CLIENT ALERTS & INSIGHTS

Privacy Points 2023: New State Laws Introduce New Audit and Internal Review Requirements for Personal Information Collection and Processing

FEBRUARY 7, 2023

Some states will affirmatively require annual audits of a business's data collection and processing practices and—in some cases—to submit those audits to state regulators.

With new US state data protection laws taking effect at the beginning of 2023 and continuing throughout the rest of the year, businesses are adapting to new requirements, such as regular reviews and audits of their data collection and processing activities.

At the dawn of 2023, California and Virginia both had new data protection laws take effect. Soon, Connecticut, Colorado, and Utah will join their ranks as US states are quickly filling the void left by a lack of Federal and Congressional action on omnibus data protection reform.

To view our previous commentary on the effective dates and scope of the US state data protection laws, see here.

From a practical standpoint-businesses that fall under any of the new US state data protection laws will need to undergo some form of reviews and assessments to determine (1) what data they are collecting; (2) cybersecurity protections that are in place; (3) access controls to that data; and (4) what that data is used for and how long it is retained. An in-scope business will not be able to ascertain their legal requirements without first undergoing an internal review.

From a legal standpoint-as it relates to mandatory reviews and audits-the US state data protection laws differ. California requires annual audits where a business's data processing creates a high risk to an individual's privacy or security. Colorado, Connecticut, and Virginia require in-scope businesses to conduct and document "data protection assessments" if certain activities (such as the sale of information) are occurring. Utah stands out, as it does not have an affirmative review, audit, or assessment requirement.

In addition to legal requirements placed directly on the business or controller of the personal information, the data protection laws in Colorado, Connecticut, and Virginia require the in-scope businesses to require its subcontractors and third parties that collect, store, use, or process the personal information on the business's behalf to allow the in-scope business to audit that subcontractor's or third party's compliance with the applicable law.

California Cybersecurity Review

The California Privacy Rights Act ("CPRA") itself does not address any requirement for in-scope businesses to conduct regular audits, reviews, and assessments, whether related to data processing or information security measures.

However, the CPRA requires the newly minted state privacy regulator, the California Privacy Protection Agency ("CPPA") to issue regulations "requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security". The text of the CPRA goes on to state that any such business whose processing creates such risks must conduct an annual cybersecurity review.

The current draft CPRA regulations do not directly address this topic and instead only address when the CPPA itself can conduct audits of businesses who the CPPA suspects of violating the data protection law.

From the CPRA text itself though, a business can glean an annual review of data collection and processing activities requirement on every business, because in order to know whether the CPRA's annual cybersecurity audit requirement applies, a business must first know whether their data processing presents a significant risk to a consumers' privacy or security. While a full blown cybersecurity audit may not be required in every instance, any business within the scope of the CPRA will need to conduct some form of annual review of its data processing practices gauging whether it is required to meet the CPRA's audit requirements.

In fact, the CPRA sets forth factors that businesses should use to determine whether their data processing presents a significant risk: (1) the size and complexity of the business; and (2) the nature and scope of the processing activities. For example, a business that only collects and processes a small amount of business contact personal information for business to business sales purposes presents a lower risk than processing tens of thousands of consumers' names and demographic information in order to direct marketing to them in a business to consumer model.

If a business determines that its data processing does present a significant risk to consumers' privacy or security, they must conduct the annual cybersecurity audit. Such an audit, according to the CPRA, cannot be ad hoc and instead needs to follow an established process-most likely in the form of a written policy and accompanying procedure.

Additionally, in-scope business who fall under the annual cybersecurity audit requirement, are also required to submit a risk assessment on a "regular basis" to the CPPA. This is in contrast to Colorado, Connecticut, and Virginia, which only require the assessments required under those laws be made available on request.

The assessment must indicate (1) whether sensitive personal information is in-scope; (2) identify and weigh the benefits resulting from the processing-both from the consumer and business perspective-against the potential risks to the rights of the individual the information identifies.

Colorado, Connecticut, and Virginia Data Protection Assessments

The data protection laws in Colorado, Connecticut, and Virginia offer a bit more guidance on when exactly assessments and audits are required.

If a business is under any of these three states' data protection laws, they are prohibited from processing personal information in a manner that presents a higher risk of harm to the individual consumer without first conducing and documenting a data protection assessment. High risk processing includes: (1) targeted advertising or profiling that presents a reasonably foreseeable risk of (a) financial harm, (b) unfair or deceptive treatment, (c) intrusion on the solitude or seclusion of private affairs (based on a "reasonable person" standard), or (d) other substantial injury to the consumer; (2) the sale of personal data; or (3) any processing that involves sensitive personal information.

If a data protection assessment is required, it must identify and weigh the benefits of the processing against the potential risks-specifically the risks to the individual rights a consumer has over their personal information. Any such assessment should also factor in the existence or possibility of safeguards that mitigate the risks.

These would include heightened encryption standards, anonymization and/or aggregation of the information, access control measures, etc. In fact, the assessment needs to specifically weigh the use of de-identified information and what the consumer's reasonable expectations are based on their relationship to the in-scope business.

Finally, in all three states, the data protection assessments must be made available to the applicable state's attorney general as they may request.

It is important to note that separate assessments covering individual processing activities are not necessary. A single data protection assessment can be used to cover multiple processing activities so long as the processing and information involved is sufficiently similar.

Audits of Subcontractors

Each of the US state data protection laws require that in-scope businesses have specific contractual requirements in place with its subcontractors and third parties that collect, store, use, or process the personal information on the business's behalf.

In Colorado, Connecticut, and Virginia, one of the required contractual provisions is a right for the in-scope business to receive information necessary to confirm the third party is compliant with the law, and a requirement that the third party contribute to reasonable audits.

Specifically, there must be contractual provisions in place that require the third party to (i) make available all information necessary to demonstrate compliance with the obligation in the specific law; and (ii) allow for and contribute to reasonable audits and inspections by the in-scope business or a qualified third party-at least annually-to review the third party's technical and organizational security measures and compliance with the applicable law.

Both California and Utah lack an affirmative legal requirement in this regard. However, in-scope businesses likely remain liable for any third party action or inaction if the in-scope business is having the third party collect, use, store, or otherwise process personal information on the business's behalf. Therefore, from a practical standpoint, in-scope businesses should still look to include some form of compliance certification or audit right related to data protection in there third party contracts.

As more states continue to implement their own variations of data protection laws and business juggle the various requirements, the Benesch Data Protection and Privacy team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Lucas Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.