WSGR Getting Ready for the GDPR Series

Session 4:
The GDPR, Privacy Shield, and EU-U.S. Data Transfers – What to Do Now?

Cédric Burton
Of Counsel

Christopher Kuner
Senior Privacy Counsel

WSGR Webcast, Brussels, September 13, 2016

Wilson Sonsini Goodrich & Rosati, LLP

Agenda

- Introduction.
- Part I: Data Transfer Rules under the GDPR.
- Part II: The EU-U.S. Privacy Shield.
- Questions & Answers.

Current data transfer rules

- Prohibition of data transfers outside the EEA to “non-adequate” countries:
  - EU Commission considers only a few countries as “adequate”:

Andorra	Israel
Argentina	Jersey
Canada (for organizations subjected to PIPED Act)	New Zealand
Guernsey	Switzerland
The Isle of Man	Uruguay
Faroe Islands	~~EU- U.S. Safe Harbor~~ EU-U.S. Privacy Shield

- Instruments to provide adequate protection:
  - EU Commission’s Standard Contractual Clauses;
  - “Ad hoc” data transfer agreements;
  - Binding Corporate Rules (BCRs).
- Limited derogations (e.g., consent):
  - Strict interpretation by DPAs.

High level of legal uncertainty since *Schrems*

- June 2013: Following Snowden revelations, Max Schrems files complaint with Irish DPA regarding Facebook's data transfers under Safe Harbor.
- November 2013:
  - 13 recommendations by EU Commission to improve Safe Harbor.
  - Beginning of EU–U.S. negotiations.
- October 2015: EU Court of Justice declares EU Commission's adequacy decision regarding Safe Harbor invalid (*Schrems,* C-362/14)*:*
  - High threshold for adequacy decisions and possibly impact on other data transfer mechanisms.
  - Ability of each EU DPA to suspend data transfers under adequacy decisions.
  - Over 4,000 U.S. companies had to implement an alternative data transfer mechanism.
- July 2016: EU Commission adopts adequacy decision regarding new EU-U.S. Privacy Shield:
  - Since August 1, U.S. companies can sign up for Privacy Shield.
  - Risk of legal challenges by EU DPAs and privacy activists.
- Current case regarding validity of Standard Contractual Clauses before courts in Ireland.

Part I:

Data Transfer Rules under the GDPR

What's new under the GDPR?

- EU General Data Protection Regulation (GDPR) 2016/679, adopted on April 27, 2016; enforceable as of May 25, 2018.
- The GDPR maintains the current core principles for data transfers, but introduces some novelties.
  - A new set of criteria for EU Commission to assess whether the level of data protection in a third country is adequate.
  - BCRs are specifically included in the GDPR.
  - New data transfer mechanisms: approved codes of conduct and approved certification mechanism together with binding commitments.
  - New derogation of a limited scope: compelling interests of the controller.
  - New obligations for processors.
- Certain administrative burdens are reduced (e.g., no authorization required for EU Commission and DPA Standard Contractual Clauses).
- New administrative burdens are introduced (internal documentation; obligation to include information about data transfers in privacy notice).
- High sanctions for non-compliance with data transfer rules: up to 20 million EUR or 4 percent of worldwide turnover.

Data transfers under the GDPR

- Adequacy decisions adopted by EU Commission.
- In the absence of an adequacy decision, appropriate safeguards:
  - BCRs.
  - Standard Contractual Clauses.
  - Approved codes of conduct and certification mechanisms with binding commitments.
  - “Ad hoc” contractual clauses authorized by DPAs.
- In the absence of an adequacy decision or appropriate safeguards, derogations, e.g.:
  - Consent.
  - Performance of a contract.
  - Public interest.
  - Legitimate interests of a controller (with limitations).
- No “sunset” clause!

