GDPR Privacy Workshop - Welcome!

TrustArc
the new TRUSTe

Overview of GDPR Privacy Workshop Series

The GDPR Privacy Workshops are free events that feature informative discussions, case studies and practical solutions to achieve GDPR compliance.

TrustArc the new TRUSTe | Ogletree Deakins

Topics discussed will include Data Mapping, Building a Record of Processing (Article 30 Reports), Ongoing Risk Assessments & DPIAs and GDPR HR Data Considerations.

The workshops are part of our renowned Privacy Insight Series that includes webinars that drew over 15,000 registrations in 2016.

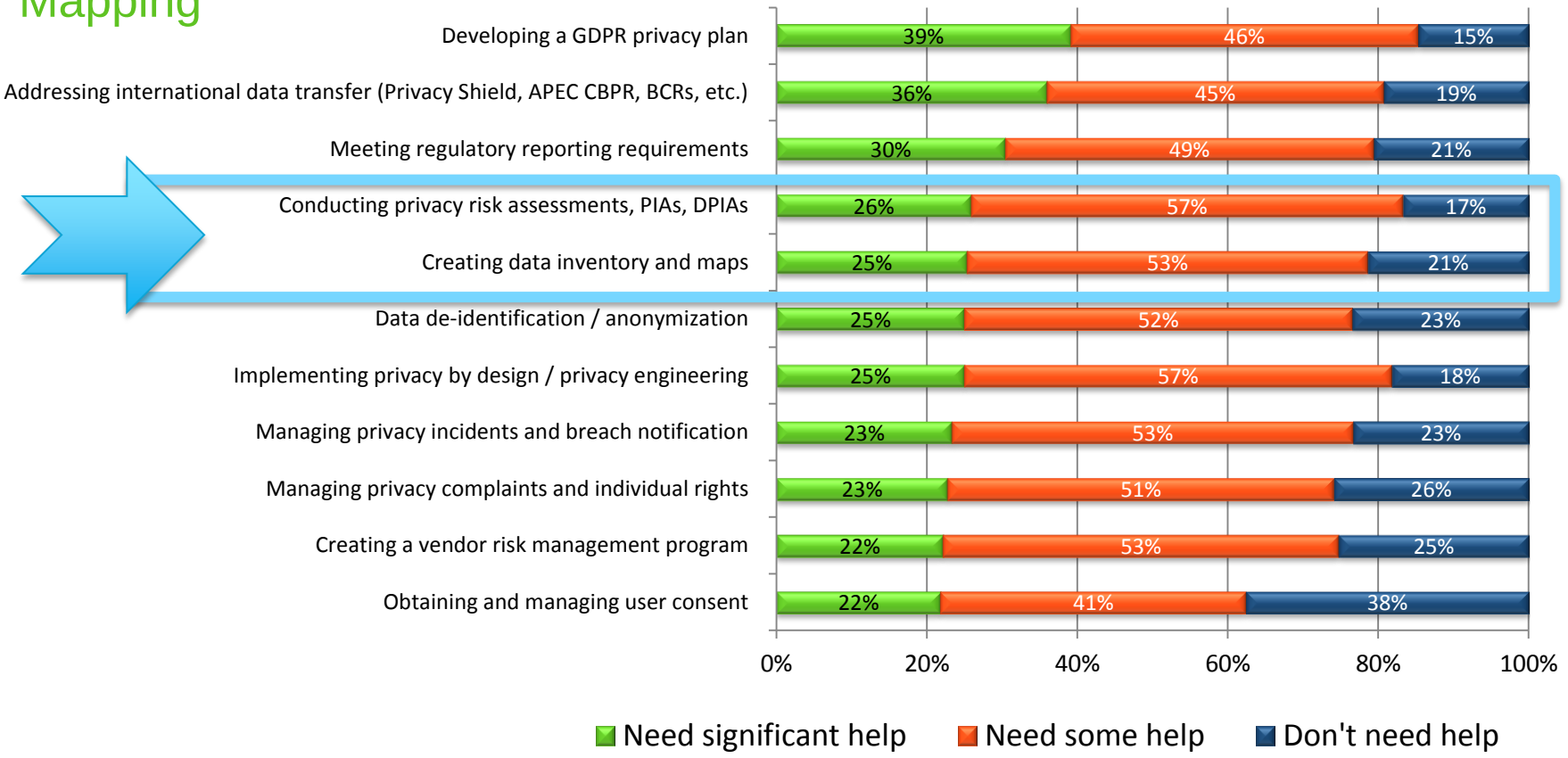
9/26: Boston	10/19: Minneapolis	11/9: Dallas
9/26: Orange County	10/19: Paris	11/9: Geneva
9/28: Philadelphia	10/24: Houston	11/9: San Diego
10/3: Richmond	10/26: Pittsburgh	11/14: Berlin
10/3: San Francisco	10/26: Miami	11/14: Seattle
10/5: New York	11/2: Portland	11/14: Los Angeles
10/5: Denver	11/2: Austin	11/16: Toronto
10/17: Chicago	11/7: Atlanta	11/16: Singapore
10/18: London	11/7: Phoenix	

Agenda

- Introductions
- Everything you need to know about the GDPR in 13 slides!
- GDPR Deeper Dive
  - Building your Data Inventory & Records of Business Processing
  - Managing DPIAs/PIAs and Demonstrating Compliance
- Demo of TrustArc Platform Solutions
- GDPR HR Requirements & National Derogations
- Questions

Help is Needed Across Wide Range of Areas

3 out of 4 Companies looking for help with DPIAs and 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

Introduction to TrustArc

TrustArc
the new TRUSTe

TrustArc is the New TRUSTe

We changed our name to reflect our evolution from a privacy certification company into a global provider of technology powered privacy compliance and risk management solutions.

