Interoperability and Cross-Border Data Transfer: APEC, EU BCRs, and Beyond

October 22, 2015

ALSTON & BIRD

TRUSTe

Agenda

Introduction and Overview
***Chris Babel**, CEO, TRUSTe*

Operation of the APEC Cross Border Privacy Rules
***Josh Harris**, Director of Policy, TRUSTe*

Binding Corporate Rules
***Jan Dhont**, Partner, Alston & Bird*

APEC-BCR Interoperability
***Josh Harris**, Director of Policy, TRUSTe*

APEC Privacy Framework (2005)

Includes nine high level Privacy Principles (preventing harm, notice, collection limitation, uses of personal information, choice, integrity of personal information, security safeguards, access and correction, accountability)

APEC Privacy Principles

(1) Preventing Harm

(2) Notice

(3) Collection Limitation

(4) Uses of personal information

(5) Choice

(6) Integrity of Personal Information

(7) Security Safeguards

(8) Access and Correction

(9) Accountability

TRUSTe's Role As an Accountability Agent

- Accountability Agents must be unanimously endorsed by all 21 APEC Economies
- TRUSTe was first admitted to the CBPR system in June 2013 and re- recognized in December, 2014
- Each year, TRUSTe must provide APEC's Joint Oversight Panel a report, detailing our CBPR certification process

The Cross Border Privacy Rules System (2011)

- An enforceable privacy code of conduct for data transfers in Asia-Pacific
- Implements the nine APEC Privacy Principles
- Developed in a multi-stakeholder process
- Creates/increases consistent privacy protections and data export mechanism
- Comparable to the EU/US Safe Harbor but multilateral and no-self certification

TRUSTe

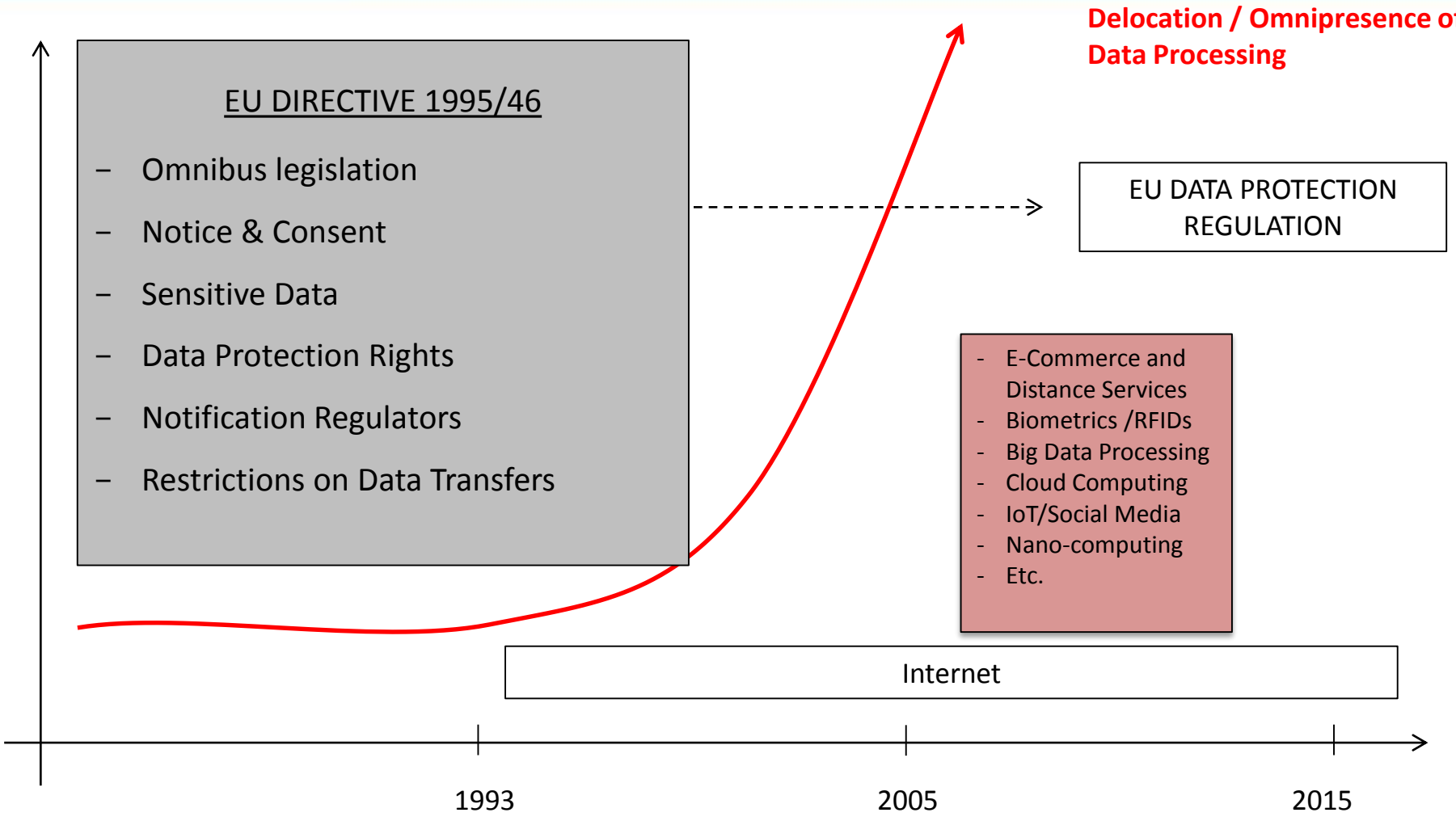
ALSTON &BIRD

Binding Corporate Rules: Building A Future-Proof Privacy Compliance Solution

Overview

- Introduction – Why Data Privacy
- EU Data Privacy In Transition
- How Prepare for Regulatory Change?
- Consider BCRs to become 'Regulation Ready'
- Key Points to Consider BCRs
- Facts and Numbers
- Types of BCRs (Controllers and Processors)
- BCR Application Process
- Future of BCRs
- Take Away's

