Complying with the EU General Data Protection Regulation (GDPR): Cross Border Transfers of Information
Complying With The EU GDPR

Bryan Cave Leighton Paisner Data Privacy and Security Team

bclplaw.com
Overview: GDPR

Module 1. Information Notices / Privacy Policies
Module 2. Conducting Data Inventories
Module 3. Data Subject Requests
Module 4. Incident Response Plans
Module 5. Third Party Vendor Management Programs
Module 6. Cross Border Transfers
Overview
Overview: Historical background
The General Data Protection Regulation (EU) 2016/679

- Replaces the EU Data Protection Directive.
- Enters into force on May 2016,
- Applies beginning May 2018,
- Directly applicable in all EU Member States,
- Aims to unify data protection law within the European Union and increases data subject’s rights,
- Still authorizes individual EU Member States to implement more specific rules in certain areas.
The Countdown

Time Until the EU GDPR comes into force

164:19:01:50

until May 25th 2018
Overview: GDPR 10 Top Talked About Provisions

1. **Penalties.** Under Directive functionally non-existent; under Directive up to 4% of revenue.
2. **Floor not ceiling.** Member states can enact additional safeguards in certain areas, including research.
3. **Extraterritorial.** Purports to impact “establishments” in the EU and other organizations that monitor behavior of EU data subjects or offer services to EU data subjects.
4. **Breach Notification.** Adopts new breach notification obligations.
5. **Children.** Adopts US-like protections concerning collection of data from children.
6. **Right to be Forgotten.** Grants data subjects a right to have their information erased.
7. **Right to Data Portability.** Grants data subjects a right to ask for their information.
8. **Data Protection Officers.** Requires some organizations to designate data protection officers.
9. **Data Privacy Impact Assessments.** Requires organizations to create internal records concerning impact of high-risk processing.
10. **Data Minimization.** Requires that personal data be kept for no longer than is necessary.
Requirements differ depending upon whether you are a “Data Controller” or a “Data Processor.”

- A “Data Controller” is defined as the entity which “determines the purposes and means of the processing of personal data.” GDPR, Art. 4(7).

- A “Data Processor” is defined as an entity “which processes personal data on behalf of the controller.” GDPR, Art. 4(8).
Overview: Core Requirements

- **Permissible Purpose**
  - Art. 6(1)
  - C/P

- **Data Minimization**
  - Art. 50(1)
  - C/P

- **Notices to Data Subjects**
  - Art. 13, 15, 24
  - C

- **Right to Access Data**
  - Art. 15, 20
  - C

- **Right to Be Forgotten**
  - Art. 17
  - C

- **Internal documentation and record keeping**
  - Art. 5, 30, 35
  - C/P

- **Designated DPO (if necessary) or other responsible individual**
  - Art. 37, 39
  - C/P

- **Appropriate data security to safeguard information**
  - Art. 50, 10, 37
  - C/P

- **Breach notification**
  - Art. 33, 34
  - C/P

- **Adequacy measures required for any country determined to have laws that do not parallel GDPR**
  - Art. 44, 45, 46, 47, 48, 49, 50
  - C/P

- **Contractual Requirements in Service Provider Agreements**
  - Art. 21, 28
  - C/P
Overview: Ability to Process Data

Core Requirements

Permissible Purpose
(Art. 6(1))

Data Minimization
(Art. 5(1)(e))

C/P
Overview: Individual Rights

- Notices to Data Subjects (Art. 12, 13, 14)
- Right to Access Data / Fix Errors (Art. 15, 20)
- Right to Be Forgotten (Art. 17)
Overview: Accountability / Governance

- Internal documentation and record keeping (Art. 5, 30, 35) - C/P
- Designated DPO (if necessary) or other responsible individual (Art. 37-39) - C/P
Overview: Data Security

- Appropriate Data Security to Safeguard Information (Art. 5(1)(f), 32) - C/P
- Breach Notification (Art. 33, 34) - C/P
Overview: Transferring Data Outside EEA

Adequacy measures required for any country determined to have laws that do not parallel EEA (Art. 44, 45, 46, 47, 48, 49, 50) C/P
Overview: Operationalizing the GDPR –
Top 10 Core Documents