Adequacy

- EU Commission may decide that a third country ensures an adequate level of protection:
  - Also possible for a territory, sector or international organization.
- Criteria for adequacy:
  - Adequacy = “essentially equivalent” level of protection.
  - Includes requirements of *Schrems* judgment.
- Obligation for EU Commission to monitor functioning of adequacy decisions:
  - Periodic review at least every four years.
  - EU Commission may repeal, amend or suspend adequacy decisions.
- Possibility to limit transfers of specific categories of data to third countries or international organizations “for important reasons of public interest”:
  - In the absence of an adequacy decision.
  - National laws implementing this restriction must be notified to EU Commission.
  - Risk of fragmentation.

Data transfer instruments

- GDPR provides the following data transfer instruments for companies:
  - BCRs:
    - Explicit recognition.
    - Available also for companies that are not part of the same corporate group but are engaged in a joint economic activity.
    - List of minimum requirements included in GDPR.
  - EU Commission's Standard Contractual Clauses:
    - Do not require DPA authorization.
  - DPA's Standard Contractual Clauses (SCCs) approved by EU Commission.
  - "Ad hoc" contractual clauses, if authorized by the DPA.
  - Approved codes of conduct and certification mechanisms together with binding and enforceable commitments.
- Consistency mechanism for DPA SCCs, DPA "ad hoc" clauses and BCRs: DPA must consult EU Data Protection Board.

Derogations

- GDPR maintains current derogations, but some of them become more restrictive:
  - Consent:
    - Must be explicit (in addition to being freely given, specific and informed).
    - Obligation to inform individuals of possible risks of data transfers due to the absence of an adequacy decision and appropriate safeguards.
  - Reasons of public interest: must be recognized in EU or Member State law.
- New derogation: Compelling legitimate interests of the controller:
  - Limited scope: Only for non-repetitive data transfers concerning limited number of individuals, not overriding their interests, rights and freedoms, following assessment and implementation of suitable safeguards.
  - Additional obligations:
    - Inform DPA and individuals of the data transfer.
    - Document assessment and safeguards in internal records.

Conflict of laws

- Transfers or disclosures not authorized by EU law:
  - Data disclosure request by court / tribunal / administrative authority of third country.
  - Only recognized or enforceable if based on an international agreement (e.g., MLAT) between third country and EU / Member State.
  - Without prejudice to other grounds for transfers pursuant to Chapter V.
  - Practical implications for companies?

Increased notice obligations regarding data transfers

- New obligation: Controllers to inform individuals about:
  - The intention to transfer personal data.
  - The existence or absence of (where appropriate):
    - an adequacy decision;
    - appropriate safeguards; or
    - controller's compelling legitimate interests.
  - How to obtain a copy of suitable safeguards or where they have been made available to individuals.

Part II:

Where do we stand?

- February: EU Commission publishes draft EU-U.S. Privacy Shield.
- April: WP29 calls for improvements.
- July 12: EU Commission adopts the amended Privacy Shield.
- July 26: WP29 states that it will actively participate in annual joint reviews and will assist individuals with their complaints.
- August 1:
  - U.S. companies can self-certify to the Privacy Shield at www.privacyshield.gov.
  - EU Commission publishes Citizens' Guide to explain individuals' rights and the redress mechanism.
- As of today, the Privacy Shield list includes 170 companies, and hundreds of others are in the process of certifying.
- End of September: companies that certify by then will benefit from a grace period to fully comply with the onward transfers principle.

Overview (1)

- The Privacy Shield replaces the invalidated U.S.-EU Safe Harbor.
- Complex set of documents: adequacy decision and its 7 annexes:
  - DoC letter;
  - The Privacy Shield Principles and Supplemental Principles along with the Arbitral Model;
  - Letter from Secretary of State, along with description of Ombudsperson mechanism;
  - FTC and DoT letters describing their enforcement powers;
  - Letter from the ODNI re: safeguards and limitations in the context of national security; and
  - Letter from the DoJ re: safeguards and limitations on U.S. Government access for law enforcement.

