“Protecting Personal Data: Key Issues with Compliance with European Union’s General Data Protection Regulations (GDPR)”

Barbara Dunn O’Neal
Barnes & Thornburg LLP
WWEMA 110th Annual Meeting
November 8, 2018
Manalapan, Florida
What is the GDPR?

• The General Data Protection Regulation (GDPR) is an iteration of the existing data protection law defined and enforced by the European Union.

• The purpose of the GDPR is to protect private information of EU residents.

• The GDPR grants certain rights and protections to EU residents with respect to their data.
GDPR

• Set of rules that regulate the collection, storage, disclosure, and use of “personal data” of EU “data subjects”
• Introduced 2012 and adopted April 2016
• Effective May 25, 2018
• In response to revelations and disclosures around the existence of various mass surveillance programs that collected data of EU residents (Edward Snowden and PRISM)
GDPR Jurisdictional Reach

- GDPR applies to **any** organization that **processes** the “personal data” of EU residents, **whether or not** based in an EU country or has an EU presence.

- GDPR applies when:
  1. EU presence;
  2. offer goods/services in the EU; or
  3. monitoring EU data subjects’ behavior (e.g., if you’re using an advertising technology platform to track EU data subjects and profiling them).
Does GDPR Apply?

- U.S. based business with an online store that makes sales to EU customers, collects addresses and payment information?
  - “Mere accessibility” not enough
  - Do you envisage sales in the EU? Target EU customers?
  - Are you “monitoring” EU customers? Site analytics? Tracking email analytics?
  - Using EU-based processor?
Does GDPR Apply?

• U.S. based retail business with on-site sales to EU citizens?
  – If no physical presence in EU, GDPR does not apply to these customers when they’re in the U.S.
  – But...if you start targeting them, marketing to them, and tracking/monitoring them
Definition: “Personal Data”

• Much broader than “Personal Information”/“PII” in the U.S.
• Any information relating to an identified or identifiable person (a “data subject”)
• Identifiers include:
  – first and last name
  – email address
  – an identification number
  – photo
  – location data
  – an online identifier (e.g. IP address, social media info)
  – one or more factors specific to the: physical, physiological, genetic, mental, economic, Cultural, or Social identity of that person
Definition: “Special Categories”

• **Prohibited Processing Categories:**
  – racial/ethnic origin
  – political opinions
  – religious/philosophical beliefs
  – trade union membership
  – genetic data
  – biometric data for the purpose of uniquely identifying a person
  – data concerning health
  – sexual orientation

• **Exceptions:**
  – explicit consent
  – others where processing required
Definition: “Processing”

• automated and non-automated operations performed on personal data

• In short: *anything* to do with personal data, up to merely viewing the data via browser
  – moving data
  – analyzing data
  – merely viewing/accessing data outside EU
Definition: “Processing”

- collection
- use
- transfer
- monitoring
- tracking
- viewing
Definition: “Data Controller”

• Controller:
  – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing
  – if purposes and means are determined by Union law, then that law can provide for who is the controller or the criteria for who is the controller

• Responsibility of the Controller
  – appropriate safeguards
  – appropriate data protection policies
  – adherence to approved codes of conduct
Definition: “Data Processor”

• Processor:
  – processes personal data on behalf of the controller

• Controllers engage processors:
  – binding contract detailing subject matter and duration

• Contract shall also include that processor:
  – document instructions
  – ensure confidentiality and security
  – assists in fulfilling the data subject’s rights and security
  – deletes or returns data after services at the choice of controller
  – makes information available for audits/inspections by controller
Legal Bases for Processing

• Personal Data may only be processed on one or more bases

  1) Consent
  2) Necessary for performance of a contract
  3) Necessary for compliance with a legal obligation
  4) Necessary to protect vital interests where consent can’t be given
  5) Necessary for public interest reasons or for controller to carry out legal function
  6) Necessary for legitimate interests
Consent

• Freely given
• Unambiguous
• Specific
• Informed
• Must be removed at any time
• Explicit of “sensitive data”
Consent

• Web forms require explicit action from the user e.g., a check box must be explicitly checked and not checked by default.

• Before soliciting consent, the individuals must be informed of specific rights.

• Must allow individuals to withdraw consent at any time.

• Organizations must track consent-related activities.
Legitimate Interests

• **2 Part Test:**
  – Identification of “legitimate interests”
  – Balancing test weighing interests vs. fundamental rights and freedoms of data subject

• **May include:**
  – Direct marketing
  – Unsolicited non-commercial messages
  – Research

• **Legitimate interest must be:**
  – Lawful (i.e., in accordance with applicable EU and national law)
  – Sufficiently clearly articulated to allow balancing test
  – Represent a real and present interest (i.e., not speculative)
Rights of Data Subjects

• The right to information and transparency
• The right to access and rectification
• The right to erasure ("right to be forgotten")
• The right to data portability
• The right to objection to processing
• The right to review of the automated decision
• The right to withdrawal of consent
• The right to lodge complaints
Privacy Policy

• Detailed description of organization’s use of personal data
• Information as to Cookies and Use of Analytics
• Right to Be Erased/Forgotten
• Right to Data Transfer
• Data Storage
• Data Protection Officer
Data Processing Agreement (DPA)

- Triage list of vendors from those which receive/have access to most data to those which have the least.
- Can be an amendment to existing agreement or a stand alone agreement.
- Who is Controller?
- Who is Processor? Are there sub-processors?
- What data will be provided and how can processor use it?
- Our DPA or Theirs?
  - Indemnification
  - Limitation of Liability
International Data Transfer

• Binding Corporate Rules
• Model Clauses
• Code of Conduct
• Model Contracts
GDPR Penalties

• Fines as high as 20 M euro or 4 percent of annual global turnover, whichever is higher
Compliance Strategy

