PRIVACY INSIGHT SERIES

Summer / Fall 2017 Webinar Program

Mastering Article 30 Compliance:

Conducting, Maintaining & Reporting on Your Data Inventory

August 16, 2017

TrustArc
the new TRUSTe

Thank you for joining the webinar

“Mastering Article 30 Compliance: Conducting, Maintaining and Reporting on your Data Inventory”

- We will start 2-3 minutes after the hour
- This webinar will be recorded – both the recording and slides will be sent out via email later today
- Please use the *GotoWebinar* Control Panel on the right hand side to submit any questions for the speakers

Today’s Speakers

Charles Nwasor

Director, Global Assurance & Advisory

Ensono

Paul Iagnocco

Senior Privacy Consultant

TrustArc

Margaret Alston, CIPP/G/C/M

Consulting Program Director

TrustArc

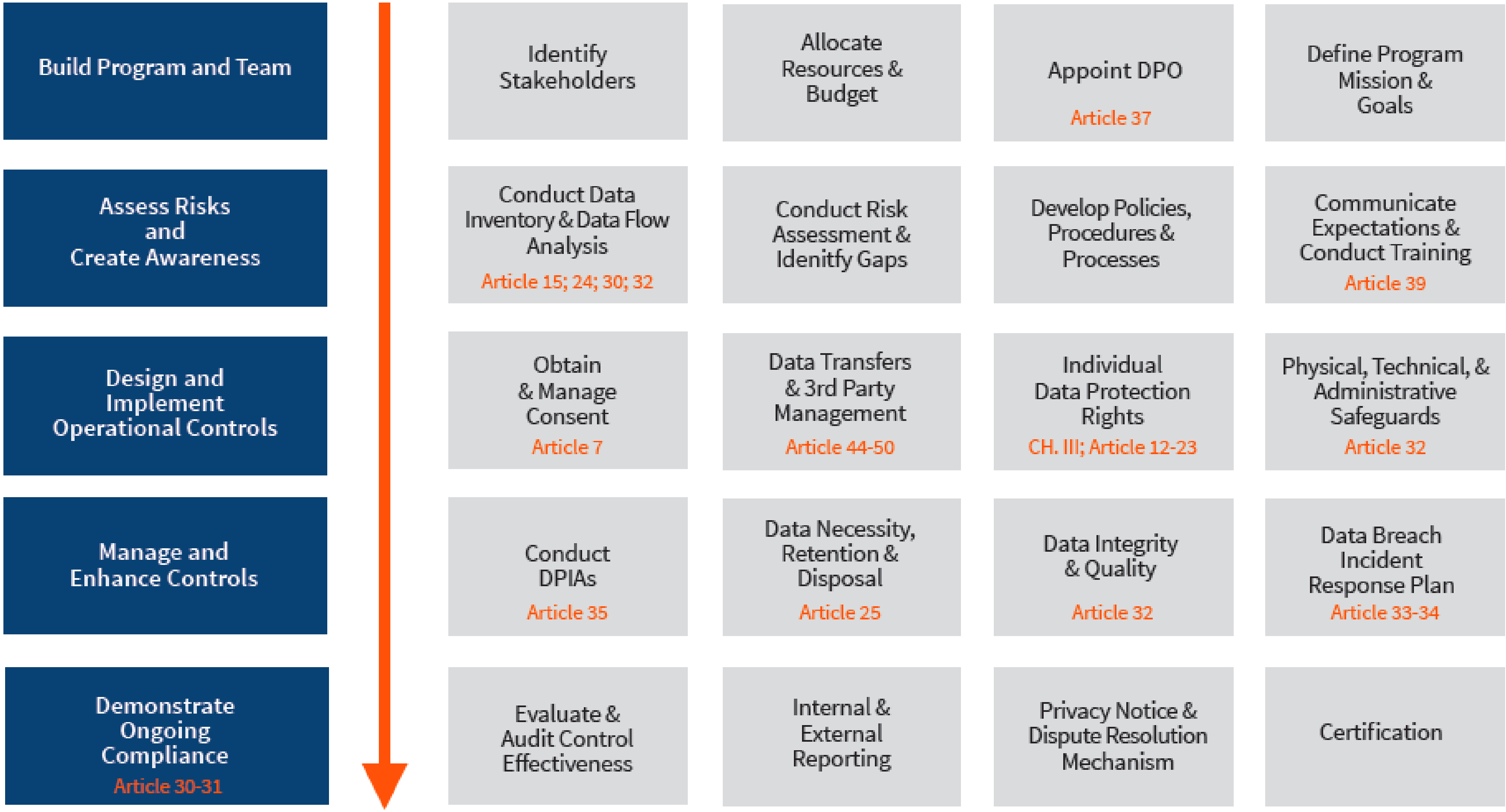
Eleanor Treharne-Jones

VP Sales & Consulting

TrustArc

The EU GDPR – May 25, 2018 Deadline

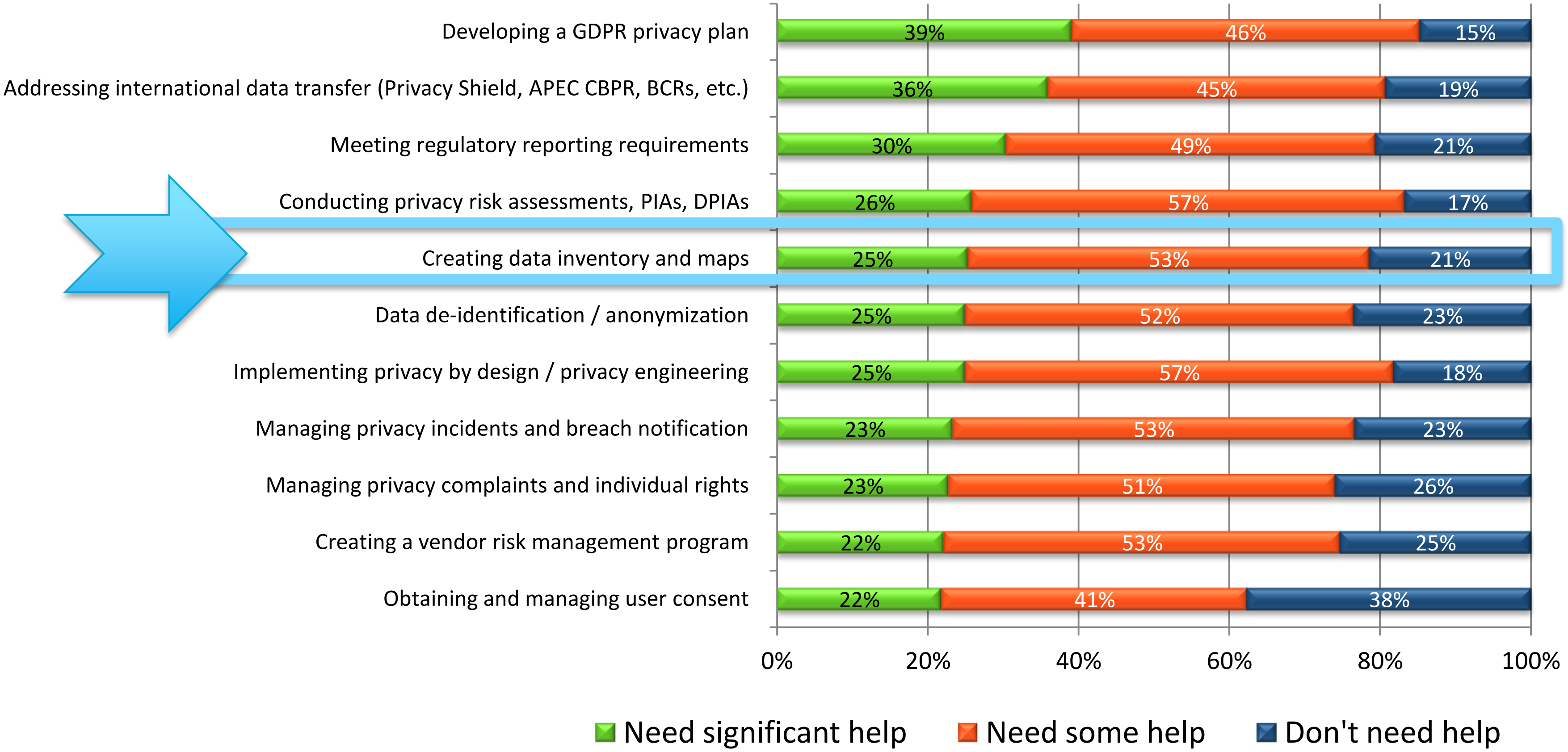
Significant Compliance Requirements



Build Program and Team	Identify Stakeholders	Allocate Resources & Budget	Appoint DPO Article 37	Define Program Mission & Goals
Assess Risks and Create Awareness	Conduct Data Inventory & Data Flow Analysis Article 15; 24; 30; 32	Conduct Risk Assessment & Idenitfy Gaps	Develop Policies, Procedures & Processes	Communicate Expectations & Conduct Training Article 39
Design and Implement Operational Controls	Obtain & Manage Consent Article 7	Data Transfers & 3rd Party Management Article 44-50	Individual Data Protection Rights CH. III; Article 12-23	Physical, Technical, & Administrative Safeguards Article 32
Manage and Enhance Controls	Conduct DPIAs Article 35	Data Necessity, Retention & Disposal Article 25	Data Integrity & Quality Article 32	Data Breach Incident Response Plan Article 33-34
Demonstrate Ongoing Compliance Article 30-31	Evaluate & Audit Control Effectiveness	Internal & External Reporting	Privacy Notice & Dispute Resolution Mechanism	Certification

Help is Needed Across Wide Range of Areas

78% of Companies looking for help with Data Inventory & Mapping



Question: *“Below is a list of tasks related to data privacy compliance. For each task please indicate the amount of additional help you will need to accomplish these tasks in 2017.”*

TrustArc / Dimensional Research 2017

Today's Agenda

- What's Required Under Article 30 of the GDPR?
- Tools & Methodologies
- Getting Internal Buy-in
- Scoping and Prioritization
- Addressing Third Parties
