



Achieving Safe Harbor Compliance

Dan Lobb

IT Compliance Analyst
Coca-Cola Enterprises

dlobb@cokece.com
770-370-6415



Bozo had an eventful first day as the circus's privacy officer



Checklist to achieve Safe Harbor

If you then decide to join the safe harbor, you should:

1. Bring your organization's policies and practices into compliance with the Safe Harbor's Requirements
2. Verify that your organization has done so
3. If you wish to assure your organization of safe harbor benefits, review the Information Required for Certification and complete and submit the Certification Form.

Source: http://www.export.gov/safeharbor/eg_main_018274.asp



- ❑ What is Safe Harbor?
- ❑ Why certify?
- ❑ Defining personally identifiable information (PII)
- ❑ How to determine an approach
- ❑ Which processes are impacted?
- ❑ Considerations for sustainability
- ❑ Safe Harbor listings
- ❑ Links and other details



“Organizations must take reasonable precautions to protect personal information”

7 Principles of compliance agreed to by the US Department of Commerce and the EU Data Privacy Council, based on the EU based privacy legislation known as the Directive on Data Protection (aka the Directive)



Notice

Inform individuals about the data we keep, why we keep it, and who can see it.

Choice

Give individuals a choice to opt out of having their data shared with a third party.

Onward Transfer (Transfers to Third Parties)

When sharing information with a third party, organizations must apply the notice and choice principles. The third party must also subscribe to safe harbor principles or contract to provide same level of protection.

Access

Individuals must have access to their personal data in order to maintain its accuracy.



Security

Organizations must take reasonable precautions to protect personal information.

Data Integrity

Data must be relevant and reliable for its intended use.

Enforcement

Recourses and mechanisms must be available so that CCE commitments are understood and maintained, individual complaints and disputes can be investigated and resolved, and the annual self certification must be completed.



Why certify?

- Concern from global legal teams
- Cumbersome and expensive data transfer agreements
- Lack of confidence around compliance with data transfer agreements
- Employee and customer data coming from EU countries into the US
- Desire to show employees and customers that data protection is a priority (CRS)



EU Data Privacy Definition

Personal data shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.



Moving
from theory
to
specifics...

Key Considerations

- Input from subject matter experts
 - Industry based research
- Observations of company specific data elements



Defining what PII means to your organization

Information Classified into Types

Personal Identification

Name

Location

Contact

Demographic

Financial

Healthcare

Performance

Miscellaneous

Healthcare Information

- Health insurance information
- Health status
- Patient medical records
- Patient coverage

Performance Information

- Performance reviews
- Performance ratings

Personal Identifiers

- National ID number
- Employee ID number
- Fingerprint
- Picture

Location

- Street address
- City, State, Zip
- Country

Demographic Information

- Date of birth
- Gender/Race/Ethnicity
- Political/Religious affiliation
- Marital status
- Physical traits
- Residence Status
- Education Level

Miscellaneous and Indirect

- Employment start/end date
- Bank name/type
- Bank account type
- Employee status
- Employee subgroup
- Pay frequency
- Organization information
- Job title
- Previous employer/work history
- Background Check Results
- Drug Test Results
- DMV Information

