The EU General Data Protection Regulation (GDPR): The Time to Act is Now

December 4, 2017

Speakers

Robert Cattanach, Ron Moscona and Jamie Nafziger, Dorsey & Whitney LLP

Materials

Program PowerPoint

About Dorsey's Cybersecurity, Privacy & Social Media Group

Dorsey eUpdate: *Proposal for New European ePrivacy Regulation*, Ron Moscona, (February 28, 2017)
Available on Dorsey.com: https://www.dorsey.com/newsresources/publications/client-alerts/2017/02/proposal-for-new-european

Dorsey eUpdate: *The 2016 EU Data Protection Legislatio*n, Ron Moscona (July 20, 2016)
Available on Dorsey.com: https://www.dorsey.com/newsresources/publications/client-alerts/2016/07/2016-eu-data-protection-legislation

Dorsey eUpdate: *U.S. Companies Face Increasing Privacy Challenges in Europe*, Bob Cattanach (April 14, 2016)
Available on Dorsey.com: https://www.dorsey.com/newsresources/publications/client-alerts/2016/04/increasing-europe-privacy-challenges-us-companies

Dorsey eUpdate: *EU-U.S. Data Transfer Privacy Shield: Political Agreement Achieved Regarding "Safe Harbor 2.0"*, Barry Glazer, Ron Moscona & Chris Koa (February 4, 2016)
Available on Dorsey.com: https://www.dorsey.com/newsresources/publications/client-alerts/2016/02/political-agreement-reached-for-safe-harbor-2

DORSEY
always ahead

THE EU GENERAL DATA PROTECTION REGULATION: COMPLACENCY IS NO LONGER AN OPTION

Ron Moscona – Partner, Dorsey & Whitney

Bob Cattanach – Partner, Dorsey & Whitney

Jamie Nafziger – Chair, Cybersecurity, Privacy and Social Media Practice Group, Dorsey & Whitney

1

Overarching Considerations

- **Big data is now big business – but carries with it big risks**
- **Data increasingly viewed as the holy grail of assets – but also liabilities**
- **Compliance considerations**
  - **Eliminate the data = eliminate the risk**
  - **Often not a practical business solution – focus is on mitigating the risk**
    - **Data security**
    - **Policies and Procedures**
  - **Opting out is not really an option; how well prepared are your systems, policies and agreements?**

Obligation to Protect Personal Data Privacy is Not Limited to "SECRET" Information

- GDPR protects ***all*** ***data*** that relates to a living ***individual***
- It does ***not*** need to be ***confidential*** or ***secret***
- Data made publicly available or voluntarily submitted by the individual is still protected
- Focus should be on individuals' reasonable expectations of privacy

Overview

- Scope: which companies are subject to GDPR
- Compliance fundamentals:
  - Operational and process changes likely will be required
  - Policies must reflect GDPR requirements
  - Contractual changes

Other Key Features of GDPR

- Enhanced focus on data security
- ePrivacy Regulation: significantly changes ecommerce (coming soon)
- Data transfer: crossing EU borders
- Data breach preparedness: new requirements

Scope: Broad Territorial Reach

Presence in EU

- Controller in member State
- Processor in member State

Presence outside of EU

- Processing involving data subjects in EU by controller/processor outside EU
- Offering goods or services to EU data subjects
- Monitoring EU data subjects' behavior

Your Company is Subject to GDPR, Now What?

- **Operational and process changes may be needed:**
- **Policies revised:**
- **Potential revision of third party contracts**

Enhanced Regulatory Enforcement Powers

Audit and investigate

- **Access all personal data of controller/processor**
- **Access premises/computer systems of controller/processor**

Issue compliance orders

- **Ban on processing**
- **Rectification/erasure**
- **Stop data flows outside the EU**
- **Withdraw compliance certifications**

Administrative penalties: up to 4% of annual revenue or EUR 20 million (whichever is higher)

Fundamentals: Compliance

- What data can my organization collect; process; keep?
- Lawful basis for processing and identifying legitimate purposes
- Obtaining consent from individuals
  - When required
  - Is it truly valid?
- Protecting the data
  - Cloud storage – can you legally transfer the risk?
  - Vendor commitments?
  - Who gets access to the data in theory? How confident are you in practice?
  - Third party data analytics may be the elephant herd in the room

