



Certifying for Safe Harbor: The Practical Aspects

September 15, 2011

Robert L. Rothman, Principal, Privacy Associates International LLC
Kimberly A. Bubnes, Global Privacy Director, General Motors Co.

Introduction

- A very few words about what Safe Harbor is
- ~~Ten~~ critical issues to consider when certifying

Eleven

Safe Harbor

- Legally, Safe Harbor is an Executive Agreement between the US and the EU
 - The 3 non-EU EFTA countries also recognize Safe Harbor certifications
 - Separate but substantially similar Safe Harbor arrangement between the US and Switzerland
- Provides an EU “adequacy determination” to US organizations that certify to the U.S. Department of Commerce that they are in compliance with the Safe Harbor requirements
- Safe Harbor leverages the US laws regarding unfair and deceptive trade practices to make promises by US organizations that they will treat specified personal data in accordance with the Safe Harbor Principles actionable
- Enforced by certain US authorities having jurisdiction over the certifying organization, most often the FTC but also Department of Transportation
 - Since most financial services companies are not supervised by these entities, they are normally not qualified to certify for Safe Harbor
 - Financial services companies CAN certify with respect to their employment data

Safe Harbor Principles

Safe Harbor Principles consist of:

- Notice
- Choice
- Onward Transfer
- Access
- Security
- Data Integrity
- Enforcement

Enforcement Considerations

- Certification is a serious matter and should not be undertaken until and unless you are convinced your organization meets all applicable requirements and has documented how it has done so.
- Corporate officer certifying compliance subject to False Statements Act
- Europeans have been demanding enforcement actions against non-compliant Safe Harbor companies for years
 - recent FTC Consent Decree in the Google Buzz Social Network matter should help
- CNIL (French DPA) recently announced intent to investigate international data transfers, in particular Safe Harbor transfers

Safe Harbor Attributes

- Most companies use a variety of legal mechanisms to transfer European Personal Data to the US and other countries that the Europeans view as not having “adequate” privacy laws
- Safe Harbor allows the transfer of European Personal Data to any organization in the US that has certified compliance with the Safe Harbor principles for the relevant category of data.
- Safe Harbor also allows the European Personal Data that has been transferred to the US Safe Harbor organization
 - to be onward transferred to another organization in the US or
 - any other country if an Onward Transfer Agreement is put in place