Core Requirements

- Permissible Purpose (Art. 6(1))
- Data Minimization (Art. 5(1)(a))
- Notices to Data Subjects (Art. 13, 14)
- Right to Access Data (Art. 15, 20)
- Right to Be Forgotten (Art. 17)
- Internal documentation and record keeping (Art. 5, 30, 33)
- Designated DPO (Processor) or other responsible individual (Art. 37-39)
- Appropriate Data Security to Safeguard Information (Art. 34(1)(f), 32)
- Breach Notification (Art. 33, 34)
- Adequacy measures required for any country determined to have laws that do not parallel EEA (Art. 34, 46, 46, 47, 48, 49, 50)
- Contractual Requirements in Service Provider Agreements (Art. 23, 28)

Functional Policies

- 1. Data Inventory
- 2. Data Retention Policy
- 3. Information Notices (Privacy policies)
- 4. Individual Access Request Policy - Authentication protocols - Requests to delete data - Response to complaints
- 5. Policy for conducting Data Protection impact Assessments (Optional)
- 6. Written Information Security Program ("WISP")
- 7. Designated DPO
- 8. Incident Response Plan
- 9. Cross Border Transfer Map & Adequacy Strategy (e.g., Binding Corporate Rules, Privacy Shield, and/or Model Clauses)
- 10. Third Party Vendor Management Program and/or Template Data Processing Addendum
Overview: GDPR
Module 1. Information Notices / Privacy Policies
Module 2. Conducting Data Inventories
Module 3. Data Subject Requests
Module 4. Incident Response Plans
Module 5. Third Party Vendor Management Programs
Module 6. Cross Border Transfers
Module 6: Outline

• Definition of cross-border transfers
• Scope of application of rules
• Adequacy decision
• Appropriate safeguards
  – Standard Contractual Clauses
  – Privacy Shield certification
  – BCRs
  – New means
• Derogations
• Practical Pointers
Module 6: Definition of cross-border transfer

• Need to provide for protective measures if data transfer by data exporter to data importer in third country
  – Data transfer: transfer of personal data
    • If server located outside the EU, and data transferred to this server, this would be a data transfer
    • Personal data: where an individual may be identified (not anonymous or pseudonymized data)
  – Data exporter: company which collects personal data within the EU and intends to send that data outside of the European Union
  – Data importer: company located outside of the European Union and intends to receive personal data that is being transmitted by a data exporter that is inside of the European Union
  – Third country deemed not to offer sufficient level of protection as the EU
module 6: Scope of application of rules for cross-border transfers

- Scope: application to transfers outside European Economic Area (EEA) to third countries or international organizations
  - EEA: all EU countries plus Norway, Iceland and Liechtenstein
  - Rules also apply to onward transfers by third party or international organizations to another third party or international organization
Module 6: Adequacy decision (Article 45 of GDPR)

- EU Commission to determine which country, territory or specific sector within country or international organization provide adequate level of protection
  - Canada, Israel, Argentina, Switzerland among others, have been recognized as ensuring adequate protection
Module 6: Adequacy decision (Article 45 of GDPR)

- Criteria taken into account by the EU Commission for adequacy decision:
  - Rule of law, respect for human rights and fundamental freedoms, relevant legislation (e.g., public security, defense, criminal law), access of public authorities to personal data, data protection rules, security measures (including rules for onward transfer of data), data subject rights, effective administrative and judicial redress for data subjects
  - Independent supervisory authority in third country with responsibility for ensuring compliance with data protection rules, for assisting data subjects with exercise of their rights and for cooperation with EU data protection authorities
  - Commitments undertaken by third country arising from binding binational or multinational conventions in relation to protection of personal data
Module 6: Adequacy decision

• Decision taken by an implementing act:
  – With mechanism for periodic review, at least every 4 years, taking into account recent developments
  – Identifying supervisor authority
  – Possible to repeal, amend or suspend decision
  – Decisions taken under Directive to remain in force

• List of adequate countries published in Official Journal of the EU:
  – UK expected to be on adequacy list after Brexit
  – If not, need to put into place protective measures
Module 6: Appropriate safeguards for International Data Transfers

If no adequacy decision,

- “a controller and processor may transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards, and on a condition that enforceable data subject rights and effective legal remedies for data subjects are available.”

(Article 46 of GDPR)
Module 6: Pre-GDPR protective measures

- Existing protective measures (pre-GDPR) if third country not recognized by EU Commission as ensuring an adequate level of protection:
  - “Standard Contractual Clauses” ("SCCs") or “Model Contractual Clauses”: contractual clauses reviewed and approved by the European Commission.
  - Binding Corporate Rules or “BCRs”: set of internal policies adopted group-wide that are approved by a data protection authority.
  - Certification to the Privacy Shield: agreement entered into between the United States Department of Commerce and the European Union Commission providing for privacy principles.