Fundamentals: Compliance

- Privacy policy statement
  - When required
  - Ensuring content complies
  - Notification on repurposing
- Do you need to appoint a data protection officer?
- Do you need to appoint an EU representative?
- Transferring data outside the EU
  - Model clauses/binding corporate rules
  - EU-US privacy shield

Fundamentals: Compliance

- Privacy due diligence
- Comprehensive review of internal policies and procedures
- Ability to demonstrate compliance
- Third party vendors with access to your data may be an enormous, yet unquantified, risk

High Risk: Triggers for Data Protection Impact Assessment

- "Likely to result in a high risk to the rights and freedoms of natural persons"
- Primary focus on data protection and privacy
- Other fundamental rights
  - Freedom of speech
  - Freedom of thought
  - Freedom of movement

High Risk: Examples of "Likely High Risk"

- Automated processing or profiling
- Large scale processing (big data)
- Systematic monitoring of public areas
- Public availability may not matter

Source: Article 29 Working Party

High Risk: Sensitive Data – Use Only Under Strict Conditions

- Health data and patient records
- Trade union membership
- Sexual orientation or sex life
- Political data
- Racial/Ethnic origin
- Religious/philosophical beliefs
- Genetic data and biometric (ID) data
- Criminal convictions and offences

Need not be confidential

Rights: Duties to Data Subjects

- Notifications to subjects
- Must have a legal basis to collect or process
- Limit activity to the justified basis

Rights: Data Subjects

- Know how data is being used
- Ability to change/update
  - Right to be forgotten (erasure/data cleansing)
- Third party notifications
- Right to data portability
- Right to object (opt-out)
  - Profiling
  - Direct marketing
  - Automated decision making
  - Harmful processing

Consent

- Other legal basis to justify processing data
- Consent must be free, specific, informed and unambiguous
- By statement or affirmative action
- Consent may ***not*** be folded into terms and conditions
- Consent cannot be given as part of a privacy policy
- Obtaining consent for processing of sensitive data
- Obtaining consent from employees
- Data contributed/posted by data subject

Information Governance and Data Security

- Articulated basis for collecting and disseminating personal data
- Established internal responsibilities and authorizations
- IT security and anonymization
- Ensuring appropriate data security implementation by service providers
- Data maintenance and cleansing policy
- Established procedures for responding to data subject requests

Required Documentation for Compliance

- Consent forms
- Data processing agreements
- Data exporting agreements
- Joint controller agreements
- Privacy policy statements

Operational Requirements – Data Protection By Design

- Analyze data flows
- Process consents and opt-outs
- Access control and authorization
- Encryption/data security
- Anonymisation/pseudonymisation
- Repurposing – notification to data subjects/consent
- Data tracking (3rd party notifications)

GDPR's Data Security Obligation: Appropriate technical and organizational measures to ensure level of security appropriate to risk posed to personal data

- Policies and procedures
- Access control
- Records
- Training
- Audits
- Penetration testing

Marketing Poses Special Challenges: the ePrivacy Regulation

- Unsolicited marketing communications – spamming
- Direct marketing by email, fax, phone, text, social media…
- Do not send me this again
- Cookies and tracking devices
- Recast ePrivacy legislation proposal
  - Communications content and metadata:
    - Not just consent
    - Necessity
    - Consent cannot be condition to access service
  - Personalized/targeted advertising
  - Browser software requirements

Engagement with EU Regulators

- Appointment of compliance officer (DPO)
- EU representative
- Data processing impact assessments
- When do regulators need to be engaged?
  - Dialogue regarding compliance obligations
  - Potential initial step in breach response triage

Children

- Parental / guardian consent required for valid consent by a child under 16
- Member states can set a lower age limit (UK < 13)
- Normal rules of contractual capacity apply

Data Transfer: Exporting Data Outside EU

- Privacy shield/certifications
- Model contractual clauses
- Binding corporate rules
- Data subject consent
- Notification requirement

Data Breach Preparedness

- Incident Response Plan (IRP)
- Incident Response Team (IRT)
- Table top exercises

Personal Data Breach Notification Under the GDPR

- **Basic security considerations**
- **What is a personal data breach?**
  - **Definition**
  - **Types of personal data breaches**
  - **The possible consequences of a personal data breach**