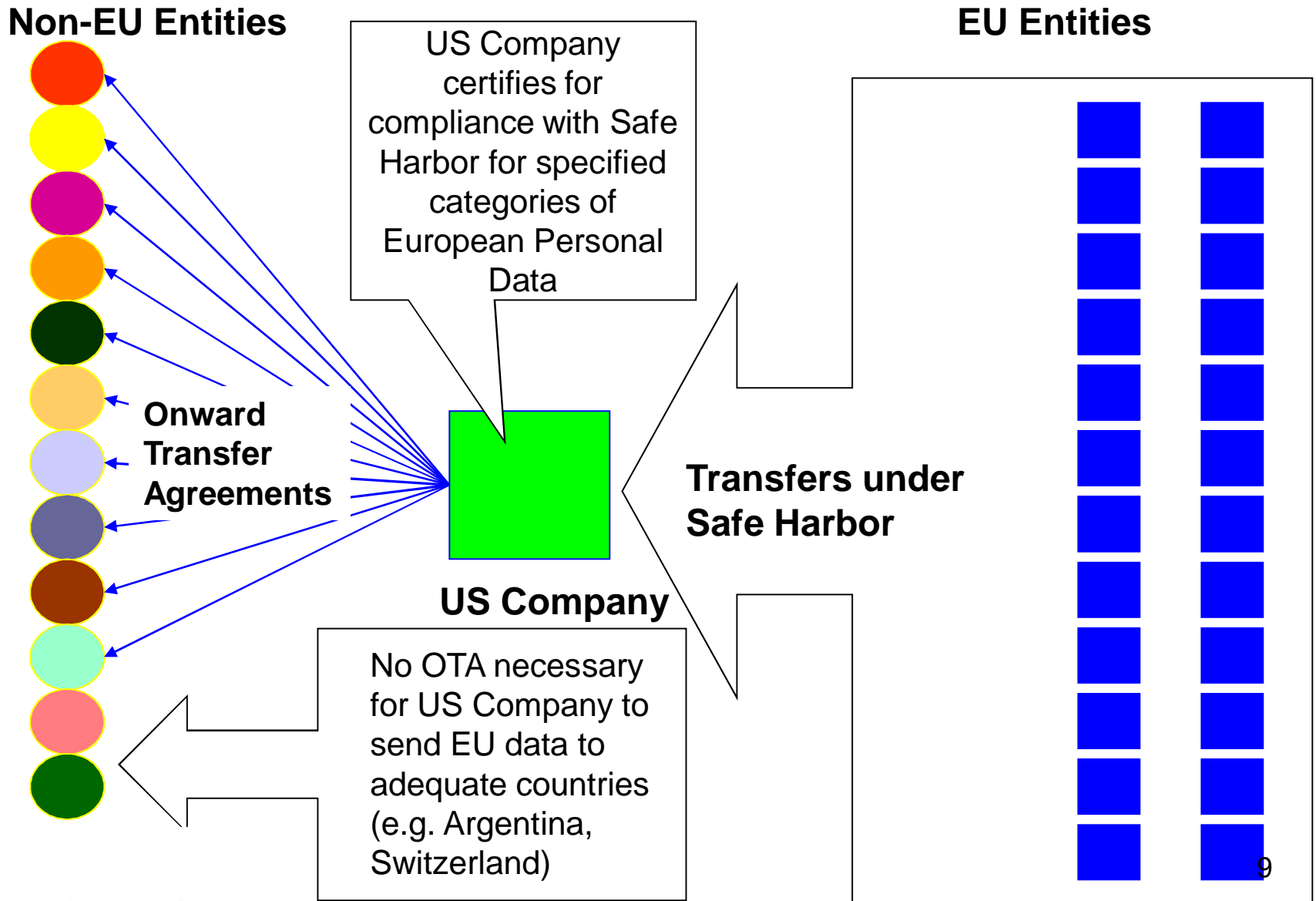
Safe Harbor Attributes

- Safe Harbor is very flexible, if European Personal Data is being sent to the US
 - NO required government approvals in the US, either no approval or automatic government approval in Europe (supposedly!)
 - Ability to define exactly what European Personal Data you are promising to handle in accordance with the Safe Harbor principles
 - Right to modify the scope of your certification as the situation changes
 - Can minimize the need for exact data identification and data mapping

Navigating Potential Hazards

- You will still need to collect consent for sensitive information that you may have to collect and process (i.e., some types of employment information)
- Safe Harbor does not help with direct transfers from Europe to entities not located in the US
- Individuals may still “opt out” of onward transfer of information beyond the US

Safe Harbor Structure



ELEVEN

~~Ten~~ Critical Issues to
Consider When Certifying
for Safe Harbor

1. Understanding Data Flows: Scope of Certification

- Need to understand what personal data is flowing from Europe to the U.S.
 - Because Safe Harbor is an adequacy determination, do not have to map data flows in minute detail, as long as all data subject to the necessary safeguards
 - Need general idea of data being transferred
- What categories of personal data will you include in the certification?
 - Too narrow, will need to find other legal bases to cover transfers
 - Too broad, may make works councils and labor unions nervous
 - May not be ready to comply with all Safe Harbor requirements for all categories of data – e.g. notice
 - Consider use of preconditions in language of your certification
 - Ease fears of Works Councils and labor unions
 - Help assure that any transfers through channels not covered by safeguards are not inadvertently covered by certification

2. Creating the Team and Accountability

- Need a variety of subject matter experts to assure fulfillment of all Safe Harbor requirements
- Typical core team might include representatives from:
 - Privacy and/or legal, U.S. and Europe
 - U.S. labor and/or marketing
 - European labor and/or marketing
 - Internal audit
 - IT
 - Training
- Extended team might include representatives from legal or privacy in “onward transfer” countries
- Document, document
- Use written certification trees

3. Dealing with the Notice Requirement: Coordinating with Europe

- Safe Harbor puts the burden on the “organization” for giving European data subjects notice regarding various matters
 - Purpose for which information is collected and used
 - Contact information for inquiries and complaints
 - Third party disclosures
 - Choices for limiting use and disclosure
- “Organization” is widely accepted to refer to the US entity
- Often makes little sense for US entity to try to have direct contact with European data subjects
- Normally companies address this by entering into an arrangement with the European entities from which the information is sourced to give this notice on behalf of the US entity
- Often just a slight modification to the notice the European entity already has to give under domestic law.