Solutions backed by unmatched people, process, and technology

Deep Privacy Expertise

- Large, global, 175+ person team
- Dozens of CIPPs, former CPOs, world renowned policy experts
- Many with decades of experience at top brands across all industries

Proven Methodology

- Informed by 20 years & thousands of engagements
- Based on key global standards: GDPR, FIPPs, OECD, etc
- Developed by privacy experts, powered by industry leading technology

Powerful Technology

- Purpose build for privacy
- Flexible SaaS architecture
- Used by 1,000+ clients
- Operating at high scale for 6 years
- Ongoing enhancements
- Large engineering & support team

We power privacy for over 1,000 clients*

**All paying clients, many who have been TRUSTe clients for over a decade!*

100s of Billions of Privacy Safe Ads

10s Billions Consent Notices

10s Billions Hosted Seal Impressions

10s Millions Web Privacy Scans

1,000s of PIAs, GDPR, Risk Assessments

#1 Privacy Platform | #1 Privacy Shield Verification | #1 APEC Accountability Agent

Note - Figures are annual estimates

We are at the center of privacy innovation

Key Industry Partnerships

Active and long-standing participant in key organizations driving the global privacy agenda

FPF · iapp · APEC · Digital Advertising Alliance · The Information Accountability Foundation · Centre for Information Policy Leadership

Analyst Recognition

Covered in 3 Gartner Hype Cycles - Privacy; Legal & Regulatory Info Governance; Risk Management

Gartner

Leading Edge Thought Leadership

Advisories, Benchmarking Studies, Hot Topic Webinars, Educational Conferences

Innovation Awards

2016 Risk Management

IAPP Recognition

Selected to Power 1st IAPP GDPR Assessment

iapp | Powered by TRUSTe

TrustArc

GDPR Overview

TrustArc
the new TRUSTe

What is the GDPR?

General **D**ata **P**rotection **R**egulation

GOAL: One single privacy law for the EU

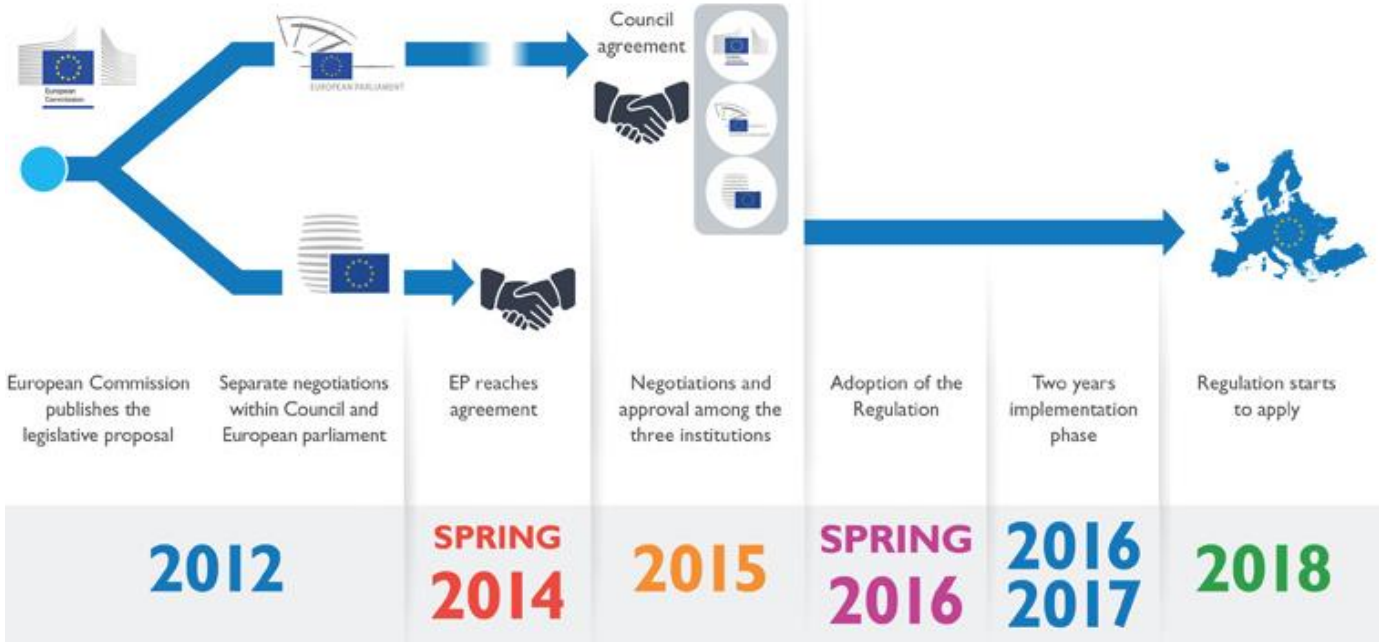
- Replaces previous 1995 Directive and national laws that had variations
- Applicability is now extra-territorial
  - Based on “residency of individuals in EU”
  - Applies to any business offering goods or services
- Where the organization is processing personal data
  - Data that relates to an individual who can be identified from it (or other data associated with it)
  - Regardless of format (digital, paper, audio, video, etc.)
  - Doesn’t have to be names (ID by picture, IP addresses, device IDs, Cookies, etc.)
- Evidence of demonstrable compliance is the standard
- Takes effect May 2018

GDPR Compliance Roadmap

Build Program and Team	Assess Risks and Create Awareness	Design and Implement Operational Controls	Manage and Enhance Controls	Demonstrate Ongoing Compliance
Identify Stakeholders	Conduct Data Inventory & Data Flow Analysis	Obtain & Manage Consent	Conduct PIAs (DPIAs)	Evaluate & Control Control Effectiveness
Allocate Resources & Budget	Conduct Risk Assessment & Identify Gaps	Data Transfers & 3rd Party Management	Data Necessity, Retention & Disposal	Internal & External Reporting
Appoint DPO	Develop Policies, Procedures & Processes	Individual Data Protection Rights	Data Integrity & Quality	Privacy Notice & Dispute Resolution Mechanism
Define Program Mission & Goals	Communicate Expectations & Conduct Training	Physical, Technical & Administrative Safeguards	Data Breach Incident Response Plan	Certification

Effective Date: 25 May 2018

The GDPR took 4 years to negotiate and is the most comprehensive data protection regulation ever enacted.



To Do

- Determine your exposure (more on that in a moment…)
- Determine your action plan for compliance, if needed
- Determine your response to customers who ask for your compliance status
- … because they **will** ask!

Core Rules Remain the Same

- GDPR retains same core rules as the current Data Protection Directive, with some notable changes
- "Sensitive" personal data has been expanded to include genetic and biometric data
- "New" rights have been codified, such as data portability and the "right to be forgotten"
- New obligations have been added around management, documentation, data breach notification, and more

To Do

- Review existing compliance (you are compliant, right?)
- Review new requirements

Extra-Territorial Reach

- Primarily applies to businesses established in EU
- BUT, also applies to businesses based outside EU that
  - offer goods/services to EU residents
  - collect data about EU residents

To Do

- Determine if you have EU residents' personal data
- Determine if you **want** to have EU residents' personal data

Controllers versus Processors

- Controller – "alone or jointly with others, determines the purposes and means of processing of personal data"
  - Must conduct Impact Assessments if processing is "likely to result in a high risk to the rights and freedoms of natural persons"
  - Assure protections of data subject rights, including erasure, reporting and notice, maintaining records of processing activities
  - Data breach notification responsibility
- Processor – "processes personal data on behalf of the controller"
  - Provide sufficient guarantees of their technical and management measures ("assess the processor"), including maintaining records of processing activities and practices
  - Additional duties and restrictions on vetting subprocessors

