DATA PRIVACY AND CYBERSECURITY – FROM RISK TO REWARD

34th Annual Labor & Employment Law Conference

Charles M. Russman
(248) 988-5868
crussman@clarkhill.com

CLARK HILL

THE DATA YOU HAVE

- Every business has important data, all that changes is what that data is in your business. Today, we are going to call this Sensitive Information.
- Sensitive Information can be subject to legal protection, contractual protection, or just have value to you or others

THE DATA YOU HAVE

- Examples of Sensitive Information:
  - Social Security and Tax ID Numbers
  - Health and benefit information
  - Credit card and bank account number
  - Physical and email addresses
  - Trade secrets
  - Business practices and procedures
  - Business know-how
  - Customer contact information

WHAT LAWS APPLY

- Data is subject to a lot of laws, including:
  - Michigan Privacy laws
  - HIPAA
  - FTC Act
  - California Online Privacy Protection Act (CalOPPA)
  - COPPA
  - State data breach laws
  - GDPR, PIPEDA and international laws

MICHIGAN SPECIFIC LAWS

- Social media and employee

MICHIGAN SPECIFIC LAWS

- GPS tracking

MICHIGAN SPECIFIC LAWS

- Social Security Numbers

MICHIGAN SPECIFIC LAWS

- Mental Health, HIV and Behavioral Health

MICHIGAN SPECIFIC LAWS

- Other Rights to Privacy in Michigan

HIPAA

- HIPAA may apply to your business, even if you are not a medical based business
- HIPAA applies to health plans when health information is received
  - Self-insured plans
  - Fully-insured plans

HIPAA

- When possible, consider not receiving health information
- When you do get health information, comply with HIPAA:
  - Use it only as permitted by HIPAA
  - Think about the minimum necessary
  - Obtain appropriate agreements
  - Conduct a risk assessment
  - Implement appropriate administrative, technical and physical safeguards
  - Train employees

FTC ACT

- Applies to websites that collect information from those that visit the website
- Monetary penalties apply for noncompliance
- Determine what your website collects and who has access. Not using what you have access to is not an excuse for noncompliance.
- Say all you do and do only what you say

CALOPPA

- Applies when interacting with residents of California
- Is in addition to FTC requirements, not instead of it
- Requires significantly more information, including:
  - Whether third parties have access to data
  - What rights and choices individuals have about the collection and use of data
  - Whether you respond to do not track requests and
  - Who to contact with questions or concerns

COPPA

- Not to be confused with CalOPPA
- Sets strict requirements for collecting data about children under age 13
- When it applies, there are requirements and procedures for how to ensure parental consent is obtained
- Consumer facing privacy notices should include whether you expect to collect information from or about children under age 13

STATE DATA BREACH LAWS

- Which apply depends on the location of those whose data was breached and where you are located
- Requirements and restrictions vary significantly by state
- Establishing a plan in advance and using appropriate security standards can reduce or eliminate your reporting obligations
- Timely and accurate reporting is necessary
- Negotiate this obligation with third parties who receive data

GDPR – MEET THE FUTURE

- GDPR is an EU regulation that establishes requirements for collecting and processing data of EU citizens and residents
- It applies if your business:
  - Has a physical presence or offer goods or services for sale in the EU
  - Monitors the behavior of EU individuals
  - Collects, processes or holds personal data about EU individuals
- Personal data is very broadly defined

GDPR – PENALTIES

- 2% of global turnover (or €10 million) for records-related issues, failure to notify the government and data subjects of a breach and not conducting an impact assessment
- 4% of global turnover (or €20 million) for other violations
- Time and expense of audit and investigation
- Negative publicity and reputational problems
- Breach of contract claims and revenue loss

GDPR – PERSPECTIVE

- Privacy by design

GDPR – MAPPING AND INVENTORY

- Essential to complying with most of GDPR
- Proper inventory and mapping should include:
  - When data is collected and processed
  - Where data is being stored (from server location to what vendors store data)
  - Mapping where and how data goes is transferred inside and outside of the company
  - How long you are processing and storing data
  - Electronic and paper storage of data

GDPR – IMPACT ASSESSMENTS

- Required if there is a high risk to the rights and freedoms of individuals or is a systematic and extensive processing of special categories of data
- The privacy impact assessment should include:
  - Detailed descriptions of collection, processing and purpose, including necessity and scale of processing
  - Best and worst case implications for individuals' rights
  - How risks are being minimized, reduced and alleviated
  - Possible discussion with applicable government entities

GDPR – IMPACT ASSESSMENTS (CONT.)

