The Impact of Data Security Laws on IRS Audits

Presented by:
Charles E. Hodges II, Moderator*
Jones Day
1420 Peachtree Street, NE, Suite 800
Atlanta, Georgia 30309

Kristin M. Hadgis*
Morgan, Lewis & Bockius LLP
1701 Market Street
Philadelphia, PA 19103-2921

Nathaniel B. Parker
Internal Revenue Service

* Author of Presentation Materials.
Data Privacy: What is it?

• A multinational enterprise (MNE) conducts business and executes transactions throughout the world over the internet, telephone, social networks, texts, and even via facsimile.

• The correspondence transmitted by the MNE could contain information on the company’s employees, competitors, and global partners.

• This correspondence may contain sensitive “personal data”.

• In a general sense, data privacy and data security deal with the collection, storing, and disclosure of personal information.

• And to the extent the MNE has a significant presence in a particular country (or state), the MNE may find itself subject to data protection laws of that country (or state).
In the EU, “personal data” is broader and usually refers to any information that relates to an identified or identifiable person. According to the EU, personal data can include:

- a name and surname
- a home address
- An e-mail address referencing a specific name: cehodges@jonesday.com
- An identification card number
- Location data
- IP address
- Data held by a hospital or doctor

Personal data usually does not include a company’s EIN or a company’s general e-mail address: info@jonesday.com
Data Privacy Laws

• Many data privacy laws focus on whether data can be legally **collected** and **stored** as well as shared with third parties, such as the IRS.

• Data privacy laws regulate **collection** and **use** of personal data.

• In many instances, an employer cannot rely upon the **consent** of an employee for the collection and distribution of personal data based on the perceived unfair balance in the employer-employee relationship.

• In many instances, e-mails and other correspondence possessed by a MNE contain personal data of employees around the world.

• Laws or guidelines can be imposed at the federal, state, as well as industry-specific level regarding the collection, storage, and disclosure of personal data.

• The penalties for violating privacy laws are generally severe.
Good News/Bad News

- **Good News** – There is no all-encompassing data privacy or cybersecurity statute in the U.S.
- **Bad News** – There is no all-encompassing data privacy cybersecurity statute in the U.S.:

  - Attorney General Enforcement
  - FTC Act
  - FCRA
  - CAN-SPAM
  - COPPA
  - Breach Notification Laws
  - Data Disposal Laws
  - Gramm-Leach-Bliley
  - MA Data Security Laws
  - Red Flags Rule
  - FACTA
  - Consumer Class Actions
  - PCI and DSS Credit Card Rules
  - Document Retention Requirements
  - HIPAA
  - CA Online Privacy Act
  - Stored Communications Act/ECPA
  - Do Not Call Lists
  - Telephone Consumer Protection Act
  - Video Privacy Protection Act
  - Wire Tapping liability
  - Invasion of Privacy Torts
  - Data Encryption Laws
  - Identity Theft Assistance
  - E-Sign
  - Computer Fraud and Abuse Act
  - Communications Decency Act
  - Spyware Laws
  - RFID Statutes
  - FDCPA
  - Driver’s Privacy Act
  - Social Security Number Laws
  - Regulation Z
Privacy and Cybersecurity Requirements Otherwise Addressed on State-by-State Basis in the US

• Privacy Policies
  – Must have a privacy policy when gathering information
  – Basic principles: notice, access and control
  – Not many substantive requirements
  – Violations of policy
  – Discrepancy between policy and practice

• Data Disposal
  – How to dispose of personal information (not when or if)
  – No dumpsters
  – Shredding, incinerating, or “make unreadable”
  – Financial, health, even names and addresses

• Data Security
  – Administrative, Technical and Physical Safeguards
  – Incident Response Plan

• Breach Notification
Generally Applicable State Laws – “Reasonable Security” on Sensitive Personal Information

• “Reasonable Security”:
  – Physical, technical, and administrative protections
  – Locked drawers, secure buildings
  – Firewalls, encryption, no email
  – Need-to-know access only
  – Regular assessment of threats

• “Sensitive Personal Information”
  – Varies – rationale is where disclosure may cause harm
  – Social Security numbers and credit card numbers – every state
  – Some states – medical, biometric, login credentials, phone passwords
State Data Breach Notification Laws

- All 50 states
- A company that maintains sensitive information about residents of that state must notify affected individuals of a breach of the security of that information.
- Exceptions vary, but for:
  - Encryption
  - Lack of harm
  - Good-faith acquisition by an agent with no further disclosure
- State Attorneys General enforce, but also a subject in class actions
GDPR Coming to the US: California Consumer Privacy Act of 2018 (CCPA)

On June 28, 2018, California enacted the California Consumer Privacy Act (CCPA)
- A unique and comprehensive consumer privacy law
- Unlike any other US privacy law
- “GDPR-like” consumer privacy rights
- New private right of action for security breaches and potential statutory damages

Organizations subject to the CCPA must comply by January 1, 2020
- A year is not long for changing processes to comply with new privacy requirements
- Recently amended to allow enforcement grace period to July 1, 2020.