EU Data Privacy in Transition



EU Data Privacy in Transition

The Future Data Protection Regulation Will Be 'Game Changer'

- Direct binding effect
- Applicable to processing activities related to offering of services to individuals in the EEA
- Broader obligations for data processors (Internal documentation, PIAs, data breach, international transfers)
- Data breach notification
- Accountability obligations (PIAs, Internal Documentation)
- Privacy by design/default
- Administrative sanctions (currently) up to EUR 100,000,000 or up to 5 percent of annual global TO

EU Data Privacy in Transition

- Invalidation of Safe Harbor (Schrems v. Facebook).
- October 16 Statement of Article 29 Working Party
  - End of January 2016 deadline for DPA enforcement actions
  - BCRs remain a valid option
- Low vulnerability of BCRs

How Prepare for Regulatory Change?

The Regulation will come with a 2 years implementation period. Where will you start?

- Track and document information practices
- Assess core risks and determine (non)-acceptable risk thresholds
- Invest in governance structure
- Adopt or improve policies and procedures
- Invest in breach response and pro-active data governance

You May Consider Binding Corporate Rules to Become 'Regulation-Ready'…

Set of rules that set forth a data privacy regime to exchange personal information within a group of companies

Take the form of a code of conduct, backed by policies, procedures, and control mechanisms, which are negotiated and approved by the national DPAs

Binding Corporate Rules for Data Controllers and Data Processors

You May Consider Binding Corporate Rules to Become 'Regulation-Ready'…

BCRs are not only a mechanism to transfer personal information. They help to obtain:

- Accountability
- Adequate Data Privacy Governance
- Awareness and Effective Data Protection

Facts and Numbers

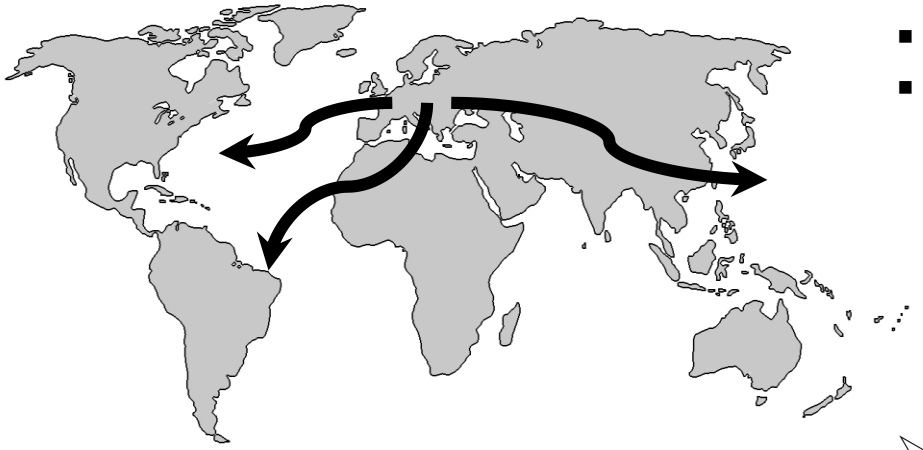
- 72 BCRs approved

- Timing:

  - 5 months in average for lead DPAs to handle application
  - 3-4 months for mutual recognition and cooperation procedure with other DPAs
  - 8 months response time applicant

Key Points When Considering BCRs

- **Relevancy**
  - Multiplicity of jurisdictions
  - Required flexibility to transfer PII globally



