HB 18-1128: Consumer Data Privacy

HB 18-1128 imposes data privacy requirements on school districts and BOCES. With the aim of improving consumer data privacy statewide, the bill applies to essentially all private and public organizations in Colorado. This bill became effective on September 1, 2018.

Several federal and state laws already govern various aspects of data privacy in schools. Fortunately, HB 18-1128 contains exclusions from its requirements for entities regulated by state or federal law (e.g., school districts and BOCES) that maintain procedures for data protection, data destruction and security breach notification pursuant to their applicable regulatory frameworks. Most districts and BOCES already have policies and procedures which satisfy some of HB 18-1128's requirements. However, given the scope of HB 18-1128, which encompasses some student data as well as employee data, we recommend reviewing local board policy and procedures to ensure compliance with HB 18-1128's requirements.

The new law imposes three main requirements on school districts,[1] which are explained in detail below:

1. implementation of "reasonable security procedures and practices" to protect personal identifying information;

2. implementation of data destruction policies; and

3. notification of data security breaches to affected Colorado residents, the Colorado Attorney General and consumer reporting agencies.

Definitions

HB 18-1128 defines the following key terms. These statutory terms are ***italicized and bold*** throughout this memo for ease of reference.

- ***Personal Identifying Information (PII)*** – a social security number; personal identification number; password; pass code; official state or government-issued driver's license or identification card number; government passport number; biometric data, as defined in C.R.S. 24-73-103(1)(a); employer, student or military identification number; or a financial transaction device, as defined in C.R.S. 18-5-701(3).

- ***Personal Information*** – a Colorado resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when the data elements are not encrypted, redacted, or otherwise secured: social security number; driver's license number or identification card number; student, military or passport identification number; medical information; health insurance identification number; or biometric data, as defined in C.R.S. 24-73-103(1)(a).

[1]HB 18-1128 applies to school districts and BOCES. For purposes of this memo, the term "school districts" also includes BOCES.

- ***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 an online account or a Colorado resident's account number or credit or debit card number in combination with any required security code, access code or password that would permit access to that account.

  Personal Information does not include publicly available information that is lawfully made available to the public from federal, state or local government records or widely distributed media.

  Note: HB 18-1128's definitions of ***PII*** *and* ***personal information*** differ from the definitions of similar terminology in other state and federal laws.

- ***Third-Party Service Provider*** – an entity that has been contracted to maintain, store or process ***personal information*** on behalf of a school district.

- ***Security Breach*** – the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality or integrity of ***personal information*** maintained by a school district. Good faith acquisition of ***personal information*** by an employee or agent of a school district for school district purposes is not a ***security breach*** if the ***personal information*** is not used for a purpose unrelated to the lawful school district purpose or is not subject to further unauthorized disclosure.

- ***Determination that a Security Breach Occurred*** – the point in time at which there is sufficient evidence to conclude that a ***security breach*** has taken place.

1. <u>Data protection</u>

HB 18-1128 requires a school district that maintains, owns or licenses ***PII*** to implement and maintain "reasonable security procedures and practices" that are appropriate to the nature of the ***PII*** and to the nature and size of the school district. The law does not set forth a standard defining what qualifies as "reasonable*"* security procedures and practices.

Unless a school district agrees to provide its own security protection for information it discloses to a ***third-party service provider***, the school district must require the ***third-party service provider*** to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the disclosed ***PII*** and reasonably designed to help protect the ***PII*** from unauthorized access, use, modification, disclosure or destruction.

HB 18-1128 provides that an entity regulated by state or federal law (e.g., a school district) that maintains procedures for storage of ***PII*** pursuant to the laws, rules, regulations or guidelines established by its state or federal regulator is in compliance with HB 18-1128's data protection requirements. *See*, CASB sample policies **EHC***, **Safeguarding Personal Identifying Information**; **GBJ**, **Personnel Records and Files**; **JRA/JRC**, **Student Records/Release of Information on Students**; and **JRCB***, **Privacy and Protection of Confidential Student Information**.

2. <u>Data destruction</u>

HB 18-1128 requires school districts that maintain paper or electronic documents containing ***PII*** to create a written policy for destruction or disposal of the documents. The policy must require the school district to destroy such documents when they are no longer needed. The destruction or disposal must be accomplished by shredding,

erasing or otherwise modifying the documents to make the ***PII*** unreadable or indecipherable through any means.

HB 18-1128 provides that an entity regulated by state or federal law (e.g., a school district) that maintains procedures for disposal of ***PII*** pursuant to the laws, rules, regulations or guidelines established by its state or federal regulator is in compliance with HB 18-1128's data destruction requirements. *See*, CASB sample policies **EGAEA**, **Electronic Communication**; **EHB**, **Record Retention**; and **EHC***, **Safeguarding Personal Identifying Information**.

3. Security breaches

HB 18-1128 establishes detailed notification obligations for school districts that maintain, own or license computerized data that includes ***personal information*** about a Colorado resident in the event of a data breach. Upon discovering that a ***security breach*** may have occurred, a school district shall:

- Conduct a prompt investigation in good faith to determine the likelihood that ***personal information*** has been or will be misused.
- Unless the investigation determines that misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur, the school district must give notice of the breach to the affected individuals.
- Notice must be made in the most expedient time possible and without unreasonable delay, but not later than 30 days after the date of ***determination that a security breach occurred***. HB 18-1128 prescribes certain information the school district must include in the notice. *See*, C.R.S. 24-73-103(2). For a breach of an individual's username or email address, in combination with password information, there are additional notice requirements. Notice may be delayed if a law enforcement agency determines notice will impede a criminal investigation.
- If the breach affects 500 or more Colorado residents, the school district must notify the Colorado Attorney General, unless investigation determines that the misuse of information about a Colorado resident has not occurred and is not likely to occur. Notice must be made in the most expedient time possible but not later than 30 days after the date of ***determination that a security breach occurred***.
- If the breach affects 1,000 or more Colorado residents, the school district must notify, in the most expedient time possible and without unreasonable delay, all consumer reporting agencies that compile and maintain consumer files on a nationwide basis of the anticipated date of the notification to the affected residents and the approximate number of affected residents.
- If a school district uses a ***third-party service provider*** to maintain computerized data that includes ***personal information***, the ***third-party service provider*** must give notice to and cooperate with the school district in the event of a ***security breach***.

HB 18-1128 provides two exclusions from its ***security breach*** requirements:

1. for a school district that maintains its own notification procedures as part of an information security policy, if the procedures are consistent with the timing requirements in the new law; or

2. for an entity regulated by state or federal law (e.g., a school district) that maintains ***security breach*** procedures pursuant to the laws, rules, regulations, or guidelines established by its state or federal regulator.

Notably though, even if a school district is exempt from HB 18-1128's ***security breach*** requirements per one of these exclusions, HB 18-1128 still requires the school district to comply with its provision for notice of a ***security breach*** to the Colorado Attorney General in certain circumstances. *See*, CASB sample policy **EHC***, **Safeguarding Personal Identifying Information**.

COLORADO ASSOCIATION OF SCHOOL BOARDS
2253 S. Oneida Street, Ste. 300, Denver, CO 80224
(303) 832-1000 or 1-800-530-8430
www.casb.org

Created April 2019