Obligation to Notify the Supervisory Authority

- **When to Notify**
  - **Article 33 requirements**
  - **When does a controller become "aware"?**
  - **Processor obligations**

Providing Information to Supervisory Authority

- Information to be provided
- Notification in phases
- Delayed notifications
- Breaches affecting individuals in more than one member state
- Conditions where notification is not required

Communication to Data Subject

- Article 34: Informing individuals
- Information to be provided
- Contacting individuals
- Conditions where notification is not required

Other Key Aspects of Responding to a Breach

- Assessing the risk
  - Will help determine whether notifications are required
  - Factors to consider when assessing risk
- Accountability and record keeping
  - Documenting the breach and the response
- Role of the Data Protection Officer

Other Jurisdictions to Keep in Mind

- Canada (much like EU)
- China (interpretation still being provided)
- Russia
- Brazil (very comprehensive)

The EU is ***not*** automatically the highest common denominator default

Questions?

DORSEY™
always ahead

Dorsey's Cybersecurity, Privacy & Social Media Capabilities

Cybersecurity and social media touch virtually every aspect of commerce and modern culture. Dorsey's Cybersecurity, Privacy and Social Media practice reflects the multi-dimensional nature of this subject area by integrating over a dozen of our specialty areas under a single unified group.

International in scope, our Cybersecurity, Privacy and Social Media group encompasses not only the core areas of cybersecurity, data protection and breach, social media, and intellectual property, but also sector-specific expertise. Our clients range from Fortune 100 public companies to private companies in a range of industries and across jurisdictions including the U.S. and the European Union (EU). Six Dorsey attorneys are Certified Information Privacy Professionals. One of our partners serves on the CIPP/US Exam Development Board of the International Association of Privacy Professionals, another Co-chairs the IAPP's Minneapolis KnowledgeNet, and one of our partners recently served for four years on the Web 2.0 Working Group of the International Trademark Association's Internet Committee. Several Dorsey attorneys write and speak nationally and internationally in the cybersecurity and social media areas.

Experience

Written Information Security / Data Privacy Program

The first step requires the evaluation of the core components of the company's data structure in order to ensure that the written program complies with the laws and regulations of relevant jurisdictions:

1. The type of data held by the company
2. Where the data comes from (countries, states, etc.)
3. How and where is the data being stored
4. How the data flows among jurisdictions

The next step is to define the data privacy and security policy and objectives of the program. Is the program solely for compliance purposes, or are there broader privacy goals that the company wants to achieve?

We help our clients develop the proper team to guide the development of the privacy and security program. Team members should include each critical component of the enterprise: legal, IT, corporate compliance, information security, human resources, finance, risk management, customer relations, and those other business units specific to a company's core functions.

In collaboration with that team, we help design the program to encompass both the front-end policies and procedures intended to keep data secure, as well as the response protocols for responding to a breach or cybersecurity incident.

Policies, Procedures, and Governance Structure

Once the risks are identified, the responsible team is in place, and the proper policies and procedures have been drafted and approved by top management, and now increasingly the Board of Directors itself, they are implemented through more granular steps we help our clients develop, including access, notice, retention, assignment of specific responsibilities, and ongoing monitoring and verification.

Contractual Provisions

Another increasingly important aspect of proper Cybersecurity management requires the development of appropriate contractual provisions with customers and third party vendors and overall risk management responsibilities demonstrated through recent breaches, third party contractors can pose a serious privacy/cybersecurity vulnerability.

Data Incident and Breach Investigation and Response

Dorsey provided analysis of, and assisted clients with investigating and managing the response to, data incidents involving both computerized and non-computerized data. This included (i) disclosing data breaches under state data breach notification laws and the federal HIPAA / HITECH and Gramm-Leach-Bliley Acts to affected persons, state attorneys general, regulators, credit reporting agencies and others, (ii) working with law enforcement and government authorities and (iii) analyzing disclosure obligations under federal securities laws for public companies. Dorsey also advised on data incidents that extended beyond U.S. borders in collaboration with our established network of foreign counsel.

Incident Response Plan

The first step in an effective response to a data breach is a well-developed and practiced incident response plan. Dorsey works collaboratively with each of our clients to establish a breach-response team and develop a plan suited to its business operations, and then conducts regular training exercises to ensure that the team members are prepared to respond immediately and efficiently to a breach.