- What is a Data Map?
- You've completed a Data Inventory Mapping Exercise – What's Next?

Poll Question

Have you completed a data inventory yet?

A. We haven’t started

B. We have an existing inventory that we’re looking to update

C. We have allocated resources (people/technology) to complete this

D. We are in the process of completing our inventory

E. We have a completed data inventory

TrustArc / Dimensional Research 2017

PRIVACY INSIGHT SERIES

Summer / Fall 2017 Webinar Program

What’s required under Article 30 of the GDPR?

TrustArc
the new TRUSTe

GDPR Article 30 – What's Actually Required?

Art. 30 GDPR = Records of Processing Activities

- Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility.

- Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller

- The records shall be in writing, including in electronic form.

- **The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.**

- The obligations shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

What’s Actually Required?

- Applies equally to controllers and processors
- What’s meant by a “record”?
- Available on demand following request from a regulator
- No explicit requirement for data mapping
- Certain exemptions for SMEs

Records of Processing Activities for Controllers

Each **controller** and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

- the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
- the purposes of the processing;
- a description of the categories of data subjects and of the categories of personal data;
- the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
- where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
- where possible, the envisaged time limits for erasure of the different categories of data;
- where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

Records of Processing Activities for Processors

Each **processor** and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

- the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
- the categories of processing carried out on behalf of each controller;
- where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
- where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

PRIVACY INSIGHT SERIES

Summer / Fall 2017 Webinar Program

Approach, Methodology & Tools

TrustArc
the new TRUSTe

Systems vs Business Process Inventory

IT/Systems Based Approach

"Show me all the **systems and applications** being used to process or store our data."

