Is Your Business Ready for the GDPR?

Moderator: Dominic Paluzzi, Co-Chair

Panelists: Christine Czuprynski, Attorney; Sam Goldstick, Attorney; Cody Wamsley, Attorney

November 28, 2017

Agenda

- What is the GDPR?
- Expanded Territorial Scope
- Data Processors/Vendor Management
- Data Subject Rights
- Data Breach Notification
- Penalties
- Compliance Programs

What is the GDPR?

- The GDPR is an omnibus data protection regulation that replaces the European Data Protection Directive 95/46/EC.
- The GDPR relates to the processing of "personal data." Personal data means any information related to a natural person that can be used to directly or indirectly identify the person. This includes name, photo, email address, bank details, posts on social networking websites, medical information, or computer IP address.
- The GDPR also includes specific provisions for sensitive personal data, or "special categories of data," which includes passwords for access to IT systems and websites, credit card details, Social Security numbers, passport numbers, and genetic and biometric data.
- The processing of data includes collecting, using, storing, disclosing, and discarding.

Expanded Territorial Scope

- GDPR applies not only to organizations established within the EU (regardless of whether such processing takes place in the EU), but also to organizations based outside the EU that process the personal data of EU data subjects in connection with either:
  - The “offering of goods or services” to data subjects in the EU (irrespective of whether payment is required), or
  - The “monitoring” of their behavior within the EU.

Expanded Territorial Scope

- The GDPR explains that having a commerce-oriented website that is accessible to EU data subjects does not by itself constitute offering goods or services. However, the existence of certain factors could indicate a non-EU company's intention to attract EU data subjects as customers and, as a result, become subject to the GDPR. Such factors include:
  - Marketing goods or services in the same language generally used in an EU member state.
  - Listing prices in EU member state's currencies and enabling EU residents to place orders using such currency.
  - Referencing EU users or customers in its publications or online.

Expanded Territorial Scope (Examples)

Situation	Caught by the Existing Law?	Caught by the GDPR?
US social media company with no European group companies, targeting the service at individuals in Europe.	**No**	**Yes**
US retailer with e-commerce website, in the English language, accessible by EU data subjects. The company only delivers to addresses in the US.	**No**	**No**
US retailer with e-commerce website, in English language, which allows purchases and deliveries to EU data subjects in their local currency.	**No**	**Yes**
US website which uses cookies which monitors behavior and sends targeted marketing to IP addresses, which include those from EU data subjects.	**No**	**Yes**

Data Processors/Vendor Management

- GDPR imposes direct statutory obligations on data processors.
- Data processors may be subject to direct enforcement by supervisory authorities, serious fines for non-compliance and compensation claims by data subjects for any damage caused by breaching specific provisions of the GDPR.
- Some of the main obligations imposed on data processors by the GDPR include the following:
  - Appointing a representative in the EU if not established in the EU.
  - Ensuring certain minimum clauses in contracts with data controllers and complying with the mandatory requirements with regard to the content of the Processing Agreement entered into with each data controller.
  - Keeping a written record of processing activities carried out on behalf of each controller.
  - Cooperating, on request, with the supervisory authority in the performance of its tasks.
  - Notifying the data controller without undue delay after becoming aware of a data breach.
  - Designating a data protection officer (DPO) in specified circumstances.
  - Obtaining prior written authorization from the data controller before subcontracting out any data processing.

Right to Portability

- Data subjects have the right obtain and reuse their data for their own purposes and across different services.
- Data controllers need to provide functionality that enables the data subject to move, copy or transfer personal data easily from one IT environment to another, without hindrance (even if honoring this right could result in handing over valuable personal data to a competitor).
- Notably, the right to portability is limited, as it applies only where the data is processed:
  - By automated means (therefore excluding paper files), and
  - On the basis of consent or as necessary for the performance of a contract to which the data subject is a party (but not where the data was obtained on other grounds – e.g., compliance with a legal obligation)

Consent from Data Subjects

- Consent is not always required to process personal data. But where consent is relied upon for lawful processing, it must meet specific requirements.
- Consent in the GDPR is any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- Consent cannot be inferred by silence or through the use of pre-selected check boxes; it must be opt-in consent.
- "Explicit" consent is required for processing sensitive data.
- Parental consent may be required to process data on children.