- Involve your data privacy officer (or equivalent) throughout the process
- It is sometimes required and always prudent to seek opinions and perspective from individuals and governmental agencies
- When the process that required a privacy impact assessment changes, the process needs to be revisited
- Have a process or procedure in place for when and how to perform privacy impact assessments

GDPR – SAFEGUARDS

- GDPR requires appropriate technical and organizational safeguards be implemented
- This standard is based on your circumstances, but must take into account the individual's fundamental right to privacy
- This requires testing of procedures and technology and training of employees

GDPR – CONFIDENTIALITY, AVAILABILITY AND RESILIENCE

- Confidentiality covers the idea that information should be assumed to be private and is not to be used or disclosed
- Availability refers to the need to have the data readily accessible by those who should have it and that others do not have access
- Resilience is about ensuring the data will be accessible in a crisis or an emergency and will be backed up to prevent inappropriate or unexpected destruction

GDPR – LAWFUL BASIS

- You can only collect and process data with a lawful basis, which include:
  - Contractual necessity
  - Legal obligations
  - Vital interests of the data subject
  - Public interest
  - Legitimate interests (subject to objection and proper weighing of interests)
  - Consent

GDPR – CONSENT

- Consent requirements are very different from in the U.S.
- Consent must be a clearly affirmative statement that is freely given, specific, informed and unambiguous
- Consent needs to be clearly distinguishable from other consents or agreements
- A permissible consent from before GDPR was effective is sufficient, but opt-out consent is not acceptable

GDPR – BREACH NOTIFICATION

- Must be made as soon as possible, not to exceed 72 hours
- Notice is to those who are impacted and the supervisory (governmental) authority
- Notification should be handled by the DPO (or an equivalent)
- Without a plan in place, compliance will be virtually impossible

GDPR – VENDOR MANAGEMENT

- You are required to ensure your vendors comply if they collect or process data on your behalf
- A written agreement covering the GDPR requirements is important and a purchase order is not likely to be sufficient
- Do not assume what vendors provide is sufficient. We have model language that can and should be used.
- The time is right to focus on standardization, proper vendor selection and a clear exception process

GDPR – DATA PROTECTION OFFICERS

- A Data Protection Officer (DPO) is responsible for GDPR compliance and should be involved in all aspects of personal data protection
- A DPO is required if your core activities consist of processing that (1) involves regular and systematic monitoring of data subjects on a large scale or (2) involves large amounts of special categories of personal data or data relating to criminal convictions
- A DPO should be independent, highly knowledgeable and can be outsourced to third parties

GDPR – INDIVIDUAL RIGHTS

- To be informed about collection and processing of their data
- To have access to their data
- To have their data corrected or amended
- To erasure or to be forgotten
- To limit the processing of their data
- To have their data ported to another provider
- To object to the collection or processing of their data
- To object to and make certain requests about automated decision making and profiling

GDPR – AUTOMATED DECISION MAKING AND PROFILING

- Individuals must be informed about automated decision making and profiling
- There must be an alternative process, unless the automated decision making or profiling is the purpose of the service

GDPR – CROSS-BORDER TRANSFERS

- In order to transfer information out of the EU, certain requirements must be met, including:
  - Determining if the country has an adequacy decision with the EU
  - Entering into appropriate agreements with third parties who will receive or transfer the data
  - Having internal policies and training in place
  - Properly informing the individuals about the transfer

CANADA – PIPEDA AND BEYOND

- Canada's current law is Personal Information Protection and Electronic Documents Act (PIPEDA)
- PIPEDA similar to GDPR, but less strict, smaller scope and smaller penalties
- Canada is very close to passing legislation that would update PIPEDA to be substantially similar to GDPR

QUESTIONS?

Charles M. Russman

(248) 988-5868

crussman@clarkhill.com

THANK YOU

Legal Disclaimer: This document is not intended to give legal advice. It is comprised of general information. Employers facing specific issues should seek the assistance of an attorney.

CLARK HILL