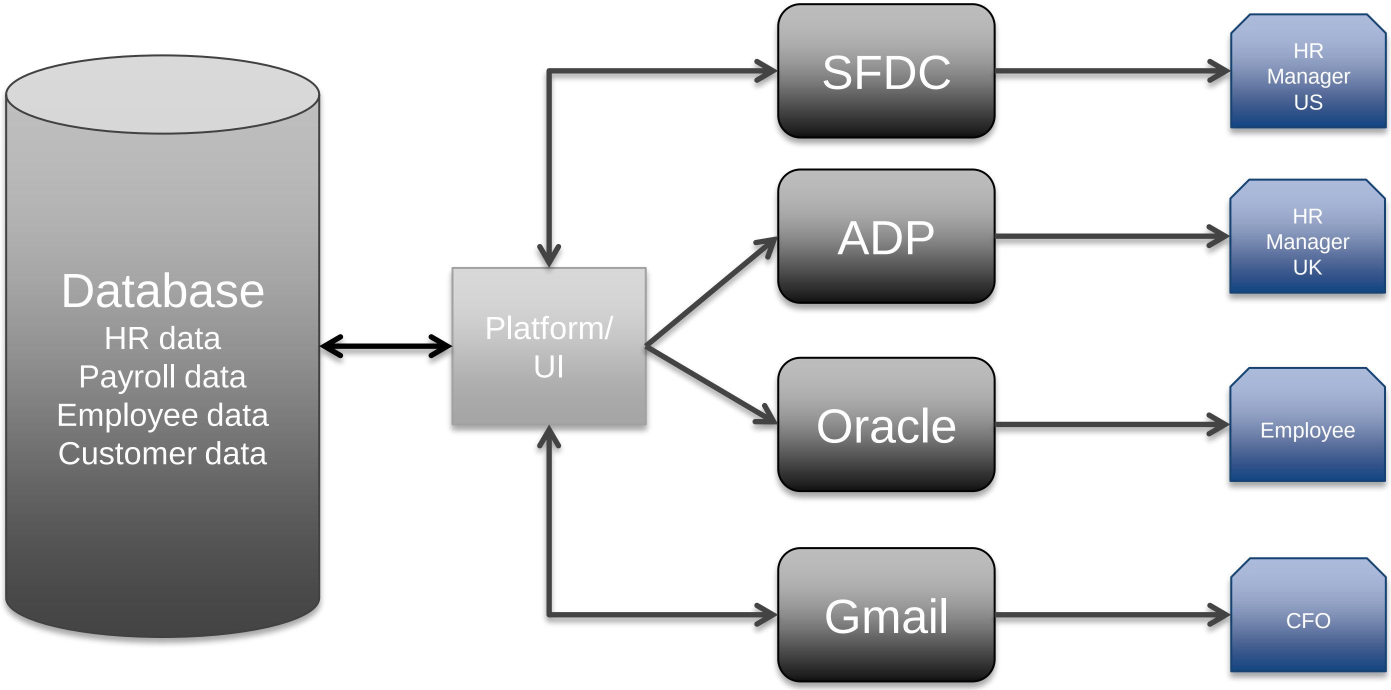
Process Based Approach

"Show me all of our **business processes** that contain personal information."

Systems vs Business Process Inventory

IT/Systems Based Approach:

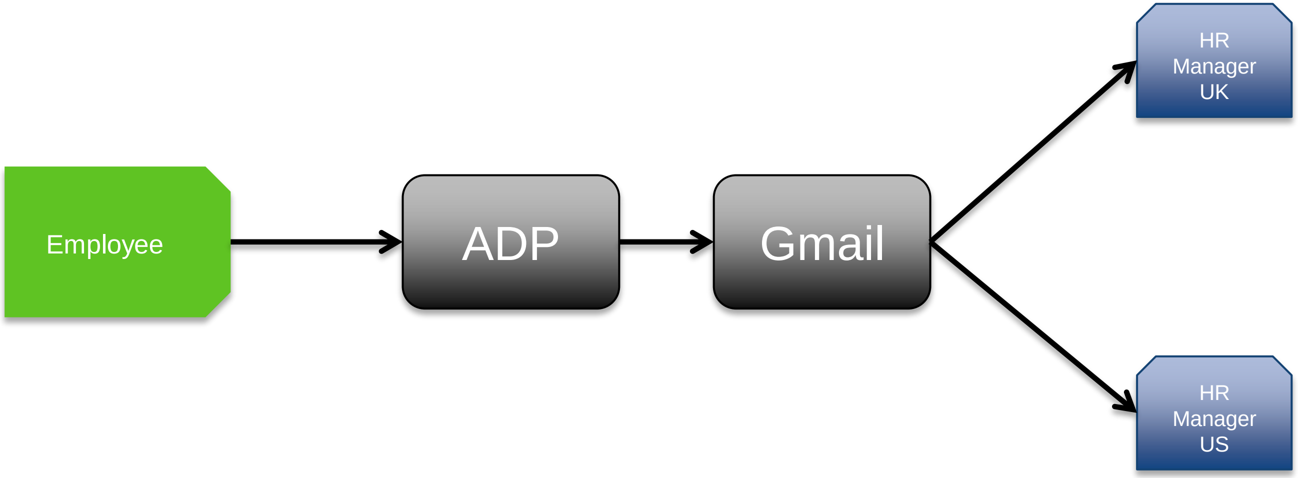
“Show me all the systems and applications being used to process or store our data”



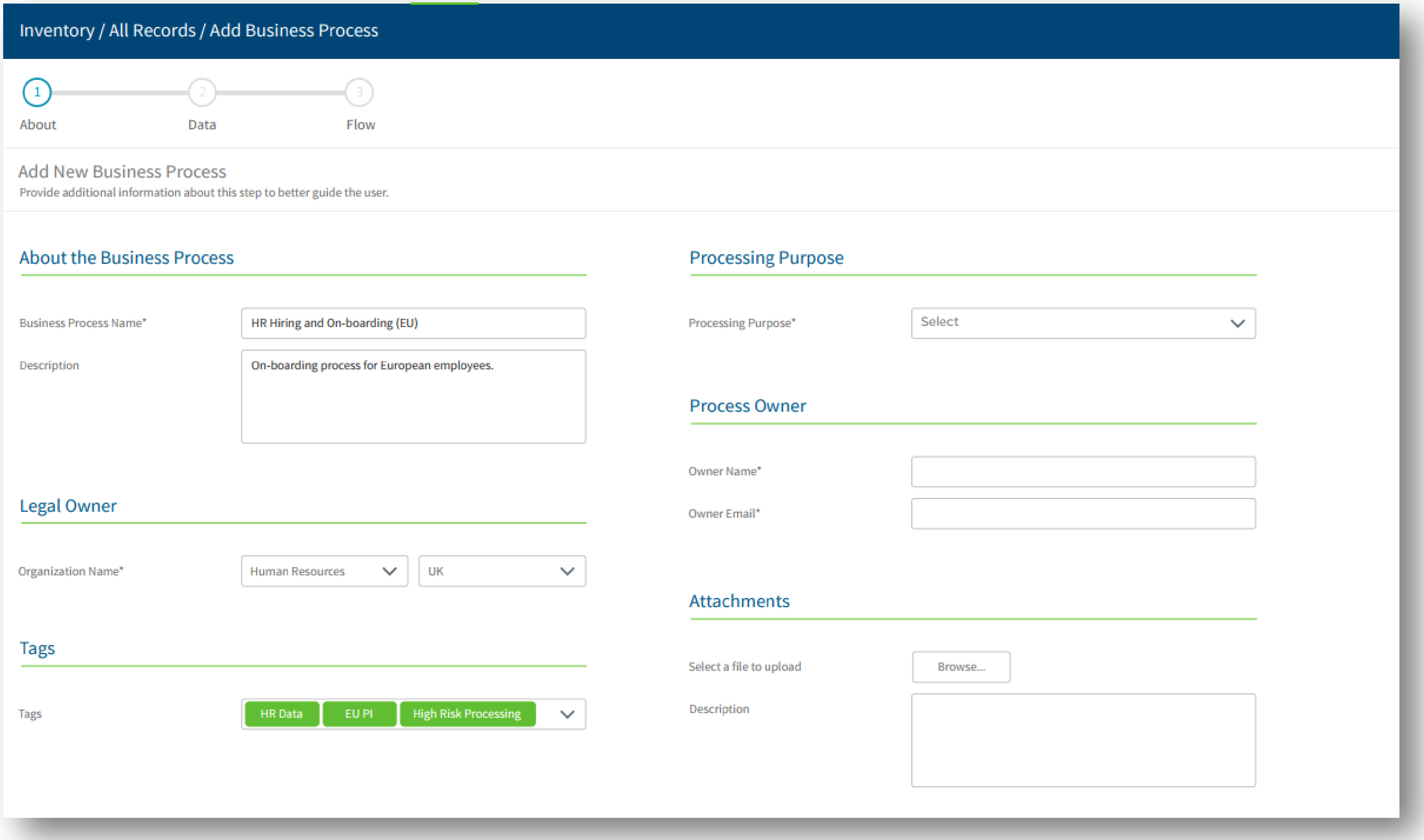
Systems vs Business Process Inventory

Process Based Approach:

“Show me all of our business processes that contain personal information”



Sample Business Process Documentation



Inventory / All Records / Add Business Process

Add New Business Process

Provide additional information about this step to better guide the user.

