CLEARSTAR®

ACADEMY

Using Your Provider's Privacy Shield Certification

Kerstin Bagus, CIPP/C/EU/US
Director of Global Initiatives

Paul de Naray
Director, Cybersecurity

CLEARSTAR® ACADEMY

Why This Topic?

Concerns about understanding if your Provider's Privacy Shield Certification means you are totally covered by Privacy Shield.

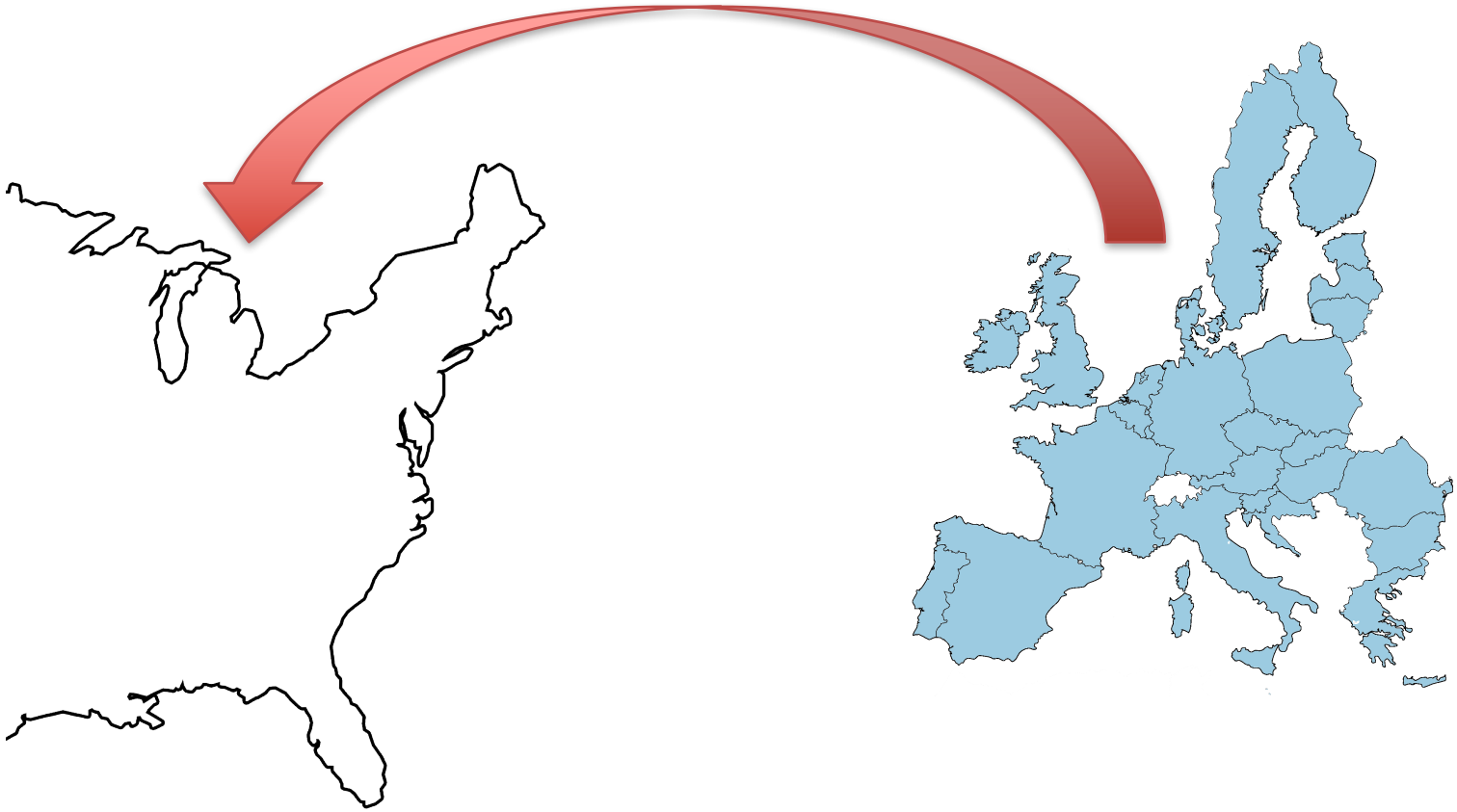
CLEARSTAR® ACADEMY

Agenda

- Overview of EU data transfer restrictions
- Overview of the Privacy Shield
- “Onward Transfer” requirements of the Privacy Shield
- Security requirements of the Privacy Shield
- What you can take from your provider’s Privacy Shield Certification

CLEARSTAR® ACADEMY

Scope



CLEARSTAR® ACADEMY

First Some Definitions

Personal Data*

"Personal data" and "personal information" are data about an identified or identifiable individual that are within the scope of the Directive, received by an organization in the United States from the European Union, and recorded in any form."