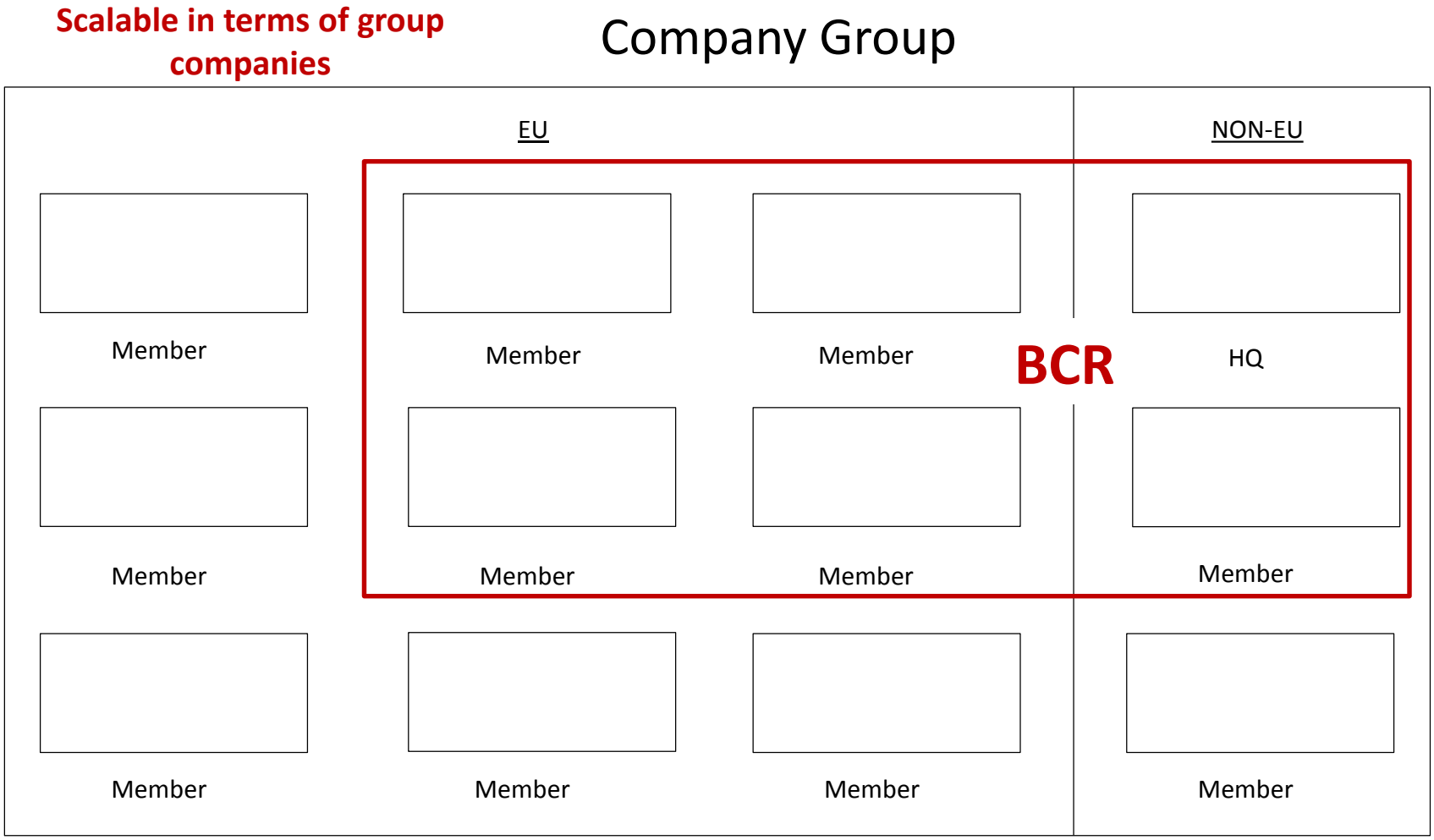
- **Effort**
  - Status current privacy compliance and governance

- **Vision**
  - Long-term view on privacy
  - Legal certainty
  - Structure, streamline and reduce administrative burden of privacy compliance for the future

- **Commercial benefits**
  - Increases customers' and partners' trust and improves company's public reputation

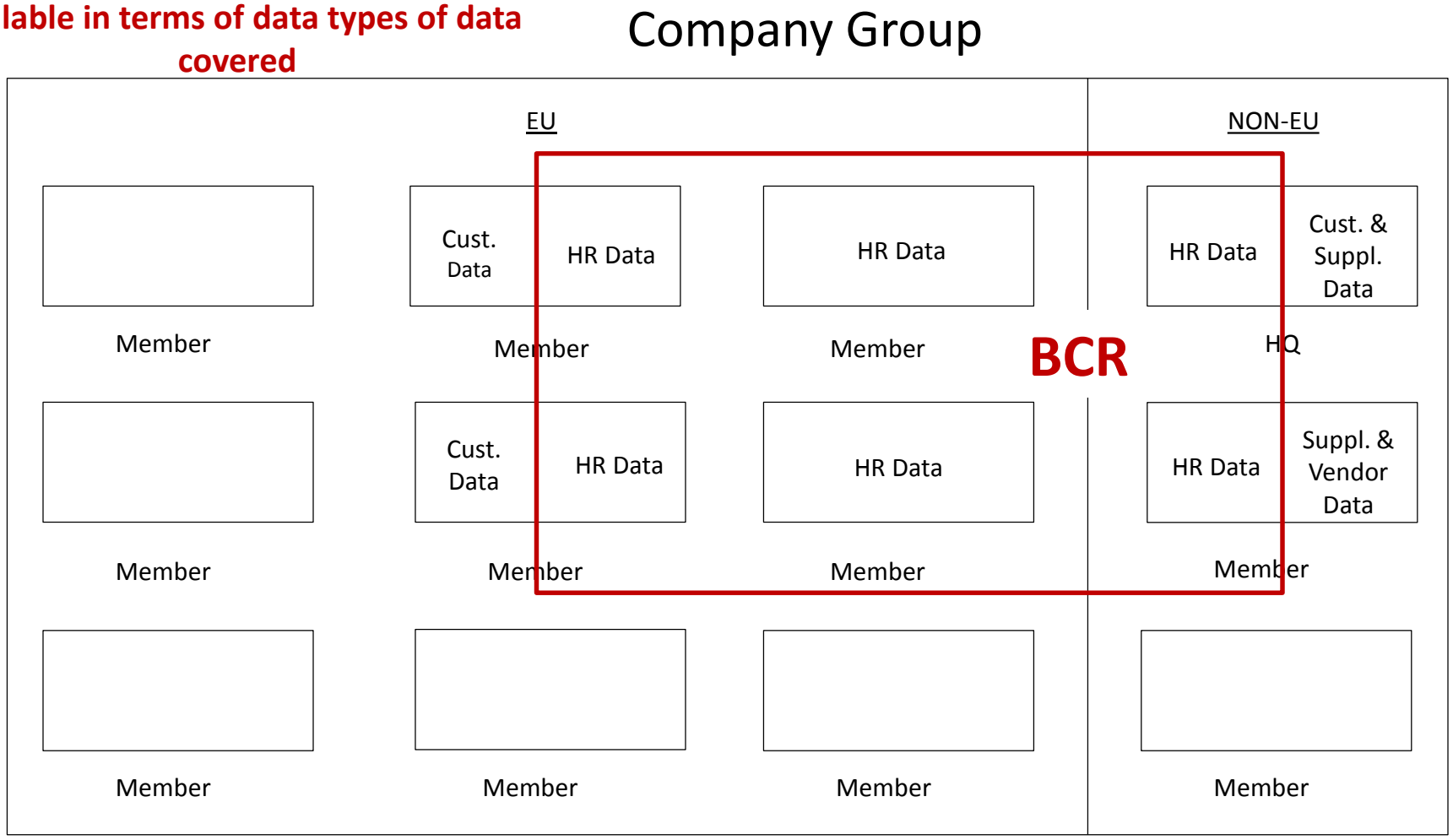
Scalable (1)

