Update on EU Data Protection Law
&
U.S. Perspectives on Data-Related Contracts (and Privacy Policies)

Laura De Boel & Jon Adams

Privacy and Data Protection Group

TTG Attorney Meeting

March 10, 2016

Wilson Sonsini Goodrich & Rosati, LLP

Agenda

- New General Data Protection Regulation (“GDPR”).
  - New requirements and increased enforcement.
- Invalidation of “Safe Harbor” and the introduction of the “EU-U.S. Privacy Shield”*.*
- EU Model Contracts.
- Questions.

Current EU Data Protection Legal Framework

- Main piece of EU data protection legislation: Data Protection Directive 95/46/EC:
  - No direct effect; requires national implementation.
  - Minimum framework; no full harmonization.
  - Interpretation by Article 29 Working Party (WP29), body comprised of national regulators, European Data Protection Supervisor (EDPS) (EU regulator), and EU Commission representative.
- National laws:
  - 28 national data protection laws; country-specific requirements.
  - Interpretation by national Data Protection Authorities (DPAs) and courts.
  - Stricter jurisdictions: e.g., Germany, France.
  - More flexible jurisdictions: e.g., UK, Ireland.

Current EU Data Protection Legal Framework Key Concepts

- Controller:
  - The entity that, alone or jointly with others, determines the purposes and means of the data processing.
  - Fully responsible for data protection compliance.
  - “Jointly with others”: co-controller (allocation of responsibilities).
- Processor:
  - The entity that processes personal data on behalf of and under the instructions of the controller (under data protection agreement / clauses).
  - Responsible for (minimum):
    - complying with the controller’s instructions (contract); and
    - implementing appropriate security measures.

GDPR: Introduction

- New EU General Data Protection Regulation (GDPR):
  - Direct effect; does not require national implementation.
  - Will replace the Data Protection Directive.
- Timing:
  - Proposed in January 2012; political agreement in December 2015.
  - Expected to be adopted by Spring / Summer 2016, and to become effective by Spring / Summer 2018 (two years after adoption).
- Key issues:

Scope of application	Internal documentation
Concept of personal data	High sanctions
Consent	Data transfers

GDPR: Scope of Application

- Current framework. EU Data Protection Directive applies to data processing activities of:
  - EU-based companies; and
  - Non-EU-based companies that use ‘equipment’ in the EU (interpreted broadly).
- Future framework. GDPR will apply to data processing activities of:
  - EU-based companies; and
  - Non-EU-based companies offering goods / services (no payment required) or monitoring the behavior of individuals in the EU (targeted approach).
    - E.g.: online profiling, websites targeting EU consumers.
    - Non-EU controllers and processors must appoint representative in EU.

⇨ Assume that EU data protection law will apply as soon as company collects and uses personal data of individuals in EU.

GDPR: Concept of Personal Data

- Any information relating to an identified or identifiable individual (directly / indirectly):
  - Any information that can be “linked back” to an individual by anyone and by any means.
  - Bottom line: as soon as individual can be singled out, information qualifies as personal data.
- GDPR: Presumption that online identifiers (e.g., IP address, unique device ID, cookie identifiers) are personal data.
- Pending case before the Court of Justice of the European Union (CJEU) on whether IP addresses are personal data when stored by service provider.

➪ More difficult to argue that no personal data are processed.

GDPR: Consent

- One of the legal grounds for data processing (main other grounds are: legitimate interest, performance of contract, legal obligation).
- Freely given, specific, informed, unambiguous indication of will that can be revoked at any time:
  - Explicit (e.g., check box) or implicit (e.g., “By using the service, you agree…” followed by an action e.g., “submit” button).
- GDPR specifies requirements for valid consent:
  - No pre-ticked boxes and no consent “hidden” in Privacy Policy or T&Cs.
- GDPR introduces conditions for processing of children’s data in relation to ‘information society services’ (e.g., websites):
  - Need parental consent for children under 16;
  - Member States law may set lower age limit, but not below 13.

⇨ Review existing consent practices and forms (including when children’s data are collected).

⇨ Document how consent is obtained + rationale for relying on one legal ground over another (burden of proof is on the controller).

GDPR: Internal Documentation

- Current requirement: controllers must file registration with national DPA (subject to exceptions).
- GDPR reduces red tape by repealing registrations, but requires to keep internal records (e.g., data inventories) that must be communicated to the DPA upon request.
- Appointment of Data Protection Officer (DPO) mandatory when core activities of company consist of very sensitive data processing.

⇨ Shift from filing registrations with DPAs to keeping internal records of data processing activities.

