TrustArc

Essential Guide to the GDPR

Practical Steps to Manage EU General Data Protection Regulation Compliance

How to Build, Implement, and Demonstrate GDPR Compliance

This guide distills the 200+ page GDPR into five discrete phases to help a business maintain its GDPR compliance. The guide is designed for professionals across a wide range of functions who will be impacted by the GDPR. You can find a copy of the full GDPR text at: https://www.TrustArc.com/eugdpr. As with all regulatory matters, please consult with your legal team to ensure your plans are consistent with internal guidelines and requirements. If you have questions on any information in this guide, or want to get an update on emerging GDPR news, please contact a TrustArc representative.

Whatever your team decides, the plan also needs to account for the unexpected. Invest time up-front to perform the proper analysis and planning, so that you can be confident your company's GDPR Compliance Program will efficiently and effectively mitigate risk while meeting business objectives.

GDPR Compliance Roadmap - 5 Phases

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

Table of Contents

Chapter I: Introduction to the EU General Data Protection Regulation (EU GDPR)

The EU GDPR is a law designed to enhance data protection for EU residents and provide a consolidated framework to guide business usage of personal data across the EU, replacing the patchwork of existing regulations and frameworks. The 200-plus page GDPR replaced the 20 year old Directive (95/46/EC).

The deadline for compliance was May 25, 2018

Who does it apply to?

The reach of the GDPR extends beyond the Directive it replaces, so even if your company did not have to comply with EU data privacy laws before, the GDPR may apply to your company.

Answering these three questions can help determine whether your company is impacted by the GDPR.

- ☑ Does my company offer goods or services to Individuals?
- ☑ Does my company monitor the behavior of Individuals?
- ☑ Does my company have employees in the EU?

If the answer is "yes" to any of these questions, the GDPR may apply to your company.

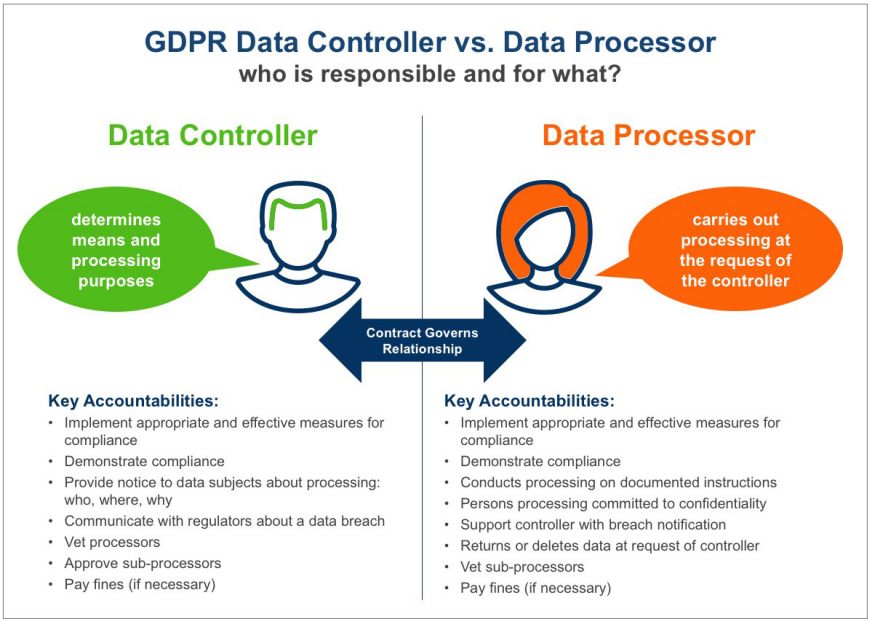
Gaining a comprehensive view on whether your company is involved in any of these activities may require input from different departments within your company. Think broadly – conduct a review with key contacts in the departments:

- Engineering
- Human resources
- Information security
- Legal
- Marketing
- Procurement
- Product management
- Website development

If a department deals with personal data of any kind (employee, contractor, vendor, consumer, or customers), then you need to research further to see if the GDPR applies.

Some Things to Keep in Mind

- The GDPR protects the personal data of Individuals, which includes anyone physically residing in the EU, even if they are not EU citizens.
- By defining the scope of the GDPR to include monitoring the behavior of Individuals, the applicability is broad and encompassing. Practically every website and app tracks digital activities of its visitors in some fashion.
- The GDPR now extends due diligence obligations and potential liability to Data Processors, not just Data Controllers.
- The GDPR defines personal data fairly broadly. For example, business contact information, such as an individual's work email address, is typically covered by the GDPR.



Am I a Data Processor or Controller?

Tip

A Data Processor is the entity that processes data on behalf of the Data Controller. For example, a company providing a SaaS based CRM platform that stores data for its Client, a large bank, would be a Data Processor.

The company that collects the data is the Data Controller. In the example above, the Bank would be the Data Controller.

Non-Compliance Implications

The GDPR comes with significant penalties for non-compliance - fines up to 20,000,000 EUR or 4% of total worldwide annual turnover of the preceding year (whichever is higher).

Sample Potential Fines

Annual Turnover (EUR)	Maximum Potential Fine (EUR)
200,000,000 – 300,000,000	8,000,000 – 12,000,000

These penalties do not include any loss of business, loss of brand trust, loss of goodwill that may come along with non-compliance violations, or internal / external legal fees associated with responding to an inquiry.

Aside from financial penalties, many businesses will require their vendors to be fully compliant with the GDPR as a condition to doing business. These requirements will typically be part of the RFP process and / or privacy & security audits. Non-compliance could lead to significant loss of business to competitors who are able to demonstrate their GDPR compliance.