Scalable in terms of group companies



Scalable (2)

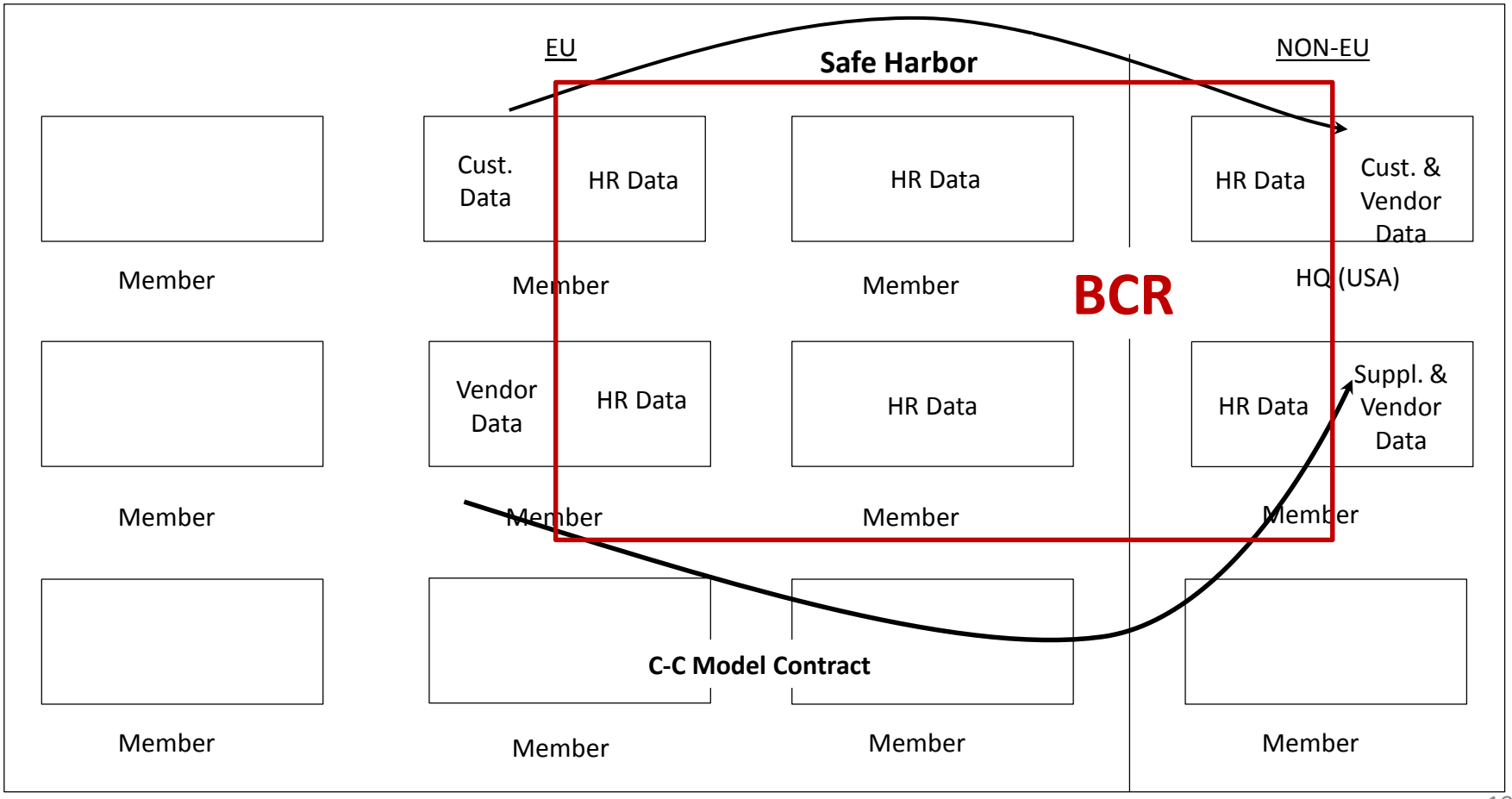
Scalable in terms of data types of data covered



Scalable (3)

Other International Data Transfer Mechanisms

Company Group



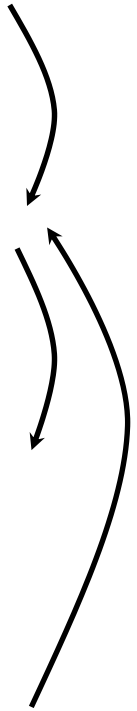
Robust Privacy Governance Structure

Robust privacy governance structure is required to successfully apply for BCRs

- Policy
- Implementation
- Effectiveness
- Control

BCR ADVANTAGES:

- Facilitates data flows within group
- Provides structure for privacy governance
- Ensures high level of privacy compliance and awareness
- Increases legal certainty due to DPA check