4. Choice: The Need for a Plan B

- Safe Harbor requires European data subjects be given choice with respect to:
 - Disclosures to third parties other than agents such as processors performing tasks on behalf of the US organization
 - Use for a purpose not covered by the disclosure the European data subject received by or on behalf of the US organization
 - Opt out choice acceptable for personal data other than sensitive personal data, for which opt-in choice is required
- European data subjects generally have no choice with respect to having their non-sensitive personal data sent to the US under Safe Harbor
- Data subjects do have a choice with respect to onward transfers unless it goes to an organization in a country with “adequate” data protection laws or another Safe Harbor company
- Where data subjects have choice, companies may need a Plan B to get the personal information to the onward transfer entity

5. Drafting the Safe Harbor Privacy Statement

- Safe Harbor requires that the US organization publish a privacy statement covering data transferred from Europe under Safe Harbor that complies with the seven Safe Harbor Principles and the FAQ's
- Statement has to be publically available
 - An employee statement can be on an intranet site
 - Must be made available to third parties upon request
- Statement can be a general privacy statement applicable to all similar data or unique to the European personal data transferred under Safe Harbor
 - Companies must draft statements carefully to both make the promises necessary under Safe Harbor and to reflect reality
 - May not want to commit to comply with Safe Harbor Principles for all data, or even for all European data, since some data may be transferred under another legal basis, such as consent
- European sensitivities – 2004 Report urged the FTC to be more proactive in monitoring the quality of privacy policies

6. Preparing a Strategy to Deal with the Works Councils on Employee Data

- Laws and practices in Europe normally require some level of consultation with appropriate Works Councils or labor unions before employee data can be transferred to US under any basis
- Depending on industry and company this can be more of an issue than Safe Harbor compliance
- Privacy represents both a concern of labor representatives in Europe and a right that can be used as a bargaining point by such representatives to reach other objectives
- European company labor relations personnel normally engage labor in Safe Harbor consultations
 - American side must be patient: privacy normally one of many issues being addressed
 - May have want to certify for all HR data, but agree with Works Council to go forward in stages

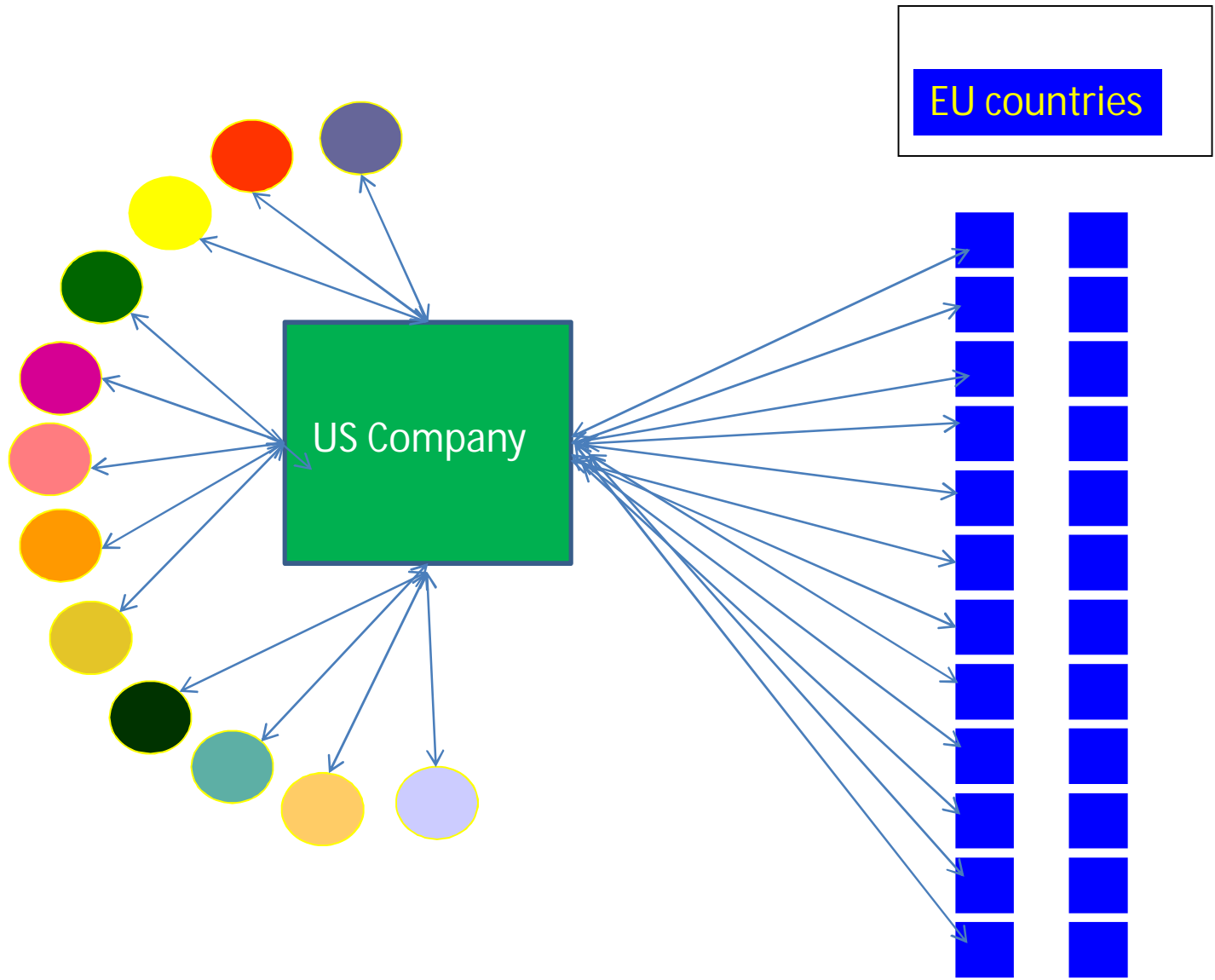
7. The Annual Objective Verification of Compliance Requirement