Overview (2)

- Voluntary self-certification mechanism, which needs to be renewed on a yearly basis.
- Companies must publicly disclose their commitments to comply with the Privacy Shield.
- DoC maintains a list of certified companies and a list of formerly certified companies (together with reasons for removal).
- Subject to enforcement powers of FTC (or DoT).
- Built on the skeleton of Safe Harbor (Principles and FAQs), but:
  - Introduces new definitions;
  - Substantially tightens certain core restrictions;
  - Creates new recourse mechanisms; and
  - Regulates access by U.S. public authorities to EU personal data.

The Privacy Shield Principles

7 Principles:

1. Notice
2. Choice
3. Accountability for Onward Transfers
4. Security
5. Data Integrity and Purpose Limitation
6. Access
7. Recourse, Enforcement and Liability

Complemented by 16 Supplemental Principles:

1. Sensitive data
2. Journalistic Exceptions
3. Secondary Liability
4. Performing Due Diligence and Conducting Audits
5. The Role of Data Protection Authorities
6. Self-Certification
7. Verification
8. Access
9. HR Data
10. Obligatory Contracts for Onward Transfers
11. Dispute Resolution and Enforcement
12. Choice – Timing of Opt-Out
13. Travel Information
14. Pharmaceutical and Medical Products
15. Public Record and Publicly Available Information
16. Access Requests by Public Authorities

1. Notice

- Elements to include in privacy policies:
  - Participation in the Privacy Shield and link to the Privacy Shield list;
  - Types of personal data collected and purposes of the data collection and use;
  - Affiliates and subsidiaries adhering to the Privacy Shield;
  - Commitment to subject all personal data received from the EU in reliance on the Privacy Shield;
  - Contact details for inquiries and complaints, including any EU establishment that can respond to complaints;
  - Categories or identity of data recipients and purposes of data disclosures;
  - Individuals' right of access and individuals' choices;
  - independent dispute resolution body (and whether it is the EU DPAs Panel; ADR in the EU or U.S);
  - Confirmation of the jurisdiction of the FTC / DoT;
  - Possibility for individuals to invoke binding arbitration;
  - Requirement to disclose personal data to lawful public authorities' requests, including for national security and law enforcement requirements; and
  - Liability in case of onward transfers to third parties.
- Triggers need for lengthier and more detailed privacy policies.
- One privacy policy v. two policies?

2. Choice

- The Safe Harbor Choice Principle is broadly maintained, but modified:
  - Opt-out via a clear, conspicuous and readily available mechanism in 2 situations:
    - Data are disclosed to a third party acting as a controller.
    - Data are to be used for a purpose that is materially different from the purpose of collection.
  - Opt-out is not required when data are disclosed to agents (processors).
  - Affirmative express consent (opt-in) is required for sensitive data.
  - Opt-out from marketing communications.
- EU Commission's Guide to the Privacy Shield:
  - Use for incompatible purpose is not permitted.
  - Choice Principle applies to use for a new purpose that is different but related to the original one (i.e., materially different).
- Triggers need for internal policies / procedures that ensure individuals are provided with opt-out mechanisms.

3. Accountability for onward transfer (1)

- Much more prescriptive and detailed rules on onward transfers:
  - To a third party controller:
    - Comply with Notice and Choice Principles (i.e., provide notice & opt-out); and
    - Conclude agreement requiring the third party controller to:
      - Process data for limited and specific purposes consistent with the purpose of collection;
      - Protect the data with the same level of protection as provided by the Privacy Shield Principles; and
      - Notify the Privacy Shield company if it cannot meet the latter obligation, and stop processing or take steps to remediate.
    - However, the third party controller does not need to be Privacy Shield-certified and to have an independent recourse mechanism, provided that a similar mechanism is available.
    - For data transfers within the same corporate group, possibility to rely on other data transfer mechanisms (such as BCRs, Intra-Group Agreement) instead of the above agreement.