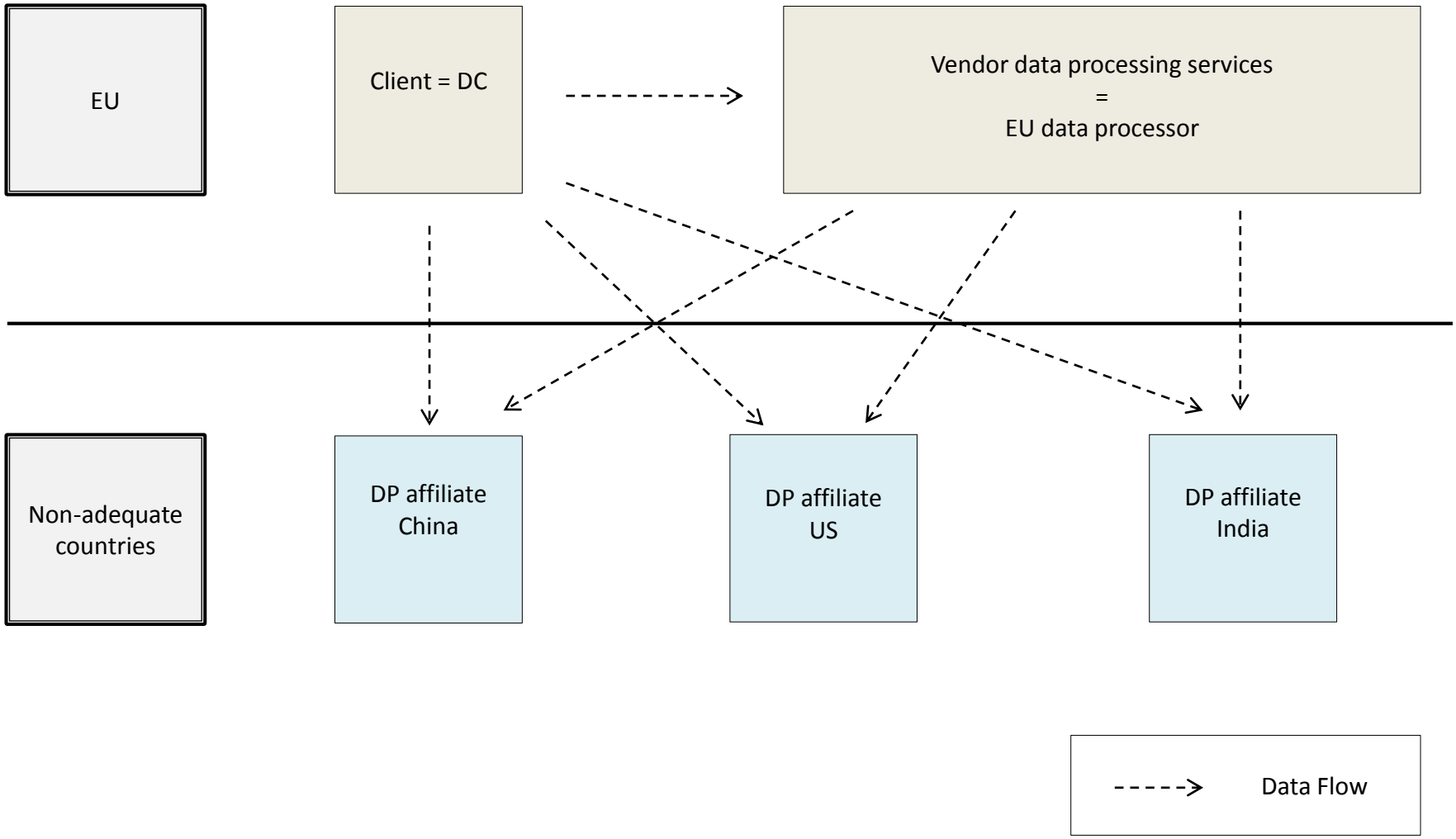
BCRs for Vendors (Processor Agents)

- Until 2013: No adequate mechanism for vendors in the EU to export data

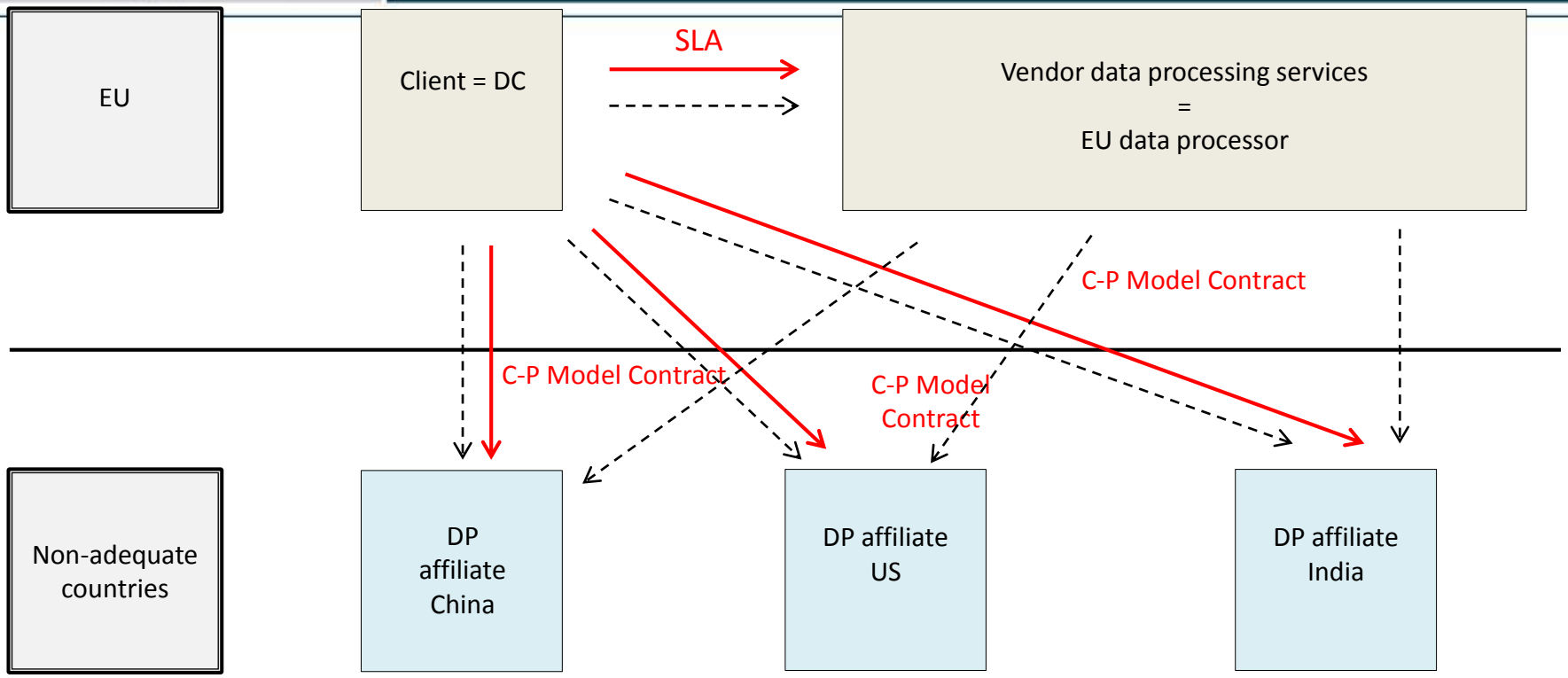
→ Vendors/Cloud providers obliged to impose burden on clients or execute C-P Model Contracts