- SCCs, most commonly used by 90% of companies
- Only 92 companies adopted BCRs
- 2,743 companies self-certified to the European Union-US Privacy Shield framework.
Module 6: New appropriate safeguards (Article 46 of GDPR)

Two new safeguards introduced by the GDPR:

• An approved code of conduct with commitments of the controller or processor to apply appropriate safeguards that may be approved at a later date and to which data importers may commit to adhere; or

• An approved certification mechanism providing for privacy standards to which data importers may adhere and commit.
Module 6: SCCs, most commonly used safeguard

• 90% of companies rely on SCCs

• Standard data protection clauses adopted by a supervisory authority and approved by the Commission, commonly referred to as “Standard Contractual Clauses” (“SCCs) or “Model Contractual Clauses”.
  – There currently exist two types of clauses:
    • SCCs to cover the transfer of personal data from a controller within the EEA to a Controller outside of the EEA (i.e., controller-to-controller clauses),
    • SCCs to facilitate the transfer of personal data from a controller within the EEA to a processor outside of the EEA (i.e., controller-to-processor clauses)
    • These authorizations based on Article 26 of the Directive shall remain valid
Module 6: How to deal with onward international data transfers?
1. Data transfer from an EU data controller to a non-EU data controller which transfers to another non-EU data controller.

A and B enter into controller to controller SCCs.

Transfer between the two non-EU data controllers must be governed by an agreement that provides for the same obligations as those provided in the SCCs between A and B.
Module 6: Onward Transfers

2. Data transfer from an EU controller to a non-EU controller which transfers the data to a non-EU processor (2 options)

Option 1
A and B enter into controller to controller SCCs.
A and C enter intro controller to processor SCCs.

Source: CNIL
Module 6: Onward Transfers

Option 2 (recommended)

A and B enter into controller to controller SCCs.

B being controller, it may also enter into an agreement equivalent to controller to processor SCCs.

The agreement between A and B must provide for B’s obligation to enter into an agreement equivalent to controller to processor SCCs with C.

Source: CNIL
Module 6: Onward Transfers

3. Data transfer from an EU controller to a non-EU processor which transfers the data to another non-EU processor

A and B enter into controller to processor SCCs. Transfer between the two non-EU processors must be governed by an agreement providing for the same obligations as those provided in the SCCs between A and B.

(1) The prior written agreement from the controller (A) authorizing the subsequent processing is expressly provided in the 2010 model clauses (Article 11 para. 1). This agreement may be general or specific for each subsequent processing.

Source: CNIL
Module 6: Onward Transfers

4. Data transfer from an EU controller to an EU processor which transfers the data to a non-EU processor: 2 options.

A and B do not have to enter into controller to processor SCCs because the data remains within the EU. B being a processor, it cannot enter into SCCs with C which is also a processor. There are two options.

**Option 1**

A and C enter into controller to processor SCCs.

Source: CNIL
Option 2

B enters into controller to processor SCCs with C in the name and on behalf of A (under a power of attorney from A to B).

A Data controller in France

B Data processor in the UK

C Data processor in Indonesia

Controller to processor SCCs

Power of attorney from A to B to enter into SCCs with C in its name and on its behalf.

Source: CNIL
5. Data transfer from an EU controller to another EU controller which transfers the data to a non-EU processor.

A and B do not have to enter into controller to controller SCCs because the data remains within the EU. However, B has to protect the data transfer to C as C is located outside the EU.

Same rationale if B is located in a country recognized by an adequacy decision from the EU Commission. The transfer from B to C will have to be governed by B's local law in this case.

Source: CNIL
Module 6: Onward Transfers

6. Data transfer from an EU controller to a non-EU processor which transfers the data to a non-EU controller (e.g. A is an EU company that transfers data to a non-EU payroll service provider (B) which then transfers the data to an non-EU entity belonging to the same corporate group as A).

A and B enter into controller to processor SCCs.

B being a processor, it cannot enter into SCCs with C which is a controller. A must enter into controller to controller SCCs with C.
Model 6: Controller to Controller SCCs

2 sets:

• Set 1 approved in 2001: perceived as being contrary to the desires of many contracting parties.
  – Set 1 requires that the exporting controller remain jointly and severally liable for the actions of the importing controller.