About the Business Process

Business Process Name*: HR Hiring and On-boarding (EU)

Description: On-boarding process for European employees.

Legal Owner

Organization Name*: Human Resources | UK

Tags

Tags: HR Data | EU PI | High Risk Processing

Processing Purpose

Processing Purpose*: Select

Process Owner

Owner Name*:

Owner Email*:

Attachments

Select a file to upload: Browse...

Description:

Poll Question

What approach have you taken to your data inventory?

A. Business Process inventory

B. Asset/systems inventory

C. Not yet started a data inventory

TrustArc / Dimensional Research 2017

Methodology & Tools

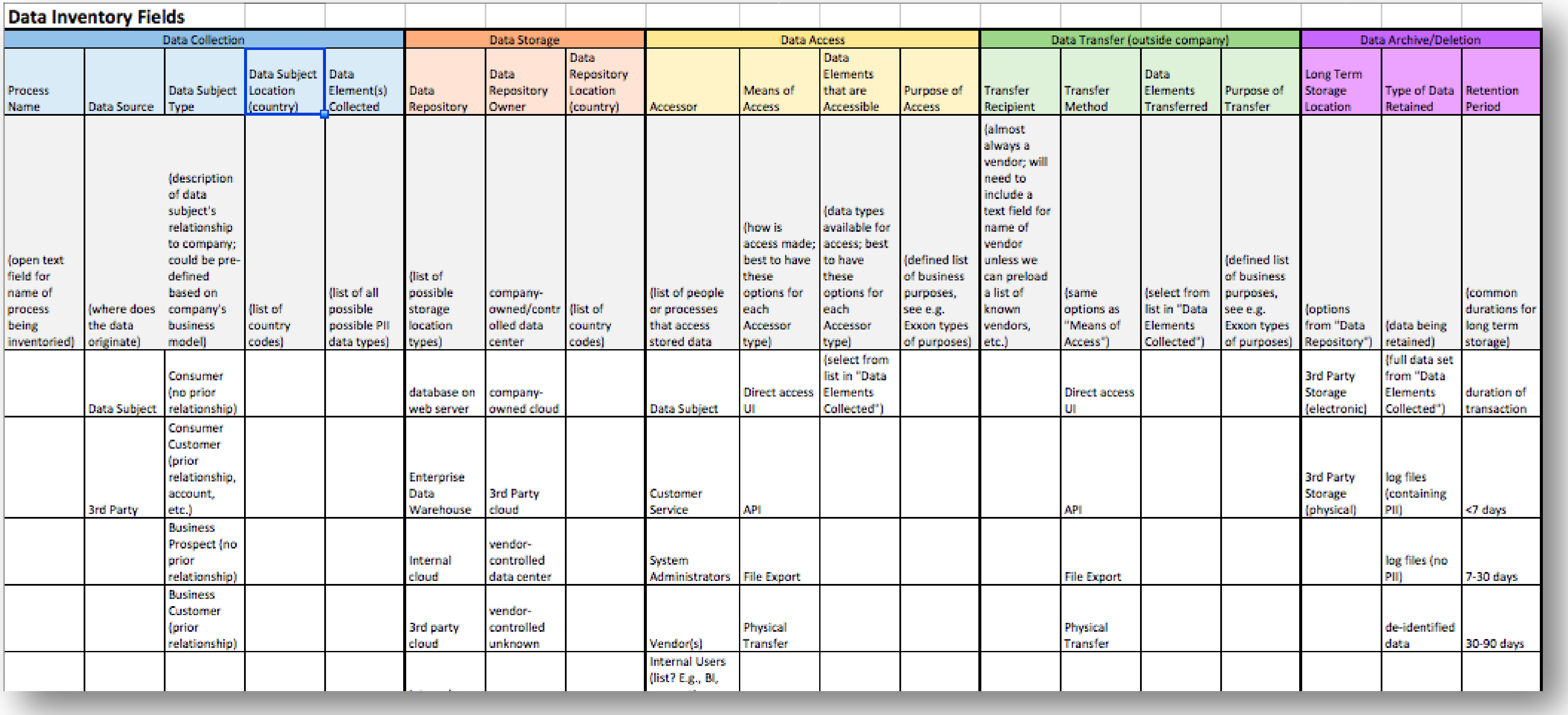
Discovery Process

- Questionnaires
- Interviews
- Automated Scanning
- Automated Feeds/Uploads

Ongoing maintenance

- Spreadsheets
- Data Inventory & Mapping Tools

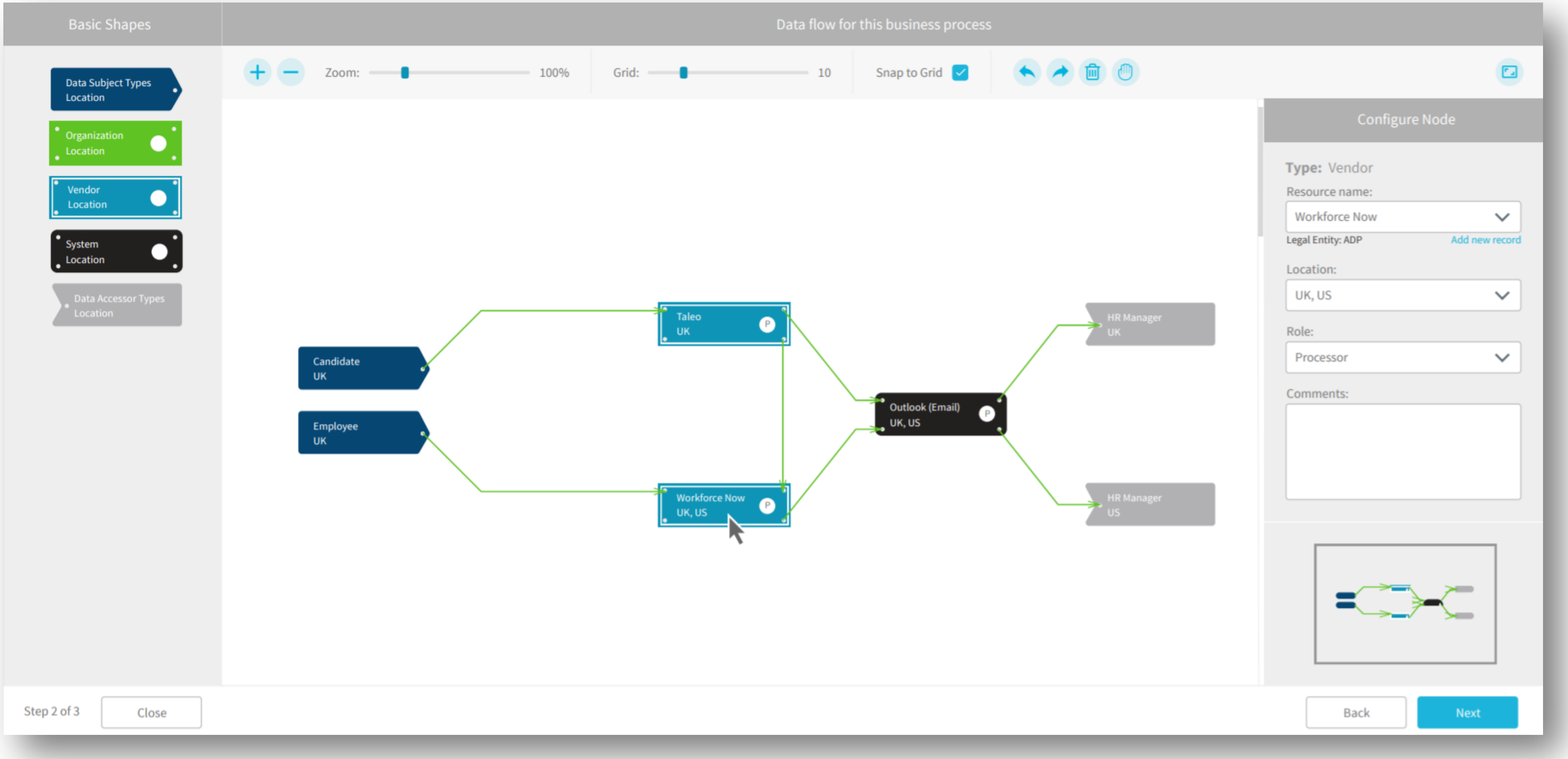
Sample Data Inventory Spreadsheets



Data Inventory Fields

Data Collection					Data Storage			Data Access				Data Transfer (outside company)				Data Archive/Deletion		
Process Name	Data Source	Data Subject Type	Data Subject Location (country)	Data Element(s) Collected	Data Repository	Data Repository Owner	Data Repository Location (country)	Accessor	Means of Access	Data Elements that are Accessible	Purpose of Access	Transfer Recipient	Transfer Method	Data Elements Transferred	Purpose of Transfer	Long Term Storage Location	Type of Data Retained	Retention Period
(open text field for name of process being inventoried)	(where does the data originate)	(description of data subject's relationship to company; could be pre-defined based on company's business model)	(list of country codes)	(list of all possible possible PII data types)	(list of possible storage location types)	company-owned/controlled data center	(list of country codes)	(list of people or processes that access stored data	(how is access made; best to have these options for each Accessor type)	(data types available for access; best to have these options for each Accessor type)	(defined list of business purposes, see e.g. Exxon types of purposes)	(almost always a vendor; will need to include a text field for name of vendor unless we can preload a list of known vendors, etc.)	(same options as "Means of Access")	(select from list in "Data Elements Collected")	(defined list of business purposes, see e.g. Exxon types of purposes)	(options from "Data Repository")	(data being retained)	(common durations for long term storage)
	Data Subject	Consumer (no prior relationship)			database on web server	company-owned cloud		Data Subject	Direct access UI	(select from list in "Data Elements Collected")			Direct access UI			3rd Party Storage (electronic)	(full data set from "Data Elements Collected")	duration of transaction