- As of 2013: BCRs recognized as data transfer mechanism for data transfers to and between group entities of vendors/data processors

Challenges Global Data Processors - Reality



Challenges Global Data Processors – Solutions before 2013

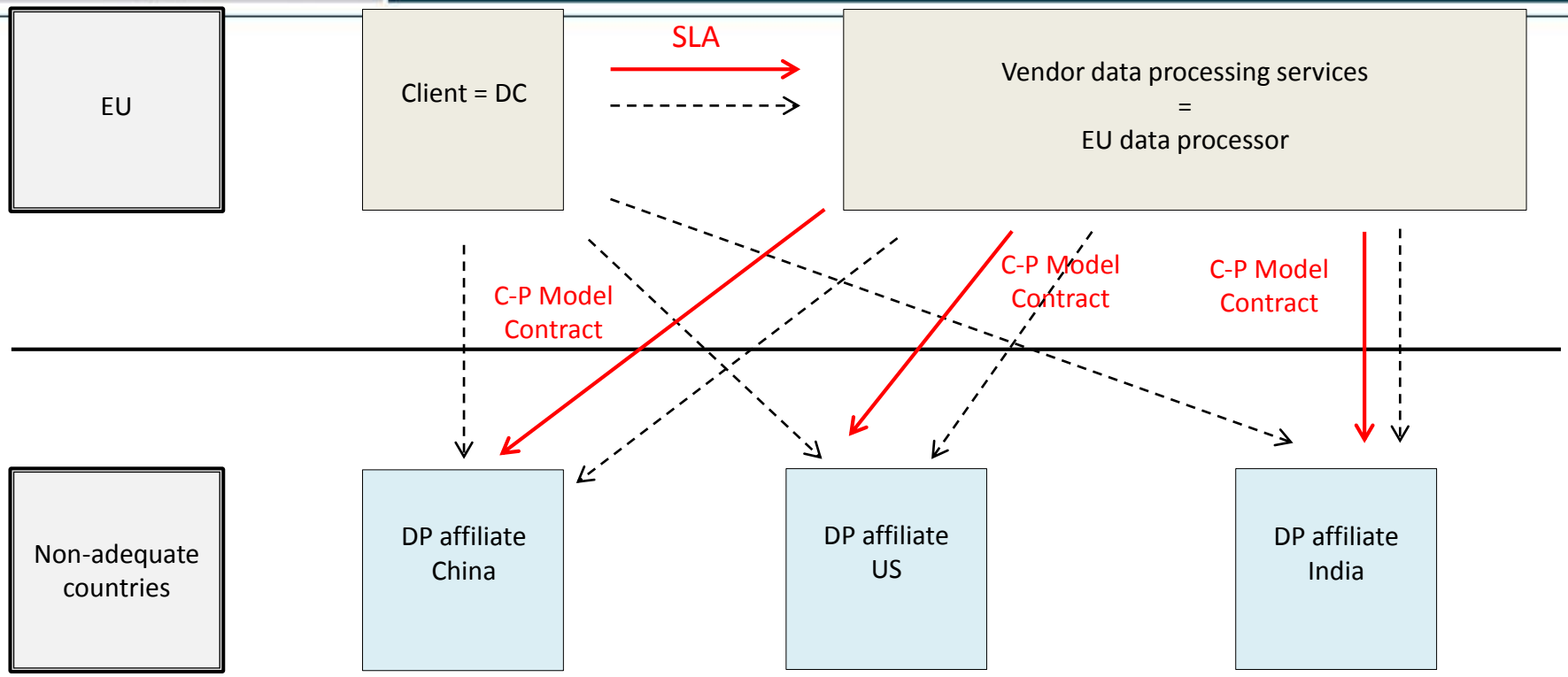


→ Burdensome for clients
- Commercially impractical
- High administrative burden related to multiple model contracts

