



ATTORNEYS AT LAW

12/4/2018 | Insights Tech & Data Insights

New Colorado Data Protection Laws

Colorado Tightens Consumer Data Privacy Laws

The global trend of stricter consumer privacy laws has raged on following the introduction of the European Union's General Data Protection Regulation (the "GDPR"). The GDPR has sparked the passage and/or implementation of various consumer data privacy laws in different countries around the globe. While the United States has not yet passed a federal bill on that topic, states have taken it upon themselves to pass data privacy laws reflecting the intentions/protections underlying the GDPR. As we have previously discussed, California was the first state to do so by passing the California Consumer Privacy Act (the "CCPA"). Now, Colorado has taken steps to follow California's lead in that regard.

Last January, Colorado lawmakers introduced a bipartisan bill aimed at providing more security for consumers' personal identifying information. The bill, titled HB 1128, went into effect on September 1, 2018. The bill affects all "covered entities," which are defined as an individual, corporation, business trust, estate, trust, partnership, unincorporated association, or two or more thereof having a joint or common interest, or any other legal or commercial entity. The bill addresses three major points:

- data breach notification requirements
- security procedure requirements
- data disposal requirements

Data Breach Notification Requirements

Colorado previously required reporting breaches under the circumstance that specific information was compromised. HB 1128 expands the particular personal information breaches giving rise to notification requirements. Specifically, HB 1128 requires reporting of a breach where the information inappropriately disclosed is not encrypted, redacted, or secured by any other method rendering the name or the data unreadable or unusable, and includes both a Colorado resident's first name or first initial and last name and any one or more of the following pieces of data that relate to the resident: (i) social security number; (ii) student, military, or passport identification number; (iii) driver's license number or identification card number; (iv) medical information; (v) health insurance identification number; or (vi) biometric data. Personal information also includes a Colorado resident's username or email address, in combination with a password or security questions and answers that would permit access to any online account. Additionally, a Colorado resident's account number or credit/debit card number in combination with any security code or access code constitutes personal information under HB 1128.

If the above mentioned personal information is compromised in a data breach, a company must notify the affected residents within 30 days following the discovery of the breach. If more than 500 Colorado residents are affected, the company must also notify the state's Attorney General. Further, if there is a conflicting notice requirement under another state or federal law, the shortest notice period applies, meaning that HB 1128's requirement provides only a minimum obligation on such covered entities.

Security Procedure Requirements

HB 1128 adds requirements for businesses to implement reasonable security measures to protect personal identifying information. HB 1128 attributes a separate definition for “personal identifying information” as opposed to “personal information,” and it necessarily includes one of the following: (i) a social security number; (ii) personal identification number; (iii) password; (iv) passcode; (v) official state or government-issued driver’s license or identification card number; (vi) government passport number; (vii) biometric data; (viii) employer, student, or military identification number; or (ix) financial transaction device. Companies are also required to ensure third-party service providers to which they disclose personal identifying information to implement and maintain reasonable security measures regarding such information disclosed.

Data Disposal Requirements

HB 1128 also requires a covered entity to institute procedures for disposal of data no longer serving prescribed purpose. Such a company must develop and maintain a written policy detailing the destruction and proper disposal of paper and electronic documents containing personal identifying information. The bill states that once these documents are no longer necessary to fulfill the purposes of the business, the covered entity must shred, erase or otherwise modify the information to make it unreadable or indecipherable.

Moving Forward: Implications

HB 1128 differs from the CCPA and the GDPR. The CCPA and the GDPR are much broader laws with larger impacts on companies, while HB 1128 is tailored to specifically focus on data security and data breach reporting issues. However, it still will impact the way companies do business with Colorado consumers. The bill is consistent with the spirit of the GDPR and CCPA, both of which are intended to create transparency between consumers and covered entities with consumer information. HB 1128 aims not only to promote transparency in the form of faster breach notifications but also to ensure consumers that their data is secure.

Companies that are not yet compliant with the GDPR and CCPA are not only severely exposed to liability under those regulations but now are at risk pursuant to HB 1128 and other data privacy regulations that are appearing regularly. Companies that are compliant under those bills are in an excellent position to become compliant under HB 1128, due to overlap in the necessary infrastructure to be compliant under all three data privacy laws.

Our experienced attorneys at Dickie, McCamey & Chilcote, P.C. have advised clients on international and domestic data privacy compliance for years and will continue to provide updates on this latest development (and others to be forthcoming of course) as the global trend toward stricter data privacy inevitably continues. If you have any questions or concerns, please contact us.



Jason L. Ott, Esq.
412-392-5578
jott@dmclaw.com



Derrick L. Maultsby, Jr.
Law Clerk

The material on this site is for general informational purposes only and is not intended to be, and should not be construed to be, legal advice. There shall be no liability accepted as a result of any improper reliance on the material on this site. A qualified lawyer should always be consulted with regard to any specific legal issue or problem.