To Do

- Determine (and document) your Controller versus Processor status
- Update agreements with subprocessors
- Prepare for new agreements and assessment requests from Controllers
- Begin to document your technical and management measures

Cross-Border Data Transfers

- Transfer of personal data outside of EU is prohibited unless certain conditions are met (same as today)
- "Adequacy" can be met through
  - Binding Corporate Rules
  - Standard Contractual Clauses
  - Code of Conduct and Certification Programs (tbd)
  - EU-US Privacy Shield
  - Allows for "explicit consent" but regulators have expressed skepticism

To Do

- Review your current transfers
- Determine and implement appropriate transfer mechanism

Consent

- Consent is viewed more skeptically
  - Service cannot be conditioned on consent unless necessary for the service
  - Conduct or choice of browser settings may not suffice
- Consent may be withdrawn at any time
- Consent to process sensitive data or to transfer outside EU must be explicit
- But consent isn't always required; there are other justifications

To Do

- Review existing processes to determine if consent is used as the basis for processing
- Review any consent mechanism for validity under GDPR standards
- Determine if there are any alternative bases for processing (e.g., your fall-back if consent is withdrawn)

Special Categories of Personal Data

- "Special categories of personal data"
- "Particularly sensitive in relation to fundamental rights and freedoms" and, therefore, "merit specific protection."
- Include data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"

To Do

- Review data sets for any sensitive data elements
- Review whether sensitive data is necessary for services
- Determine adequacy of consent mechanisms

Data Subject Rights

- Enhanced rights to notice, access, correction
- "Right to be forgotten" – erase data "without undue delay"
  - If no longer necessary, objection, or unlawful processing
- Data Portability
  - "Automated" processes, Controller must provide data in "machine-readable" format, transmittable to any other controller, even directly to a competitor
- Profiling and the Right to Object
  - "Automated" processes that assess or predict things like: performance, economic situation (e.g., credit), health, personal preferences, interests and behavior, location and movements

To Do

- Review the applicability of these rights to your processes and impact of any exercise of those rights
- Develop processes to receive and process requests

Privacy Notices

- Increased level of detail in Privacy Notices
- Yet the must be concise and readable

To Do

- You **will** have to update your Privacy Notices
- Review Privacy Notices to ensure they reflect your current services, processes, vendors
- Review how notices are delivered, e.g., layered notices and "just-in-time"

Accountability

- You must not only comply, you must be able to demonstrate your compliance
- You must have a privacy impact assessment program for any "high risk to rights and freedoms" from processing and may be required to consult with your regulator

To Do

- Create and maintain a record of your data processing activities and privacy risk management activities
- Develop Privacy by Design, privacy-related training, etc., to ensure integration of privacy considerations into product development and engineering processes
- Develop a Privacy Impact Assessment program for any processing where data risk may arise

Data Protection Officers

- A Data Protection Officer is required when the core activities of a Controller involve large scale data collection or processing of the "special categories" of data
- They must have "expert knowledge of data protection law and practices" and commensurate with the type of processing
- Report to highest level of management; may not be dismissed for performance of their protection obligations
- No company-size limitation

To Do

- Determine if you need a DPO or decide to appoint one voluntarily
- Determine if you want a dedicated DPO, add DPO duties to existing role (if it does not conflict); outside entities may also perform DPO duties

Data Security

- Controllers and Processors must “implement appropriate technical and organizational measures” taking into account “the state of the art and the costs of implementation” and “the nature, scope, context, and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.”

- Few specific requirements, but things like encryption, pseudonymization, data recovery, regular testing/assessments, are all referred to
- Breach notification standards: 72 hours after awareness (unless "reasoned justification" which will need to be communicated to DPA)

To Do

- Develop a Breach Response plan with pre-defined notification templates
- Regularly test response plan, update with latest contacts and defined responsibilities
- Review adequacy of security audits, including review and audits of key service providers

Sanctions

- Base Violations: Up to €10m or 2% of global annual turnover of previous fiscal year
- Serious Violations: Up to €20m or 4% of global annual turnover of previous fiscal year
  - This category includes data transfer violations

To Do

- Review your current level of compliance; identify gaps and develop remediation plan to be implemented and validated before May 2018
- Consider overall risk appetite vs risk exposure; perform cost/benefit analysis on higher risk activities
- Develop a risk assessment framework (consider GDPR but also other risk factors: legal, regulatory, reputational, contractual obligations to partners/customers, etc.)

GDPR Privacy Workshops

Deeper Dive - EU GDPR Article 30

TrustArc
the new TRUSTe

GDPR Compliance Roadmap

Build Program and Team	Assess Risks and Create Awareness	Design and Implement Operational Controls	Manage and Enhance Controls	Demonstrate Ongoing Compliance
Identify Stakeholders	Conduct Data Inventory & Data Flow Analysis	Obtain & Manage Consent	Conduct PIAs (DPIAs)	Evaluate & Control Control Effectiveness
Allocate Resources & Budget	Conduct Risk Assessment & Identify Gaps	Data Transfers & 3rd Party Management	Data Necessity, Retention & Disposal	Internal & External Reporting
Appoint DPO	Develop Policies, Procedures & Processes	Individual Data Protection Rights	Data Integrity & Quality	Privacy Notice & Dispute Resolution Mechanism
Define Program Mission & Goals	Communicate Expectations & Conduct Training	Physical, Technical & Administrative Safeguards	Data Breach Incident Response Plan	Certification

Understanding Article 30

TrustArc
the new TRUSTe

Foundation for Article 30 Compliance

Who, What, Why Behind Article 30

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.