→ Accurate reflections of data flows

Data Flow
Contractual arrangements

Challenges Global Data Processors – Solutions before 2013

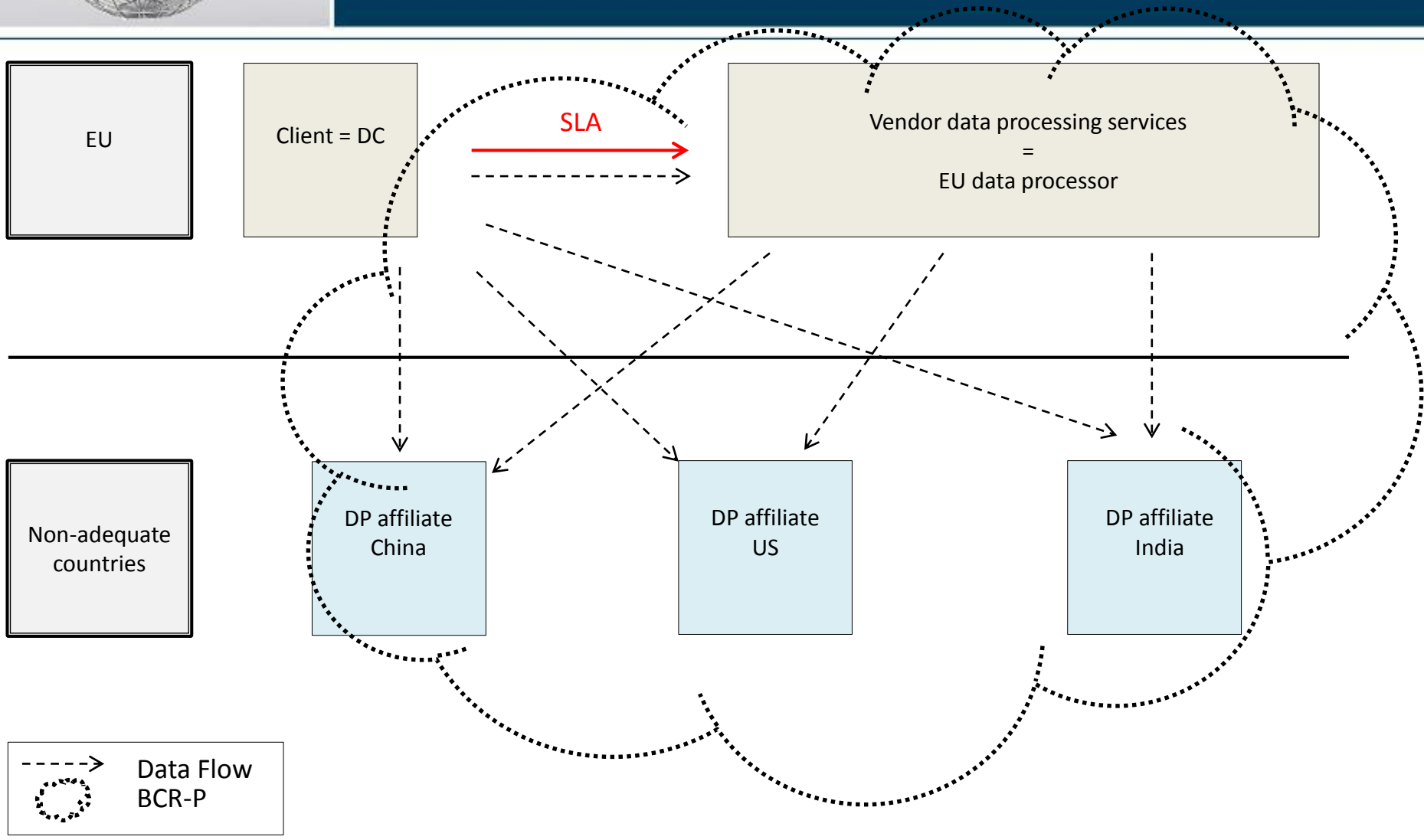


→ Commercial advantage:
- Reduce burden for clients

→ Legal Risks:
- Does not reflect reality (i.e. Not compliant with actual data flow + requalification of processor as controller)
- Shift unwanted liability to EU processor

