EU General Data Protection Regulation

Presented March 8, 2018

Sarah Sargent
414-298-8338
ssargent@reinhartlaw.com

Derek Campbell
414-298-8374
dcampbell@reinhartlaw.com

Reinhart Boerner Van Deuren s.c.
1000 North Water Street, Suite 1700, Milwaukee, WI 53202
www.reinhartlaw.com

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Agenda

- GDPR Basics
- Who GDPR Applies to
- What Does Compliance Require
- U.S. Privacy Shield
- How to Create a Compliance Program
- Practical Tips & Resources

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

GDPR Enforcement in 77 Days

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

What is the GDPR?

- Protects Personal Data
- Requires Informed Consent From Data Subjects
- Potentially Heavy Penalties for Non-Compliance

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

What is Personal Data?

- "Any Information Relating to an Identified or Identifiable Natural Person"

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

What is Processing?

- Any Operation Performed on Personal Data
- Activity on Social Network Sites (SNS) May Be Exempted
- Includes Automated Operations

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

The GDPR Proudly Introduces:

- Extra-territorial Applicability
- Specific Suggestions for Data Security
- Data Breach Handling
- Consent
- Required Notification of Rights

Fines

- Two Tiers:
  - Greater of:
    - 4% of Annual Revenue
    - €20,000,000
  - Greater of:
    - 2% of Annual Revenue
    - €10,000,000

Who Does GDPR Apply to?

Article 3: Territorial scope

"applies to the processing of personal data of data subjects who are in the Union by a controller or processor **not** established in the Union . . . ."

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Who Does GDPR Apply to?

Established in the EU	Offering Goods or Services to people in the EU	Monitoring of data subjects in the EU
• HR company located in Germany • Data hosting service provider located in Ireland • Company with a distribution center in Italy	• U.S. online retail store sells and ships to customers in the EU with a website that offers payment in euros	• U.S. company with a website that places cookies on and tracks the IP addresses of EU-based website visitors • U.S. based company that traces emails to customers in the EU

Three Questions to Ask:

1. Establishment test: is the business activity in the EU?
2. Goods and services test: is the company offering goods and services to people in the EU?
3. Monitoring test: is the company tracking and profiling people in the EU?

Hypothetical:

EU resident visits a store in Boston, gives personal data, and returns to the EU

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

What DOES GDPR REQUIRE?

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Guiding Principles

- Lawfulness, Fairness and Transparency
- Accuracy
- Purpose Limitation
- Data Minimization
- Storage Limitation
- Integrity and Confidentiality

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Consent to Collect

- Must be "informed and unambiguous"
- Easily Withdrawn
- Must be Specific
- Explicit Consent for Special Categories of Personal Data

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Data Subject Rights

- Right of Access
- Right of Rectification
- Right of Erasure
- Right of Data Portability
- Right of Restricted Processing
- Right to Lodge a Complaint

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Updating Your Privacy Policy

- Must be "Concise, Transparent, and Intelligible"

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Updating Your Privacy Policy (cont.)

- Identity and Contact Details About the Controller
- Purpose of the Processing
- Basis of the Processing
- Any Recipient(s) of the Data, Where Applicable
- Where Applicable, If Data Will Be Transferred to a Third Country
- Time Period the Data Will Be Stored
- Rights of Access, Rectification, Erasure, Portability
- Right to Withdraw Consent, Where Applicable
- Right to Lodge a Complaint
- The Existence of Automated Decision-making, Such as Profiling With Consequences

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Delegation of Responsibilities

- Controller Must Ensure Compliance
- Controller Answers to Supervisory Authority; Processor to the Controller
- Controllers Liable for Processing "which infringes" the GDPR

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Data Protection Officer

- May be Required for Large Scale Monitoring
- Obligated to Implement Data Protection Measures "by design and default"
- Prepare Impact Assessments
- Direct Reporting to Management
- Third-Party Service Provider

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Impact Assessment

- Describe Processing
- Assess Likelihood and Severity of High Risk for Processing
- Identify Safeguards and Mitigation Mechanisms

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Direct Marketing Requirements

- Covers Communications Directed to Particular Individuals or Companies
- Must Still Provide Opt-Out Mechanism
- Update Privacy Policy
- eCommunications Must Comply with Europe's e-Privacy Directive

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Data Breach Requirements

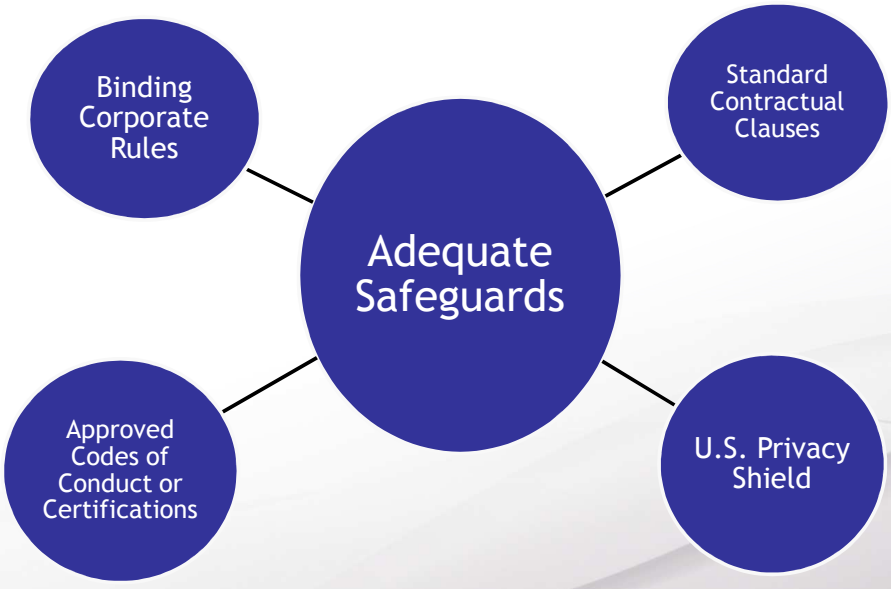
- Broadly Defined
- Notification to Supervisory Authority
- Requirements of SA Notification
- Data Subject Notification?