Name

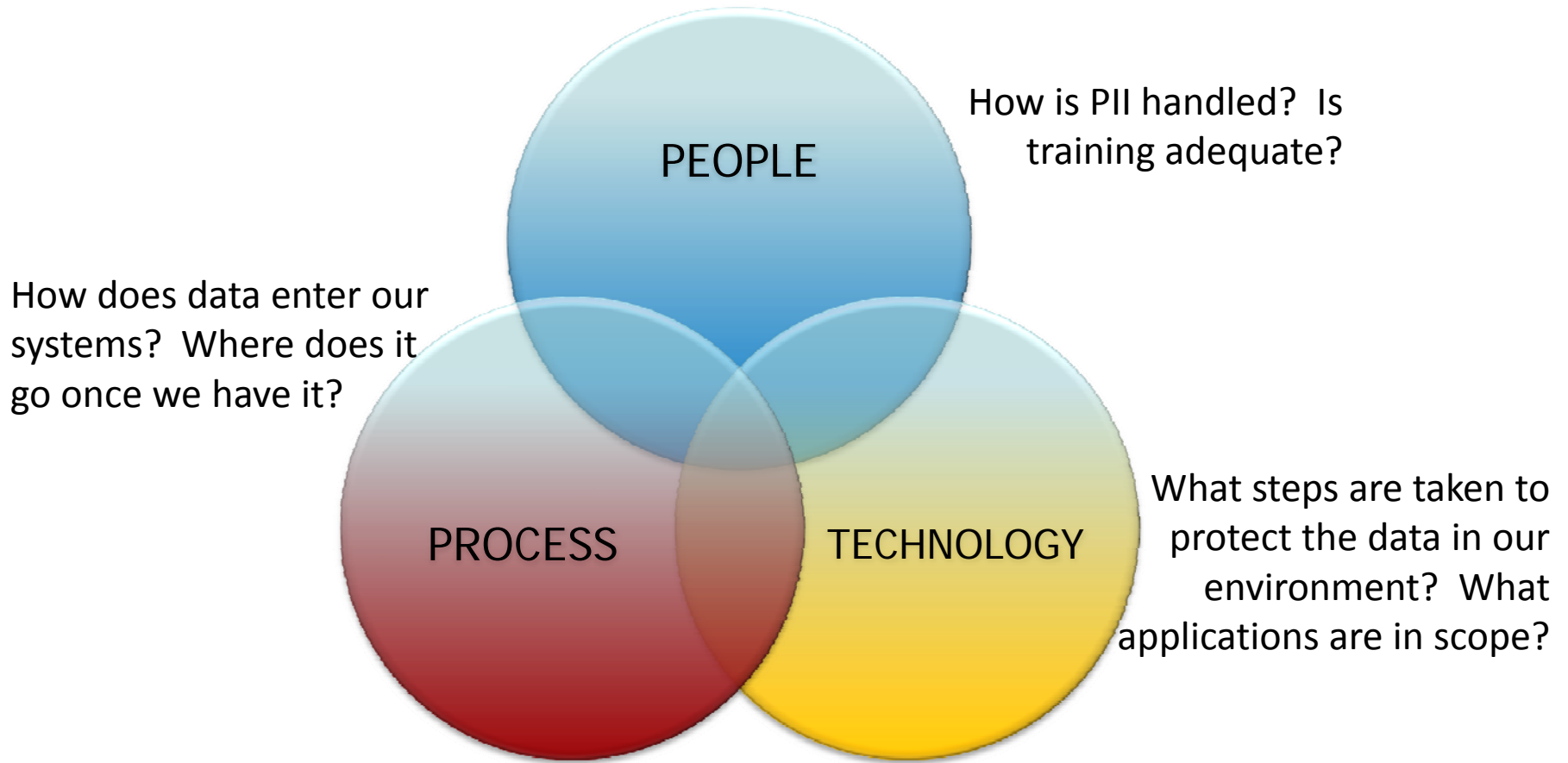
- First/Middle/Last name
- Known As name
- Maiden name
- Children name

Contact Information

- Email address
- Phone number

Financial Information

- Compensation information
- Credit rating
- Bank account number
- Credit card number/expiration
- Debit card number/expiration



Our approach included analysis of HR processes, people, and technology to better understand how we take in, handle and use EU employee personally identifiable information.



Human Resources

Reviewed European human resource, payroll and benefit management practices

Analyzed points of entry and egress

Quantified policies/materials presented to employees

Technology

Analyzed transfers to 3rd parties

Reviewed security measures for data storage and handling

Assessed relevance of policies and standards

Survey of application/data owners

Legal

Evaluated procurement process for contract and vendor management considerations



Human Resources

Prospective employees are asked to accept CCE data privacy statement but it does not mention Safe Harbor principles

Code of Business Conduct includes language for the proper use of data

Process in place to allow for employees to access, review and update their PII

Training for employees that handle PII is not available

Technology

3rd party transfers for benefit management do not pass EU data

EU Employee PII is primarily housed in SAP, subject to centralized security and governance practices

Data Classification and Handling policies call out PII but a Data Privacy Policy does not exist