GDPR: Other Issues

- New general EU-wide data breach notification obligation:
  - Notification to DPA and, if high risk breach, to individuals.
  - Processor must notify controller.
- New notice requirements: additional information to be included in Privacy Policies.
- New requirements for data processing agreements:
  - Currently, only a few national laws prescribe specific content for data processing agreements / clauses (e.g., Germany).
  - GDPR will provide minimum content (e.g., processor must obtain prior written consent of controller for subprocessing).

GDPR: High Fines

- Currently: important differences in enforcement between EU Member States.
- GDPR harmonizes data protection enforcement in the EU, but divergences will remain due to cultural differences.
- Under GDPR, DPAs can impose high fines. Two levels of fines:
  - up to EUR 10 million or 2% of the undertaking’s global annual turnover, whichever is higher, for certain infringements; and
  - up to EUR 20 million or 4% of the undertaking’s global annual turnover, whichever is higher, for more severe infringements.
- Other DPA powers include audits, order to change data processing activities, suspension of data transfers.
- Reputational risks; loss of business.

⇨ Much more enforcement is expected.

GDPR: International Data Transfers

- “Data transfer” means the disclosure of personal data to a third party, including retrieval or access to the data (e.g., virtual access).
- International data transfer restrictions remain broadly the same under GDPR.
- Data transfers outside of the EU are prohibited unless:
  - Recipient country provides “adequate protection’’ that is “essentially equivalent” (list of EU Commission adequacy decisions);
  - Companies have implemented a data transfer mechanism
    - EU Model Contracts (Controller-to-Controller or Controller-to-Processor);
    - Binding Corporate Rules (BCRs); or
  - Companies can rely on a statutory derogation:
    - Main derogation: consent. However, consent is not suitable for structural data transfers, rather one-time solution if no other option. When used, consent must be specific to the data transfer.
- EU-U.S. Safe Harbor no longer “adequate”.

Safe Harbor / Privacy Shield: Background (1)

- June 2013: Complaint by Max Schrems with Irish DPA:
  - Facebook Ireland Ltd. transfers personal data to Facebook, Inc. in the U.S. under Safe Harbor.
  - Alleged access to EU Facebook users' data by NSA.
- Irish DPA refuses to investigate:
  - Bound by the EU Commission's adequacy decision on Safe Harbor.
- Appeal to the Irish High Court: Preliminary questions to the CJEU.
- **October 6, 2015: CJEU delivers its judgment in *Schrems* (C-362/14):**
  - **invalidates EU Commission's decision on Safe Harbor; and**
  - **confirms the power of DPAs to investigate data transfers.**

Safe Harbor / Privacy Shield: Background (2)

Schrems Judgment:

- Even if data transfers are based on EU Commission's adequacy decision, DPAs can still investigate and suspend data transfers.
- EU Commission's adequacy decision on Safe Harbor did not meet criteria required by EU fundamental rights to privacy and data protection:
  - Safe Harbor did not provide protection that is *essentially equivalent* to protection provided by EU fundamental rights.
  - National security exception in Safe Harbor was too broad, no effective legal protection for EU individuals.
    - NSA surveillance demonstrates flaws of Safe Harbor.
  - Conditions under which DPAs could suspend data transfers were too restrictive in Safe Harbor.

Safe Harbor / Privacy Shield: Background (3)

- The CJEU decision applied immediately – no grace period.
- Reaction of WP29: Statement of October 16, 2015:
  - Post-*Schrems* data transfers under Safe Harbor are unlawful.
  - DPAs can investigate data transfers (e.g., complaints).
  - WP29 will analyze EU Model Contracts and BCRs in light of *Schrems* judgment, but these data transfer mechanisms can still be used.
  - If no solution with the U.S. by end of January 2016, coordinated enforcement actions could take place.

Safe Harbor / Privacy Shield: Current Status (1)

- Many companies rushed to put EU Model Contracts in place before January 31, 2016.
- Large multinational companies are implementing BCRs.
- Legal uncertainty: still no guidance from WP29 on validity of EU Model Contracts and BCRs.
- Which mechanism to use depends on:
  - company’s business;
  - corporate structure;
  - whether it is active in the B2B or B2C sector;
  - its visibility; and
  - the type of data processing activities.
- EU Model Contracts are not always feasible.
- Key is to enable businesses to transfer data.

Safe Harbor / Privacy Shield: Current Status (2)

- February 2, 2016: Political agreement on “EU-U.S. Privacy Shield”.
- February 29, 2016: Documents were published:
  - Same principles as Safe Harbor, but stricter obligations for companies (e.g., tightened conditions for onward transfers).
  - New redress mechanisms:
    - Individuals can complain: (i) directly to companies, which will have 45 days to resolve the complaint; or (ii) directly to EU DPAs, which will cooperate with U.S. DOC and FTC (EU DPAs’ advice is binding in HR context).
    - Individuals have access to Alternative Dispute Resolution mechanism selected by company (free or charge for individuals).
    - Last resort and under certain conditions: individuals can seek redress from Privacy Shield Panel (binding arbitration).
  - Limitations on U.S. government data access: ombudsperson will handle complaints.
  - Annual joint review mechanism.
- WP29 will review Privacy Shield documents in light of *Schrems* judgment (statement expected in April).