	3rd Party	Consumer Customer (prior relationship, account, etc.)			Enterprise Data Warehouse	3rd Party cloud		Customer Service	API				API			3rd Party Storage (physical)	log files (containing PII)	<7 days
		Business Prospect (no prior relationship)			Internal cloud	vendor-controlled data center		System Administrators	File Export				File Export				log files (no PII)	7-30 days
		Business Customer (prior relationship)			3rd party cloud	vendor-controlled unknown		Vendor(s)	Physical Transfer				Physical Transfer				de-identified data	30-90 days
								Internal Users (list? E.g., BI,										

Sample Business Process Mapping



Type: Vendor

Resource name: Workforce Now

Legal Entity: ADP

Location: UK, US

Role: Processor

Comments:

PRIVACY INSIGHT SERIES

Summer / Fall 2017 Webinar Program

Getting Internal Buy-In

TrustArc
the new TRUSTe

Getting Buy-In

Business Unit	Engagement Focus	Benefits to BU & Business
Information Technology	identifying storage redundancies	• Reduce infrastructure complexity • Cost savings
Information Security	understanding what data reside in which systems	• Prioritize protection efforts – focus on high risk, high value • Establish appropriate access controls • Cost savings
Operations	visualizing flows and uses of data throughout the company	• Reduce redundancies • Improve efficiencies • Cost savings
Procurement	identifying points at which the company shares information with third party vendors and understanding the sensitivity of the data being shared	• Support risk-based vendor management • Greater efficiency in contract management • Cost savings

PRIVACY INSIGHT SERIES

Summer / Fall 2017 Webinar Program

Scoping & Prioritization

TrustArc
the new TRUSTe

Knowing where to start…

- Identify any previous **inventories or documentation** within the business that you can leverage – examples include:
  - asset inventory (typically held by IT)
  - vendor lists
- Start by identifying the people you want to speak to (**key stakeholders**) within each of your business units and use these numbers to start to build approximate numbers and details of business processes in scope
- Consider starting with a **pilot project** with one business unit to test and validate your methodology and use early deliverables to secure better engagement for the broader project

PRIVACY INSIGHT SERIES

Summer / Fall 2017 Webinar Program

Addressing Third Parties

TrustArc
the new TRUSTe

Addressing Third Parties

- Need to know which third party vendors are either in the EU or that may handle EU personal data
- Make an inventory, then classify the vendors
- Develop customized policy and procedures for initial vendor vetting, on-going reviews and audits, and end-of-relationship activities

Poll Question

What are the main obstacles that you have encountered?