Chapter II: How to Comply

For most companies, the GDPR brought new requirements that raised the bar. Despite its complexity and new requirements, complying with the GDPR can be accomplished by following the roadmap outlined below.

Overview – People, Process, & Technology

For all five phases, use a combination of your team, a defined process, and technology tools.

People - Identify the team members who will be responsible for conducting the tasks and whose informational inputs are necessary for a comprehensive assessment. Ensure that everyone involved is trained on the process and technology. Ideally team members will be well versed in data privacy management requirements and best practices.

Process - Design the workflow of information gathering and identify gaps against the requirements. Leveraging best practices and templates in questionnaire form instead of manual checklists will build efficiency. A business will likely need multiple templates to address different types of risk; however, a single template may be effectively used to address a set of processing operations that present similar high risks.

Technology - Data privacy management technology platforms with built-in digital data discovery, data inventory, DPIA / PIA and assessment templates, cookie consent, workflows, and reporting will enable a team to collaborate, guide the workflow process, serve as the central repository of compliance evidence, and facilitate ongoing periodic audits that reflect business changes.

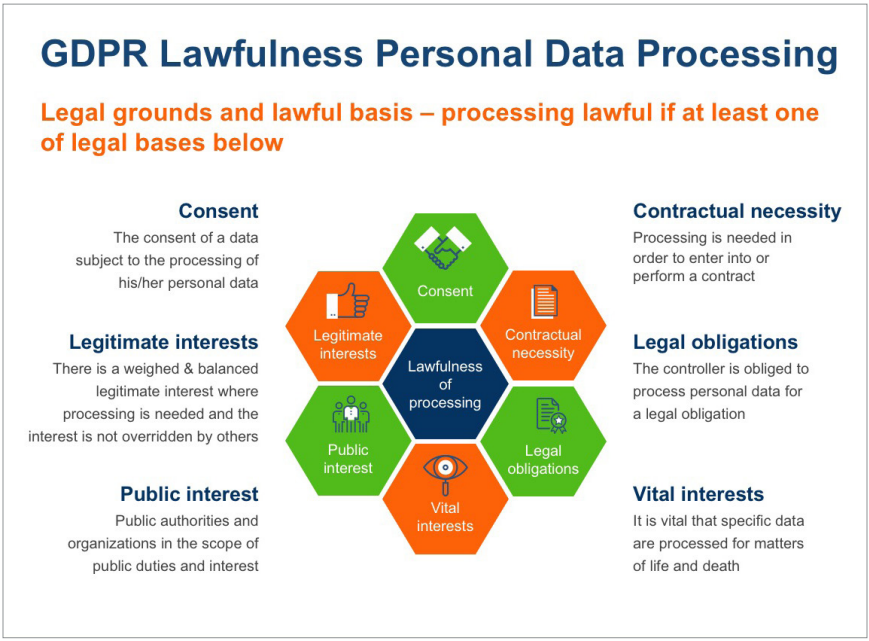
Phase 1 – Build Consensus and a Team

Begin by going back to the stakeholders you first spoke to when determining whether the GDPR applies to your company. Key stakeholders may reside in these departments:

- Engineering
- Human resources
- Information security
- Legal
- Marketing
- Procurement
- Product management
- Website development

With help from these stakeholders, you can gain a high level understanding of your current compliance posture. You need to compare your current practices against a comprehensive list of the requirements, including the following areas:

Collection and Purpose Limitation – does your company have the right to collect the information it collects, and does it use the information only for those limited purposes?



Consent – does your company obtain the right consent for its data processing activities?

Data Breach Readiness and Response – is your company ready to handle data breaches according to the GDPR's requirements?

Data Quality – what measures does your company take to help ensure the relevance, timeliness, accuracy, and completeness of the personal information it holds?

Individual Rights & Remedies – a key change under the GDPR is the expansion of individual rights to include, for example, the Right to Information, Right to Access, Right to Rectification, Right to Restrict Processing, Right to Object, Right to Erasure and Right to Data Portability. Because of this expansion, companies' existing policies, processes, and procedures must be reviewed. In some cases technological changes will need to be made.

Privacy Program Management – how does your company build, oversee, and demonstrate sound privacy practices?

Security in the Context of Privacy – what technical and procedural measures are in place and designed to protect your company's personal data?

Transparency – how does your company disclose its data handling practices to data subjects?

Identify the Designated DPO

See Article 37

A Data Protection Officer (DPO) must be appointed where the core activities of the controller or the processor involve "regular and systematic monitoring of data subjects on a large scale" or where the entity conducts large-scale processing of "special categories of personal data" (e.g., race / ethnicity, political beliefs, defined in Article 9).

The DPO may be an employee or a third party service provider (e.g., consulting or law firm), but should be a direct report "to the highest management level" and shall operate with significant independence, (i.e., the GDPR expressly prevents dismissal or penalty of the DPO for performance of duties and imposes no limitation on length of tenure). Given the rights and responsibilities assigned to the role, the proper selection of the individual is crucial.

The IAPP has estimated – based largely on company size – that as many as 75,000 DPOs may need to be appointed globally in response to the GDPR.

IAPP & TRUSTe(2016). Preparing for the GDPR: DPOs, PIAs, and Data Mapping. https://trustarc.com/resources?doc=643

Phase 2 – Assess Risks and Create Awareness

Conduct a Comprehensive Data Mapping Analysis

See Articles 15; 24; 30; 32

To help ensure you have uncovered all of the risks and appropriately prioritized your plan, you must have a solid understanding of your organization's complete data lifecycle. The process to document this lifecycle is referred to as a data inventory analysis or data mapping. This process generally involves:

- Gathering information from key contacts across the company about what information they collect and use, how it is used, where it is stored, how it flows through and out of the company, who has access to it, and what protections are in place at each point; in other words, gather details about data collection, storage, usage, transfer, processing, and disposal.
- Documenting this information in the form of inventories of data and visual "maps" of the data movement.
- Analyzing risk points and triggers for various GDPR or other requirements.

