Strafford

Presenting a live 90-minute webinar with interactive Q&A

U.S. and EU GDPR Data Breach Notification Laws: Protecting Workplace Privacy and Data Security

THURSDAY, MAY 3, 2018

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

Risa B. Boerner, CIPP/US, Partner and Chair,

Data Security and Workplace Privacy Practice Group, **Fisher & Phillips**, Philadelphia

Danielle S. Urban, CIPP/E, Partner, **Fisher & Phillips**, Denver

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 1**.

Tips for Optimal Quality

FOR LIVE EVENT ONLY

Sound Quality

If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, you may listen via the phone: dial **1-866-370-2805** and enter your PIN when prompted. Otherwise, please **send us a chat** or e-mail **sound@straffordpub.com** immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality

To maximize your screen, press the F11 key on your keyboard. To exit full screen, press the F11 key again.

Continuing Education Credits

FOR LIVE EVENT ONLY

In order for us to process your continuing education credit, you must confirm your participation in this webinar by completing and submitting the Attendance Affirmation/Evaluation after the webinar.

A link to the Attendance Affirmation/Evaluation will be in the thank you email that you will receive immediately following the program.

For additional information about continuing education, call us at 1-800-926-7926 ext. 2.

Today's webinar will begin shortly. We are waiting for attendees to log on.

Presented by:

Risa B. Boerner, CIPP/US

Phone: (610) 230-2132

Email: rboerner@fisherphillips.com

Danielle S. Urban, CIPP/E

Phone: (303) 218-3650

Email: durban@fisherphillips.com

U.S. and EU GDPR Data Breach Notification Laws: Protecting Workplace Privacy and Data Security

Presented by:

Risa B. Boerner, CIPP/US

Phone: (610) 230-2132

Email: rboerner@fisherphillips.com

Danielle S. Urban, CIPP/E

Phone: (303) 218-3650

Email: durban@fisherphillips.com

Data Breach Notification Overview

- Common threats and best practices to reduce the likelihood of a data breach
- U.S. data breach notification laws
- GDPR data breach notification requirements
- Steps employers should take in responding to a data breach
- Potential employer liability and risk exposure

Data Breach Risks

Common internal and external threats to confidential/proprietary data and personally identifiable information:

- Malicious employees
- Careless employees
- Hackers/phishing/criminal activity
- Mobile devices
- Cloud computing
- Vendors/third-parties
- Competitors

Data Breach Prevention: Best Practices

- Develop and implement appropriate policies to identify and limit access to and disclosure of sensitive data
- Provide training and written guidance to employees with access to sensitive data
- Ensure encryption of data and devices containing data
- Adhere to appropriate security standards/frameworks

Data Breach Prevention: Best Practices

- Conduct periodic audits to ensure compliance with security standards
- Require strong passwords, changed frequently, and multi-factor authentication
- Implement appropriate bring-your-own-device ("BYOD") policies
- Install software updates regularly

Preventing a Data Breach: Best Practices

- Limit employees' ability to install software
- Limit internet access/access to websites that may contain malware
- Execute appropriate agreements with vendors to protect data
- Purchase appropriate cyber insurance

U.S. Data Breach Notification Laws: Sources of Data Privacy Obligations

- With recent laws enacted in Alabama and South Dakota, 50 states have enacted data privacy laws requiring businesses to safeguard certain types of employee and consumer information and to notify affected individuals in case of a data security breach.
- Federal laws and regulatory schemes apply to certain industries, such as healthcare and financial services, but there is no uniform federally imposed standard for data breach notification.
- Contractual obligations with customers, vendors, employees.
- Potential common law obligations, which may differ from state to state.

U.S. Data Breach Notification Laws: State Law Requirements

State data breach notification requirements vary with respect to several key areas:

- Scope of covered personally identifiable information ("PII")
- Trigger for notification obligations
- Recipients of notice
- Content of notice
- Timing of notice
- Enforcement

U.S. Data Breach Notification Laws: State Law Requirements

Information that is "PII" under most state law definitions:

- First name or first initial plus last name and one of the following:
  - Social security number
  - Drivers' license or state identification card number
  - Account number, credit card number, or debit card number combined with security code, access code, PIN or password needed to access account

U.S. Data Breach Notification Laws: State Law Requirements

Examples of information that is currently defined as "PII" in some, but not most, states:

- Biometric data (*e.g.* DE, IL, IA, MD, NE, NM, NC, WI, WY)
- Username or email address combined with password or security question answer (*e.g.* DE, RI)
- Medical information (*e.g.* CA, FL, IL, MO, OR, RI, WY)
- Health insurance information/policy number (*e.g.* CA, DE, FL, IL, MD, MO, OR, RI, WY)
- Mother's maiden name (*e.g.* NC, ND)
- Digital signature (*e.g.* NC, ND)