• Phase 1: Assess:
  – Assess applicability: Does GDPR or CCPA Apply?
  – Data Mapping:
    • What data is being collected?
    • Where is the data being collected?
    • Why is the data being collected?
    • How is the data being processed?
    • Who has access?
    • How long is the data being retained?
    • Where is the data being transferred to?
  – Awareness: Educate decision makers. Form team. Understand the impact
Compliance Strategy

• Phase 2: Analyze
  – Gap Analysis: Assess current practices vs. requirements
  – Plan: Develop detailed remediation and compliance plan
Compliance Strategy

• **Phase 3: Compliance Steps**

1. Map Personal Data and Divide into Categories
2. Determine Lawful Basis for Each Category (e.g., legitimate interest or consent)
3. Develop Consent Forms and Obtain Consent
4. Update Privacy Policies
5. Develop Compliant Privacy Policies for internal processes
6. Develop and Execute Data Processing Agreements
Insurance

• Cyber-liability insurance
  – Covers GDPR claims
  – Provides assistance with incident response plan
  – Coverage beginning at $2M and up
  – Consider whether such insurance covers affiliates or chapters
Staff Training

• Train all staff for basic GDPR awareness
• Develop internal policy re GDPR compliance
• Ensure consultants/contractors are aware of such policy
Ongoing Care and Feeding

- DPOs/Staffing: Determine whether DPO or new staff (e.g., CPO) needed. Hire, train, implement.
- Incident response plan for data breaches
- Document, document, document
- Ensure compliance with EU Resident request re their PD
- Make sure data coming in the door is “clean”
- Make sure data going out the door is “clean”
Five Months Later....

• NYOB files complaints against Facebook, Instagram, WhatsApp and Google’s Android relating to “forced consent”
• “Claudette” has made her debut
• EU has its own data breach
• Japan and EU may soon have reciprocal adequacy agreement
• California passed California Consumer Privacy Act on 6/28/18 (limited application compared to GDPR; goes into effect on 1/1/20)
California Consumer Privacy Act of 2018 (CCPA)
CCPA

• California became the first state with a comprehensive consumer privacy law on June 28, 2018, when it enacted the California Consumer Privacy Act of 2018 (CCPA)

• The CCPA grants consumers new rights regarding their personal information and imposes various data protection duties on certain entities conducting business in California.

• The law becomes effective January 1, 2020
CCPA Scope

• The CCPA provides new rights and protections for consumers, defined as natural persons who are California residents who are either:
  • in California for other than a temporary or transitory purpose
  • domiciled in California but are currently outside the state for a temporary or transitory purpose
CCPA Scope

• The CCPA applies to businesses that collect a personal information of California’s residents and:
  1. Their annual gross revenue exceeds $25 million,
  2. They annually buy, receive, share, or sell personal information for more than 50,000 California’s consumers, households, or devices, or
  3. They derive 50% or more of their annual revenues from selling consumers' personal information.
Definition of “Personal Data”

Any information that directly or indirectly identifies, describes, or can reasonably link to a particular consumer or household
• Aliases.
• Unique personal or online identifiers, including:
  – name;
  – postal address;
  – email address;
  – internet protocol (IP) address;
  – account name;
  – Social Security number;
  – driver's license or passport number; or
  – other forms of persistent or probabilistic identifiers that organizations can use to identify a particular consumer, family, or device.
Definition of “Personal Data”

• Characteristics like race or national origin
• Commercial information, including records of personal property and purchasing habits
• Biometric information, including genetic, physiological, behavioral, and biological characteristics, or activity patterns from which organizations can extract a template or other identifier or identifying information, such as:
  – fingerprints, face prints, and voiceprints;
  – iris or retina scans;
  – keystroke, gait, or other physical patterns; and
  – sleep, health, or exercise data.
• Internet or other similar network activity
• Geolocation data
Consumer Rights

• **Know** what personal information a business collects, sells, or discloses about them,

• **Receive notice**, before or at the point of collection, about what personal information categories a business collects and its intended use purposes

• **Access** and in some cases receive a portable electronic version of their personal information

• Receive additional details regarding the personal information that a business collects and its **use** purposes
Consumer Rights

• Request that a business and its service providers **delete** their personal information

• **Opt-out** of the sale of their personal information if they are 16 years old or older.

• For children, affirmatively opt-in to the sale of their personal information, by providing direct authorization if they are between 13 and 16 years old,

• **Not face discrimination** for asserting their CCPA rights
Business Obligations

• Provide a privacy policy, updated annually and accessible on their websites

• Clearly and conspicuously link to a “Do Not Sell My Personal Information” webpage allowing consumers to exercise their opt-out rights.

• Implement procedures to respond to consumers’ verifiable requests within the allotted time periods, typically 45 days.

• Train employees responsible for handing consumer inquiries about their privacy practices and compliance requirements.

• Not resell consumer information they receive from third parties unless the consumer has received notice and an opt-out opportunity.
Exceptions

• Collecting or selling a consumer’s personal information if every aspect of the commercial conduct takes place wholly outside of California.

• Completing single, one-time transactions that do not retain collected personal information.

• Selling personal information as part of a larger merger or acquisition transaction.

• Complying with other laws, defending legal claims, or cooperating with law enforcement.
Penalties

• Civil penalties can reach up to $2,500 per violation or $7,500 per intentional violation, for each affected consumer.
Private Right of Action

• The CCPA permits a private right of action for unauthorized access, theft, or disclosure of personal information in certain situations.

• The law provides statutory damages of $100 to $750 per consumer.
QUESTIONS?

THANK YOU
(and good luck)

Barbara Dunn O’Neal
312/214-4837; barbara.dunnoneal@btlaw.com