IAPP estimates that the law will likely affect more than 500,000 US companies doing business in California
- Including many small and midsized businesses
Businesses Subject to the CCPA

• A “business” subject to the CCPA must be a for-profit organization or legal entity that
  – Does business in California
  – Collects consumers’ personal information, either directly or through a third party on its behalf
    – “Collects” is broadly defined to include “buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means.”
    – Either alone, or jointly with others, determines the purposes and means of processing of consumers’ personal information
      – Resembles GDPR’s “data controller” concept
  
• A business must also satisfy one of three thresholds:
  1) The annual gross revenue in excess of $25 million
  2) Annually buys, receives for the business’s commercial purposes, sells, or shares for commercial purposes the personal information of 50,000 or more consumers, households, or devices, alone or in combination
  3) Derives 50% or more of its annual revenue from selling consumers’ personal information
Broad Definition of “Personal Information”

- Personal information includes any information that “identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household”
  - Much broader than the definition of personal information under CA’s security breach notification law

- Extremely broad definition intended to include the sort of robust consumer profile and preference data collected by social media companies and online advertisers
New Statutory Rights

- Right to know the categories of information
- Right of access and data portability
- Right to be forgotten
- Right to opt out of the sale of personal information to third parties
- Right to equal service and price
Amendments and Regulations

• The CCPA will be amended; the question is, how substantially?
• Will other state legislatures take the CCPA as a model?
  – Will CCPA catch on like CA’s data breach notification law?
  – Or will it be a one-off experiment, like the Shine the Light law?
  – Either way, likely to be a de facto national standard
• AG will seek public comment on regulations to implement the CCPA, including updates, as needed
  – Definition of “unique identifier” to address changes in technology
General Data Protection Regulation (GDPR)

- Most significant change in EU data protection law in 20 years
- GDPR is a switch from a Directive (need national laws) to a Regulation (direct effect)
- GDPR replaced EU Data Protection Directive on May 25, 2018
- Applies to all companies across all industry sectors – in and outside the EU
- “Demonstration of compliance” will be key from a management perspective
- Sanctions increase to 4% of annual worldwide turnover
GDPR cont.

- GDPR applies to:
  - EU established entities where personal data processed "in the context of its activities"
  - Other entities where:
    - An EU resident’s personal data is processed in connection with goods or services offered to such EU resident; or
    - The behavior of individuals within the EU is monitored.
The principles of data processing include (i) lawfulness, (ii) fair processing, (iii) transparency, and one of a list of conditions are satisfied:

- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity & confidentiality
- Accountability

Controller must have legal basis for data processing, including either consent, performance of contract, compliance with legal obligation, vital interest of individual, public interest, or “legitimate interest”.
The key issues under GDPR include:
- Information obligations
- Accountability and record keeping
- Data Protection Officer
- Third party processing agreements
- Privacy by design
- Data Protection Impact Assessments

Customers/employees/vendors have rights under GDPR such as:
- Right of access to data
- Right to rectification & right to erasure
- Right to restriction of processing
- Right to data portability
- Right to not be subject to automated decision making
GDPR International Data Transfers

• General prohibition of data transfers to countries outside the EU, when safeguards are in place:
  – Adequacy decision of European Commission (Andorra, Argentina, Canada (where PIPEDA applies), Switzerland, Faero Islands, Guernsey, Israel, Isle of Man, Jersey, Uruguay and New Zealand)
  – EU Standard Contractual Clauses
  – Binding Corporate Rules (intra-group data transfers)
  – For the US: EU-U.S. Privacy Shield
    – Approved Code of Conduct or Certification mechanism
    – Derogations (consent, contract, establish legal claims)
• Data disclosure request by non-EU authority only enforceable if based on international agreement such as mutual legal assistance treaty
Who is Covered by GDPR?

- Common misconception that GDPR protects all EU citizens, regardless of physical location.
  - Not so. GDPR protects individuals located within the EU at the time data is collected and processed.
- Applies to controllers and processors based outside the EU territory where the processing of personal data regarding EU data subjects relates to:
  - the offering of goods or services (regardless of payment)
  - the monitoring of data subjects’ behavior within the EU
- Penalties for breach of GDPR – up to higher of 4% global turnover or €20,000,000
- Personal data must be processed fairly and lawfully, with legitimate purpose
- Controllers and processors will be directly liable under GDPR
What is personal data under GDPR?