3. Accountability for onward transfer (2)

- To a third party agent (processor): Written contract.
  - Only transfer data for limited and specified purposes.
  - Ascertain that the agent is obligated to provide at least the same level of protection.
  - Require the agent to notify when it cannot meet the latter obligation.
  - Ensure the agent uses data in a manner consistent with companies' obligations under the Principles.
  - Upon notice, take steps to stop and remediate unauthorized processing.
  - Upon request, provide a copy/summary of data processor agreement to DoC.
  - Companies are liable for non-compliance by agent, unless they prove that they are not responsible for event giving rise to damage.

- EU law requires data processing agreement with processor independently of the Privacy Shield.
- Relationship between Privacy Shield requirements and SCCs requirements for sub-processing?
- Triggers need to review contracts with third parties (both controllers and agents).
- This can be a massive task, but there is a 9 month grace period to review contractual arrangements if companies certify **before end of September**.

4. Security

- Higher threshold for security measures.
- Companies must take reasonable and appropriate measures (instead of “precautions”) to protect data from loss, misuse and unauthorized access, disclosure, alteration and destruction; and take into due account the risks involved in the processing and the nature of the personal data.
- Closer to security requirements of current EU Data Protection Directive.
- Triggers need to review data security policies / procedures.

5. Data integrity and purpose limitation

- Broadly similar to Safe Harbor, but adds the concepts of purpose limitation and data retention.
- Data integrity: data must be reliable for its intended use, accurate, complete and current.
- Purpose limitation:
  - Obligation to limit the data to what is relevant for the purpose of processing.
  - Three steps assessment:
    - Incompatible purpose: prohibited unless specific authorization is obtained (i.e., new processing).
    - Materially different purpose: opt-out.
    - Linked and compatible purpose.
- Data retention: information may be retained in an identifiable form only as long as it serves the purpose of the collection.
- A company must protect the data in accordance with the Principles for as long as it retains the data.
- Triggers need for internal data handling and data retention policies / procedures.

6. Access

- Similar but more detailed principle; the right of access is generally stronger.
- Individuals must have access to personal data and be able to correct, amend, or delete it when it is inaccurate, or when it has been processed in violation of the Principles.
- Close to EU data protection law:
  - Confirmation of whether or not the organization is processing personal data, including information on the categories of data, purpose of processing and categories of recipients.
  - Communicate the data so that individuals can verify its accuracy and lawfulness.
  - Have data corrected, amended or deleted where it is inaccurate, outdated, or processed in violation of the Principles.

Modalities	Exceptions
Obligation to make good faith efforts to comply with individuals' access requests.	Burden or expense of providing access would be disproportionate.
Timeframe (reasonable time period).	Confidential commercial information.
Format (in a reasonable manner, and in a form that is readily intelligible to the individual).	Violation of third parties' rights.
Individuals do not have to justify requests for access to the company (unless request too broad or vague).	Breach of a legal or other professional obligation; prejudicing employee security investigations.
Possibility to charge fees (not excessive).	Confidentiality requirements.
Any denial of, or limitation to the right of access has to be necessary and duly justified.	Conflict with legal obligations.

7. Recourse, enforcement and liability

1. Verification mechanism: self-assessment or outside compliance review.
   - Content is specified (conformity of the privacy policy, information re: the complaint handling procedure, training and disciplinary sanctions, periodical objective reviews, signed by a corporate officer).
   - Outside compliance can be auditing, random reviews, use of “decoys” or technology tools.
   - Obligation to maintain records on the implementation of Privacy Shield privacy practices.
2. Independent recourse mechanism:
   - 3 ways to satisfy the requirements: (i) private sector privacy programs with effective enforcement mechanism; (ii) compliance with legal or regulatory supervisory authorities; or (iii) commitment to cooperate with EU DPAs.
   - Must be readily available, at no cost for the individuals, and expeditiously resolved.
   - Selected by the company prior to self-certifying.
   - Remedies: non-compliance is reversed, compliance of future processing and stop the violation.
     - Including publicity for findings of non-compliance, deletion of data, compensation for individuals.
   - Failure to comply with ruling of dispute resolution body must be notified to the DoC and the FTC / DoT / Courts.
   - Organizations and their independent recourse mechanism must respond promptly to DoC requests and to complaints referred by EU DPAs via the DoC.
   - Privacy notice must include information about independent dispute resolution body.
3. Obligation to remedy problems arising out of non-compliance.