43% of companies report they already conduct data inventory and mapping projects, and another 30% are planning to do so in the next 12 months.

IAPP & TRUSTe (2016). Preparing for the GDPR: DPOs, PIAs, and Data Mapping. https://trustarc.com/resources?doc=643

Data Inventory Projects are characterized by a high degree of cross-functional collaboration, with 70% reporting they work with IT and 62% with Information Security to complete the projects. 49% also reported the projects are either solely or partially (along with privacy) funded from the IT / Security / Compliance budgets – while 19% reported the projects are solely funded from the privacy budget.

IAPP & TRUSTe (2016). Preparing for the GDPR: DPOs, PIAs, and Data Mapping. https://trustarc.com/resources?doc=643

TIP

Getting Buy-In

Getting buy-in requires you to speak the language of the department you are trying to engage. Here are some examples:

- Information Technology: identifying storage redundancies can reduce IT complexity and save IT dollars.
- Information Security: understanding what data reside in which systems can help Security prioritize their protection efforts and establish appropriate access controls.
- Operations: visualizing flows and uses of data throughout the company can help Operations identify redundancies and improve efficiencies.
- Procurement: identifying points at which the company shares information with third party vendors and understanding the sensitivity of the data being shared can help procurement approach third party management and contracts in a risk-based, efficient approach.

Below is an example of a common data classification schema:

Special Data Categories	Personally Identifiable Information (PII) – Sensitive	Personally Identifiable Information (PII) – Non-Sensitive
Payment or Financial Information Health, Biometric, or Genetic Information Children's Personal Information	Data Concerning Health or Data Concerning a Natural Person's Sex Life or Sexual Orientation Racial or Ethnic Origin; Political Opinions; Religious or Philosophical beliefs	Office Location; Business Phone Information Releasable to Public

Conduct Gap Assessment and Assign a Level of Effort

With the results from your Data Inventory you can now conduct a Gap Assessment and develop a Level of Effort (LOE) Matrix to help prioritize what needs to get done first. The table below illustrates sample Level of Effort (LOE) estimates – Low, Medium, and High, which will help visualize your plan's priorities.

Risk Level vs. Level of Effort

Risk Level	Level of Effort: HIGH	Level of Effort: MODERATE	Level of Effort: LOW
HIGH	Data Lifecycle Management Process Privacy Audit Program	Vendor Review Framework Employee Training Privacy Team Data Flow Monitoring Privacy Breach Preparedness	Contract Language for Vendors Privacy Ownership across Organization Data Governance Committee
LOW			Privacy Team Training

Develop Policies, Procedures, & Processes

Armed with the results of the Gap Assessment and understanding of Level of Effort required to address these gaps, assign tasks to each functional area within the business with a timeline for completion. The risk and level of effort associated with each gap can inform task scheduling, with high risk items prioritized first and tasks requiring significant levels of effort begun in advance of easier ones.

Most companies will find that policies, procedures, and training are critical components of filling in GDPR compliance gaps. Documenting expectations for employees and vendors, carefully describing how individuals should apply those expectations in their daily work lives, and training individuals so that they have the ability to apply those expectations are essential to compliance with the GDPR. Remember also that it is not enough to conform to data handling requirements under the GDPR – your company also must be able to demonstrate that it conforms.

TIP

High Risk Processing

See Articles 9; 10; 35

EU regulators have identified categories of criteria that are likely to result in high risk processing that would trigger the need for a DPIA. This table below provides the categories.

- Evaluation or Scoring
- Automated Decision Making with Legal or Similar Significant Effect
- Systematic Monitoring
- Sensitive data or data of a highly personal nature
- Data Processed on a Large Scale
- Datasets that have been Matched or Combined
- Data Concerning Vulnerable Subjects
- Innovative Use or New Technology
- Interference with Rights or Opportunities
- Other Likely High Risks to the Fundamental Rights or Freedoms of Individuals

Communicate Expectations

See Article 39

Building consensus up-front is critical to the success of any privacy program within an organization, especially a program addressing the complexity of the GDPR. Fundamental leadership principles and organizational decision-making must come into play. Given the expanded scope of the GDPR and likely higher investments required to comply, building consensus will be critical to secure funding.

Make the Case

Approach this process like building any business requirements case by developing a narrative that shows the pros and cons of making the investment. You should use these key communication strategies to establish a compelling story for your GDPR compliance efforts:

Develop the Pitch

The GDPR Impacts our Company…Posing Threats and Opportunities

- Fines and / or expenses responding to regulatory inquiries
- Lost business due to inability to meet customer and partner privacy / security standards
- Loss of goodwill and damage to brand
- Lost business versus companies using strong privacy posture as a competitive advantage

Our Company Has Compliance Gaps That Require Remediation

- Initial GDPR Readiness Assessment results identified multiple gaps and risks
- Cite any internal history of privacy breaches, regulatory inquiries, or enforcement actions

Our GDPR Compliance Program Will Require New Investments

- Proposed project overview with timeline, methodology, and metrics
- Outline the personnel, tools, training, and new processes required
- Benchmark reports depicting GDPR actions by competitors

Share the Pitch with Key Stakeholders

Facilitate an internal kickoff and ongoing planning sessions with relevant stakeholders across the organization. Include representatives throughout the company including colleagues at executive and board levels. Build and deliver an engaging presentation leveraging all of the evidence you gathered to tell the story. Involve any department that touches customer or employee data, whether they are on the collection end or simply have access to the data.

