GDPR 101

Michael Kohagen
Bagchi Law, PLLC

Who We Are …

DIY TOOLKIT
DIY assessment, training, customized policies & procedures and much more …

CONSULTING
Professional services to help you with your Compliance needs

MANAGED SERVICES
Managed compliance and security services to focus on your key business outcome.

About Michael

Michael Kohagen

MICHAEL KOHAGEN (ATTORNEY) Prior to joining Bagchi Law, Michael was in-house counsel at a local startup company. Today, Michael handles for the firm's domestic and foreign clients a variety of corporate and commercial matters, such as GDPR compliance, and transactions including venture capital financings and mergers and acquisitions. Bagchi Law: Bagchi Law (www.bagchilaw.com) is a global commercial transactions / contracts boutique law firm that serves as a trusted advisor to management teams across a variety of industries including information technology, manufacturing, and life sciences. We provide unique solutions to complex commercial problems.

What is GDPR?

- GDPR stands for General Data Protection Regulation
- Implemented by the EU Parliament April 14, 2016, effective May 25, 2018
- Designed to harmonize data privacy laws across Europe with respect to how information related to individuals may be collected and used

DISCLAIMER

Consult your attorney

This webinar has been provided for educational and informational purposes only and is not intended and should not be construed to constitute legal advice.

Please consult your attorneys in connection with any fact-specific situation under federal law and the applicable state or local laws that may impose additional obligations on you and your company.

WHY IS GDPR IMPORTANT?

As the world becomes more connected, our personal information is increasingly at risk.

- Every day, 6,152,850 electronic data records are lost or stolen as a result of data breaches, and this number is increasing dramatically as more of our valuable personal information is digitized
- Individuals are increasingly concerned with the security of their information
  - 40% of Americans feel their personal information is less secure than it was 5 years ago
  - Over 73% of American consumers want companies to be transparent about use of personal data
  - 86% of internet users actively try to minimize, anonymize and hide the visibility of their digital footprint

GDPR IS NOT ALONE

GDPR represents the first of many efforts to modernize data privacy and protection laws.

- California Consumer Privacy Act (CCPA)
- New York Cybersecurity Requirements for Financial Services Companies
- People's Republic of China Cybersecurity Law
- Brazilian General Data Protection Law (LGPD)

To What Does GDPR Apply?

GDPR applies to entities which “process” “personal data” related to residents of the European Economic Area.

The concepts of “processing” and “personal data” are key to understanding the impact of GDPR.

WHAT IS "PROCESSING" UNDER GDPR?

Defined in Article 4 of GDPR as "**any operation** or set of operations which is **performed on personal data** or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

WHAT IS "PERSONAL DATA" UNDER GDPR?

Defined in Article 4 of GDPR as "any **information relating to an identified or identifiable natural person** ('data subject'); an identifiable natural 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, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

TO WHOM DOES GDPR APPLY?

Controllers: Article 4 defines "controller" as "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 of personal data**"

Processors: Article 4 defines "processor" as "a natural or legal person, public authority, agency or other body which **processes personal data on behalf of the controller**"

KEY TOPICS

1. Guiding Principals
2. Legal Basis for Processing
3. Data Subject Rights
4. Accountability and Recordkeeping
5. Transfers of Personal Data
6. Contractual Requirements

Guiding Principals (Article 5)

Personal Data must be:

1. Processed lawfully, fairly and in a transparent manner
2. Collected for specified, explicit, legitimate purposes
3. Collected only as necessary, relevant and adequate for the intended purpose
4. Accurate
5. Retained in personally identifiable form only for so long as necessary
6. Held and processed in a secure manner

LAWFUL BASIS FOR PROCESSING

A “lawful basis” is required to process personal data:

- Consent; or
- Processing is necessary for:
  - Performance of a contract
  - Compliance with a legal obligation
  - To protect vital interests
  - Performance of a task benefiting certain public interest
  - The performance of a “legitimate interest”

DATA SUBJECT RIGHTS

- GDPR provides numerous rights to individuals

- If an individual directly requests exercise of such rights, an entity must respond within one (1) month (subject to certain extensions)