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Cross Border Data Transfers

- Can Only Transfer Data To An Entity In A Non-member Country If:
  - Adequacy Determination by the Commission
  - Derogations (Explicit Consent)
  - Ensure Adequate Safeguards

Reinhart
Boerner Van Deuren s.c. Attorneys at Law



Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Privacy Shield

- Must Self-certify Annually to the Department of Commerce
- Agree to Adhere to the Privacy Shield Principles
- Commitment Is Enforceable By the FTC or the DOT

Privacy Shield Principles

- Notice
- Choice
- Accountability for Onward Transfer
- Access
- Security
- Data Integrity and Purpose Limitation
- Recourse, Enforcement, and Liability

Privacy Shield Process

- Develop a Compliant Privacy Policy
- Identify Process for Handling Complaints
- Pay Required Fees
- Identify Self-verification Process
- Designate a Contact
- Submit Self-certification

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Implementing Compliance

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Assemble the Team

- C-Suite
- IT/CISO
- Procurement
- HR
- Marketing/Sales
- R&D

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Fact Gathering

- Data Flows
- Privacy Notices
- Vendor Agreements
- Information Security Polices
- Response Plans

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Conduct a Gap Analysis

- Compare Where You Are Now to Where You Need to Be
- Create a Project Plan With Concrete Steps Towards Compliance
- Assign Tasks to Specific Team Members
- Prioritize Time and Resources to the Most Urgent Areas

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Example of GDPR Project Plan

Action	Compliance Requirement	Deliverable	Team Member	Timing
1. Privacy Policy	Add required disclosures, including the rights of data subjects and purpose of data collection	Revised Privacy Policy	Legal IT	May 1, 2018

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Example: Privacy Policy

What Information We Collect and How We Use It

We collect personally identifiable information that you choose to provide to us when you register for a [redacted], subscribe to our [redacted] (either directly or through another company such as a [redacted]), sign up for email newsletters, enter a sweepstakes or contest, participate in surveys, or otherwise submit through our website. During the registration process we may request certain contact information and demographic information about you such as your name, mailing address, email address, company name, size of company and title. We also may receive information about you from other sources and add it to the information you have provided to us. If you choose to register for a [redacted] on this website, you may also be asked to provide your credit card information to fulfill your registration request.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Example: Privacy Policy

HOW WE USE THE INFORMATION WE COLLECT

When we collect information from you, we may use it for a number of purposes, including to:

- Review and process your application for the position you posted for and if applicable, shared for other job opportunities
- Respond to your comments and inquiries
- Comply with your request for current investor information
- Perform a review of eligibility for program funding from the [redacted]
- Helps us understand website activity and improve your use of our website
- Helps us prevent unauthorized activity, claims and other liabilities
- Measure and manage the advertising effectiveness of our job postings and events
- Comply with and enforce applicable legal requirements, industry standards and our policies and our Terms of Use
- Operate, evaluate and improve our talent acquisition process (including managing our communication and administering our website)

In addition, we use information collected online through automated means for purposes such as (i) customizing our users' visits to our websites or experience in a mobile app; (ii) delivering content (including advertising) tailored to our users' interests and the manner in which our users browse or interact with us; (iii) measuring and managing the advertising effectiveness of our online and offline advertisements and events; and (iv) managing our business. We also use this information to help diagnose technical and service problems, administer our websites and mobile apps, identify users of our websites and mobile apps, and gather demographic information about our users. We use clickstream data to determine how much time users spend on web pages of our websites or our mobile apps, how users navigate through our websites and mobile apps, and how we may tailor our offerings to better meet the needs of our users. In order for us to maintain the accuracy of your personal information and improve our communication with you, we may also supplement the information we collect with other public demographic information.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Going Forward

- Cross-Department Cooperation
- Consolidate and Audit Personal Data
- Personnel Training
- Review Data Service Vendor Contracts
- Document Your Compliance Efforts

Resources

- Privacy Shield
  - https://www.privacyshield.gov/welcome
  - https://www.export.gov/article?id=How-to-Join-Privacy-Shield-part-1
  - https://www.ftc.gov/news-events/blogs/business-blog/2017/09/ftc-cases-affirm-commitment-privacy-shield

Resources (cont.)

- GDPR
  - http://ec.europa.eu/newsroom/article29/news.cfm?searchfield=GDPR#
  - https://www.eugdpr.org/more-resources.html
  - https://www.export.gov/article?id=EU-NEW-DATA-PRIVACY-LEGISLATION-GDPR

Questions?

Thank you

ssargent@reinhartlaw.com
dcampbell@reinhartlaw.com