At the outset, it will be important to clearly state the following goals of the kick-off session:

- Formalize GDPR program team structure / roles / responsibilities
- Establish the GDPR program as a priority initiative
- Agree on short, medium, and long-term goals of the GDPR program
- Set measurable objectives with success criteria and key milestones
- Secure budget and resources based on Level of Effort estimates

If your company already has a Privacy Working Group, this campaign would be an add-on to that existing process. If your company does not have a working group, building one will provide ongoing value for years to come. Schedule ongoing planning meetings with a regular cadence to develop the full plan, implement all required operational changes, and provide a dashboard report on the GDPR program's progress.

Once everyone understands the urgency, conduct training to help stakeholders understand what is required and the types of changes your company will be making.

TIP

Sample Training Agenda

- Overview of the GDPR – why it is important and what it requires.
- Describe how the GDPR impacts your company.
- Discuss the company's GDPR activities and timelines.
- Explain how each stakeholder will participate in these activities.

After you have completed your plan and achieved organizational support, you can begin to implement the various components required to operationalize your compliance. These will include a range of initiatives, from hiring new personnel, training existing personnel, establishing new processes, and implementing new technology.

Many of these items can be completed in parallel, depending on your organization's resources and risk status as outlined in the planning cycle. The time to complete this phase will vary greatly by company size, budget, and compliance gaps.

Phase 3 – Design and Implement Operational Controls

Mechanisms to Obtain and Manage Consent

See Article 7

Requirements regarding Consent under the GDPR are significantly more robust and are delineated for specific circumstances.

- Informed / Affirmative Consent to Data Processing. "A statement or a clear affirmative action" from the data subject, must be "freely given, specific, informed and unambiguous." While the data subject can affirmatively tick a box, "silence, pre-ticked boxes or inactivity" would be insufficient. Consent must be specific to each data processing operation and the data subject can withdraw consent at any time.
- Explicit Consent to Process Special Categories of Data. Explicit consent is required for "special categories" of data, such as genetic data, biometric data, and data concerning sexual orientation.
- Explicit Parental Consent for Children's Personal Data. Affirmative parental consent is required for data belonging to children under the age of consent (16 years). Member states may set a lower age that is not below 13 years. "Reasonable efforts" must be made to verify that the parent or guardian provided proper consent.

Address International Data Transfer - Standard Data Protection Clauses

See Articles 44-50

The GDPR allows for data transfers to non-EU countries by way of mechanisms that provide appropriate safeguards. Under Article 46, appropriate safeguards include: Binding Corporate Rules (BCRs), Model Contract Clauses (MCCs) also known as Standard Contractual Clauses (SCCs), and legally binding documents and enforceable instruments between public authorities or bodies.

Depending upon your organization and its goals, there can be benefits and drawbacks of each mechanism. For example, BCRs are often considered the gold standard, but the cost and effort required is prohibitive for some companies.

Individual Data Protection Rights

See Chapter III; Articles 12-23

The GDPR provides the following protections for individual rights, for example, Right to Information, Right to Access, Right to Rectification, Right to Restrict Processing, Right to Object, Right to Erasure and Right to Data Portability. New processes and technological capabilities may have to be created within your organization to receive, escalate, and accommodate requests pertaining to these rights.

Physical, Technical, & Administrative Safeguards

See Article 32

The GDPR recognizes that sound privacy is not possible without good security. With this in mind, companies must take physical, technical, and administrative measures to keep personal data safe. Though the GDPR does not refer to a specific security standard or certification, as part of its GDPR compliance efforts, your company should carefully review security protections and address gaps.

Phase 4 – Enhance Controls

Develop DPIA Program

See Article 35

Conduct a Data Privacy Impact Assessment for any data processing that may result in "high risk".

Each DPIA shall contain:

- A systematic description of the processing operations and their purposes
- An assessment of the necessity and proportionality
- An assessment of the risks
- The measures needed to address the risks

Research conducted by the IAPP and TRUSTe showed that the majority of organizations use a combination of manual methods and technology.

71% companies conduct DPIAs regardless of any impending legislation

IAPP & TRUSTe(2016). Preparing for the GDPR: DPOs, PIAs, and Data Mapping. https://trustarc.com/resources?doc=643

With the increased requirement to do more DPIAs, and be able to produce records on demand, ensure you have an efficient process and a centralized system designed specifically for DPIAs.

The frequency of assessments varies widely across companies – from as few as 1-2 to as many as 1,000+ per year. The time investment also varies widely, ranging from 25% taking less than one week to 15% taking longer than a month.

IAPP & TRUSTe (2016). Preparing for the GDPR: DPOs, PIAs, and Data Mapping. https://trustarc.com/resources?doc=643

If you don't already have a DPIA process in place at your organization, it's critical to start building one so that you can conduct the initial DPIAs and additional DPIAs to cover ongoing changes to the business.

As you work through the DPIAs and identify compliance gaps and the measures needed to remediate, the next step is to remediate. It's important to document remediation activities and track gap closure in one central place so you'll have accountability-on-demand in the event of an inquiry.

Data Necessity, Retention, & Disposal

See Article 25

Process only the data that you need. Companies should consider anonymization and pseudonymization techniques after it is no longer necessary to retain or store information in an identifiable form.

Data Integrity & Quality

See Article 32

Maintain assurance that data are not changed without authorization; and take measures to help ensure that data are accurate, relevant, timely and complete.

Build Security & Data Breach Response Plans

See Articles 33-34

Revise information security policies, breach incident response plans & deploy training so that your company can comply with the new 72 hour notification (which applies to notification of the DPA), "without undue delay", for breaches with potential for serious harm.