Processing*

"Processing" of personal data means any operation or set of operations which is performed upon personal data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure or dissemination, and erasure or destruction."

Controller *

"Controller" means a person or organization which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Processor**

"a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller"

Agent

Referred to in the Privacy Shield Framework text but is not defined. Presumed to be a Processor / service provider acting on behalf of an organization in the Privacy Shield.

*Privacy Shield Framework: https://www.privacyshield.gov/article?id=OVERVIEW
**EU Directive: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

CLEARSTAR® ACADEMY

EU Directive Controller Obligations

- Personal Data must be processed legally and fairly;
- It must be collected for explicit and legitimate purposes and used accordingly;
- It must be adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed;
- It must be accurate, and updated where necessary;
- Data controllers must ensure that data subjects can rectify, remove or block incorrect data about themselves;
- Data that identifies individuals (personal data) must not be kept any longer than strictly necessary;
- Data controllers must protect personal data against accidental or unlawful destruction, loss, alteration and disclosure, particularly when processing involves data transmission over networks. They shall implement the appropriate security measures;
- These protection measures must ensure a level of protection appropriate to the data.

http://ec.europa.eu/justice/data-protection/data-collection/obligations/index_en.htm

CLEARSTAR® ACADEMY

Transfer Out of EU Only Allowed When "Adequate" Protection is Provided

- Andorra
- Argentina
- Canada (commercial organizations)
- Faeroe Islands
- Guernsey
- Israel
- Isle of Man
- Jersey
- New Zealand
- Switzerland
- Uruguay
- US Privacy Shield

CLEARSTAR® ACADEMY

Enter the Privacy Shield

CLEARSTAR® ACADEMY

Privacy Shield Recap

- Privacy Shield is voluntary program
- Contains compliance obligations that live past Privacy Shield participation
- Privacy Shield is about providing protection of a person's data to the level in the EU
  - Covers data handling
  - Part of data handling is data security

CLEARSTAR® ACADEMY

Privacy Shield Primary Principles

- Notice
- Choice
- Accountability for Onward Transfer
- Security
- Data Integrity & Purpose Limitation
- Access
- Recourse, Enforcement, & Liability