A. Lack of budget

B. Lack of engagement

C. Managing alongside business priorities

D. Scoping

E. Tools to manage on an ongoing basis

TrustArc / Dimensional Research 2017

PRIVACY INSIGHT SERIES

Summer / Fall 2017 Webinar Program

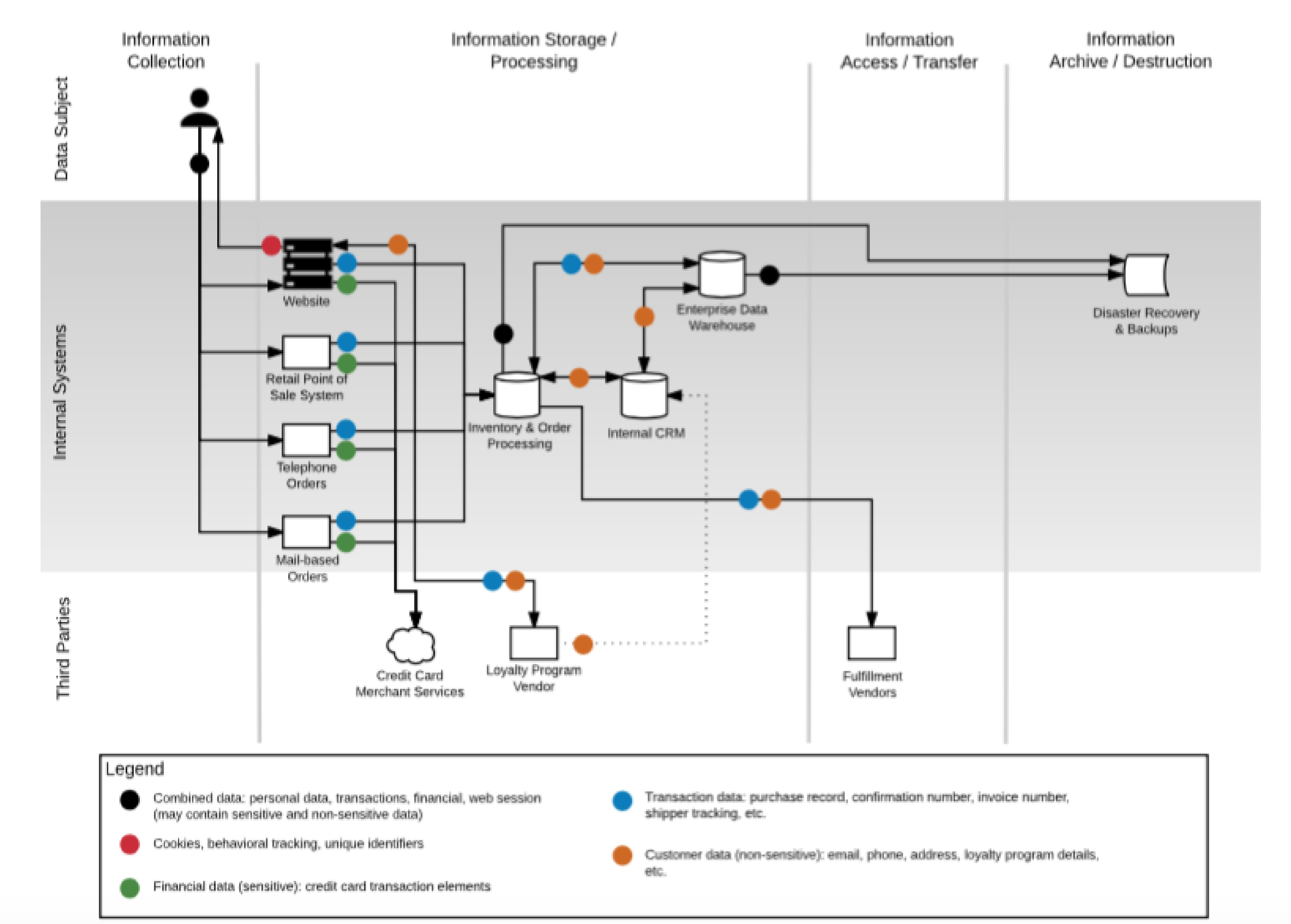
What’s a Data Map?

TrustArc
the new TRUSTe

Data Mapping

- The GDPR doesn’t actually require data maps rather a “record of processing activities”
- However it is hard to capture the multi-linear connections between different data flows and assets without some form of visualization
- Data visualizations or “maps” help companies to understand the data they hold and build in controls to manage any inherent risk
- Many different approaches exist – common tools include *Visio* and *LucidChart*

Data Mapping – TrustArc Today


Information Collection
Information Storage / Processing
Information Access / Transfer
Information Archive / Destruction
Data Subject
Internal Systems
Third Parties
Website
Retail Point of Sale System
Telephone Orders
Mail-based Orders
Inventory & Order Processing
Enterprise Data Warehouse
Internal CRM
Disaster Recovery & Backups
Credit Card Merchant Services
Loyalty Program Vendor
Fulfillment Vendors

Legend

⚫ Combined data: personal data, transactions, financial, web session (may contain sensitive and non-sensitive data)

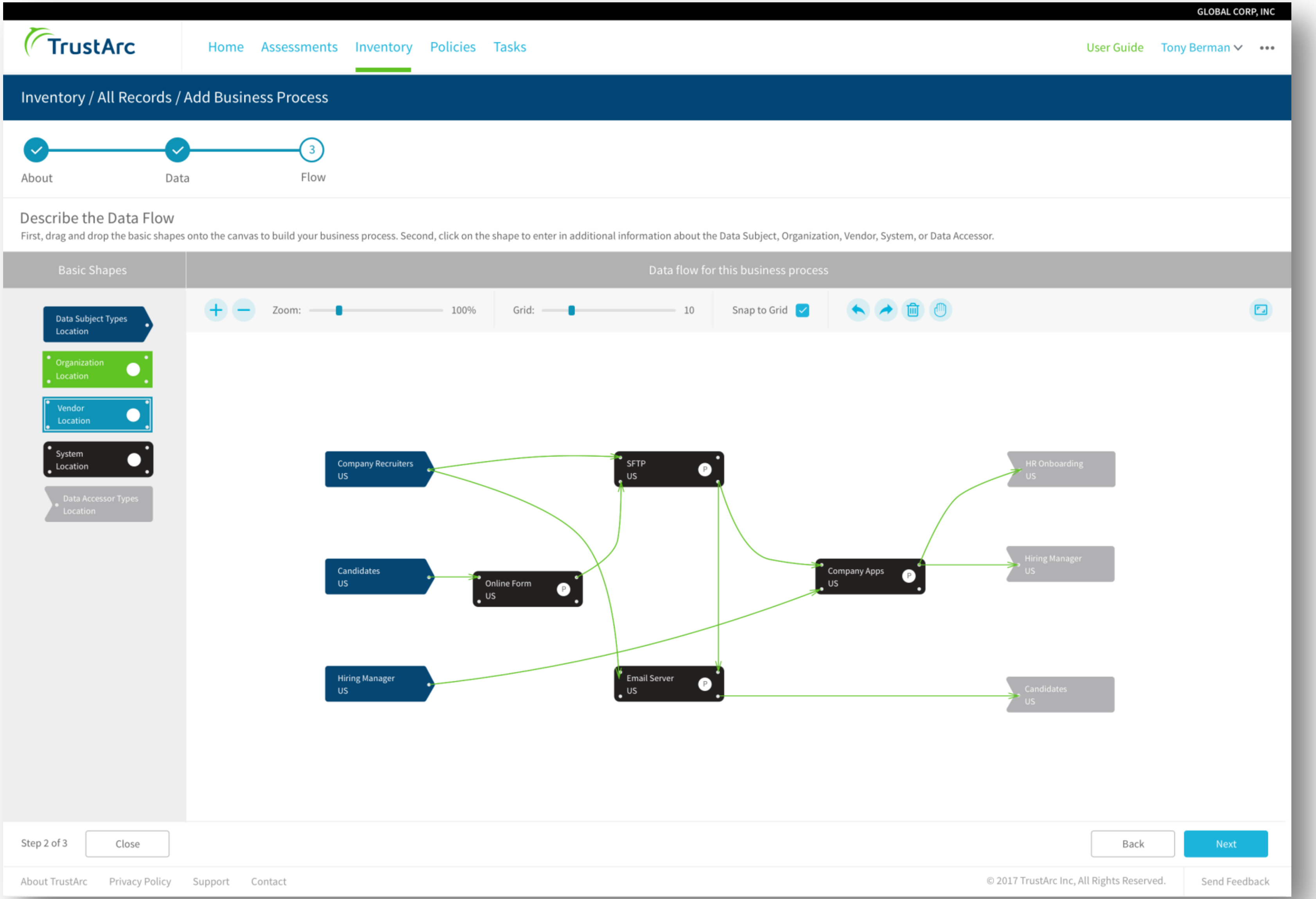
🔴 Cookies, behavioral tracking, unique identifiers