Foundation for Article 30 Compliance

Requirements and examples

Category	Requirement	Example	C	P
Records	Processing Activities	HR Onboarding	✓	
	Categories of Processing Activities carried out on behalf of a controller			✓
Contact Info	Name and contact details	Our DPO is Jane Smith; (123) 456-7899	✓	✓
Purpose of Processing	Purpose of processing	Employee hiring	✓	
Data Subjects	Categories of data subjects	Employee	✓	
Recipients	Categories of recipients who will receive the data	Executive, First line manager, data subjects themselves	✓	
Cross-Border Transfers	Where the data is going; 49(1) document suitable safeguards		✓	✓
Time limits	Retention period	1 month	✓	
Security	Security measures referred to in Article 32(1)	Encryption at rest	✓	✓

Foundation for Article 30 Compliance

The two approaches

IT/Systems Based Approach

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

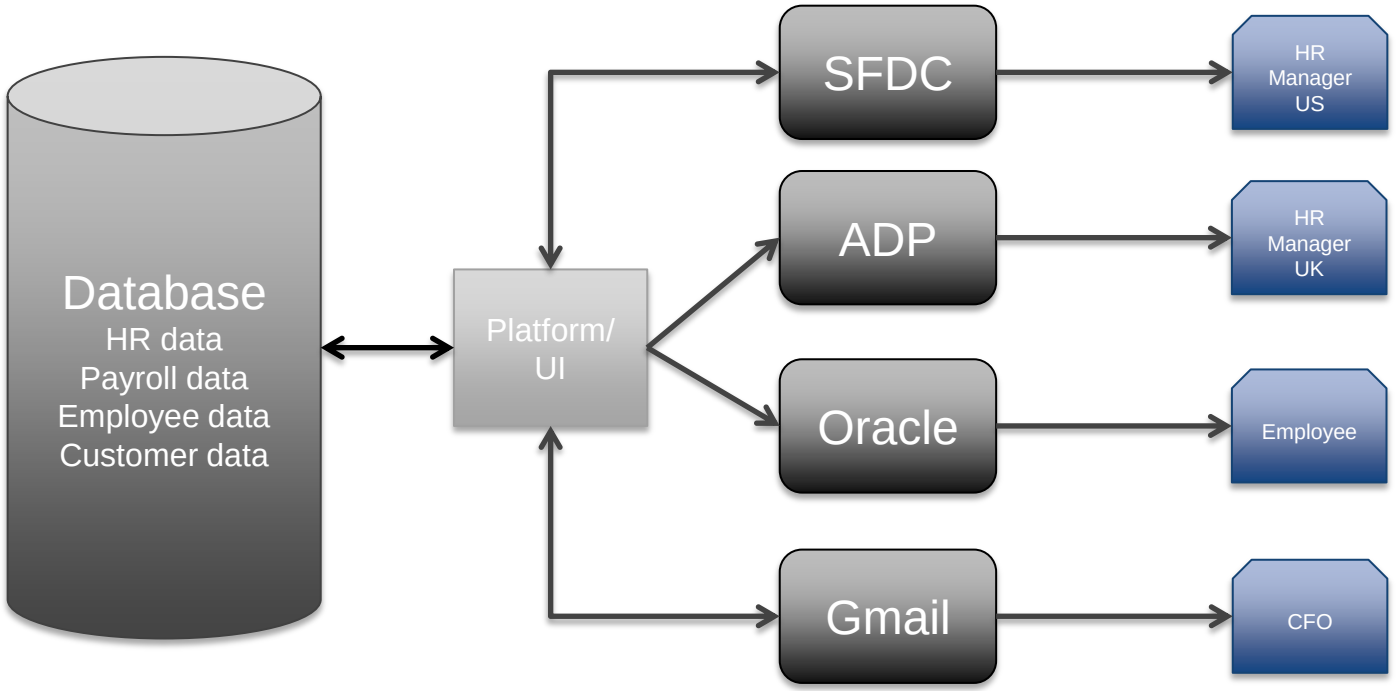
Process Based Approach

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

Foundation for Article 30 Compliance

IT/Systems based approach

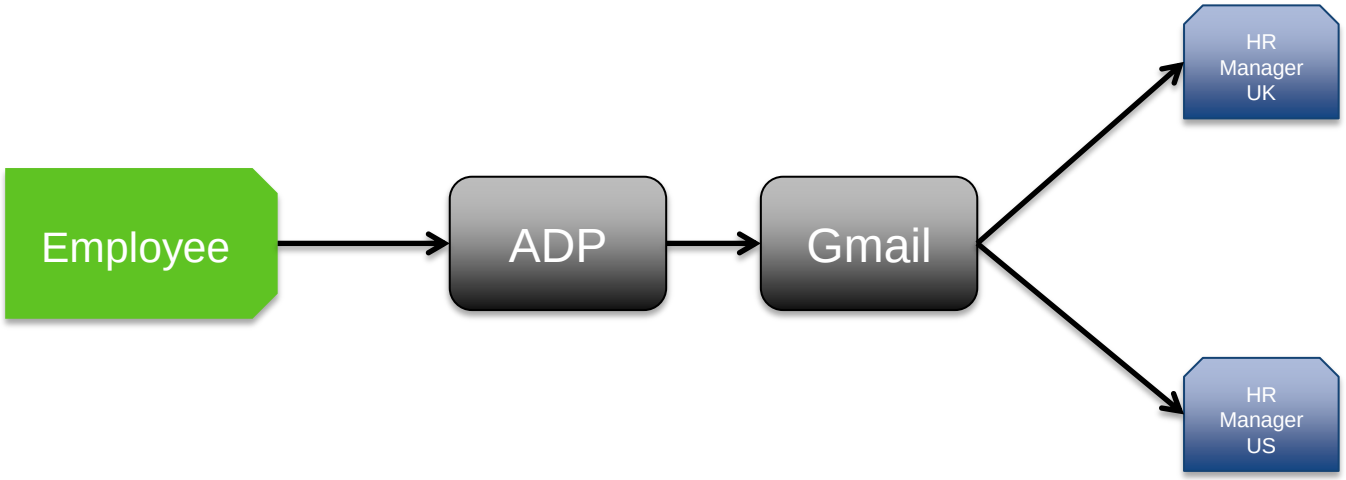
“Show me all the systems and applications being used to process or store our data”