Safe Harbor / Privacy Shield: What’s Next?

- Privacy Shield is not a valid data transfer mechanism yet:
  - Formal approval by EU Commission will take at least a few months.
- Focus on alternative data transfer mechanisms (e.g., EU Model Contracts):
  - EU companies (in particular in Germany, Austria) may not trust Privacy Shield and may require additional data transfer mechanism.
  - As soon as Privacy Shield is adopted, privacy activists may introduce complaints and DPAs may decide to block data transfers.
- Verify if Privacy Policy needs to be updated in light of invalidation of Safe Harbor.

EU Model Contracts: Key Issues (1)

- Standard contractual clauses that are prepared by EU Commission:
  - Lose pre-approved value if changes are made.
  - Companies only need to complete annexes (with information on the data transfers).
  - Controller-to-Controller (C2C) data transfers (2 versions) and Controller-to-Processor (C2P) data transfers (1 version).
- Compliance with data transfer restrictions is responsibility of EU controller:
  - Some EU DPAs require filing the Model Contract (e.g., Belgium) or obtaining prior authorization (e.g., Austria).
- Two approaches for service providers:
  - Reactive: have completed C2P Model Contract ready when EU customers inquire about compliance with data transfer laws.
  - Proactive: add C2P Model Contract as an appendix to customer agreement (e.g., MSA).

EU Model Contracts: Key Issues (2)

- Key obligations:
  - Audit rights for data exporters (for both contracts) and DPAs (only for C2P).
  - Onward transfers in general and sub-processing in the C2P are very strictly regulated.
  - Obligation to notify data exporter of certain events (e.g., law enforcement request, data breach, individuals' access requests, legislation that conflicts with EU Model Contract), depending on type of contract.
  - Data importers must accept that individuals have third-party beneficiary rights under the EU Model Contract:
    - EU Model Contracts are designed so that individuals can enforce the clauses against the data exporter but also against the data importer (and the sub-processor for their own violations) if the data exporter or data importer has ceased to exist (and there is no successor).

Questions?

Thanks!

Laura De Boel

Associate

ldeboel@wsgr.com

WSGR Regulation Observatory:
www.wsgr.com/EUDataRegulation

Perspectives on Data-Related Contracts (and Privacy Policies)

Agenda

- Model Contracts (the U.S. perspective)
- Business Associate Agreements
- Data Security Addenda
- Privacy Policies

Model Contracts – The U.S. Perspective

- Square pegs, round holes
  - Some scenarios are tough to shoehorn into C2C or C2P model contracts
  - Recent example: U.S. entity, global websites, EU order fulfillment company with U.S. back-end processor. How to comply?
- Form vs. Function
  - Keep in mind third party beneficiaries (data subjects)
- Risk based analysis
- EU constructs as a way towards improved data practices

Business Associate Agreements

- Basics:
  - Covered Entity: health care provider, health plan, health care clearinghouses, hospitals, certain affiliates, etc.
  - Business Associates: a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. (45 CFR 160.103)
  - Business associate functions and activities include: claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing.
- The Privacy Rule requires that a covered entity obtain satisfactory assurances from its business associate that the business associate will appropriately safeguard the protected health information it receives or creates on behalf of the covered entity.

Business Associate Agreements (cont.)

- What needs to be there:
  - Use Cases. Establish the permitted/required uses and disclosures of PHI by the business associate.
  - Non-disclosure. The BAA may not authorize the BA to use or further disclose the PHI in a manner that would violate the Privacy Rule if done by the covered entity, except that the BAA may:
    - Permit the BA to use and disclose PHI for the proper management and administration of the business associate.
    - Permit the BA to provide data aggregation services relating to the health care operations of the covered entity.
    - Permit the BA to disclose PHI for the foregoing purposes if (1) the disclosure is required by law, or (2) the BA obtains reasonable assurances of confidentially and compliance.

Business Associate Agreements (cont.)

- Other required clauses:
  - More Non-Disclosure:
    - The BA will not use or further disclose the PHI other than as permitted or required by the BAA or as required by law
    - The BA will employ appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by the BAA
  - Security. The BA will, where applicable, comply with Security Rules with respect to electronic PHI
  - Security Breaches. The BA will report to the covered entity any security incidents or use or disclosure of PHI not provided for by the BAA of which it becomes aware, including breaches of unsecured PHI as required by 45 CFR § 164.410

Business Associate Agreements (cont.)

