The GDPR:
An introduction

Webinar for the Massachusetts Health Data Consortium, CIO Forum

Andrew Shindler, Partner, London
Tom Smedinghoff, Of Counsel, Chicago
David Szabo, Partner, Boston

24 April 2018

© 2018 Locke Lord LLP

Agenda

- What is the GDPR and why should I care?
- Basic concepts and terminology
- Application of GDPR to MHDC members
- Compliance
- Data Subjects' Rights

What Is GDPR?

- General Data Protection Regulation
- New, comprehensive EU regulation governing privacy of personal data
  - Approved by European Parliament April 27, 2016
  - Effective May 25, 2018
- Automatically applies to all EU countries
- Repeals and replaces the 1995 EU Privacy Directive
- Provides a consistent privacy law across the EU

Why Should I Care?

- You may be subject to GDPR
  - Even as a U.S.–only entity
  - Extra-territorial impact
- The potential fines for violations are huge – i.e., the greater of –
  - 20 Million Euros, or
  - 4% of total gross worldwide revenue
- Establishment of international standards?

Basic Terminology

- **Personal data** - information relating to an identified or identifiable natural person
- **Data subject** – the person to whom the personal data relates
- **Processing** - any operation performed on personal data – e.g. collection, organizing, storing, altering, disclosing, transmitting, using or erasing
- **Controller** - entity which determines the purposes and means of processing
- **Processor** – entity which processes personal data on behalf of a controller
- **Special categories of personal data:**
  - concerning health
  - concerning sex life or sexual orientation
  - genetic or biometric data
  - revealing racial origin.

Who Is Subject to GDPR?

Applicability of GDPR – Article 3

- GDPR applies to organizations in 3 situations

1. Process personal data (anywhere) in context of activities of "*an establishment*" in the EU

2. Process personal data of EU data subjects related to offering them goods or services

3. Process personal data of EU data subjects relating to monitoring their behavior in EU

1. An Establishment in the EU?

- Could be in the form of a legal presence, such a subsidiary

- Or any “effective and real exercise of activity through stable arrangements,” could include
  - one-person office; or
  - a simple agent, if presence sufficiently stable

1. Establishment

- Processing does not need to be ***by*** establishment
- Just *"in the context"* of an establishment
- Will apply where there is an inextricable link between activities of EU establishment and the data controller

2. Offering Goods or Services to EU Data Subjects

- Applies to organisations not established in the EU
- Who process personal data of individuals in the EU when offering goods or services (even where free)
- “Offering” depends on “intention” – mere availability not enough

2. Offering Goods or Services

- Offer itself must be to data subject – an individual
- Won't apply where offer is to business, even if process personal data of individuals at business
- Data subjects only have to be "in" EU – not citizens or residents – visitors included

2. Offering Goods or Services

- Indications of intention on websites:
  - use of EU foreign language;
  - use of EU currency;
  - use of EU top-level domain name;
  - mentions of EU based customers;
  - targeted advertising to consumers in EU.

3. Processing Related to Monitoring Behaviour of EU Individuals

- Monitoring appears to mean "*whether tracked on internet*"
- Includes, but probably doesn't require "*subsequent profiling*"
- Monitoring and tracking not further defined

3. Monitoring

- *Monitoring* – “watching and checking carefully to discover something about “
- *Tracking on the internet* – “following internet activity such as browsing or purchasing”
- *Profiling* – “any form of automated processing to evaluate certain personal aspects”

3. Monitoring

- Again, no need for individual to be EU subject, citizen or resident

- Applies to monitoring of behaviour which takes place within EU – e.g., visitor browsing on internet in hotel room

Compliance Obligations

Scope

- Very broad
- **Personal data**
  - any information relating to identifiable natural person;
  - by reference to name, location data, online identifier or factor(s) specific to physical, physiological, genetic, mental or social identity
- **Processing**
  - any operation, from collection to destruction and everything in between

You Need a "Legal Basis" for Processing Personal Data

- Processing is only lawful if **necessary** for:
  1. complying with an EU legal obligation to which the controller is subject;
  2. protecting the vital interests of the data subject or another;
  3. performing a task carried out in the public interest;
  4. legitimate interests pursued by the controller not overridden by the interests or fundamental rights and freedoms of data subject;
  5. performing a contract to which the data subject is party;

- Or,

6. The data subject has given **consent** to the processing of his/her personal data for a specific purpose

If relying on Consent - not easy to get!