Foundation for Article 30 Compliance

Business Process based approach

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



Implementation

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

Knowing where to start…

Scope out the project

Don’t reinvent the wheel

Start small, then expand

Methodology & Tools

Questionnaires & Interviews

Automated Scanning & Feeds

Spreadsheets

Combinations

Sample Data Inventory Spreadsheets

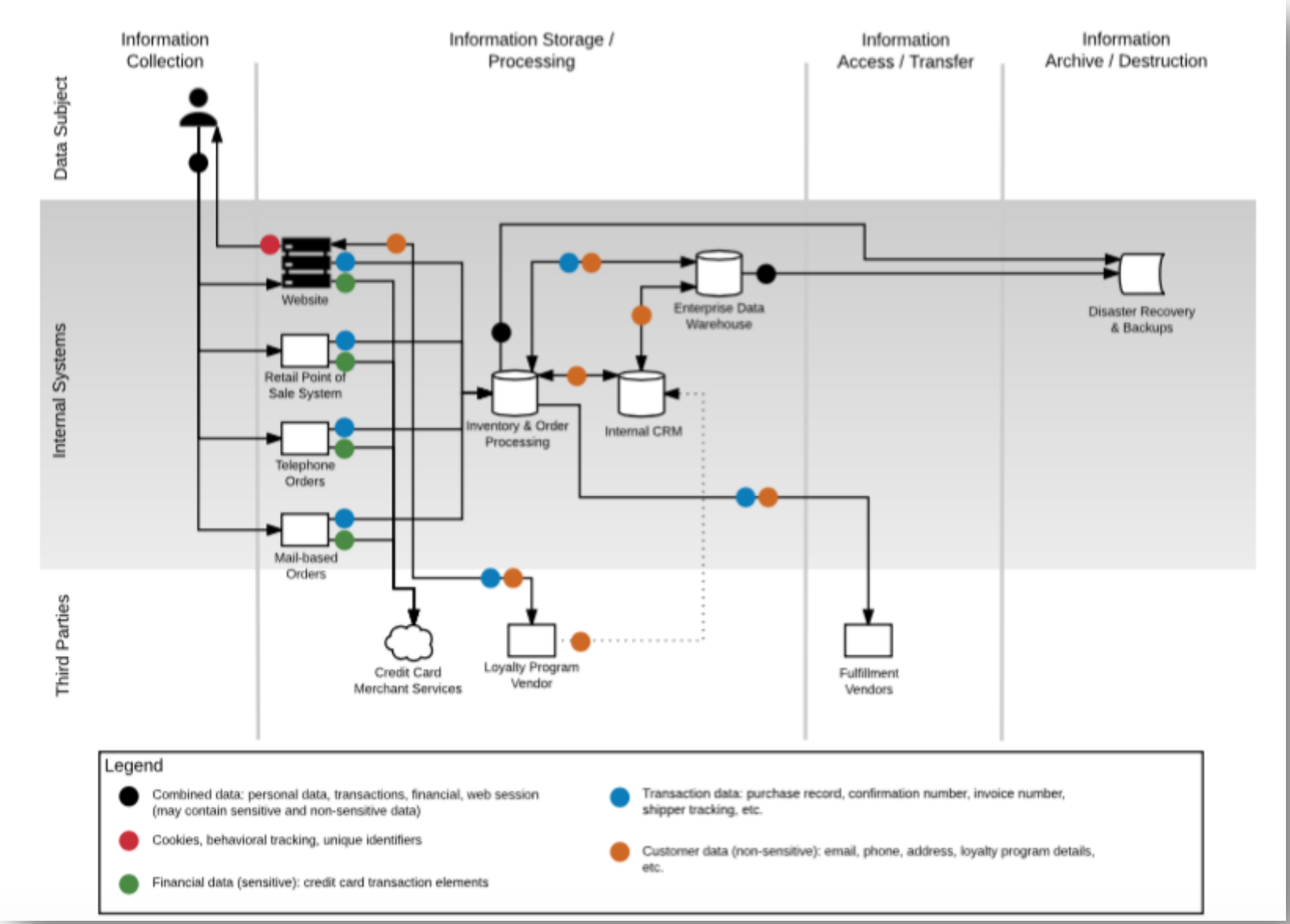
Inventory Fields

Data Collection					Data Storage			Data Access				Data Transfer (outside co		
	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 Transferr
ext ried)	(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/contr olled 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 fr list in "D Elements Collected
	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	Consumer Customer (prior relationship, account, etc.)			Enterprise Data Warehouse	3rd Party cloud		Customer Service	API				API	
		Business Prospect (no prior relationship)			Internal cloud	vendor-controlled data center		System Administrators	File Export				File Export	
		Business Customer (prior relationship)			3rd party cloud	vendor-controlled unknown		Vendor(s)	Physical Transfer				Physical Transfer	
								Internal Users (list? E.g., BI,						

Data Mapping

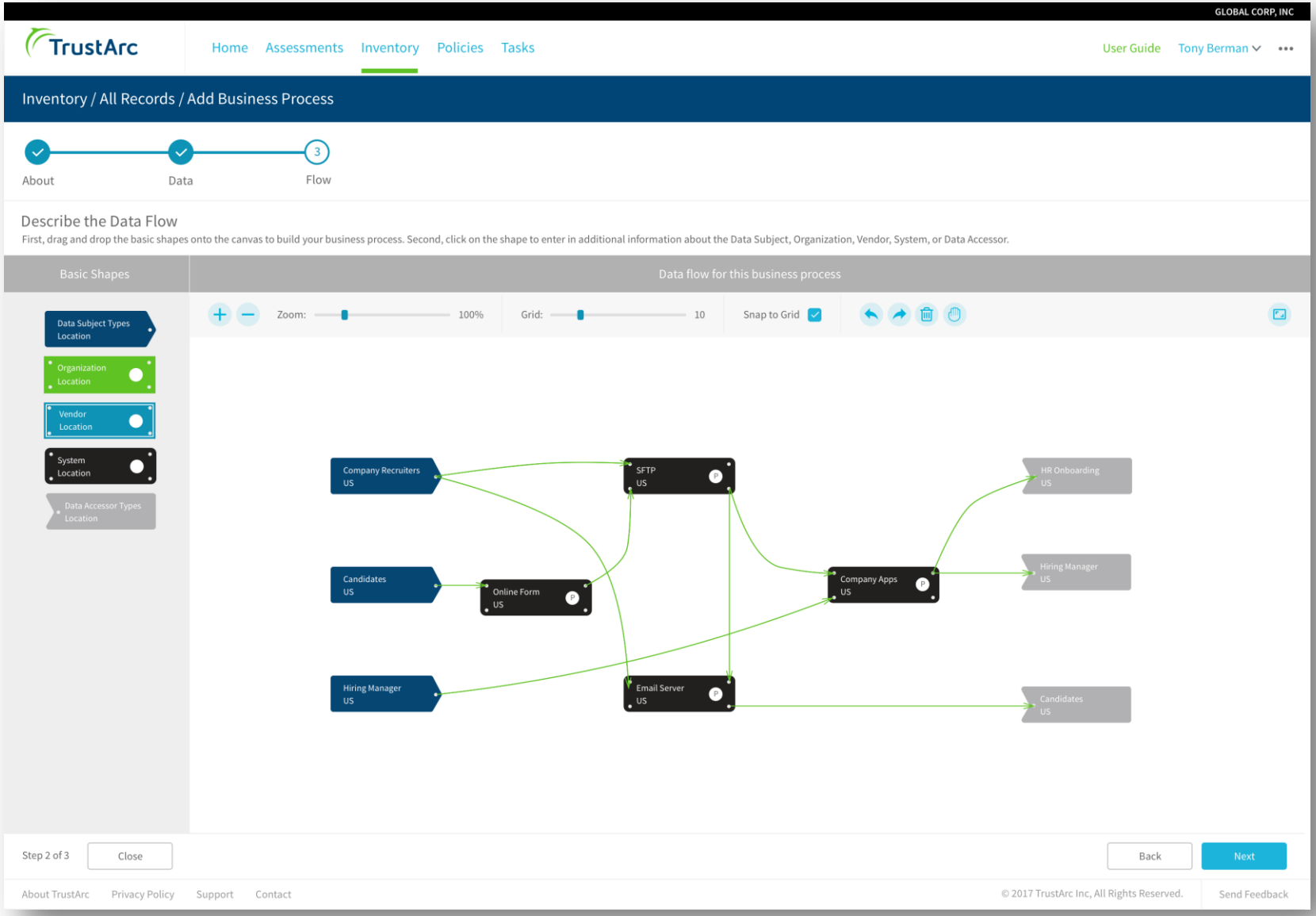
- The GDPR doesn't actually require data maps rather a "record of processing activities"
- However it is hard to capture the multi-linear connections between different data flows and assets without some form of visualization
- Data visualizations or "maps" help companies to understand the data they hold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