- Exercise of data subject rights generally must be provided at no cost to data subjects

KEY DATA SUBJECT RIGHTS

Article	Description of Data Subject Right
15	**Right of Access** Right to obtain a copy of all personal data held by an entity
16	**Right of Rectification** Right to have personal data corrected
17	**Right of Erasure / "Right to be Forgotten"** Can have personal data deleted in certain circumstances (e.g. consent revoked)
18	**Right to Restrict Processing** Right to suspend use of personal data in certain circumstances (e.g. data needs to be verified)
20	**Right to Data Portability** Right to obtain personal data in a structured, commonly used machine-readable format
21	**Right to Object** Right to object to certain direct marketing activities based on use of personal data

ACCOUNTABILITY AND RECORDKEEPING

- Must comply at all times with obligations set forth in GDPR, and be able to demonstrate such compliance
- Must adequately identify and respond to security breaches with respect to personal data, including by providing notice to data subjects or controllers
- Processors must provide certain access to records related to its processing of a controller's personal data (more on this in a minute)

DATA TRANSFERS

- If personal data related to EEA residents is transferred to a "third country", an approved data transfer mechanism must be in place to ensure security of transfer

- In general, two mechanisms are used to ensure safe transfer:

  - Model Clauses: also known as the "standard contractual clauses," the model clauses" constitute standard language approved by the EU Commission for transfer of data

  - EU-US Privacy Shield: a framework designed by the US Department of Commerce and EU Commission for transfer of personal data. Requires self-certification under the privacy shield

CONTRACTUAL REQUIREMENTS

Article 28 Section 3 of GDPR requires processing by a processor to be governed by a contract that sets out:

- the subject-matter of the processing;
- the duration of the processing;
- the nature and purpose of the processing;
- the types of personal data subject to processing;
- the categories of data subjects (whose data is being processed); and
- the rights and obligations of the controller.

CONTRACTUAL REQUIREMENTS (CONT.)

In addition, GDPR requires each such contract to stipulate:

- the processor must act only on the controller's documented instructions unless required by law;
- the processor must ensure that individuals processing the controller's personal data are subject to an appropriate duty of confidence;
- the processor must take appropriate measures to ensure the security of processing;
- the processor may only engage with a sub-processor with the controller's prior authorization and pursuant to a written contract containing appropriate protections;

CONTRACTUAL REQUIREMENTS (CONT.)

- the processor must take appropriate measures to help the controller respond to request from individuals to exercise the rights provided to them under GDPR;
- taking into account the nature of processing and the information available, the processor must assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of personal data breaches and data protection impact assessments;
- the processor must delete or return all personal data to the controller upon the termination of the provision of services relating to processing; and
- the processor must submit to certain audits and inspections.

QUESTIONS?

CONTACT INFORMATION

Michael Kohagen

Email: michael@bagchilaw.com

www.bagchilaw.com

DISCLAIMER

TO ENSURE COMPLIANCE WITH REQUIREMENTS IMPOSED BY THE IRS, WE INFORM YOU THAT ANY U.S. FEDERAL TAX ADVICE CONTAINED IN THIS DOCUMENT IS NOT INTENDED OR WRITTEN TO BE USED, AND CANNOT BE USED, FOR THE PURPOSE OF (I) AVOIDING PENALTIES UNDER THE INTERNAL REVENUE CODE OR (II) PROMOTING, MARKETING OR RECOMMENDING TO ANOTHER PARTY ANY TRANSACTION OR MATTER ADDRESSED WITHIN.

******

Upcoming Events

- How to Comply with California Consumer Privacy Act - 8/15

Register at databrackets.com/webinars

Find Us

CALL US
866-276 8309

SERVICE
info@databrackets.com

LOCATION
150, Cornerstone Dr.
Cary, NC

SOCIALIZE
Facebook
Twitter

Twitter: https://twitter.com/databrackets **Facebook:** https://www.facebook.com/databrackets/ **Instagram:** https://www.instagram.com/databrackets1/

Bagchi LAW

ENTREPRENEURSHIP ~ GLOBALIZATION ~ INNOVATION