Complaints handling: overview

- Complex complaint handling system composed of different layers:

1. Individuals are encouraged to first complain directly to companies (readily available, free of charge, 45 days to respond to the complaint); or directly to EU DPAs, which will cooperate with DoC and FTC (EU DPAs' advice is binding in HR context).

2. Individuals have access to independent recourse body selected by the company.

3. Backed-up by commitments from the DoC and the FTC.

   - DoC: *Ex officio* reviews, contact person for EU DPAs and process for EU DPAs to refer complaints.

   - FTC: Commitments to give priority consideration to referrals of non-compliance (from dispute resolution bodies, self-regulatory bodies, DoC, EU DPAs).

4. In certain situations and for residual claims, seek redress from the Privacy Shield Panel:

   - Binding arbitration.

   - Only for determining whether Privacy Shield company has violated its obligations, and whether any such violation remains fully or partially unremedied.

   - Possibility to impose "individual-specific, non-monetary equitable relief" (e.g., deletion of the data).

   - Possibility to seek judicial review and enforcement of the decisions pursuant to the U.S. Federal Arbitration Act.

5. If persistent failure to comply: the company will lose the benefits of the Privacy Shield, and be removed from the Privacy Shield List.

Monitoring, annual joint review and suspension

- EU Commission has obligations to monitor the Privacy Shield:
  - Periodic factual & legal checks.
  - Continuous monitoring of the overall functioning of the Privacy Shield, and compliance by U.S. authorities with their representations and commitments.
- The EU and the U.S. will conduct an annual joint review:
  - Covering the functioning of all aspects of the Privacy Shield, including national security, and involving all relevant stakeholders (e.g., U.S. national intelligence experts, EU DPAs, NGOs through the participation at a public conference).
  - Taking into account the U.S. government commitments and the transparency reports published by companies.
  - The result will be presented to EU Parliament and Council of the EU.
- If the U.S. does not fulfill its commitments, the Privacy Shield may be suspended by EU Commission.
- Next review: likely mid-2017.
- Will the Privacy Shield survive legal challenges?
- Will the Privacy Shield survive the GDPR?

Processing for national security purposes

- Notice obligation.
- Written assurances from the U.S. that access of public authorities will be subject to clear limitations, safeguards and oversight mechanisms:
  - ODNI letter describes “the operation of U.S. Intelligence Community signals intelligence collection activity”:
    - Collection, retention and dissemination are limited; compliance and oversight mechanisms are in place.
    - U.S. authorities affirm absence of “mass and indiscriminate” surveillance.
  - DoJ letter provides an overview of tools used to obtain commercial data from companies in the U.S.
- Companies will be able to report approximate number of government access requests (supplemental principle).
- U.S. committed to establishing a redress possibility in the area of national intelligence for Europeans through an Ombudsperson mechanism:
  - Created within the Department of State;
  - Independent from national security services; and
  - In charge of following-up individuals’ complaints and informing them whether the relevant laws have been complied with.
- These written commitments were also published in the U.S. Federal Register on August 2, 2016.

What to do now?