• Set 2 approved in 2004: drafted by a coalition of business associations including the International Chamber of Commerce
  – Primary difference: joint and several liability between the parties removed; instead, each party liable to data subject for its own acts
  – Data exporter also has an obligation to reasonably monitor the actions of the data importer
  – Liability regime based on due diligence obligations where the data exporter and the data importer would be liable vis-à-vis the data subjects for their respective breach of their contractual obligations; the data exporter is also liable for not using reasonable efforts to determine that the data importer is able to satisfy its legal obligations under the clauses (culpa in eligendo) and the data subject can take action against the data exporter in this respect.
  – Set 2 also permits the parties to agree to arbitrate disputes, and to indemnify each other for actions that arise out of their breach of the agreement.
Module 6: Controller to Processor SCCs

• Controller to Processor clauses adopted in 2010
  – Clauses need to be amended as the GDPR introduced new obligations for data processors which must be set out in a contract or in another legal act
  – Current SCCs don’t address the following requirements:
    • Duration of processing,
    • Onward transfers outside the EU without the controller’s permission
    • Confidentiality provision
    • Obligation to assist controller in the event of data subject requests
    • Obligation to cooperate in a DPIA conducted by controller
    • Obligation to assist controller in case of a data breach
    • New requirements for audits
## Module 6: Comparison Against Controller/Processor Model Clause (1)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Reference</th>
<th>Controller-Processor Contractual Clauses</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary of Requirement</strong></td>
<td></td>
<td><strong>Requirement Satisfied by Standard Clauses</strong></td>
<td></td>
</tr>
<tr>
<td><strong>1. Description of Processing.</strong> The parties must specify:**</td>
<td></td>
<td><strong>Partial Gap</strong></td>
<td>Appendix 1 of the Standard Contractual Clause describes (1) subject matter of processing, (2) nature and purpose of processing, (3) type of personal data, and (4) categories of data subjects. The standard contractual clause, and the Appendix, do not discuss the duration of processing.</td>
</tr>
<tr>
<td>1. subject matter of processing.</td>
<td>Art. 23(3)</td>
<td><strong>Partial Gap</strong></td>
<td></td>
</tr>
<tr>
<td>2. duration of processing.</td>
<td></td>
<td><strong>Partial Gap</strong></td>
<td></td>
</tr>
<tr>
<td>3. nature and purpose of processing.</td>
<td></td>
<td><strong>Partial Gap</strong></td>
<td></td>
</tr>
<tr>
<td>4. type of personal data to be processed</td>
<td></td>
<td><strong>Partial Gap</strong></td>
<td></td>
</tr>
<tr>
<td>5. categories of data subjects about which the data relates.</td>
<td></td>
<td><strong>Partial Gap</strong></td>
<td></td>
</tr>
<tr>
<td><strong>2. Documented Instructions.</strong> A service provider can only process personal data consistent with a controller’s documented instructions.</td>
<td>Art. 28(3)(a)</td>
<td><strong>Satisfied.</strong></td>
<td>Clause 5(a) and (b) of the Standard Contractual Clauses contain a requirement that processing can only occur based on a controller’s instructions.</td>
</tr>
<tr>
<td><strong>3. Confidentiality.</strong> It must contain a confidentiality provision. That provision must ensure that persons authorized to process personal data have committed themselves to confidentiality.</td>
<td>Art. 28(3)(b)</td>
<td><strong>Gap</strong></td>
<td>The Standard Contractual Clauses do not contain a representation by a data importer concerning confidentiality.</td>
</tr>
<tr>
<td><strong>4. Processor Security.</strong> Service provider will implement appropriate technical and organizational measures to secure information.**</td>
<td>Art. 28(1) Art. 28(3)(c) Art. 32(1) (c/p)</td>
<td><strong>Satisfied.</strong></td>
<td>Clause 5(c) of the Standard Contractual Clauses requires the processor to agree to the security provisions contained in Appendix II. Presuming that Appendix II contains a description of appropriate security there would be no gap.</td>
</tr>
</tbody>
</table>
# Module 6: Comparison Against Controller/Processor Model Clause (2)