Right to be Forgotten

- A data subject has the right to request that a data controller erase that data subject's personal data from its records. This right of erasure, or right to be forgotten, is not absolute. The data controller is only required to erase the data in certain circumstances, namely that the:
  - Data is no longer necessary for the purpose it was collected
  - Data subject withdraws consent
  - Data subject objects to the processing and there is no legitimate interest for continued processing
  - Data was unlawfully processed in the first place
  - Data must be erased to comply with a legal obligation
  - Data is processed in relation to online services to a child
- This right to be forgotten exists in the GDPR to allow data subjects to take control over their own data when there is no compelling reason for that data to be held. A data controller can refuse to erase the data if the personal data is processed for public health purposes in the public interest, to comply with a legal obligation, or in the exercise or defense of a legal claim, among other reasons.

Data Breach Notification Comparison Chart

	U.S. States (Generally)	GDPR
Covered Information	"Personal Information" (PI) – Name + another identifier (SSN; driver's license #; financial account information; online account credentials; health/medical data; etc.)	"Personal Data" – *any* information that can be directly or indirectly related to an identified or identifiable natural person.
A breach occurs when there is…	Unauthorized access to and/or acquisition of PI.	"The accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."
Harm Threshold	Risk of financial harm, identity theft or fraud	1. For notifying *supervisory authorities*: if the breach is likely "to result in a **risk** to the rights and freedoms of natural persons." 2. For notifying *individual data subjects*: if the breach is likely "to result in a **high risk** to the rights and freedoms of natural persons."
Assessing Risk	1. PI "**materially compromised**" and has caused, or is reasonably believed to cause, economic loss to the individual. (AZ) 2. PI has not and will not be "**misused**." (CO, ID, KS) 3. Consultation with local law enforcement reveals that there is **no reasonable likelihood of financial harm** to consumers will result from breach (IA) **4.** **Illegal use** of PI has occurred or is reasonably likely to occur, and that creates **risk of harm** to the person (HI) **5.** **Actually causes** or leads the information holder to reasonably believe has caused or will cause ID theft (KY)	Risk Factors from WP29 250 Draft Opinion: **1.** **Severity of potential consequences for individuals, including various types of harm** (financial, physical, psychological, reputational, cultural harm; social disadvantage) **2.** **Any special characteristics of the individuals** (children or anyone who is particularly vulnerable) **3.** **Special characteristics of controller** (medical org.?) **4.** **Characteristics of the recipient** (trusted not to read or access data sent in error and properly destroy it?) **5.** **Nature, sensitivity and volume of data** **6.** **Total Number of affected individuals** **7.** **Ease of identification of individuals**

Data Breach Notification Comparison Chart

	U.S. States (Generally)	GDPR
Exceptions/ Safe Harbors	(1). Encryption, when encryption key not compromised (2). Publicly available/accessible information (3). Good faith acquisition, not subject to further disclosure (4). Entities regulated by other laws (HIPAA, GLBA)	(1). Personal data was publicly available (2). Appropriate technical and organizational protection measures applied to data impacted in the breach that renders it unintelligible to unauthorized users (encryption) (3). Subsequent security measures taken ensure that risks to the affected individuals' rights and freedoms are no longer likely to materialize. (4). Individual notice would involve disproportionate effort, in which case the controller may provide public notice.
Notification Requirements (Regulatory)	(1). Timing—Varies by state ranging from 5 to 90 days, with 30-45 being more common when specific timing required; otherwise, "without unreasonable delay." (2). Content—Varies by state, but typically includes: **(i)** description of incident in general terms; **(ii)** types of information affected by breach; **(iii)** remedial or protective steps taken; **(iv)** contact information for the organization; **(v)** sample notice letter sent to affected residents, with credit monitoring details (if available); and **(vi)** # of residents impacted. (3). Method—Varies by state; postal delivery usually accepted, although some states prefer email or online submission.	(1). Timing—"Without undue delay and where feasible, not later than 72 hours after having become aware of the breach." [**WP29 Proposed Guidance* – controller does not becomes "aware" until *after* initial investigation has been conducted and incident has been identified.] (2). Content—**(i)** nature of breach, including approx. # of data subjects affected and records concerned, plus type of data involved; **(ii)** name and contact information for controller's DPO; **(iii)** description of the likely consequences of the breach; and **(iv)** measures being taken by the controller to address the breach. (3). Method—not specified.
Notification Requirements (Consumer)	(1). Timing—Varies; for states with deadlines, typically between 30-45 days; other states: "without unreasonable delay." (2). Content—Varies by state; typically the same as for regulatory notification, but includes advice directing person to remain vigilant against ID theft by reviewing account statements and monitoring free credit reports, and providing them with details on security freezes/fraud alerts and contact information for CRAs, FTC and State AGs (where applicable). [MA prohibits sharing facts/circumstances surrounding breach] (3). Method—Typically postal delivery; email notice possible but additional requirements may apply; "substitute notice" available in limited circumstances	(1). Timing—"Without undue delay" (i.e., ASAP) (2). Content—A description "in clear and plain language" of the nature of the breach and items (2)-(4) of the regulatory notification. (3). Method—not specified (breach should be communicated directly to data subjects, unless doing so would involve disproportionate effect)