Chapter III: Maintain Compliance

After your company has taken the time to diligently work through all of the activities in the plan, you will have started to secure GDPR compliance and protect the company's hard-earned brand reputation, goodwill, and business valuation.

Now it's time to maintain compliance by maintaining these activities going forward.

Sample Timeline

This sample timeline suggests how to maintain your GDPR compliance program. Some ways to conduct program health checks and maintenance include: practicing incident response, practicing individual rights responses, creating resources and training for your Data Protection Officer (if applicable), and establishing a calendar for review of compliance activities. Third party management should include auditing third parties your company works with and spot checking on-boarding and off-boarding procedures. Additional maintenance can include checking opt-ins, opt-outs, and database quality.

This guide will provide tips on how to maintain the following components of a GDPR compliance plan, and it will give best practices tips and case study examples: maintaining records of processing, conducting DPIAs / PIAs, consent management, and individual rights management.

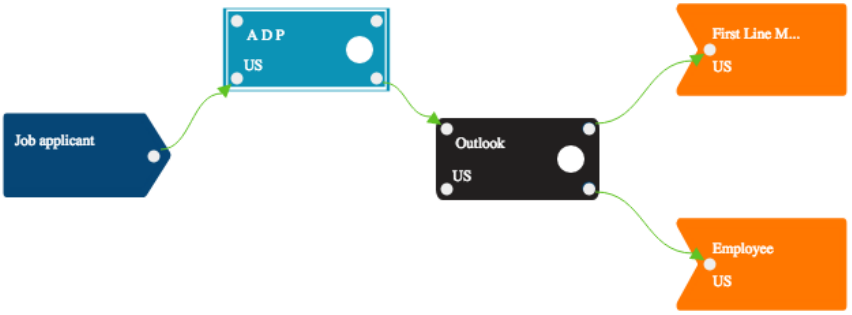
Maintaining Records of Processing

Article 30 requires companies to produce "records of processing activities", which will allow regulators to see that companies are adhering to GDPR. With this goal in mind, the records should show why and how the data is being processed. Although May 25th has passed, companies still need to be compliant every day after. A fundamental key to staying compliant is introducing a process.

A process that focuses on how data is collected and why it is collected will help you adhere to GDPR requirements. Strictly focusing on the data elements themselves may cause a company to overlook important elements. For example, if an online clothing retailer collected a customer's national identification number, asking why they need this information would likely tell the retailer it is not necessary to collect that information. Having a process in place will help your teams to keep these things in mind.

Follow the Data

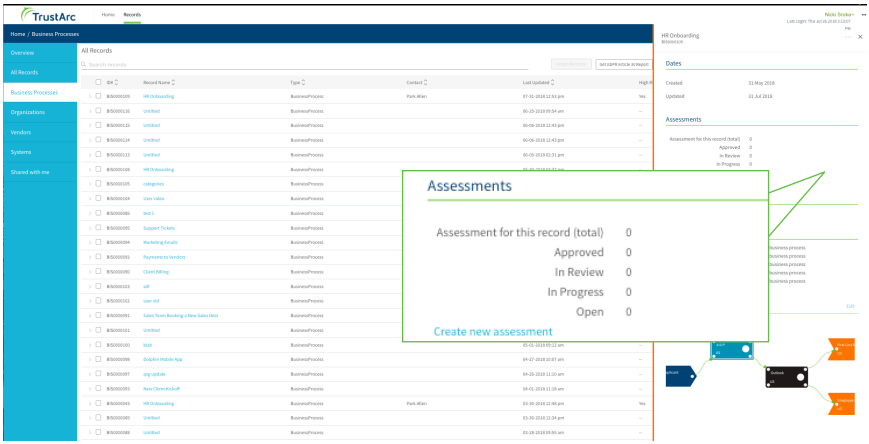
Your process should "follow the data" at a high level. Decision trees aren't needed - look at what data is being collected, who is accessing it, and how long it is stored. If you use an IT system oriented architecture map as a starting point, make sure decision trees aren't included. Assume that data will move to the next step because you need to see how the data flows through the organization in order to assess risk.



Sample data flow map in TrustArc Data Flow Manager

Tie in Data Inventory Upkeep to Your DPIA / PIA Process

Each time there is a new process or a process change with an organization, vendor, or system, you should update your data inventory. Additionally, changes in practices as reflected in your data inventory may indicate a new high risk processing activity. The key is keeping records up to date and treating them as living documents because this will help in managing data privacy risk profiles. It will also help in identifying changes in processing activities that may trigger high risk, requiring further assessment.



TrustArc Data Flow Manager and DPIA Assessment are connected

By creating this process you will be going beyond just checking off checkboxes, you will be implementing a privacy risk program.

Case Study

Scenario: My company still hasn't implemented a PIA/DPIA process yet. What should we do first?

First, review business processes you have documented in your data inventory to identify those that are high risk activities. If you are using TrustArc Data Flow Manager, to view high risk activities, click on the Business Processes left hand menu item to see a list of your business processes. Those processes with a "yes" in the High Risk column may require a DPIA.

Once you have conducted initial required DPIAs, consider touch points in your processes in which the PIA/DPIA process should begin. Some organizations use a business process being classified as "high risk" to trigger a DPIA, but there may be other points at which a risk assessment is useful. For example, Procurement may trigger a risk assessment whenever a new vendor is being considered. Product Managers may trigger a risk assessment whenever a user story is being considered that impacts personal data.

The privacy office should work with the owners of key business processes to determine the factors for when a privacy risk assessment needs to be conducted. Ensure that the risk assessment is being conducted early in the data life cycle, especially if the organization is collecting or creating new data.