Sample Data Map



TrustArc

Data Mapping & Inventory – TrustArc



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

TrustArc
the new TRUSTe

What's Next?

Maintenance

Article 30 reporting 

GDPR Compliance

Share 

Questions?

TrustArc
the new TRUSTe

GDPR Privacy Workshops

Building a DPIA/PIA Program

TrustArc
the new TRUSTe

GDPR Compliance Roadmap

Build Program and Team	Assess Risks and Create Awareness	Design and Implement Operational Controls	Manage and Enhance Controls	Demonstrate Ongoing Compliance
Identify Stakeholders	Conduct Data Inventory & Data Flow Analysis	Obtain & Manage Consent	Conduct PIAs (DPIAs)	Evaluate & Audit Control Effectiveness
Allocate Resources & Budget	Conduct Risk Assessment & Identify Gaps	Data Transfers & 3rd Party Management	Data Necessity, Retention & Disposal	Internal & External Reporting
Appoint DPO	Develop Policies, Procedures & Processes	Individual Data Protection Rights	Data Integrity & Quality	Privacy Notice & Dispute Resolution Mechanism
Define Program Mission & Goals	Communicate Expectations & Conduct Training	Physical, Technical & Administrative Safeguards	Data Breach Incident Response Plan	Certification

DPIAs and PIAs

TrustArc
the new TRUSTe

PIAs and DPIAs: Similarities and Differences

- The terms “PIA” and “DPIA” are often used interchangeably by many organizations. An organization may use a DPIA, even if a DPIA is not required, to conduct an assessment to ensure the required data protection controls are in place and to demonstrate compliance with GDPR requirements.

- DPIAs are required of organizations acting as Data Controllers. Data Processors may also use DPIAs to assess whether they are processing data in a manner that supports the Controller in meeting its compliance obligations under the GDPR.

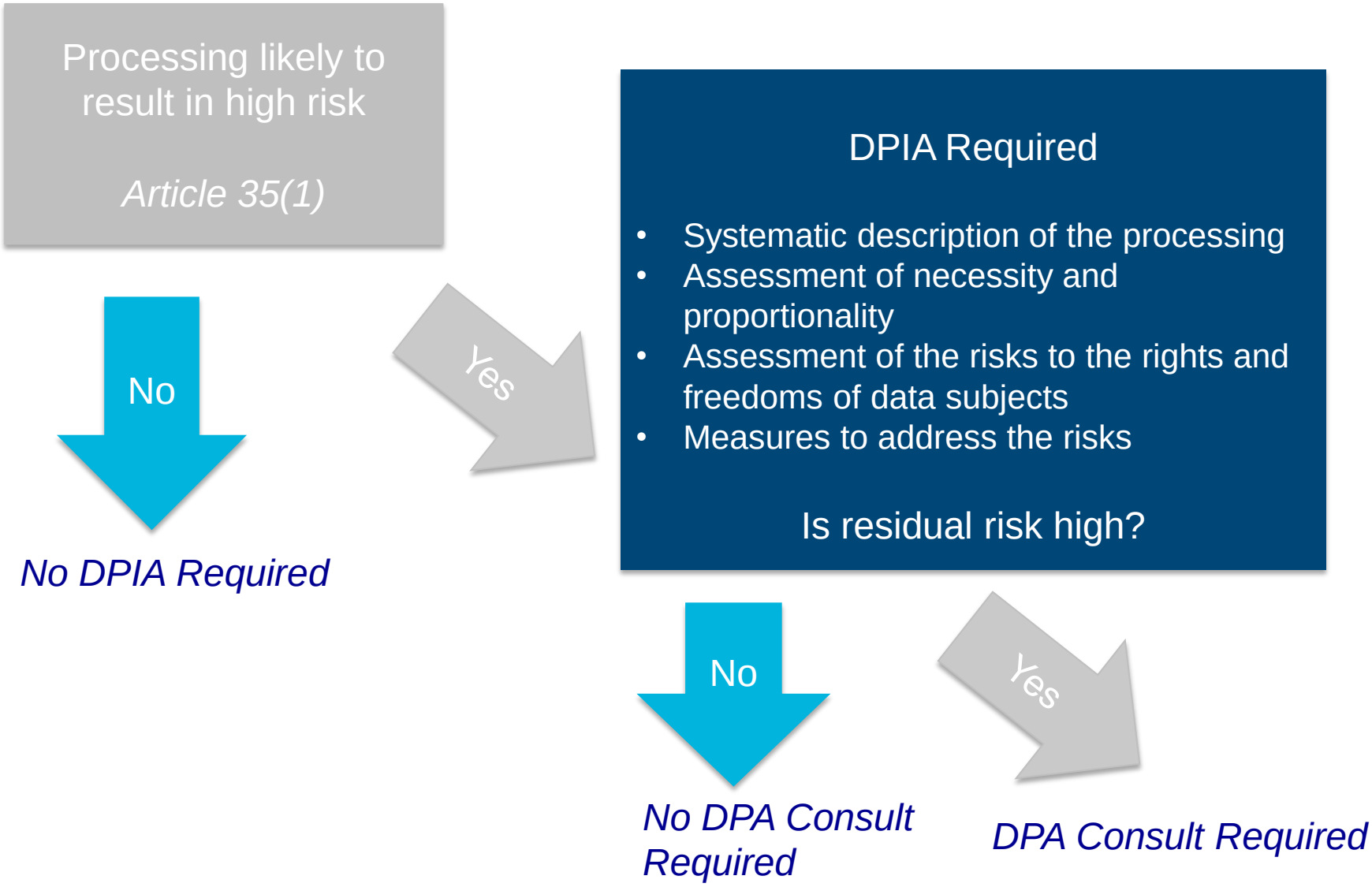
- Both PIAs and DPIAs enable organizations to identify the controls needed to address and reduce risk—be it a risk to the rights of individuals, a compliance risk of the organization, or both.