- Safe Harbor requires an annual certified verification by internal or external personal
- Scope of verification is complicated, but generally aimed at compliance with the Safe Harbor requirements, the training of employees and the maintenance of internal procedures for conducting objective reviews of compliance
 - A statement verifying the annual review must be signed by a corporate officer (internal review) or the external reviewer or a corporate officer (external review) and records retained
 - Many companies handle as part of their normal internal audit cycle
- Extensive pre-certification work required by privacy function to help internal auditors develop an audit program that meets the Safe Harbor requirements
 - Must translate the Safe Harbor requirements into terms that are specific to the organization and auditors can use without making their own interpretations of the rules
 - Privacy function must help train auditors and be available to answer questions
- Audit of affiliated onward transferees also important

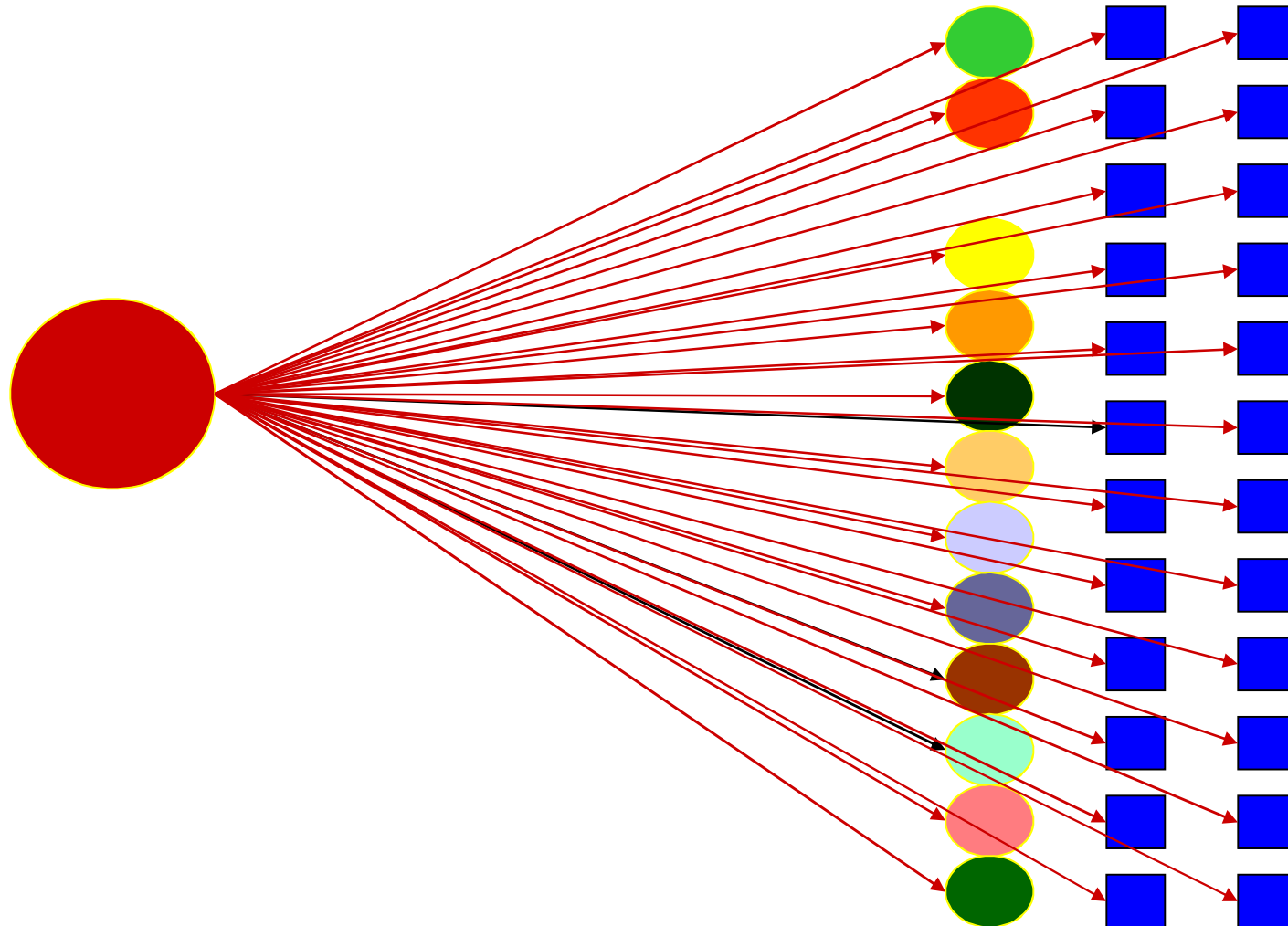
8. Onward Transfers: Extracting Multiple Uses from Onward Transfer Agreements

- For many multinationals, onward transfer agreements can be drafted to serve more than one purpose
- European onward transfer agreements can be in any form as long as they include obligations on the part of the onward transferees to comply with the Safe Harbor requirements
- These requirements are substantially similar to the laws of many countries that are based on the EU scheme and allow cross-border transfers under protective contracts
 - With some minor additions a Safe Harbor onward transfer agreement can also serve as the primary basis for transferring personal data from Australia, Argentina, Japan, etc. (a Company-Wide Transfer Agreement)
 - Most easily accomplished with a single multiparty agreement that is web based and can be signed electronically