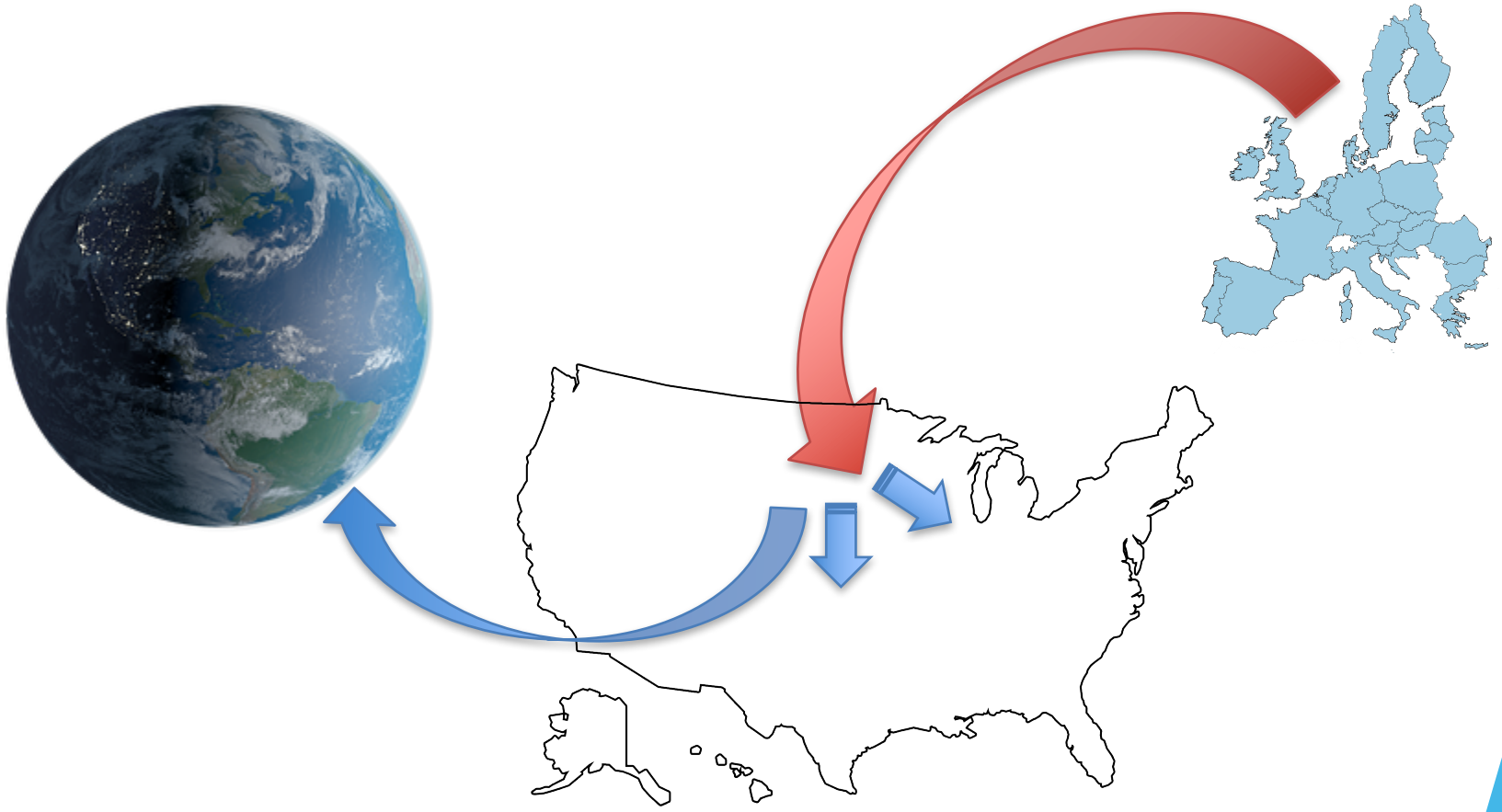
CLEARSTAR® ACADEMY

My Supplier is Privacy Shield Certified; I'm done right?

- No. Your Supplier transferred the data under Privacy Shield but you also have obligations
- Onward Transfer Applies
  - Requires defined contract
  - Requires same level of protection (Section 3, Accountability for Onward Transfer)

CLEARSTAR® ACADEMY

Onward Transfer



CLEARSTAR® ACADEMY

Privacy Shield Lacks Clear Structure for Such Transfers But Onward Protection Seems Clear

3. ACCOUNTABILITY FOR ONWARD TRANSFER

a. To transfer personal information to a third party acting as a controller, organizations must comply with the Notice and Choice Principles. Organizations must also enter into a contract with the third-party controller that provides that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles and will notify the organization if it makes a determination that it can no longer meet this obligation. The contract shall provide that when such a determination is made the third party controller ceases processing or takes other reasonable and appropriate steps to remediate.

b. To transfer personal data to a third party acting as an agent, organizations must: (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles; (iv) require the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles; (v) upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.

Onward Transfer Applicability

- Privacy Shield Certified Entity agreed to certain requirements (3 - Privacy Shield Principles)
- Controllers & Processors create “reasonable and appropriate” protection requirements (4 - Security)
- Flow down obligations from Privacy Shield to next entity
  - Contracts
  - Security

CLEARSTAR® ACADEMY

Reasonable and Appropriate Protection?

- No formal definition, will be a mixture of domain and locality expectations
- EU Background Screening:
  - EU Data Protection Directive
  - EU General Data Protection Directive (May 2018)
  - ISO 27000 series
  - Individual country requirements

Reasonable and Appropriate Protection? (cont.)

- US Background Screening
  - Fair Credit Reporting Act
  - EI3PA Certification (Credit Reports)
  - PCI Certification (Credit Card Data)
  - SSAE 16 SOC 1, Type 2 audit reports (Hosting)
  - NIST Cybersecurity and Risk Management
  - HIPAA (Medical Data)
- Leverage US protection for EU onward transfer requirements

CLEARSTAR® ACADEMY

Leveraging Services

- If possible, leverage services for your own Privacy Shield Certification
  - Controller or processor may provide services to leverage for protection
    - Leverage portal containment of data (e.g. company certifications & security policy)
    - Leverage hosting service (e.g. SSAE 16 SOC 1 report)

Onward Transfer Takeaways

- Check with Controller or Processor for their service protections to leverage for your own PS certification
- Define onward transfer contract if you further transfer data. Transfer/define your own protection requirements
- Leverage existing protection (e.g. US requirements) to fulfill Privacy Shield

CLEARSTAR® ACADEMY

Beyond the EU

CLEARSTAR® ACADEMY

In Summary

CLEARSTAR® ACADEMY

Questions (and Answers)

CLEARSTAR® ACADEMY

Resources

- Privacy Shield Website: www.privacyshield.gov
  - Framework Text: https://www.privacyshield.gov/EU-US-Framework

- EU Data Transfer Website: http://ec.europa.eu/justice/data-protection/data-collection/data-transfer/index_en.htm

- EU Directive 95/46/EC: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31995L0046

CLEARSTAR® ACADEMY

Thank you!

Contact: craigc@clearstar.net