Data Flow
Contractual arrangements

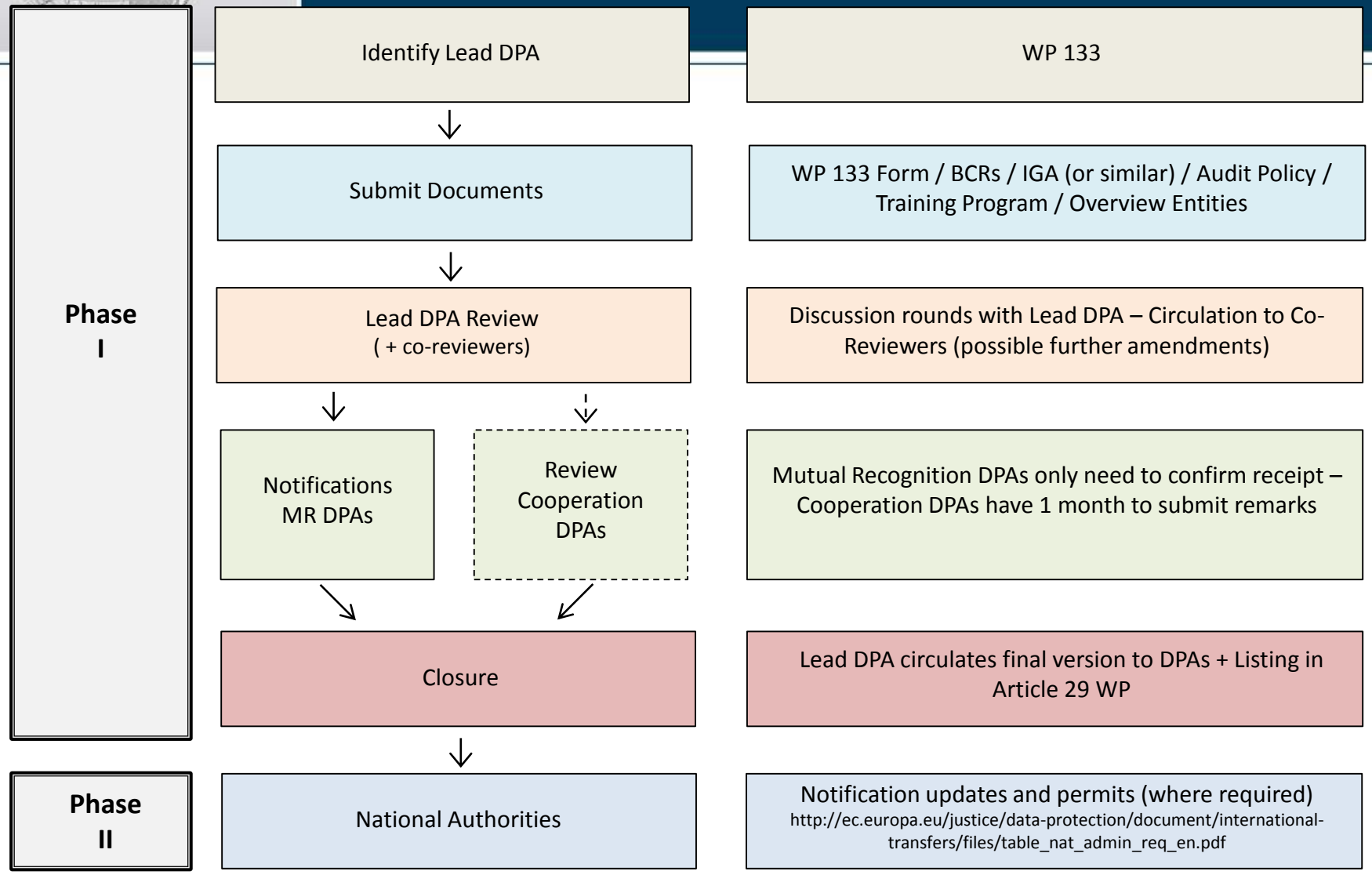
Challenges Global Data Processors – Solutions as of 2013



BCRs In Perspective

	Safe Harbor	Model Contracts	Consent & Derogations	BCRs
Scope	N/A	• EU → Global • No businesses excluded • Structural transfers	• EU → Global • No businesses excluded • No structural transfers	• EU → Global • No businesses excluded • Structural transfers
Legal Certainty	N/A	• High	• Low	• High
Maintenance	N/A	• High • Requires updates and amendments	• Low	• Medium
Administrative Burden	N/A	• High (permits)	• Low – High (exemptions – consent forms)	• High at start, low once obtained
Cost/Complexity	N/A	• Cost = Complexity (corporate structure)	• Consent: Cost = Complexity (# of DS) • Derogations: Cost (liability risk) > Complexity	• Cost < Complexity

BCR Application Process



First Phase DPA Review

➢ MR Procedure

Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Estonia, France, Germany, Ireland, Italy, Latvia, Luxembourg, Malta, the Netherlands, Spain, Slovakia, Slovenia and the UK.

➢ Co-operation Procedure

Croatia, Denmark, Finland, Greece, Hungary, Lithuania, Poland, Portugal, Romania and Sweden.

Future of BCRs

- **Current situation:**
  - Phase II approvals in some jurisdictions
  - Group of undertakings
- **Future:**
  - No Phase II approvals
  - BCRs also open to "group of enterprises engaged in joint activity"

Take Aways I

- **BCRs are Ideal Preparation for Future Regulation**
- Comprehensive privacy governance structure required under BCRs ensures compliance with stricter accountability obligations under future Regulation.

Accountability under GDPR	BCR
Concise, transparent, clear and easily accessible policies demonstrating compliance	✓
Demonstrable technical/organizational measures	✓
PIAs	✓
Documentation obligations	✓
DPO requirements (?)	✓
Audit requirements	✓

Take Aways II

- BCRs allow streamlining of company privacy policies and create awareness.

- DPAs are very supportive. Exponential growing number of BCR applicants. Alternatively, companies are getting "BCR-ready".

- Expected that BCR applications will "explode" as of adoption of Regulation.

We appreciate the opportunity to be of service to you.

Jan Dhont, Partner

Alston & Bird LLP
Level 20 Bastion Tower
Place de Champ de Mars
B-1050 Brussels
+32 2 550 3709

BCR/CBPR Interoperability

Creation of Joint EU-APEC Working Team: 2012

- Recognized value of collaboration to provide industry greater clarity on how to meet requirements of EU and APEC simultaneously

Development of "Referential": 2014

- Mapped requirements of APEC CBPR System and EU BCR System
- Identified common and divergent elements to help inform companies seeking to develop policies and practices in compliance with both systems

Next Steps

- Work together to develop practical tools to facilitate dual certification to complement referential
- APEC Data Privacy Subgroup expression of interest to Article 29 Working Party regarding tools recommended by joint working team in January 2015
- Join work plan released, June 2015

TRUSTe

Resources

- **Official APEC CBPR Website :** (containing all CBPR and PRP documents and information) www.cbprs.org

- **APEC-EU Referential:** http://www.apec.org/~/media/Files/Groups/ECSG/20140307_Referential-BCR-CBPR-reqs.pdf

- **"APEC Privacy Rules for Cross-Border Data Flows—A Model for Global Privacy Protections" ,** *BNA Bloomberg Privacy & Security Law Report, 3 March 2015*

- https://www.hunton.com/files/Uploads/Documents/Centre/APEC_Privacy_Rules_for_Cross-Border_Data_Flows.pdf

TRUSTe