Bilateral OTA Structure



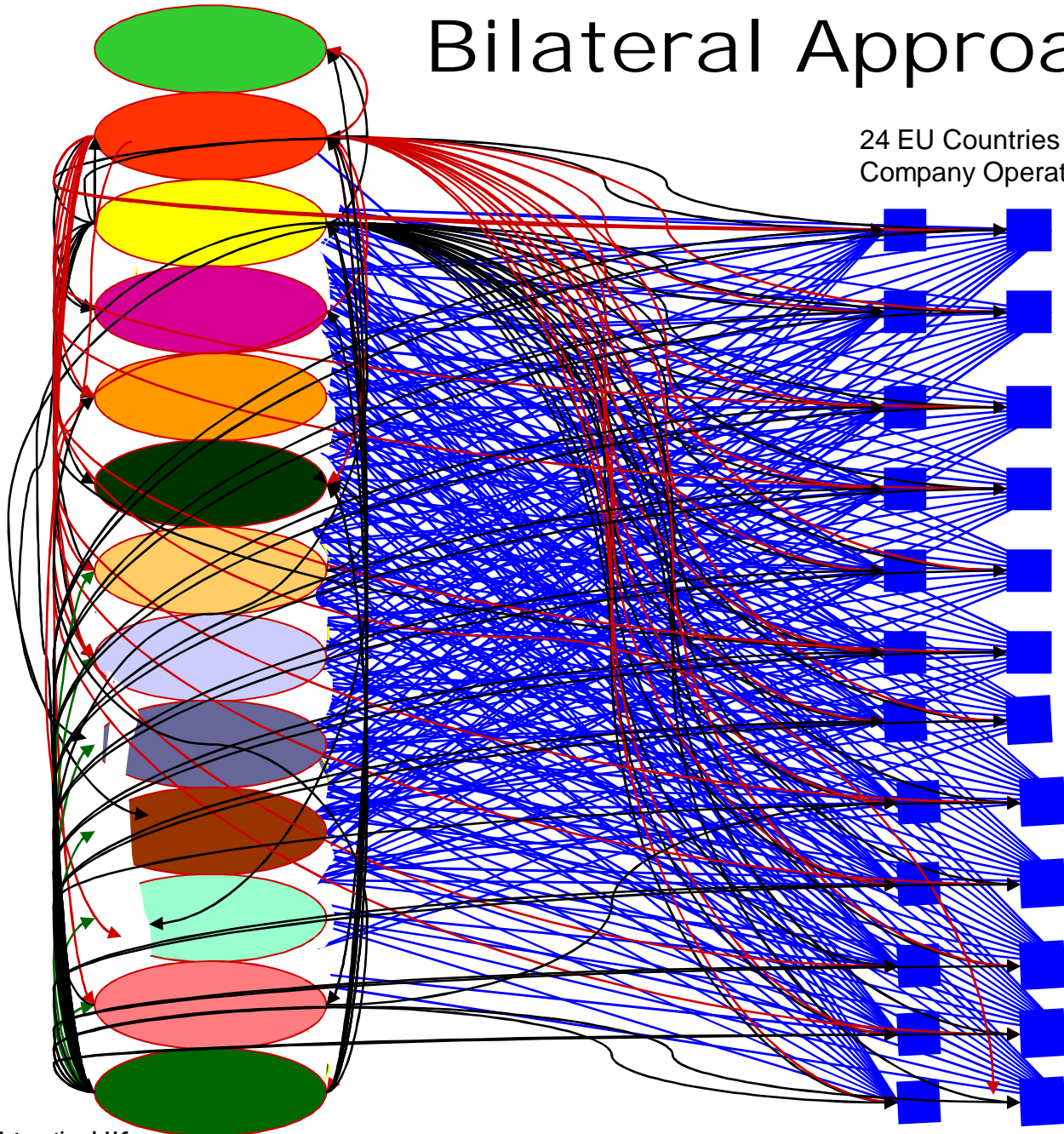
Global Companies May Have to Put Other Compliance Contracts in Place e.g. Australia