## GDPR

<table>
<thead>
<tr>
<th>Summary of Requirement</th>
<th>Reference</th>
<th>Requirement Satisfied by Standard Clauses</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Subcontracting authorization. A service provider must obtain written authorization before subcontracting, and must inform the Company before it makes any changes to its subcontractors.</td>
<td>Art. 28(2) Art. 28(3)(d).</td>
<td>Satisfied.</td>
<td>Clauses 5(h) and 11(1) of the Standard Contractual Clauses requires that a processor notify the controller before using a subprocessor, and obtain their prior written consent.</td>
</tr>
<tr>
<td>6. Subcontracting flow down obligations. Service provider will flow down these obligations to any subprocessors.</td>
<td>Art. 28(3)(d) Art. 28(4)</td>
<td>Satisfied.</td>
<td>Clause 11(1) of the Standard Contractual Clauses requires that a processor flow down obligations to any subprocessors.</td>
</tr>
<tr>
<td>7. Subcontracting liability. A service provider must remain fully liable to the controller for the performance of a sub-processors obligations.</td>
<td>Art. 28(3)(d)</td>
<td>Satisfied.</td>
<td>Clause 11(1) of the Standard Contractual Clauses requires that a processor remain fully liable for the actions of its subprocessors.</td>
</tr>
<tr>
<td>8. Responding to data subjects. Service provider will assist the Company to respond to any requests by a data subject.</td>
<td>Art. 28(3)(e) Art. 12 – 23</td>
<td>Partial Gap</td>
<td>Clause 5(d)(iii) and clause 5(e) of the Standard Contractual Clauses require that a subprocessor notify a controller of a data subject request. The clauses do not specifically discuss an obligation to cooperate in responding to such request.</td>
</tr>
<tr>
<td>Summary of Requirement</td>
<td>Reference</td>
<td>Requirement Satisfied by Standard Clauses</td>
<td>Explanation</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>9. Assisting Controller In Responding to Data Breach. Service provider will cooperate</td>
<td>Art. 28(3)(f) Art. 33 – 34</td>
<td>Gap</td>
<td>Clause 5(d)(ii) requires that a processor notify a controller concerning a subset of what the GDPR defines as a “data breach.” It does not comply with the GDPR’s timing requirements. It also does not discuss obligations to cooperate in investigations and response.</td>
</tr>
<tr>
<td>10. Assisting Controller In Creating DPIA. Service provider will cooperate with</td>
<td>Art. 28(3)(f) Art. 35 Art. 35-36</td>
<td>Gap</td>
<td>The Standard Contractual Clauses do not discuss the obligation of a processor to participate in DPIA’s conducted by a controller.</td>
</tr>
<tr>
<td>11. Delete or return data. Service provider will delete or return data at the end of</td>
<td>Art. 28(3)(g)</td>
<td>Satisfied.</td>
<td>Clause 12(1) of the Standard Contractual Clauses requires a processor to delete or return data upon termination of an agreement.</td>
</tr>
<tr>
<td>12. Audit Right. Service provider will allow Company to conduct audits or inspections</td>
<td>Art. 28(3)(h)</td>
<td>Partial</td>
<td>Clauses 5(f) and 12(2) of the Standard Contractual Clauses refer to the ability of the controller to audit or inspect the processor for compliance with the requirements of the clauses; as the clauses do not include all of the requirements of the GDPR the audit provision is technically narrower than is required under GDPR.</td>
</tr>
<tr>
<td>13. Cross-border transfers. Service provider will not transfer data outside of the</td>
<td>Art. 28(3)(a) Art. 46</td>
<td>Partial</td>
<td>The Standard Contractual Clauses permit the transfer of data from the controller to a processor that is not based in the EU. The clauses do not discuss whether the processor is permitted to engage in onward transfers to additional countries outside of the EEA.</td>
</tr>
</tbody>
</table>
Module 6: Drafting tip for SCCs

- Amend existing processing agreements incorporating the SCCs
  - Draft a new data processing agreement or amendment with new requirements incorporating the SCCs

- Also need to indicate cross border data transfer in data register (records of processing activities) with protective measures (Article 30 of GDPR)

- Inform data subjects of data transfer, protective measures and where to obtain copy (Article 13 of GDPR)
Module 6: SCCs at risk?

- Max Shrems who initiated the safe-harbor certification claim which led to its invalidation in October 2015 also filed a complaint before the Irish Data Protection Commissioner claiming that the SCCs did not provide sufficient protection
  - Matter referred by the Irish High Court to the European Court of Justice
  - Issue to compatibility of US surveillance practices with EU law and the absence of an effective remedy before an independent tribunal
  - Today, SCCs still remain a valid basis for transfers abroad
  - CJEU not expected to render a decision before two years
Module 6: Privacy Shield

- Replaces safe-harbor certification, which was invalidated by the European Court of Justice on October 6, 2015 as it violated the Directive’s principles as well as European Union fundamental rights.