Ongoing PII inventory process needed

Legal

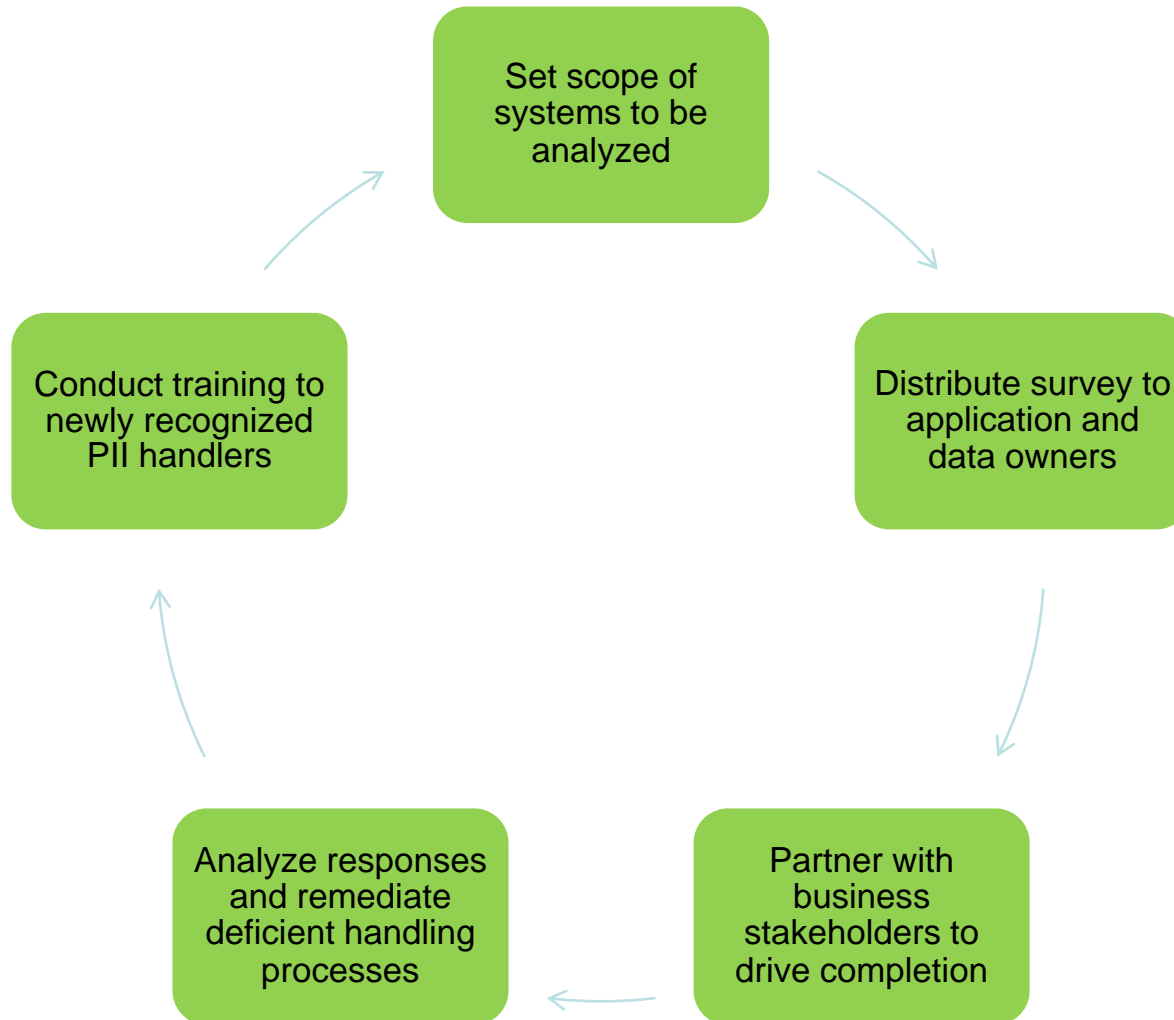
Contract language does not specifically address data privacy and Safe Harbor principles

3rd party vendors are not evaluated for Safe Harbor compliance

Observations noted prior to remediation efforts



Finding Data Outside of the Core HR Process





Approach

- Set scope of information systems to be reviewed
 - Determine frequency of review
 - Partner with stakeholders to manage assessment through survey and interaction with application and data owners
- Quantify type and amount of PII that is stored
 - Quantify who has access to PII
- Ensure proper training is conducted for those with access to PII
 - Consider PII implications in change management and architecture discussions