For example, if your company offers a SaaS technology platform for privacy compliance and the product team thinks of a new feature that will be incorporated in a new version of the product, the privacy by design concept that your company follows will make sure that privacy considerations are incorporated into the development.

Best Practice Tip

TIP

Don't choose to implement this process at the finish of the project because at that point it will be too late to make changes.

Best Practice Tip: Technology can help!

TIP

Train your organization's privacy stakeholders on the assessment process. Provide training, technology, and tools needed to implement the processes. Some organizations use data stewards at the business unit or product line level to help ingrain the assessment process throughout all levels of the organization. Data stewards help drive the assessment process by creating the assessment kickoff, updating responses, or responding to gaps identified during the assessment process. Like the stakeholders, the data stewards also need to be trained, have access to tools, and have visibility into the organization to drive these activities.

Best Practice Tip

TIP

Training is key.

Test Your Process

After developing a new process, such as tying in data inventory upkeep with your DPIA / PIA process as described above, test that process to ensure it is working. A great way to test your process is by conducting a simulated data breach, with each team member running through his or her role. To respond to the simulated breach the team will have to identify the data that was breached, which will require finding where it was residing and which processes were affected. These requirements will force the team to see whether information is being kept up to date. For example, would the team be able to identify every vendor that had access to that data? Similarly, many companies find processes that use a particular vendor that may not have been documented. Or, even if processes have been documented properly, a company may realize it requires a more granular level of detail. These simulations should be conducted with a regular cadence.

Best Practice Tip

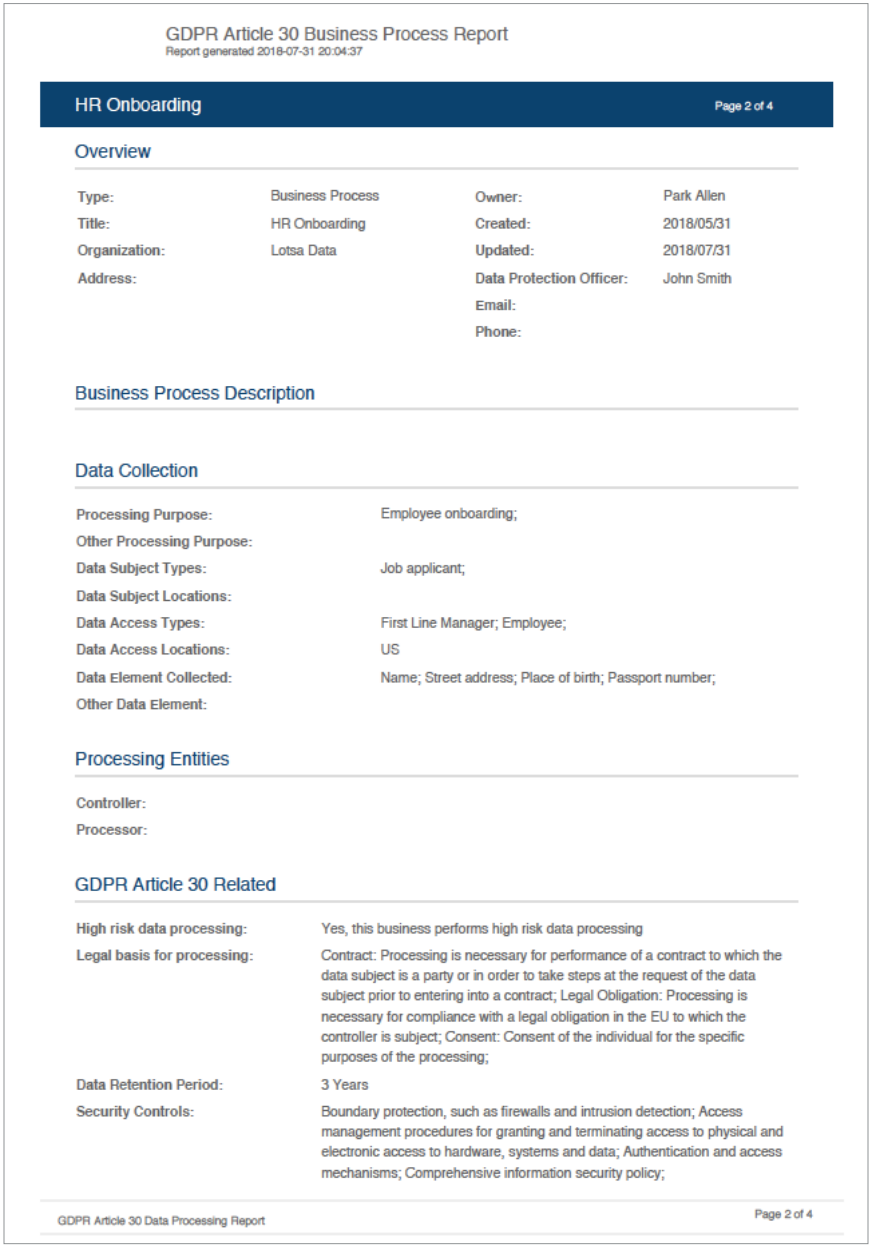
TIP

Simulating a data breach will allow you to test your new program to see whether it's working.