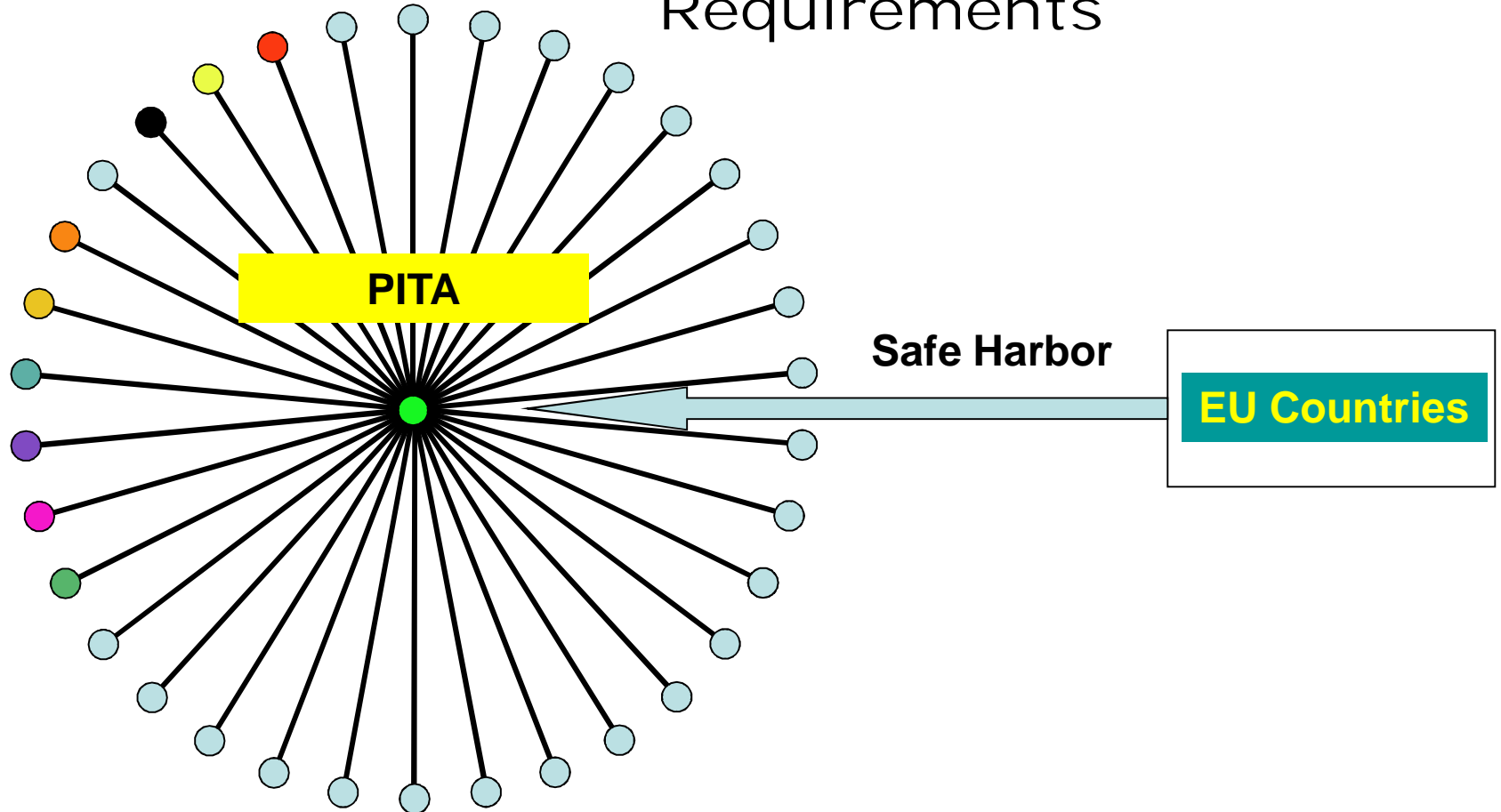
Bilateral Approach

24 EU Countries In which US Company Operates

Countries which require contract for cross-border transfers



PITA Structure Addresses OTAs and National Requirements



9. Ongoing Internal Requests for EU Personal Data: Governance and Record-Keeping

- Internal company gatekeeper required to control access to EU personal data once it is transferred to US
- Must assure that any accessing of the EU data is for a purpose that has been notified to the data subjects and, where necessary, discussed with the appropriate Works Councils
- Must make certain that any users of the information are fully aware of the handling requirements and restrictions on further transfers

10. Training & Communication

- Develop and implement training for those individuals handling personal information transferred from the EU
- Training should include
 - An overview of Safe Harbor and its Principles
 - Overview of Organization's Safe Harbor Certification
 - Obligations for handling personal information in accordance to the principles of Safe Harbor
 - Organization's processes and policies regarding providing notice, choice, access and security
- Training should be required for all persons who handle or process information and completion rates tracked
- Establish ongoing communication
 - Remind individuals handling data of their obligations
 - Communicate changes in data transferred, processes or policies

11. Cooperation with the European DPAs

- The Enforcement Principle requires that a US Safe Harbor organization must provide, among other things:
