDPR requirements to minimize any reidentification risk to data subjects and investigation or penalties for noncompliance.

Organizational Measures

Previous chapters released by the ICO have outlined the legal and practical issues relating to the process of data anonymization as it relates to GDPR and U.K. GDPR (Chapter 1), ensuring effective anonymization and avoiding reidentification risk (Chapter 2) and the key differences between pseudonymization (where the data subject can still be identified) and anonymization (Chapter 3). This Chapter 4 guidance contains ICO proposals on

how businesses can utilize their accountability and governance processes to implement best practices for anonymization. This guidance is aimed toward businesses that are anonymizing data (including personal data) themselves, but certain proposals are equally relevant for a business that may be using third-party pre-anonymized data within their operations, such as if they have purchased anonymized data sets to better understand customer behaviors in a specific industry.

Reidentification Incidents

The ICO noted that even with the most sophisticated safeguards in place, businesses are still vulnerable to security incidents. If a security incident leads to reidentification of an individual from data previously treated as anonymous, this will not be treated as a personal data breach, provided that the business can demonstrate that the data was effectively anonymized and best practices were followed in all other respects (*i.e.*, the proposals set out in the ICO guidance). Following a reidentification incident, the ICO suggests that businesses undertake reviews of their anonymization processes and consider implementing improvements to anonymization techniques in response to the emergence of new security threats.

Specific Chapter 4 Guidance Proposals

The ICO has proposed the following practical steps that businesses can take, where appropriate, to implement best practices regarding anonymization:

- **Planning: What governance structure should a business take?** Businesses undertaking anonymization should properly plan for anonymization, including by documenting the relevant procedures and the internal measures they take to ensure compliance with safeguards.
- **Authority: Who should be responsible for the anonymization process?** An individual of sufficient authority within the business should be designated to oversee the anonymization. The ICO recommends adopting a senior information risk owner (SIRO) to coordinate a corporate approach to anonymization and decide on suitable forms of disclosure.
- **Risk Assessment: Should a business undertake a Data Protection Impact Assessment?** A DPIA is compulsory for processing that is likely to result in a high risk to individuals, or if organizations plan to use innovative technology or match data or combine datasets from different sources.
- **Purpose: Is a business clear about why they want to anonymize personal data?** Anonymization is a form of "processing" for the purposes of the GDPR and U.K. GDPR, and organizations should therefore be clear on why they want to anonymize data and how this process can help achieve the purpose for which the personal data was collected.
- **Cooperation: How should a business work with other organizations, where necessary?** Organizations planning to disclose information should work with other organizations that are likely to be processing other information that could jeopardize the anonymity of the data (*e.g.*, where data from two anonymized data sets could be combined to create identifiable data).
- **Limited Access: What type of disclosure is it?** Organizations need to differentiate between publishing to the world at large (open data) and publishing to a limited group (limited access, such as within a closed community of researchers). Limited access disclosure is less risky than open disclosure, but safeguards must be put in place in either case.
- **Heightened Risk: How should a business identify potentially difficult cases?** Policies and procedures should be implemented to cater to cases where anonymization could be difficult to achieve, where the assessment of risk is difficult and where such risk may be significant. This may be the case in special category personal data, such as a data subject's health status or ethnicity, which is subsequently anonymized and likely to carry more risk.
- **Transparency: How should a business ensure transparency?** Individuals have a right to know how and why their data is being processed. As such, a clear notice or privacy policy outlining the process in an accessible format should be published. This notice can notify the public about any risks of the anonymization as well as any safeguards that have been put in place.
- **Training: How should a business ensure appropriate staff training?** Training for staff in procedures and safeguards should be undertaken, including how to mitigate risks, increasing data protection knowledge and utilizing training for anonymization tools. Individual staff members should understand their specific roles in ensuring anonymization is carried out safely.
- **Legislation and Tracking Developments: How should a business keep updated with legal and technical developments?** Maintaining up-to-date knowledge on key developments is encouraged, from emerging technologies in the anonymization field to understanding new reidentification threats.

Key Takeaways

Compliance Costs. While anonymizing data may permit a business to exploit data sets on lawful grounds for purposes which will have been made transparent to data subjects in line with GDPR and U.K. GDPR requirements, there are still material compliance costs to be budgeted for, such as training, governance and information security. These potential costs may discourage smaller innovators from using anonymized data sets.

Difficulties in cooperating with other businesses. The guidance encourages cooperation with other businesses to minimize any reidentification risks. This may be difficult in the context of research and development where the anonymized data set may be part of a larger confidential project.

Future security developments. New technologies such as data masking, which is intended to render data truly anonymous, may (1) reduce the need for businesses to protect against reidentification risks and (2) make safeguards more technology-focused rather than reliant on human controls.

Return to Table of Contents

Contacts

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

James Carroll
Partner / Boston
617.573.4801
james.carroll@skadden.com

Brian Duwe
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

David Eisman
Partner / Los Angeles
213.687.5010
david.eisman@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Todd E. Freed
Partner / New York
212.735.3714
todd.freed@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Rich Grossman
Partner / New York
212.735.2116
richard.grossman@skadden.com

Ken D. Kumayama
Partner / Palo Alto
650.470.4553
ken.kumayama@skadden.com

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Jason D. Russell
Partner / Los Angeles
213.687.5328
jason.russell@skadden.com

David Schwartz
Partner / New York
212.735.2473
david.schwartz@skadden.com

Ingrid Vandenborre
Partner / Brussels
32.2.639.0336
ingrid.vandenborre@skadden.com

Helena Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Eve-Christie Vermynck
Counsel / London
44.20.7519.7097
eve-christie.vermynck@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
One Manhattan West
New York, NY 10001
212.735.3000