Accountability on Demand

See Article 30

Having up to date business process information will be key to meeting Article 30 compliance report requirements because the company must produce the reports upon request from a Data Supervisory Authority. Maintaining up to date and accurate information on your organization's processing will also help to demonstrate accountability that the processing activities are compliant with GDPR. Using an automated solution that can help keep records of these business processes up to date and produce on demand reporting can be helpful. Meeting Article 30 requirements may require some companies to shift the way they approach looking at how data exists in their organization. Instead of creating static lists of IT applications, mapping business processes can help explain "the how and why" of a company's data processing, thereby making Article 30 reporting easier. Recording information necessary for an Article 30 report while building visual maps of how the data moves throughout the organization is an efficient way to keep track of a company's data flows and better address risk.



GDPR Article 30 Business Process Report
Report generated 2018-07-31 20:04:37

HR Onboarding Page 2 of 4

Overview

Type:	Business Process	Owner:	Park Allen
Title:	HR Onboarding	Created:	2018/05/31
Organization:	Lotsa Data	Updated:	2018/07/31
Address:		Data Protection Officer:	John Smith
		Email:	
		Phone:	

Business Process Description

Data Collection

Processing Purpose:	Employee onboarding;
Other Processing Purpose:	
Data Subject Types:	Job applicant;
Data Subject Locations:	
Data Access Types:	First Line Manager; Employee;
Data Access Locations:	US
Data Element Collected:	Name; Street address; Place of birth; Passport number;
Other Data Element:	

Processing Entities

Controller:
Processor:

GDPR Article 30 Related

High risk data processing:	Yes, this business performs high risk data processing
Legal basis for processing:	Contract: Processing is necessary for performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract; Legal Obligation: Processing is necessary for compliance with a legal obligation in the EU to which the controller is subject; Consent: Consent of the individual for the specific purposes of the processing;
Data Retention Period:	3 Years
Security Controls:	Boundary protection, such as firewalls and intrusion detection; Access management procedures for granting and terminating access to physical and electronic access to hardware, systems and data; Authentication and access mechanisms; Comprehensive information security policy;

GDPR Article 30 Data Processing Report Page 2 of 4

Sample Article 30 report in TrustArc Data Flow Manager

DPIA / PIA and DPIA / PIA program

Privacy Impact Assessment (PIA)

A PIA is a tool that can be used to identify and mitigate risk associated with a product, service, business process, or other organizational change. PIAs are typically conducted before:

- a new product launches;
- a new business process is implemented;
- new companies are acquired;
- existing products, processes or systems are changed; or
- a company expands the countries in which it conducts business.

Depending upon the level of risk involved, an organization may choose to conduct a more or less comprehensive PIA.

A DPIA is designed to help an organization assess the risk associated with data processing activities that may pose a high risk to the rights and freedoms of individuals.[1]

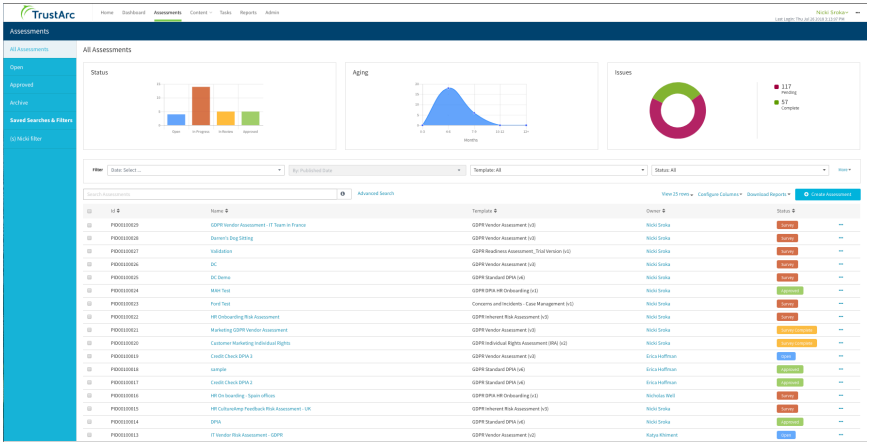
The GDPR does not specifically list the types of processing that are likely to result in such risk, however, it does indicate examples of adverse outcomes to individuals that may result from such processing, such as identity theft or fraud, discrimination and financial loss, which are similar to the types of harms recognized under some security breach notification laws in the U.S.[2] The EU Article 29 Working Party (A29) has, however, defined nine criteria for high risk processing which can serve as guidance. The categories include: evaluation or scoring, automated-decision making that has legal effects, systematic monitoring, the processing of sensitive data, data about vulnerable subjects, data on a large scale, data sets that have been matched or combined, development of new technology or innovative use of existing technology, and processing that prevents individuals from exercising a right or using a service or contract.[3]

1. GDPR Article 35(1), illustrated by Article 35(3) and complemented by Article 35(4).
2. See GDPR Recital 75; Fla. Stat. Ann. §501.171; Ind. Code §24- 4.9;
3. Article 29 Data Protection Working Party. (2017). WP 248 rev.01: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purpose of Regulation 2016/679. Retrieved from http://ec.europa.eu/newsroom/document.cfm?doc_id=47711.

The GDPR provides only a general description about how DPIAs are to be conducted. Article 35 does, though, set forth four elements that a DPIA assessment must contain [4]:

1. a systematic description of the processing operations and their purposes;
2. an assessment of the necessity and proportionality;
3. an assessment of the risks; and
4. the measures needed to address the risks.