- Privacy Shield framework faces challenges similar to those that were raised against the Safe Harbor
  - Ongoing lawsuit
  - Today, Privacy Shield remains a valid method for transferring personal data into the United States.
## Module 6: Comparison Against Privacy Shield (1)

<table>
<thead>
<tr>
<th>GDPR</th>
<th>Summary of Requirement</th>
<th>Reference</th>
<th>Requirement Satisfied by Privacy Shield</th>
<th>Explanation</th>
</tr>
</thead>
</table>
| **1. Description of Processing.** The parties must specify:  
  1. subject matter of processing.  
  2. duration of processing.  
  3. nature and purpose of processing.  
  4. type of personal data to be processed  
  5. categories of data subjects about which the data relates. | Art. 23(3) | Gap | Privacy Shield registration does not in of itself specify the type of personal data processed, the categories of data subjects involved, or the scope of permissible processing. |
| **2. Documented Instructions.** A service provider can only process personal data consistent with a controllers documented instructions. | Art. 28(3)(a) | Gap | Privacy Shield recognizes that a controller in the EU is “always required to enter into a contract when a transfer for mere processing is made . . . whether or not the processor participates in the Privacy Shield, and that the purpose of the contract is to “make sure that the processor acts only on instructions from the controller.” |
| **3. Confidentiality.** It must contain a confidentiality provision. That provision must ensure that persons authorized to process personal data have committed themselves to confidentiality. | Art. 28(3)(b). | Partial Gap | The purpose limitation contained in Privacy Shield Principle 5(a) might be interpreted as precluding a service provider from disclosing personal data, as such disclosure would presumably be “incompatible with the purposes for which [the data] has been collected . . .” |
| **4. Processor Security.** Service provider will implement appropriate technical and organizational measures to secure information. | Art. 28(1)  
Art. 28(3)(c)  
Art. 32(1) | Satisfied | Privacy Shield requires that “Organizations creating, maintaining, using or disseminating personal information must take reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.” |
<table>
<thead>
<tr>
<th>GDPR</th>
<th>Reference</th>
<th>Privacy Shield</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary of Requirement</strong></td>
<td><strong>Requirement Satisfied by Privacy Shield</strong></td>
<td><strong>Explanation</strong></td>
<td></td>
</tr>
<tr>
<td><strong>5. Subcontracting authorization.</strong> A service provider must obtain written authorization before subcontracting, and must inform the Company before it makes any changes to its subcontractors.</td>
<td>Art. 28(2) Art. 28(3)(d).</td>
<td>No.</td>
<td>Privacy Shield requires that a registrant ensure that its service providers only use information for “limited and specified purposes.” It does not, however, require that a registrant that is acting as a processor obtain the consent of the controller prior to the use of a subcontractor.</td>
</tr>
<tr>
<td><strong>6. Subcontracting flow down obligations.</strong> Service provider will flow down these obligations to any subprocessors.</td>
<td>Art. 28(3)(d) Art. 28(4)</td>
<td>Partial Gap</td>
<td>While Privacy Shield does have some flow down obligations, as not all of the provisions that must be placed in contracts by GDPR are inherent in Privacy Shield, flow down provisions created by Privacy Shield do not cover the full scope of the flow down obligations in GDPR.</td>
</tr>
<tr>
<td><strong>7. Subcontracting liability.</strong> A service provider must remain fully liable to the controller for the performance of a sub-processors obligations.</td>
<td>Art. 28(3)(d)</td>
<td>Partial Gap</td>
<td>The Privacy Shield references that an organization remains “liable under the Principles if its agent processes such personal information in a manner inconsistent with the Principles unless the organization proves that it is not responsible for the event giving rise to the damage.” It is not clear whether the exception to liability in Privacy Shield is consistent with the liability provisions in the GDPR.</td>
</tr>
<tr>
<td><strong>8. Responding to data subjects.</strong> Service provider will assist the Company to respond to any requests by a data subject.</td>
<td>Art. 28(3)(e) Art. 12 – 23</td>
<td>Partial Gap</td>
<td>Privacy Shield requires that a service provider grant access, rectification, and deletion requests to a data subject. This may be at odds with GDPR which requires that a service provider cooperate with the controller, but permit the controller to respond to such requests.</td>
</tr>
</tbody>
</table>
## Module 6: Comparison Against Privacy Shield (3)