🟢 Financial data (sensitive): credit card transaction elements

🔵 Transaction data: purchase record, confirmation number, invoice number, shipper tracking, etc.

🟠 Customer data (non-sensitive): email, phone, address, loyalty program details, etc.

Data Mapping – TrustArc Tomorrow



Inventory / All Records / Add Business Process

Describe the Data Flow

First, drag and drop the basic shapes onto the canvas to build your business process. Second, click on the shape to enter in additional information about the Data Subject, Organization, Vendor, System, or Data Accessor.

PRIVACY INSIGHT SERIES

Summer / Fall 2017 Webinar Program

You’ve Completed a Data Inventory & Mapping Exercise – What’s Next?

TrustArc
the new TRUSTe

What’s Next?

- Identifying Tools and Methodologies to Scale and Maintain the Data Inventory
- Developing Article 30 Compliance Reporting
- Using as foundation for ongoing GDPR Compliance Program
- Identifying Inherent Risk and Completing DPIAs as required under Article 35
- Ongoing Training on Inventory Change Management
- Share with Cross-functional Teams for broader organizational benefit

Questions?

TrustArc
the new TRUSTe

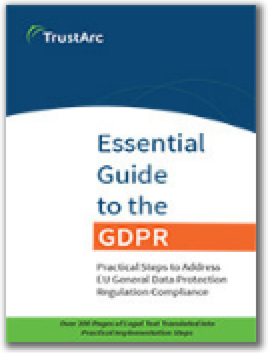
Additional Resources

TrustArc
Privacy and the EU GDPR 2017
A Survey of U.S. Privacy Professionals

2017 Privacy and the EU GDPR Research Report

This Research Report highlights the status of U.S. companies' efforts to meet privacy mandates in general, and in particular to meet the May 25, 2018 deadline for the GDPR.

REGISTER TO DOWNLOAD »


TrustArc
Essential Guide to the GDPR
Practical Steps to Address EU General Data Protection Regulation Compliance

Essential Guide to the GDPR

Comprehensive guide summarizing the key requirements for GDPR compliance and TrustArc solutions.

REGISTER TO DOWNLOAD »

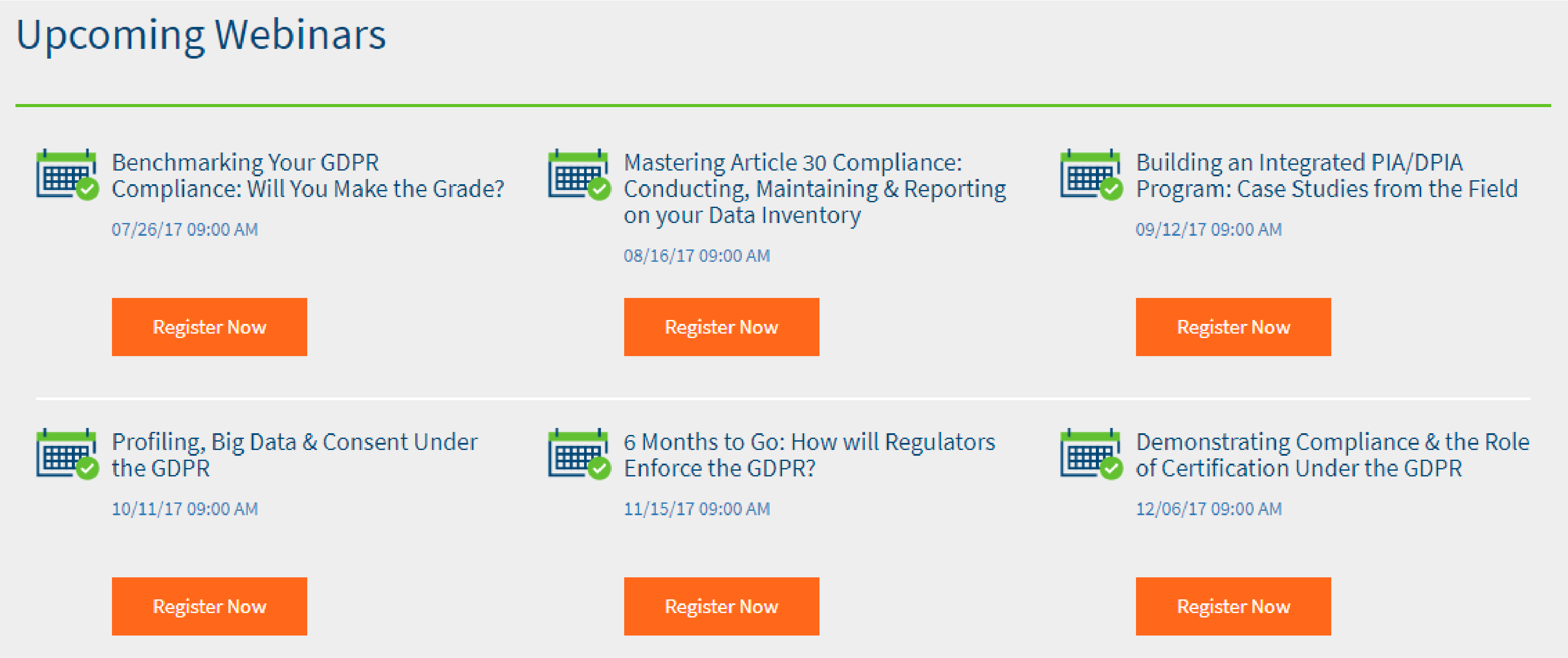
www.trustarc.com/resources

Contacts

Charles Nwasor	charles.nwasor@ensono.com
Paul Iagnocco	piagnocco@trustarc.com
Margaret Alston	malston@trustarc.com

TrustArc
the new TRUSTe

Privacy Insight Series – 2017 Calendar



Upcoming Webinars

Benchmarking Your GDPR Compliance: Will You Make the Grade?