Communication and Staffing

Experience has proven that a successful breach response requires clear and prompt communication. Customers, consumers, and employees understand that, notwithstanding the best of protections, breaches can occur whether by inadvertence or calculated attack. The speed of our client's reaction and the accuracy of the information conveyed establish credibility and help protect reputation and brand.

To ensure that our clients have immediate access to critical resources in the event of a breach, Dorsey has crafted Master Service Agreements with key vendors which are ready to respond at a moment's notice to any potential breach by providing firsthand response capabilities and/or supporting our client's in-house resources. Dorsey has developed close working relationships with forensic experts, call centers, public relations breach specialists, and identity theft/credit monitoring agencies that can be brought online with a single call when a breach is discovered.

The Importance of Planning and Rehearsing

An incident response plan should reflect the unique risks and available internal resources of each individual client. Regular table-top exercises not only ensure that contact information is current for each breach team member and backup, but that breach responses are routinely practiced and refined. These regular breach exercises significantly enhance the comfort level and efficiency of the team when an actual event occurs, and provide invaluable preparation to deal with the unexpected.

The nature and severity of a breach can vary widely, but the following questions are always key:

- What data was accessed?
- What jurisdictions are potentially affected?
- What are the notification requirements for each of those jurisdictions?

Dorsey has created a live process for immediate access to all of the breach reporting requirements for each state jurisdiction (as well as individual federal sectors), which we update constantly through automatically-generated notifications for each individual jurisdiction.

Notifications to customers and consumers, law enforcement authorities, affected vendors and suppliers, state Attorneys General, the Federal Trade Commission, the media, investors, business partners, as well as potential insurance carriers, are tailored to meet the demands of each individual breach. We provide seasoned counsel to our clients to keep the larger picture in context. For example, even in jurisdictions not requiring it, notifications may be appropriate depending on the facts and circumstances of the particular breach.

Within this context of transparency, the right to protect critical information must be preserved. Dorsey can ensure that appropriate attorney-client privileges cover key communications, and preserve the candor required for interim internal reports to the executive and technical teams.

After the Breach

The "fog of breach" invariably will put the breach response team to tests that could not have been fully anticipated. We carefully document each step in the breach response process to enable meaningful after-action reviews, and where appropriate, improvements in the incident protocols.

Litigation

Dorsey has successfully assisted a financial services company in various matters, obtaining temporary restraining orders and then permanent injunctions against former financial advisors to secure the return of confidential client information.

Compliance

Dorsey has assessed numerous companies' compliance with U.S. and international privacy laws, and prepared and reviewed comprehensive privacy programs to include website privacy, social media, mobile app policies, and record retention policies. We regularly counsel clients on how best to meet the requirements of these far-reaching privacy obligations of various jurisdictions, especially the EU. Dorsey drafted a complex set of website terms of use for a website active in 21 countries with significant user-generated content issues.

Transactions

Dorsey conducts privacy due diligence and drafts agreement provisions in cross-border mergers and acquisitions. Dorsey's international and U.S. offices collaborate on acquisition agreement provisions regarding compliance with international and U.S. requirements.

Dorsey's Track Record

We have years of experience assisting our clients in developing appropriate cybersecurity programs, responding to data breaches, and dealing with social media in all industries and jurisdictions. That experience gives us the perspective necessary to assist each client with the unique challenges of their industry, customer base, and regulatory frameworks.