Data Breach Notification – Data Controller's Obligations

- Notify the relevant Supervisory Authority (DPA) within 72 hours after having become aware of the breach.
  - Data controllers must notify the competent supervisory authority about personal data breaches unless "the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons." The controller must notify the DPA "without undue delay and, where feasible, not later than 72 hours after having become aware of it."
  - *Recent Proposed Guidance from WP29*:
    - A controller becomes "*aware*" of a data breach when it has a "reasonable degree of certainty that a security incident has occurred that has led to personal data bring compromised." During its initial investigation of the incident, which "should begin as soon as possible," the controller is **not** considered to be "aware."
    - Whether it is immediately clear that personal data was compromised or this conclusion requires some time to reach, however, "the emphasis should be on prompt action to investigate an incident to determine whether personal data have indeed been breached."
    - Once the short period of investigation has passed and the controller has identified the incident, it is considered "aware" and notification to the supervisory authority is then required "if this presents a likely risk to individuals."
  - Narrow risk of harm exception

Data Breach Notification – Data Controller's Obligations

- Notify the relevant Supervisory Authority (continued)
  - Notification should include:
    - The nature of the breach, including, where possible, the categories and approximate number of data subjects and personal data records concerned.
    - The name and contact information of the organization's DPO or other point of contact.
    - The likely consequences of the breach. [*Note*: If the types of data subjects or personal data records concerned indicate a risk of particular damage occurring as a result of the breach (e.g., ID theft, fraud, financial loss), then it is important to note these categories as they me be relevant to this 3rd content-specific requirement.]
    - The measures taken or proposed to be taken to address the breach and mitigate its possible adverse effects

- Notify the affected individual data subjects without undue delay
  - General Rule: Personal data breaches also need to be communicated to individuals if there is a "high risk to the rights and freedoms of natural persons."
  - Limited exceptions to notifying individuals:
    - If controller has used "appropriate technical and organizational protection measures … that render the personal data unintelligible to any person who is not authorized to access it" (e.g., encryption)
    - When the controller has taken immediate steps "to ensure that the high risk posed to individuals' rights and freedoms is no longer likely to materialize

Data Breach Notification – Data Processor's Obligations

- In the event that a processor becomes aware of a data breach, it must notify the controller of such breach without undue delay.

Penalties

- Egregious violations: Up to 4 percent of revenue (or "global annual turnover") or €20 million, which is approximately $23 million.
- Tiered penalties for other violations.
  - For example, a company can be fined 2 percent of its global annual turnover for failing to notify affected individuals in the event of a data security breach.

Compliance Programs

- Data Mapping
- Security Testing
- Review/revise existing policies and procedures
- Process changes
- Compliance with other similar laws, rules, and regulations?

Questions?

- Dominic Paluzzi

  dpaluzzi@mcdonaldhopkins.com
- Christine Czuprynski

  cczuprynski@mcdonaldhopkins.com
- Sam Goldstick

  sgoldstick@mcdonaldhopkins.com
- Cody Wamsley

  cwamsley@mcdonaldhopkins.com