<table>
<thead>
<tr>
<th>Summary of Requirement</th>
<th>Reference</th>
<th>Requirement Satisfied by Privacy Shield</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>9. Assisting Controller In Responding to Data Breach.</strong> Service provider will cooperate with controller in the event of a personal data breach.</td>
<td>Art. 28(3)(f) Art. 33 – 34</td>
<td>Gap</td>
<td>Privacy Shield does not discuss the obligation of a service provider to cooperate with a controller in the event of a personal data breach.</td>
</tr>
<tr>
<td><strong>10. Assisting Controller In Creating DPIA.</strong> Service provider will cooperate with controller in the event the controller initiates a data protection impact assessment.</td>
<td>Art. 28(3)(f) Art. 35 Art. 35-36</td>
<td>Gap</td>
<td>Privacy Shield does not discuss the obligation of a service provider to cooperate with a controller to conduct a DPIA.</td>
</tr>
<tr>
<td><strong>11. Delete or return data.</strong> Service provider will delete or return data at the end of the engagement.</td>
<td>Art. 28(3)(g)</td>
<td>Partial Gap</td>
<td>Privacy Shield prohibits maintaining information in an identifiable manner after it has served its permissible purpose. Note, however, that it does not mandate that the personal data be deleted or returned at the election of the controller.</td>
</tr>
<tr>
<td><strong>12. Audit Right.</strong> Service provider will allow Company to conduct audits or inspections for compliance to these obligations.</td>
<td>Art. 28(3)(h).</td>
<td>Gap</td>
<td>Privacy Shield requires that the registrant conduct their own audits of their internal privacy practices; it does not guarantee that a controller has audit rights vis-à-vis a processor.</td>
</tr>
<tr>
<td><strong>13. Cross-border transfers.</strong> Service provider will not transfer data outside of the EEA without permission of Company.</td>
<td>Art. 28(3)(a) Art. 46</td>
<td>Gap</td>
<td>Privacy Shield does not prohibit a service provider from doing an onward transfer to a Subprocessor that is located outside of the EEA (or outside of the US).</td>
</tr>
</tbody>
</table>
What are Binding Corporate Rules?

- Binding Corporate Rules (BCRs) constitute a “code of conduct” that provides rules applicable group-wide to protect personal data.
- BCRs thus allow international companies to transfer personal data from the EEA to their affiliates located outside of the EEA. They guarantee a sufficient level of protection as they are approved by the relevant DPA.
- BCRs can apply to corporate groups that act as data controllers or as data processors.
What must BCRs include? – Article 47 of the GDPR (1/2)

• (a) the structure and contact details of the group and of each of its members;
• (b) the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;
• (c) their legally binding nature, both internally and externally;
• (d) the application of the general data protection principles (data minimisation, data protection by design and by default, legal basis for processing, etc.);
• (e) the rights of data subjects in regard to processing and the means to exercise those rights (right to lodge a complaint with the DPA, right to obtain compensation for a breach of BCRs, etc.);
• (f) principle of the liability of the Member State based entity for any breaches of BCRs by any group member concerned not established in the EU;
• (g) how specific information on the BCRs is provided to the data subjects (in addition to information provided in the notices regarding the processing);
Module 6: Binding Corporate Rules

What must BCRs include? – Article 47 of the GDPR (1/2)

- (h) the tasks of any DPO or any other person or entity in charge of data protection;
- (i) the complaint procedures;
- (j) the mechanisms for ensuring the verification of compliance with the BCRs (audits and methods for ensuring corrective actions);
- (k) the mechanisms for reporting and recording changes to the BCRs and reporting those changes to the DPA;
- (l) the cooperation mechanism with the DPA to ensure compliance by any member of the group in particular by making available to the DPA the results of the measures for ensuring the verification of compliance with the BCRs;
- (m) the mechanisms for reporting to the competent DPA any legal requirements to which a member of the group is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the BCRs; and
- (n) the appropriate data protection training to personnel having permanent or regular access to personal data.
**Module 6: Binding Corporate Rules**

**How to implement BCRs?**

- **1. Draft the BCRs**
  
  The Article 29 Data Protection Working Party has issued framework for the structure of Binding Corporate Rules. These have yet to be updated in order to comply with the GDPR, however working document WP 256 sets up a table with the elements and principles to be found in BCRs that complies with the GDPR.