- Other required clauses:
  - Subcontractors. The BA will ensure that any subcontractors that receive, maintain or transmit PHI on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such PHI. Business associates may do so by requiring the subcontractors to execute a BAA with the business associate
  - Access. The BA will make available PHI consistent with the patient's right to access PHI as set forth in 45 CFR § 164.524
  - Amendment of PHI. The BA will make available PHI for amendment and incorporate any amendments to PHI in accordance with 45 CFR § 164.526

Business Associate Agreements (cont.)

- Other required clauses:
  - Information Availability. The BA will make available the information required to provide an accounting of disclosures in accordance with 45 CFR § 164.528, including required information concerning disclosures of PHI in violation of the Privacy Rule.
  - Compliance. The BA will comply with the HIPAA Privacy Rule (if acting as a stand-in for the covered entity)
  - Books & Records. The BA will make its internal practices, books and records relating to the use and disclosure of PHI received from, or created or received by the business associate on behalf of, the covered entity available to HHS for purposes of determining the covered entity's compliance with the Privacy Rule.

Business Associate Agreements (cont.)

- Termination provisions:
  - At termination of the BAA, if feasible, the BA must return or destroy all PHI received from, or created or received by the BA on behalf of, the covered entity that the BA still maintains in any form and retain no copies of such PHI.
    - If such return or destruction of PHI is not feasible, extend the protections of the BAA to the PHI and limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible.
    - Authorize termination of the BAA by the covered entity if the covered entity determines that the BA has violated a material term of the BAA

Business Associate Agreements (cont.)

- Room for maneuvering and helping clients:

Pro Covered Entity	Pro Business Associate
Insurance?	Restrict insurance
Ind. Contractor, not Agent	Restrictions on other covered entity contracts
Security Breach Requirements	Termination if ability to perform is compromised
Broader Termination Rights	Recover costs for additional requirements
Amendment Rights	Prohibition on *contra* HIPAA requests
Indemnification	Damage limitations

Data Security Addenda/Exhibits

- What information is covered?
  - PII, Sensitive PII, “confidential” information, etc.
  - Can divide or combine categories to tailor security requirements
- Compliance with Laws
  - Specific vs. General
  - Industry standards
- Authorized employees
- Secure coding
- Incident response
  - Notification obligations
  - Liability
  - Who manages response?

Data Security Addenda/Exhibits

- Injunctive Relief
- Audit Rights
  - Prior audit
  - Ongoing audit authorization
- Indemnification / Remedies
- Flowdown to service providers, subcontractors
- Catch-all to allow remediation of identified/major issues
  - Compliance with future supplemental guidance/requirements can be mandated
  - Step-in rights for managing new/major issues
- Confidentiality, Survival

Data Security Addenda/Exhibits

- Safeguards
  - Information Technology, Organizational, Physical Safeguards

    Specific Items:
    - Standards (ISO, NIST, etc.) adherence
    - Policy requirements
      - What to require in policy? What's the scope?
    - Personnel limitations
    - Access controls (physical and technical, e.g., MFA, VPN, etc.)
    - Training
    - Facility controls
    - Audit trails
    - Network, workstation configurations
    - Data storage (encryption), disposal, backup, etc.
    - Location requirements (all in U.S., never in EU, only in EU, etc.)
    - System monitoring

Data Security Addenda/Exhibits

- Case-Specific Issues:
  - Regulated industry considerations (incorporate BAA, add GLBA NPI restrictions, etc.)
  - Interface with end users/consumers (as intermediary)
  - Communications Requirements
    - Limitations on who vendor contacts and how
    - Requirements for inclusion in communications
    - Monitoring of communications
  - Access and authorizations to vendor systems or to third party systems

Privacy Policy Refresher

- What needs to be covered:
  - Data Collection
  - Data Use
  - Data Disclosures
  - Consumer Choices
  - Special Data Categories (Children, Location, etc.)
  - Information Security
  - International Data Transfers
  - Policies Regarding Privacy Policy Changes
- Why?
  - Laws (e.g., California Online Privacy Protection Act)
  - Regulated Industry/Contract Requirements
  - Consumer Expectations

Privacy Policy Refresher (cont.)

- Other factors to consider:
  - Contractual requirements
    - Google Analytics, MixPanel, Flurry
  - Industry norms
    - AdChoices, etc.
  - Who is reading the document?
    - Audience (e.g., U.S. vs. EU), Regulators, etc.
- Common issues:
  - Insufficient detail
  - Inaccurate or stale information
  - Display issues
  - Bungled material changes
- Governing philosophy: Say what you do, do what you say.

Questions?

Jon Adams

Associate

jadams@wsgr.com

THE **WSGR** DATA ADVISOR

Unique Insights on Privacy and Data Protection Worldwide

www.wsgrdataadvisor.com