 - Recourse for individuals to whom the data relates
 - An obligation to remedy problems arising out of their non-compliance with Safe Harbor obligations
- With respect to organizations handling employee personal data, these obligations must be satisfied by agreeing to “cooperate” with European DPAs
- For non-employee data, companies have a choice and can utilize self program facilities, internal mechanism followed by reference to FTC, or other scheme
- Early concern about what it means to “cooperate” (pay fines?) was replaced with a complacency when there were no European data subject complaints
- European authorities becoming more active with respect to Safe Harbor (Duesseldorfer Kreis, CNIL investigation) and US companies should carefully consider the cooperation alternative if they have a choice

Conclusion

- Safe Harbor is a flexible legal basis for transferring European personal information to the US and beyond
- The requirements can be complicated and companies must be prepared to strictly comply before they allow their officers to certify
- Expect increased scrutiny of compliance in the immediate future
- Expect changes if and when the EU Data Protection Directive is modified

Questions and Answers

Robert Rothman, Principle
Privacy Associates International, LLC
rrothman@privassoc.com
www.privassoc.com, (248) 880-3942



Privacy Associates International, LLC

40777 Lenox Park Drive, Suite 100
Novi, Michigan 48377 USA

Kimberly Bubnes, Global Privacy Director
General Motors Company
kimberly.bubnes@gm.com