- Must be
  - a freely given, specific, informed, unambiguous indication of wishes
  - by statement or clear affirmative action
  - signifying data subject's agreement to processing their personal data
  - clearly distinguishable from other matters in clear language
- Data subject must be aware of purposes of the processing
- Not freely given if
  - performance of contract dependent on consent that is not necessary
  - given in an employment context
- Revocable at any time

Legitimate Interest of Controller

- Legitimate interests sufficient to justify processing of personal data include –
  - Direct marketing purposes
  - Fraud prevention
  - Internal administrative purposes
  - Ensuring data security
  - Reporting criminal acts
- Must be balanced against the interests and fundamental rights of the data subjects

Higher standards for health and other special category data

- Consent must be “explicit” and subject to any specific law providing that consent is ineffective

- Otherwise, processing must be necessary for:
  - medicine, diagnosis, providing health or social care or treatment or contract with health professional
  - public interest in public health
  - exercising or defending legal claims
  - protecting vital interests of data subject who is physically or mentally incapable of consenting

  or
- Legitimate interest of not-for-profit body for members

Information must be provided to Data Subjects

- Identity and contact details of controller
- Purposes and legal basis of processing
- Recipients of personal data
- Details of any data transfers outside the EU
- Retention period
- Data subject's rights (see next slides)

When?

- at time of obtaining personal data from the subject; or
- within reasonable period – max. 1 month – after obtaining from another or on 1st communication

Data Subject Rights (1) - Access

- Right to access personal data includes --
  - Right to obtain confirmation whether/not their personal data processed
  - Right to obtain a copy of any personal data that is processed
  - Right to obtain the following information:
    - Purposes of the processing
    - Categories of personal data concerned
    - Recipients or categories of recipients
    - Retention period
    - Existence of right to rectification, erasure, restriction of processing or to object to processing,
    - Right to lodge a complaint with the supervisory authority,
    - Information regarding the source of the data,
    - Existence of any automated decision making, including profiling, with logic involved and consequences

Data Subject Rights (2)

- Right to rectification
  - Right to correct data that is wrong
  - Right to have incomplete data completed

- Right to erasure ("right to be forgotten")
  - Right to require controller to delete personal data when there is no longer any lawful basis for processing it
  - Not an absolute right – exceptions for –
    - the exercise of the right of freedom of expression and information
    - compliance with a legal obligation
    - the performance of a task carried out in the public interest or exercise of official authority
    - public health purposes;
    - archival, scientific, research or statistical purposes; or
    - the establishment, exercise or defense of legal claims.

Data Subject Rights (3)

- Right to restrict processing
  - Right to restrict processing is available when --
    - the accuracy of the personal data is contested by the data subject,
    - the processing is unlawful and the data subject opposes the erasure of the personal data and requests restriction of its use instead,
    - the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise, or defense of legal claims, or
    - data subject has objected to the processing pursuant to article 21 pending verification whether the legitimate grounds of the controller override those of the data subject.
  - If the data subject exercises a right to restrict processing, the controller may only process the personal data -
    - With the data subject's consent
    - If necessary to establish, exercise, or defend legal claims, or
    - For the protection of the rights of another data subject

Data Subject Rights (4)

- Right to data portability
  - Right to receive a copy of the personal data concerning him or her which he or she has provided to a controller, in a structured, commonly used, and machine readable format,
  - Right to transmit that data to another controller without hindrance from the first controller.
  - Only applies to personal data an individual has provided to a controller -
    - where the processing is based on the individual's consent or for the performance of a contract, or
    - where the processing is carried out by automated means.