Processing Likely to Result in High Risk – Key Criteria

Based on Article 29 Working Party Guidelines WP 248 (4 Apr 2017)

- Automated-decision making with legal or similar significant effect
- Evaluation or scoring
- Systematic monitoring
- Sensitive data
- Data processed on a large scale
- Datasets that have been matched or combined
- Data concerning vulnerable subjects
- Data transfer across borders outside of the EU
- Innovative use or applying technological or organizational solutions
- Where the processing itself prevents individuals from exercising a right or using a service or a contract

GDPR Requirements for DPIAs (Articles 35 *and* 36)



GDPR Privacy Workshops

Best Practices for a PIA Program

TrustArc
the new TRUSTe

Build Your DPIA Program – 6 Essential Elements

Build

Establish, maintain and evolve an integrated privacy and data governance program aligned with other data management and information risk functions such as security, IP, trade secret protection and e-discovery

Learn and Evolve Over Time

Integrated Governance	Identify stakeholders. Establish program leadership and governance. Define program mission, vision and goals.
Risk Assessment	Identify, assess and classify data-related strategic, operational, legal compliance and financial risks.
Resource Allocation	Establish budgets. Define roles and responsibilities. Assign competent personnel.
Policies & Standards	Develop policies, procedures and guidelines to define and deploy effective and sustainable governance and controls for managing data-related risks.
Processes	Establish, manage, measure and continually improve processes for PIAs, vendor assessments, incident management and breach notification, complaint handling and individual rights management.
Awareness & Training	Communicate expectations. Provide general & contextual training.

1. Integrated Governance

Identify your key stakeholders: Establish program leadership and governance. Define program mission, vision and goals.
Leverage relationships with key internal stakeholders (and build new ones) to drive change and adoption

Key Stakeholders	Key Area (examples)
IT/Security	Responsible for data protection and securing internal systems
Human Resources	Responsible for HR data and systems
Marketing	Responsible for services to customers (both internal and external)
Legal	Responsible for ensuring legal requirements are met
Internal Audit	Responsible for managing an audit trail
Procurement	Responsible for vetting and contracting with vendors and third parties

2. Risk Assessment

Identify and assess risk: Classify data-related strategic, operational, legal compliance and financial risks.

Key Risks (examples)
Significant infrastructure or systems changes
New Product development where data is collected; changes to existing products new uses for data collected
New regulations and compliance requirements (GDPR)
Mergers and acquisitions
New vendors and third party business partners
Ongoing HR related data requirements (example: employee monitoring)

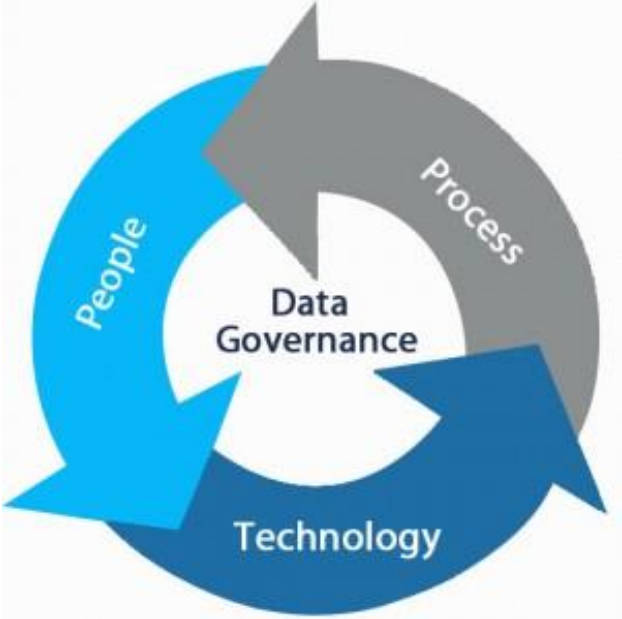
3. Resource Allocation

Identify resource needs: Establish budgets. Define roles and responsibilities. Assign knowledgeable and trained personnel.

Resource Needs to Consider
Executive Champion; “top down” support essential to success
Training and knowledgeable personnel needed to manage PIA/DPIA process; Define roles and responsibilities
Systems needed to support the program; automation
New regulations and compliance requirements (monitoring)
Outside consulting and legal resources

4. Policies and Standards

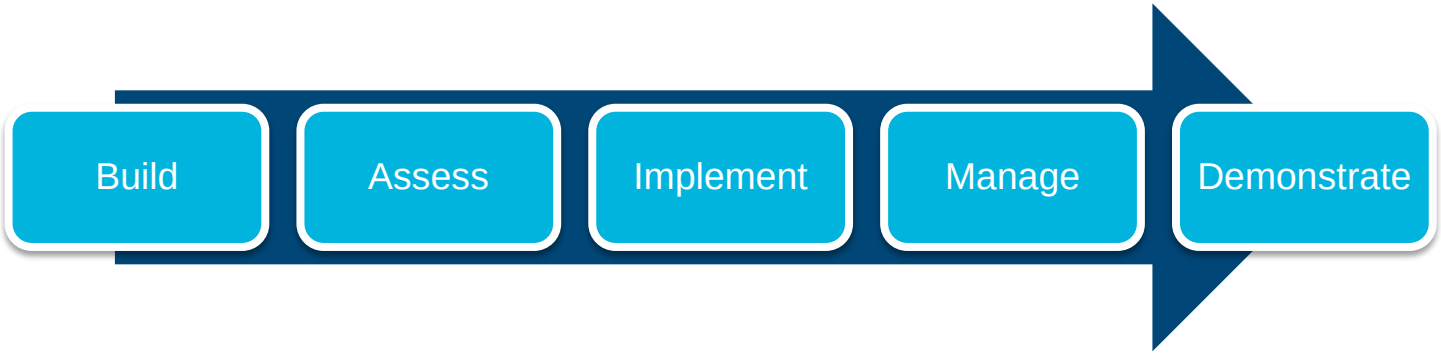
Develop policies and standards: Procedures and guidelines to define and deploy effective and sustainable governance and controls for managing data-related risks.