U.S. Data Breach Notification Laws: State Law Requirements

Trigger for notification obligations:

- Notification by access
- Risk of harm analysis
- Electronic vs. paper records

U.S. Data Breach Notification Laws: State Law Requirements

Recipients of notice:

- Affected individuals
- Attorney general
- Consumer reporting agencies/credit bureaus
- Other state agencies (e.g. FL Dept. of Legal Affairs, NY Dept. of State and Division of State Police)
- Secretary of Health and Human Services (HIPAA)

U.S. Data Breach Notification Laws: State Law Requirements

Content of notice:

- Some states require specific information, and others do not
- Examples:
  - CA: Requires specific headings, content specific in statute, including, among other things, the type of PI subject to the breach, the date the breach occurred, and a general description of the breach incident, if possible;
  - MA: Notification shall *not* include nature of the breach or unauthorized acquisition or the number of MA residents affected by the breach or unauthorized access or use.

U.S. Data Breach Notification Laws: State Law Requirements

Timing of notice:

- Common requirement for many statutes: "most expedient time possible and without unreasonable delay"
- Others have specific timing requirement
- Notification to state agencies/consumer reporting bureaus may be required within specific time frame
- May be delayed if requested by law enforcement

U.S. Data Breach Notification Laws: State Law Requirements

Enforcement:

- State data breach notification laws:
  - Attorney general
  - Private right of action in some states

U.S. Data Breach Notification Laws: Best Practices for Responding to a Data Breach

- Investigate/remediate data breach
- Identify applicable data breach notification laws
- Notify appropriate law enforcement authorities
- Notify appropriate regulators/consumer protection agencies, consistent with applicable laws

U.S. Data Breach Notification Laws: Best Practices for Responding to a Data Breach

- Identify location of individuals whose information has been compromised
- Determine whether a “breach” has occurred as defined by applicable laws
- Determine appropriate notification requirements:
  - Who should be notified
  - When to notify
  - How to notify
  - Contents of notice
- Follow-up risk mitigation steps.

U.S. Data Breach Notification Laws: Potential Employer Liability and Risk Exposure

- Fines/penalties (U.S./GDPR)
- Civil litigation
  - Statutory/common law claims
  - Title III standing issues
- Federal agency enforcement actions (*e.g.* HHS, FTC)
- Attorney general enforcement actions

General Data Protection Regulation (GDPR)

- Takes effect May 25, 2018
- Data breach notifications covered in two Articles: 33 and 34
- Article 29 Working Party guidelines adopted February 6, 2018

GDPR:
Data Controller Organizations

- Article 33 of the GDPR

- Required to notify relevant Data Protection Authorities (DPAs) within 72 hours after becoming aware of breach of personal data.

GDPR:
What is a personal data breach?

"A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data."

GDPR: What does it mean to be aware of a breach?

- Reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.

- Important to require processors to notify controllers immediately upon uncovering breach.

GDPR: Can you delay notification of breach beyond 72 hours under any circumstances?

- Incomplete notifications acceptable.
- Must explain why breach notification delayed.

GDPR: What should the notification to DPA contain?

- Describe nature of breach, categories and approximate number of data subjects and approximate number of personal data records concerned (where possible).
- Name and contact details of DPO or other point of contact for more information.
- Likely consequences of personal data breach.
- Measures taken or proposed to be taken by controller to address personal data breach, including mitigation, where appropriate.

GDPR:
Data Controller Organizations

Article 34 GDPR

- High risk breaches must be communicated to data subject without delay.

GDPR: How does an organization determine if a breach poses a high risk to data subjects?

- Disclosure of personal data, loss of access to or destruction of personal data, and/or alteration of personal data.
- Severity of consequences (identify theft, fraud, physical harm, psychological distress, humiliation, damage to reputation).
- Number and characteristics of affected individuals (children? vulnerable individuals?).
- Ability to identify individuals.

GDPR: Circumstances where risk to data subjects low

- Public data
- Encrypted so risk of personal identification low
- Only temporary loss of data
- Accidentally sent to trusted third party

GDPR: What to communicate to data subjects?

- Contact details of DPO
- Description of nature of breach
- Likely consequences
- Steps taken to address breach
- Advice to data breach subjects

GDPR: Violations of Articles 33 and 34

- Fines up to €10 Million or 2% of the Company's global annual turnover.

- Several factors will be considered when determining whether to impose a fine and amount.

GDPR: Speaking about breaches … a word about Canada

- Mandatory breach notification requirements coming into effect November 1, 2018.

- Reporting required if you determine there is a real risk of significant harm.

GDPR: What to consider when determining risk?

- Likelihood of misuse of information
- Sensitivity of information
- Harm potential (financial, psychological)

GDPR: Best Practices

1. Have plan – process that can be completed in **72** hours.
2. Review contracts with processors.
3. Know breach reporting requirements.
4. Notify employees, customers and partners of new breach reporting process.