- Right to object to profiling & automated decision making
  - Can insist on human intervention

Responsibilities of Controllers

- Data security
- Implementation of data security by design and default
- Data protection impact assessment
- Requirement of processor contracts
- Maintain records of processing activities
- Notification of breaches
- Appointment of EU representative (non-EU entities)
- Designation of data protection officer

Responsibilities of Controllers:
Duty to provide Security

- Must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk
- Security should include, as appropriate -
  - pseudonymisation and encryption of personal data;
  - ensuring the confidentiality, integrity, availability and resilience of processing systems and services;
  - ability to restore the availability and access to personal data in a timely manner following a physical or technical incident;
  - regular testing, assessing & evaluating of the effectiveness of safeguards for ensuring the security of processing.

Responsibilities of Controllers : Appointment

- Data Protection Officer required if:
  - Public authority; or
  - Core activities consist of :
    - Regular monitoring on large scale
    - Processing special categories of data on large scale

- EU Representative required where subject to GDPR but no EU establishment

Responsibilities of Controllers :
Duty to Maintain Records

- Controllers must keep written records of their processing activities, which contain all of the following information:
  - the contact details of the controller and if applicable its representative and DPO;
  - the purposes of the processing;
  - the categories of data subjects and the categories of personal data processed;
  - categories of recipients with whom the data has been or will be disclosed to;
  - information regarding the transfer of personal data outside of the EU;
  - the data retention period; and
  - a description of the security measures implemented in respect of the processing.

Responsibilities of Controllers:
Contracts with Processors

- Controllers must enter into a data processor agreement with service providers which provides that the processor will:
  - only process personal data on the controller's written instructions,;
  - ensure that authorized persons who access the personal data are bound by confidentiality obligations;
  - implement appropriate technical and organizational measures to safeguard the personal data;
  - may not engage a sub-processor without prior written authorization of the controller;
  - assist the controller in responding to requests by data subjects to exercise their rights;
  - assist the controller in ensuring compliance with data security and data protection impact assessments;
  - delete or return all the personal data to the controller following termination of the services, and
  - make available all information necessary to demonstrate compliance with its obligations under the GDPR, and allow for and contribute to audits

Responsibilities of Controllers:
Duty to Notify of Breaches

- Controller must report a data breach to the supervisory authority not later than 72 hours after having become aware of the data breach

- Where a data breach results in high risk to data subjects, the controller must communicate details of the breach to data subjects “without undue delay”

Responsibilities of Controllers:
Cross Border Transfers

- Cross-border data transfers are prohibited unless the controller or processor takes measures to compensate for the lack of data protection in the third country by
  - providing appropriate safeguards for the data subject, and
  - ensuring that enforceable data subject rights and effective legal remedies for data subjects are available.

- Most commonly used mechanisms are –
  - EU-US Privacy Shield
  - EU Standard Contractual Clauses

Fines and Penalties

- Regulators are allowed to impose fines of up to EUR €20M or 4% of the worldwide gross revenue of an organization (with fines of up to 2% or €10M for lesser infractions).
- GDPR specifies which particular violations are subject to either the 4% or 2% of gross revenue maximums.

Questions?

Andrew Shindler
Partner, London
Andrew.shindler@lockelord.com
+44 (0) 20 7861 9077

Tom Smedinghoff
Of Counsel, Chicago
Tom.smedinghoff@lockelord.com
312-201-2021

David Szabo
Partner, Boston
david.szabo@lockelord.com
617-239-0414

Atlanta | Austin | Boston | Chicago | Cincinnati | Dallas | Hartford | Hong Kong | Houston | London | Los Angeles
Miami | Morristown | New Orleans | New York | Providence | San Francisco | Stamford | Washington DC | West Palm Beach

ATTORNEY ADVERTISING. Locke Lord LLP disclaims all liability whatsoever in relation to any materials or information provided. This presentation is provided solely for educational and informational purposes. It is not intended to constitute legal advice or to create an attorney-client relationship. If you wish to secure legal advice specific to your enterprise and circumstances in connection with any of the topics addressed, we encourage you to engage counsel of your choice. © 2018 Locke Lord LLP