07/26/17 09:00 AM

Mastering Article 30 Compliance: Conducting, Maintaining & Reporting on your Data Inventory

08/16/17 09:00 AM

Building an Integrated PIA/DPIA Program: Case Studies from the Field

09/12/17 09:00 AM

Profiling, Big Data & Consent Under the GDPR

10/11/17 09:00 AM

6 Months to Go: How will Regulators Enforce the GDPR?

11/15/17 09:00 AM

Demonstrating Compliance & the Role of Certification Under the GDPR

12/06/17 09:00 AM

www.trustarc.com/insightseries

PRIVACY INSIGHT SERIES

Summer / Fall 2017 Webinar Program

Thank You!

Register for the next webinar in our Series – September 12th

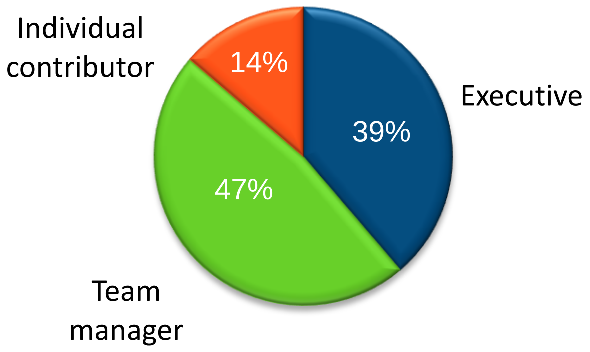
“Building an integrated PIA/DPIA Program: Case Studies from the Field”

For full Summer/Fall schedule and past webinar recordings visit: http://www.trustarc.com/insightseries

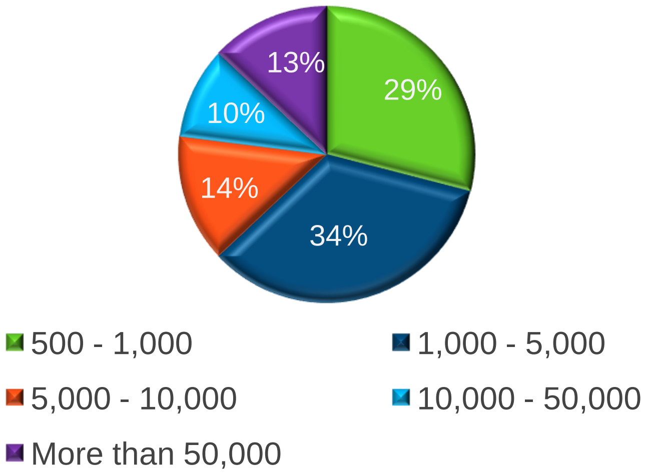
TrustArc
the new TRUSTe

Respondent Demographics

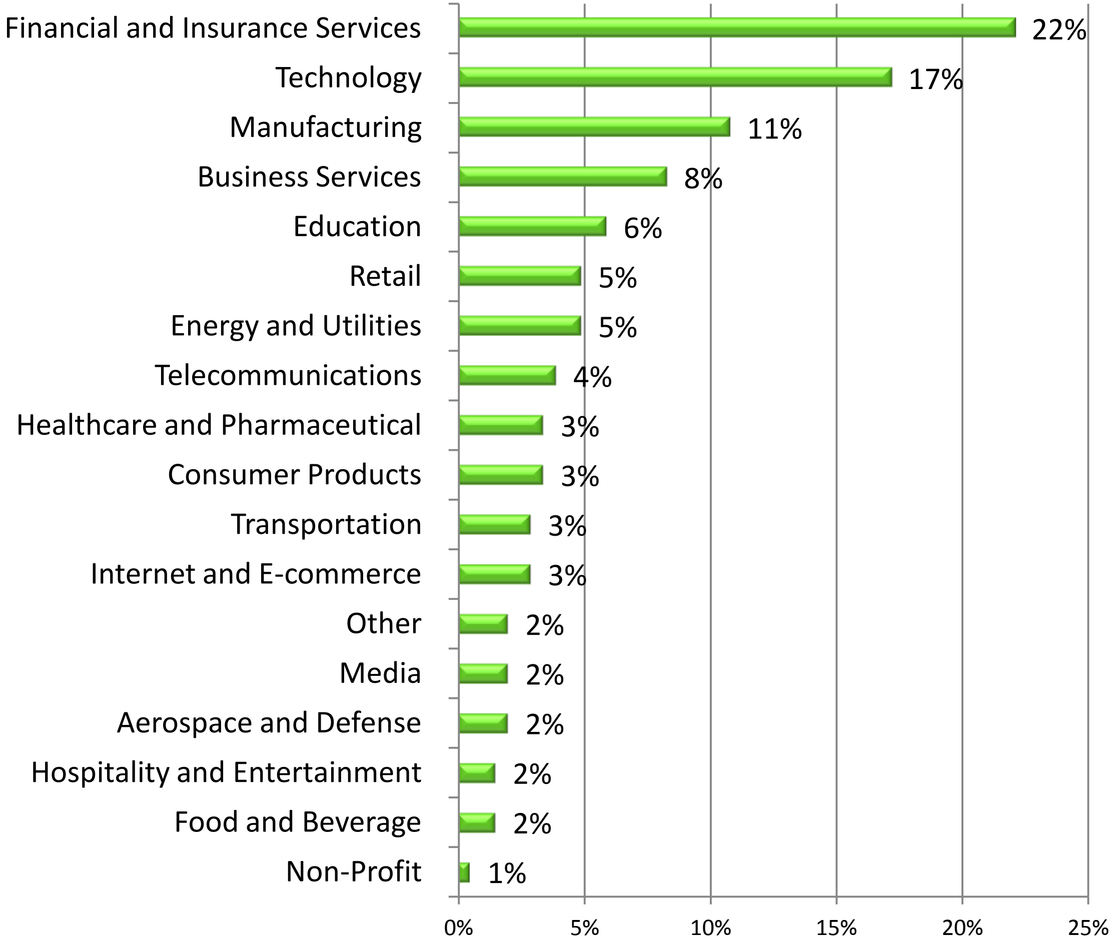
Job Level



Company Size (# employees)



Industry



TrustArc / Dimensional Research 2017

Privacy and the EU GDPR: 2017 Survey of Privacy Professionals

dimensional research

Research Overview

- Conducted May 10 - 17, 2017 by Dimensional Research
- Respondents US based privacy professionals from companies who subject to GDPR
- Minimum company size = 500 employees
- Respondent company headquarters: 92% US or Canada; 5% EU, 3% other
- Respondents work in legal, IT, compliance and privacy functions
- For 36% surveyed, privacy was their entire job
- For 64% surveyed, privacy was an important part of their job (over 25%)
- Note – due to rounding, some totals will not sum to exactly 100%