• “Personal Data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

• Updated private notices

• **Data protection impact assessment**: prior to processing if high risk for individuals

• **Data Protection Officer**: for controllers/processors processing substantial sensitive personal data or who have core activity of monitoring individuals on a large scale or public body

• Notify data breach to DPA without undue delay/within 72 hours and to individuals without undue delay if there is likely to be risk to individuals

• Consent standard higher: explicit, freely given, fully informed
  - Consent given in the context of employment is **not** considered “freely given.”
GDPR (cont’d)

• Right to request to be forgotten; have data rectified or deleted; portability

• **Privacy by design and default**: privacy safeguarding technology built-in from the start; privacy-friendly default setting until user chooses otherwise
  - Actively factor privacy considerations into the design and upgrade of all systems, policies, settings which process personal data

• **International transfers**: Binding Corporate Rules, model clauses, to certified organization, consent, transfer is “necessary” for performance of contract, establish, exercise or defend legal claims or for legitimate interests of controller (one-off and limited data subjects involved), adequate countries
GDPR Summary

New system for regulatory oversight
- One Stop Shop with lead data protection authority (DPA) for pan-European/international matters – involvement of other DPAs
- Local DPAs for local matters

Broader scope of application
- Extraterritorial application to non-EU based companies
- Broader definition of personal data and sensitive data, new data categories

Focus on accountability, governance
- Information obligations
- Data protection by design
- Data security and data breach notification
- Data processor agreements
- Data Protection Officer
- International data transfers
- Code of Conduct/Certification
- Documentation

Strengthened rights of individuals
- Right to access
- Right to deletion
- Right to data portability
- Right not to be subject to automated processing, including profiling
- Right to object

Increased enforcement, fines, liability
- Administrative fines up to 2% or 4% of annual worldwide turnover
- Individual actions, claims for damages
- Collective actions
- Criminal sanctions (in national laws)
GDPR Examples

• GDPR “applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.” GDPR Art 3(1).

• **Example:**

  A car manufacturing company headquartered in the US wholly-owns a branch/office in Brussels overseeing European operations, including marketing and advertisement.

  The “Belgian branch could therefore be considered as an establishment in the Union, within the meaning of the GDPR.” GDPR Guidelines, 1.a.

• Result could be different “in the absence of any representation or stable arrangement in the EU.”

• The data processing need not be carried out by the EU establishment; the controller or processor will be subject to GDPR wherever the processing occurs.
Mexican Data Privacy Laws

• The protection of personal data is a fundamental right contained in the Mexican Constitution.

• Every individual has the right to the protection of their personal data and the right to access, rectify, oppose and cancel personal data.

• The Mexican laws contain a specific scope of protection depending on the type of organization or individual responsible for gathering and storing the information or data (data controller).

• If personal data gathered and stored by a private organization or private individual the organization or individual must comply with the Federal Law of Protection of Personal Data held by Private Parties, effective as of July, 2010 (FLP of 2010).

• The FLP of 2010 governs how companies and individuals collect, use, store, protect, and manage personal data internally as well as the sharing of the information with third parties.
Redaction of Personal Data

• In many instances, the document requested may have to be turned over to the IRS, but the personal data may have to be redacted.

• For example, the Swiss Federal Supreme Court held that the names of bank employees and other third parties had to be redacted before being turned over to the IRS. The IRS had requested the information regarding Swiss bank accounts of US taxpayers. Decision 2C_640/2016.

• Redactions should be made similar to those communications that fall within the attorney-client privilege.
Examples of Redactions of Personal Data in Other Contexts

- **Court filings**
  - Federal Rules of Civil Procedure requires the following information be redacted from any filing with a federal court:
    - Social Security Number (last 4 digits is allowed)
    - An individual’s taxpayer identification number (last 4 digits is allowed)
    - Birth date (year of birth is allowed)
    - The name of a minor
    - A financial account number (last four digits is allowed)
  Fed. R. Civ. P. 5.2(a)

- **Mergers and Acquisitions**
  - Where the submission of documents to a regulator is required prior to a merger or acquisition, sensitive PII must be redacted.
  - The FTC’s instructions for production of documents states “Do not produce any Sensitive Personally Identifiable Information (“Sensitive PII”) or Sensitive Health Information (“SHI”) prior to discussing the information with a Commission representative. If any document responsive to a particular Specification contains unresponsive Sensitive PII or SHI, **redact** the unresponsive Sensitive PII or SHI prior to producing the document.”

Best Practices

Before producing documents to the IRS:

• Consider what personal data taxpayer possesses

• Implement a collection and review protocol
  – Include safeguards to protect personal data
  – Instructions on redacting: what to redact and how to redact

• If you rely on vendors, make sure you have an adequate data security agreement in place that:
  – Restricts the vendor’s use of your data
  – Requires the vendor to maintain reasonable technical and administrative safeguards to protect your data.
  – Gives you the right to audit

• Follow a strict collection and review protocol
Sources of Authority

• Guidelines of the European Data Protection Board
• UK.practicallaw.thomsonreuters.com
• “Resolving Data-Privacy Conflicts in Cross-Border Investigations and Litigation,” Callaghan, ABA Section of Labor and Employment Law, Boston, MA meeting, August, 2014.