- **2. Submit the draft BCRs to the Lead DPA**
  
  With the GDPR, the BCRs no longer need to be approve by two DPAs in addition to the Lead DPA.

  However, if the BCRs are intended to cover data transfers from multiple Member States, the consistency mechanism will have to apply to the approval of the BCRs (*i.e.*, they will be submitted to a new entity called the European Data Protection Board that verifies that the data protection rules are applied consistently throughout the EU).

- **3. Entry in force**
  
  Once approved by the Lead DPA (and as the case may be under the consistency mechanism), the BCRs the approval is final and no further DPA approval will be required for transfers of personal data made under the BCRs.
Module 6: Binding Corporate Rules

What are the advantages of the BCRs?

- A tool that provides a single framework for a variety of intra-group transfers
- Helps to raise awareness regarding data protection within companies

Disadvantages

- Long process to implement
Status of BCRs adopted before the entry into force of the GDPR?

• Before the GDPR, the Directive did not specifically provide for BCRs. Their content was governed by the recommendations of the Article 29 Data Protection Working Party group.

• The GDPR provides that authorizations by a Member State or supervisory authority (including approval of BCRs) made on the basis of Article 26(2) of Directive 95/46/EC will remain valid until amended, replaced or repealed, if necessary, by that supervisory authority (Article 46 § 5.)

• However, the Article 29 Data Protection Working Party recommend that groups with approved BCRs should, in preparing to the GDPR, bring their BCRs in line with GDPR requirements (see table with the elements and principles to be found in Binding Corporate Rules in WP document).
There also exists number of exceptions for specific situations, most of which preexisted the GDPR.

**Main exceptions:**
- Consent by data subject to data transfer after information as to possible risks
  - Not recommended if data subject is an employee
- Where the transfer is necessary to perform a contract between the data subject and the controller.
- For the performance of a contract between data subject and controller, or
- For the implementation of pre-contractual measures taken at the data subject’s request;
- For the conclusion or performance of a contract concluded in the interest of the data subject.
Module 6: Derogations (Article 49 of the GDPR)

- New exception introduced by the GDPR: self-assessment of adequacy in cases where the transfer could not be based on an adequacy decision, appropriate safeguards, or the other exceptions.
  - A self-assessment is not permitted, however, if the transfer is repetitive, concerns more than a limited number of data subjects, or is not necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests, rights and freedoms of the data subject.
  - Companies that rely upon a self-assessment are also responsible for implementing suitable safeguards to protect personal data after the transfer occurs.
Module 6: Don’t forget! Operational requirements

- Need to refer to the data transfer and protective measures in the processing records (or register)

- Need to disclose to the data subjects the transfer of data outside the EEA and chosen protective measures
  - Also need to indicate the protective measures implemented and where they are available or a copy can be obtained
    - Possible for example to provide a link to the protective measures

- Update protective measures and notices as appropriate
  - After privacy shield certification (or invalidation!)
  - When data transferred to a new data processor and/or for a new purpose
Module 6: Practical Pointers

- Add reference to the GDPR in a preamble to the SCCs as SCCs still refer to the Directive
- Enter into global SCCs for group-wide EU data exporting entities
  - Consider including group entities outside the EU to enhance data protection world-wide: EU to become a model legislation
- Don’t be too specific in completing Annex B to the SCCs on the description of the Transfer, to avoid the need for too many future amendments
David Zetoony is the leader of the firm's global data privacy and security practice. He has extensive experience advising clients on how to comply with state and federal privacy, security, and advertising laws, representing clients before the Federal Trade Commission, and defending national class actions. He has assisted hundreds of companies in responding to data security incidents and breaches, and has represented human resource management companies, financial institutions, facial recognition companies, and consumer tracking companies before the Federal Trade Commission on issues involving data security and data privacy.
Sarah Delon-Bouquet focuses her practice on labor and employment law, and serves as the firm’s Team Deputy Leader for European Labor and Employment.

She has significant experience in advising and representing international clients having business activities in Europe and in particular in France with day-to-day issues related to labor law, whether contentious or not. This involves all aspects of labor and employment law from drafting employment agreements to advising on issues related to working time, employee benefits, organizing personnel representative elections and consulting with the works council to negotiating termination agreements.