Application Relevance (Do we care about this application?)	
PII Existence	Name of Application:
	Contains PII? Y/N (If Y, proceed below)
PII Data Volume (How much PII data is there?)	
HR Data Volume	Approximate Number of Employee Records
	PII Data Elements per Employee Record
PII Data Storage (Where does the PII get stored?)	
Repository (Where)	SAP HR
	Taleo
	Excel Reports
	Access Database
	Third Party
	Hard Copy/Paper
	Other (Please name)
Storage (How)	Physical - Unlocked/Unsecure
	Physical - Locked/Secure
	Electronic - Unlocked/Unsecure
	Electronic - Locked/Secure
	Third Party
Retention Period (How long)	Retained Indefinitely
	Retained for Set Time Period (Please name)
PII Data Access (Who can see it?)	
PII Data Access	Number of Employees with PII Data Access
	Frequency of Access
	View Access
	Modify/Write Access
	Reporting Access
	Third Party Access
PII Data Movement (Where does the PII flow?)	
Internal Movement	Inter-department
	Intra-department
	No Internal Movement
External Movement	Third Party
	If Yes, does contract mention data privacy?
	No External Movement
Method of Movement	Physical
	Electronic (FTP/other)
	Email
	Encrypted? (Y/N)



Information Available from Safe Harbor List

Contact Information:

Contact Office: The **Coca**-Cola Company

Contact Name: John Doe, Sr. Employment Counsel, Office of the General Counsel

Phone: 404-676-1XXX Fax: 404-598-1XXX Email: jdoe@na.ko.com

Corporate Officer Information:

Corporate Officer: Chief Information Officer

Phone: 40467634XX Fax: 4045983434 Email: jarxx@na.ko.com

Safe Harbor Information:

Signed up to safe harbor 10/03/2007 03:22:15 PM

Next certification 10/03/2009

EU/EEA Countries From Which Personal Information Is Received: Cyprus, Finland, Hungary, Latvia, Malta, Portugal, Spain, Austria, Czech Republic, France, Iceland, Liechtenstein, Netherlands, Romania, Sweden, Belgium, Denmark, Germany, Ireland, Lithuania, Norway, Slovakia, United Kingdom, Bulgaria, Estonia, Greece, Italy, Luxembourg, Poland, Slovenia

Industry Sector: General Consumer Goods - (GCG)

Personal Information Received From the EU: The **Coca**-Cola Company uses consumer and customer data primarily for customer support activities, such as fulfilling product orders, administering programs in which consumers have elected to participate, and marketing activities. The **Coca**-Cola Company uses human resources data for employee management and administration generally.

Privacy Policy Effective: January 2007

Location: The **Coca**-Cola Company intranet

Regulated by: Federal Trade Commission

Privacy Programs: none

Verification: In-house

Dispute Resolution: JAMS (Judicial Arbitration and Mediation Services)

Personal Data Covered: human resources data): Human Resources Data, Consumer Data, Customer Data on-line & off-line

Human Resource Data Covered: Yes

Do you agree to cooperate and comply with the European Data Protection Authorities? Yes

Certification Status: Current



Key Links

- Quickly check the status of a company:
<https://www.export.gov/safehrbr/list.aspx>
- US Department of Commerce – Safe Harbor Website:
<http://www.export.gov/safeharbor/>



Appendix



Notice

An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party(1).

(1) It is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. The Onward Transfer Principle, on the other hand, does apply to such disclosures.

Choice

Organizations must give individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual.

For sensitive information (i.e. personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), they must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of opt in choice. In any case, an organization should treat as sensitive any information received from a third party where the third party treats and identifies it as sensitive.



Safe Harbor Principles

Onward Transfer (Transfer to Third Parties)

To disclose information to a third party, organizations must apply the Notice and Choice Principles. Where an organization wishes to transfer information to a third party that is acting as an agent, as described in the endnote, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles. If the organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing.

Access

Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

Security

Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.

Data Integrity

Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

Source: http://www.export.gov/safeharbor/eu/eg_main_018475.asp



Safe Harbor Principles

Enforcement

Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.