Representative Matters

Data Breach Investigation and Response

- Dorsey recently was approached by a number of California wineries who had been notified by a common vendor that their customer information may have been hacked. We put together a team overnight to provide breach notifications to customers of over 30 wineries for 48 different jurisdictions and to dozens of state Attorneys General within 24 hours of being retained. While the Krebs blog had a head start on us, by the time it "broke the story," customers had already been notified, and the media ignored the event.
- Dorsey developed immediate response measures for a large agricultural cooperative whose sensitive payroll information of high-level executives had been compromised as well as emergency communication procedures. Within an hour of the incident we assessed the potential scope of disclosure, possible methods for retrieval to minimize potential dissemination of material, and assessed reporting obligations.
- Our cybersecurity team assisted a health care provider with a data breach response involving unauthorized disclosure of PHI by an employee. Our team assessed potential notification requirements, retrieved data from various devices used by the former employee and her family, and developed creative alternatives to address emerging issues not covered by regulatory guidelines.
- Members of Dorsey's data protection team represented a health care organization in an Office of Civil Rights investigation of potential HIPAA violations following a data breach involving over 38,000 individuals.
- Dorsey represented a human capital management company in a class action lawsuit arising from a third-party hacker. Plaintiffs alleged that because the hacker accessed their personal information, they faced an increased risk of identity theft, and were forced to pay for credit monitoring and identify theft protection. A New Jersey trial court granted Dorsey's motion to dismiss on the grounds that Plaintiffs lacked standing to sue absent alleged actual misuse of their personal information or actual identity theft. The Third Circuit affirmed.

Proactive Prevention

- A Fortune 500 multi-national corporation turned to Dorsey to assess its privacy and data protect policies and procedures, and completely update them. Our attorneys worked with a multi-dimensional in-house team to determine data collection, flow, retention and destruction; access protocols; EU-data transfers; certification requirements; and ongoing compliance monitoring.
- A Dorsey cybersecurity team analyzed potential privacy and data protection issues associated with a risk management solutions company's potential acquisition of a mobile app authentication service.
- Dorsey counsels a nationwide retailer on the constantly evolving best practices for structuring communications to customers of its pharmacy operations.
- Dorsey's privacy group drafted a complex set of website terms for use in 21 countries, with significant user-generated content issues, using its knowledge of international privacy laws to provide insight and practical advocacy.
- Our team assisted a Fortune 100 insurance company in drafting and implementing an internal social networking policy.

- Dorsey regularly advises clients with European online presence on how they can benefit from immunity from liability in relation to user-generated content under the eCommerce Directive and on the pit-falls presented by the Privacy in Electronic Communications legislation in relation to matters, such as the use of cookies in websites and the challenges of targeted advertising.
- We have deep experience in registering both generic and country code domain names for clients and in counseling clients on managing their domain name portfolios to deter cybersquatters.

Compliance

- A Native American gaming organization turned to Dorsey for assistance in developing assessment mechanisms to ensure compliance with guidelines and regulations for data and privacy protection and reporting. This project included assessment of applicability of state breach laws to a sovereign tribe, potential waiver consequences associated with voluntary compliance and mechanisms for ongoing assessment and improvement of policies and procedures.
- Dorsey served as general counsel to a public-private Health Information Exchange formed to facilitate the exchange of health information electronically in compliance with HIPAA/HITECH.
- Working with app developers, our privacy compliance professionals have counseled on designing apps in compliance with the FTC's endorsement guidelines.
- Dorsey has extensive experience with counseling clients on complying with and drafting policies concerning the Digital Millennium Copyright Act, the CAN-SPAM Act, the Communications Decency Act, the Children's Online Privacy Protection Act, online behavioral advertising principles, and other internet-related laws.
- Dorsey has helped numerous app developers design online advertising platforms and draft user rules in compliance with the FTC's endorsement guidelines.
- Our Financial Services privacy lawyers develop and audit internal privacy procedures to address both Gramm-Leach-Bliley Act compliance and customer expectations for their personal financial information.
- Dorsey Financial Services privacy practitioners also assist in dealing with subpoenas and other legal processes served on clients that trigger Gramm-Leach-Bliley issues.
- When two of its former financial advisors refused to return confidential client information, a financial services company hired our cybersecurity litigators to represent it in two different state court actions implicating the Gramm-Leach-Bliley Act. In both matters, the courts granted motions for a temporary restraining order preventing a former financial advisor from using or further disclosing the confidential information. FINRA (Financial Industry Regulatory Authority) arbitration panels subsequently approved the company's requests for a permanent injunction requiring the former advisor to, among other things, return the information.

Cybersecurity, Privacy & Social Media – Key Contacts

Jamie N. Nafziger
Partner, Chair
Minneapolis
(612) 343-7922
nafziger.jamie@dorsey.com

Robert E. Cattanach
Partner
Minneapolis
(612) 340-2873
cattanach@dorsey.com

Ron Moscona
Partner
London
+44 (0)20 7031 3742
moscona.ron@dorsey.com