- **IT Security, Data Security and Acceptable Use**
- **Privacy Notices and Policies**
- **Data Use, Retention and Disposal**
- **Data Classification**
- **Marketing Operations**
- **Product Development**

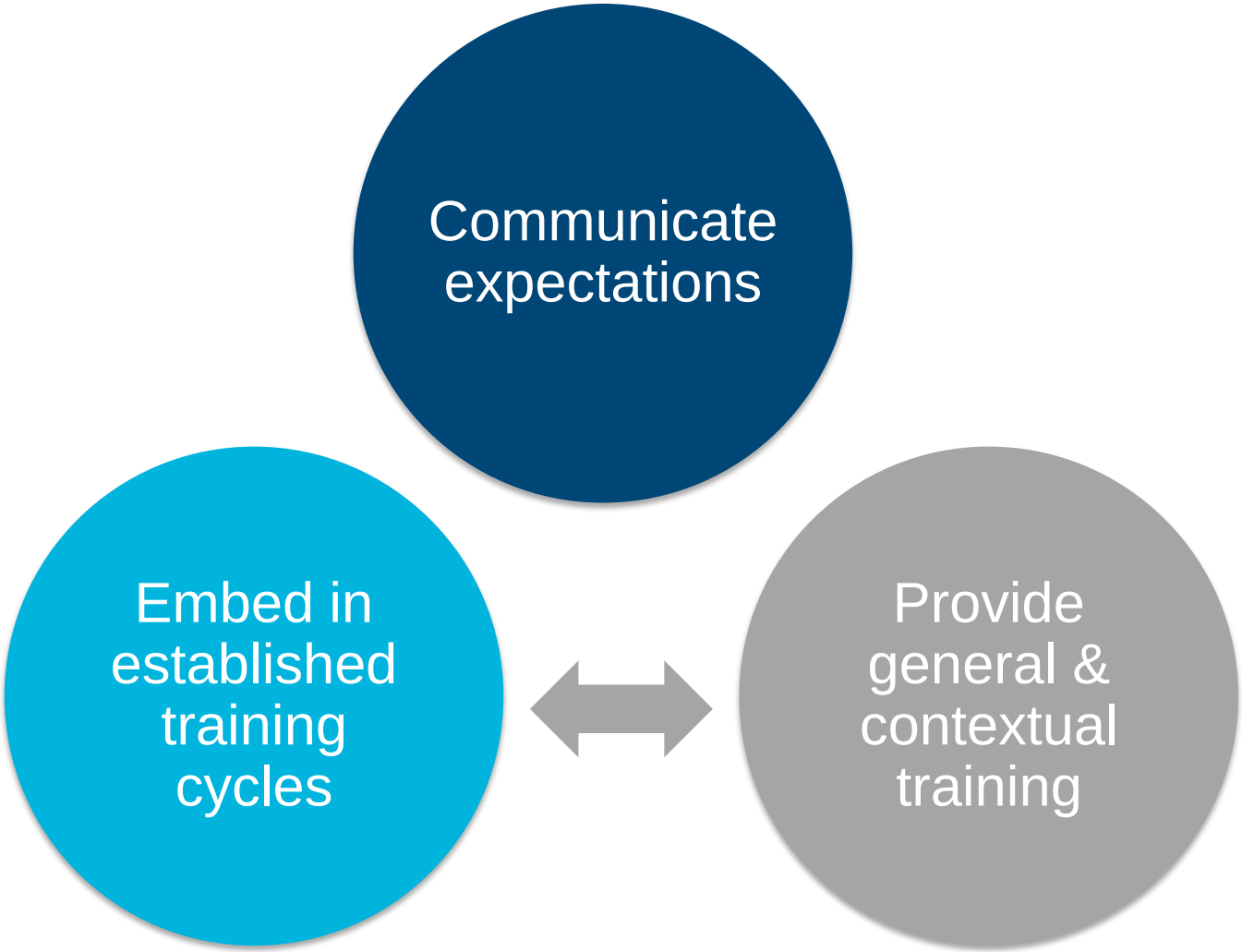
5. Processes

Establish, manage, measure and continually improve processes: Ensure a unified approach to PIAs/DPIAs, vendor assessments, incident management and breach notification, complaint handling and individual rights management.



- ***One size does not fit all.*** Organizations should develop and follow a process that makes sense for their size, type of processing, and resources
- PIAs/DPIAs need to be conducted according to a documented process to ensure consistency
- Documentation to demonstrate accountability is also critical (on demand)

6. Awareness & Training



Recommendations

TrustArc
the new TRUSTe

Recommendations for Success

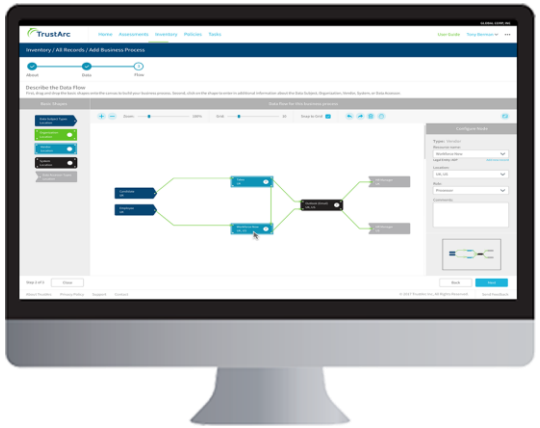
- Assign **clearly defined roles** for all stages
- Having an **Executive "Champion"** or Sponsor
- **PIA/DPIA processes** need to be simple, repeatable, concise, and they need to map to the GDPR requirements
- **One size does not fit all** – consider the level of risk
  - Also consider a process with traditional PIAs for all projects and EU DPIAs for projects that trigger EU DP rules
- Build a robust process **with scalability in mind**
  - Consider the system you are using, what it'll take to make the process more efficient and automate
- **Over communicate** and reinforce training at every opportunity

TrustArc Platform DEMO

TrustArc
the new TRUSTe

DEMO

See how TrustArc's proven technology can help you meet GDPR requirements.



Records of Processing for Article 30 Compliance

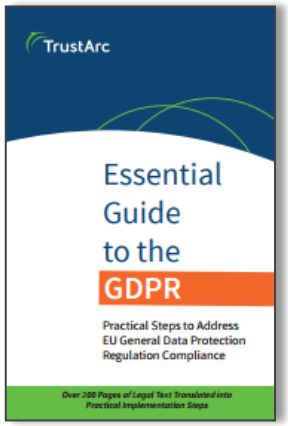
DPIA and Risk Assessments for Article 35 Compliance

Thank you!

Questions?

TrustArc
the new TRUSTe

Additional Resources



Essential Guide to the GDPR

Official Text of the GDPR

2017 Privacy and the EU GDPR Research Report

IAPP / TRUSTe GDPR Privacy Benchmarking Study

www.trustarc.com/resources