- Assess which data transfer mechanism(s) is (are) the most suitable for your business.
- Many companies follow a belt-and-suspenders approach (SCCs, BCRs, Privacy Shield).
- The Privacy Shield is a workable data transfer mechanism!
- Pros:
  - The Privacy Shield is a better fit to certain companies' data flows (e.g., B2C data transfers).
  - Many tech companies will certify to the Privacy Shield or have already done so.
  - Certifying to the Privacy Shield provides a greater opportunity to handle complaints under customary rules.
- Cons:
  - Possible additional compliance obligations.
  - Likely legal challenge in the EU, but same is true for the SCCs, which are currently being challenged by Schrems before courts in Ireland (a challenge would take time; the political context around the Privacy Shield is different).
  - May suffer lack of trust from certain EU business customers.

A few tips for certifying to the Privacy Shield

- Review your privacy policy.
  - Make sure to include all required information.
  - Use the policy as a tool to assess compliance with the 7 principles and the 16 supplemental principles.
  - DoC reviews privacy policies before listing companies on www.privacyshield.gov/list.
- Select ADR (i.e., U.S. / EU ADR, or EU DPAs). Register with the ADR as applicable.
- Prepare / update inward facing policies, procedures and processes to comply with Privacy Shield requirements.
- Review contract language with customer and sub-processor.
  - Keep in mind than certification by end of September gives you extra 9 months to get your existing contracts for onward transfers in compliance with Privacy Shield.
- Prepare certification form, complete it online and certify.
- Focus on verification principle and document compliance.
  - Prepare for stronger enforcement than under Safe Harbor.
- Be up-to-date with developments related to Privacy Shield as it may change in one year.

Outlook

- The GDPR will impact data transfers and the Privacy Shield.
- Data transfer restrictions will apply to both controller and processor and non-compliance will be sanctioned with important fines.
- The Privacy Shield is a new tool for data transfers as of August 1, 2016.
- Legal uncertainty around international data transfers remains:
  - WP29 statement of July 2016 on Privacy Shield: Certain concerns remain.
    - Follow first annual joint review. If WP29's concerns regarding mass and indiscriminate data collection are not addressed by then, this could affect other mechanisms.
    - Focus on complaints from individuals and enforcement.
  - Restoring trust of EU customers will take time!
  - Will the Privacy Shield be amended every year and survive the GDPR?
  - Risk of legal challenges before DPAs / courts; DPAs can suspend data transfers at any time.
  - Current court case in Ireland regarding SCCs.
- High level of legal uncertainty advocates in favor of a belt-and-suspenders approach to data transfers.
- Keep monitoring the developments!

Questions?

Thank you!

Cédric Burton

Of Counsel

cburton@wsgr.com

Christopher Kuner

Senior Privacy Counsel

ckuner@wsgr.com

Twitter: @EUDataPrivacy

GDPR Observatory:
www.wsgr.com/eudataregulation/

WSGR Resources

- WSGR Data Advisor: www.wsgrdataadvisor.com
- WSGR EU Data Protection Observatory: www.wsgr.com/EUDataRegulation
- Articles:
  - C. Burton, S. Cadiot, L. De Boel, S. Hoffman, "Article 29 Working Party Issues Statement Following Adoption of EU-U.S. Privacy Shield", WSGR Alert, July 26, 2016
  - C. Burton, S. Cadiot, L. De Boel, S. Hoffman, "The EU-U.S. Privacy Shield Is Adopted and Available as of August 1, 2016", WSGR Alert, July 12, 2016
  - C. Kuner, C. Burton, S. Cadiot, S. Hoffman, L. De Boel, "Uncertainty Increases Around EU-U.S. Data Flows", WSGR Alert, May 26, 2016
  - C. Kuner, C. Burton, L. De Boel, S. Hoffman, S. Cadiot, "New EU Data Protection Regulation Is Now Enacted", WSGR Alert, April 14, 2016
  - C. Kuner, C. Burton, L. De Boel, S. Cadiot, S. Hoffman, "EU Commission Publishes EU-U.S. Privacy Shield," WSGR Alert, February 29, 2016