An organization seeking more information on conducting a compliant DPIA should look to the A29 Guidance.[5] The A29 Guidance suggests, for example, that a compliant DPIA will include a systematic description of the processing, how necessity and proportionality are assessed, how the risks and freedoms of data subjects are managed, and how interested parties—such as the advice of the DPO—are involved.[6]



TrustArc Assessment Manager Dashboard

1. Article 29 Data Protection Working Party. (2017). WP 248: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purpose of Regulation 2016/679. Annex 2. Retrieved from http://ec.europa.eu/newsroom/document.cfm?doc_id=47711
2. Article 29 Data Protection Working Party. (2017). WP 248: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purpose of Regulation 2016/679. Annex 2. Retrieved from http://ec.europa.eu/newsroom/document.cfm?doc_id=47711
3. Article 29 Data Protection Working Party. (2017). WP 248: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purpose of Regulation 2016/679. Annex 2. Retrieved from http://ec.europa.eu/newsroom/document.cfm?doc_id=47711

Building and Embedding a DPIA Process

While most companies will have a DPIA process in place by now, it is worth reiterating that DPIAs need to be conducted according to a documented process to ensure consistency. Many organizations lack a defined process, or conduct assessments on an ad hoc basis, using spreadsheets and email. This is time consuming and costly. Maintaining documentation to demonstrate accountability, and to manage data processing changes across business process and system life cycles is also difficult when information is stored in various systems across multiple stakeholders.

Organizations should develop and follow a process that makes sense for their size, type of processing, and resources. The following sample process is one that can be adapted to suit the size and complexity of an organization.

Relying on a consistent and well-documented DPIA process will make identifying issues and risks requiring remediation easier and more efficient.

BUILD	the PIA/DPIA process through documented methodology, including any supporting systems
IMPLEMENT	the PIA/DPIA process by providing awareness of the process and engaging stakeholders to participate in the process
ASSESS	business activities by following the PIA/DPIA process methodology
MANAGE	completion of any remediation and any changes to those business activities by following the PIA/DPIA process methodology
DEMONSTRATE	compliance and effective risk management through reliable evidence of the PIA/DPIA process and outcomes

For example, an assessment process could alert your company's privacy team or data steward of a potential change. In turn, those changes will drive updates to the data inventory or an initial threshold assessment to see whether a DPIA is needed. If no DPIA is needed, then the reasons should be documented. If a DPIA is needed, then the on going DPIA process will be triggered. In most cases the DPIA results in reports that describe potential risks and potential action items that the company needs to address or complete for those risks.

Leveraging a technology platform with built-in DPIA templates and other solutions that help with GDPR compliance will enable organizations to implement an effective and robust DPIA assessment process.

TIP

Best Practice Tips

1. Compare changes to the data inventory to identify possible needs for additional DPIAs.
2. Train data stewards in key areas - like Procurement, IT/Security, Product Development, Marketing/Sales, HR - to help identify and escalate new DPIA needs.
3. Establish a way to track remediation efforts identified in the DPIA.
4. Establish a clear workflow for DPIA identification, creation, review/approval, and remediation handling/tracking. Make sure that at least one individual is responsible for each step and provide any necessary training.

For example, some companies use ticket tracking systems to ensure that these items get reviewed and done. Regardless of the technology, companies should make sure that someone is regularly reviewing and monitoring progress on those items. While that person is often someone on the privacy team this role can belong to someone on the legal and compliance team, and some companies split out the action items according to job function. Depending upon a company's priorities, procedural fixes, or technology fixes, remediation items can sometimes take anywhere from a few hours to over six months.

Accountability on Demand

See Article 35

Track remediation action items identified during the DPIA process.

TIP

Best Practice Tip

Keep your DPIA records indefinitely, or for at least six to seven years. DPIAs do not contain any personal information, so keeping all interim versions of each DPIA will show the evolution of how the company has approached privacy.

Consent

Consent as a Lawful Basis for Processing

The GDPR requires that EU personal data be "processed lawfully, fairly and in a transparent manner." The law sets forth six possible legal bases for processing, including a data subject's consent to processing personal data for "one or more specific purposes" per Article 6. Of note, the GDPR further obligates data controllers to inform data subjects of the legal basis for any proposed processing of personal data, for transparency purposes (such as via a company's privacy notice or other just-in-time methods). And, consent must be made as easy to withdraw as it is to give.

For companies seeking to rely on consent as their legal basis for a proposed processing, per its definition in Article 4, consent must be a "freely given, specific, informed and unambiguous" indication of a data subject's agreement to processing, and thus provided by a clear affirmative action.

GDPR Recital 32 adds further explanatory context by noting that the "affirmative" act establishing a data subject's agreement to processing may not be based on silence/inactivity, pre-checked boxes, or bundled together with other terms and conditions. Instead, consent could include--but is not limited to--ticking a box when visiting a website, choosing technical settings, or other written/oral statements that clearly indicate the data subject's acceptance to the proposed processing. In other words, consent may no longer be presumed, implied, or viewed as "opt-out" by default--companies must be able to demonstrate when and how it was obtained.

Special Use Cases for Consent

The GDPR requires a higher level of consent--explicit consent--for the processing of particularly sensitive "special categories" of personal data set forth in GDPR Article 9, which added genetic data, biometric data, data concerning health, or data regarding a person's sex life or sexual orientation to the existing list of "special categories" under EU law.

Processing of special categories of personal data

See Article 9

> *"Processing of personal 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 shall be prohibited."*

GDPR Article 8 also sets 16 years as the default age of consent without parent authorization, but allows EU Member States to set the age as low as 13 years old.

How to Operationalize Consent

As a prerequisite to any data processing activities, an organization should be sure to map all its data flows across each business process of the organization. See above, Maintaining Records of Processing, which describes the steps and clarity that come from undertaking data inventories that can then be used in service of GDPR Article 30 record-keeping obligations, whether in the organization's capacity as a data controller or a data processor.

When this data flow mapping has been completed or updated for the key business processes, and the geographical origin, collection/receipt date, type, sharing, sensitivity, and scale of personal data is understood by the organization across all possible data touch points, then the organization may identify and document the legal bases for processing any and all information.

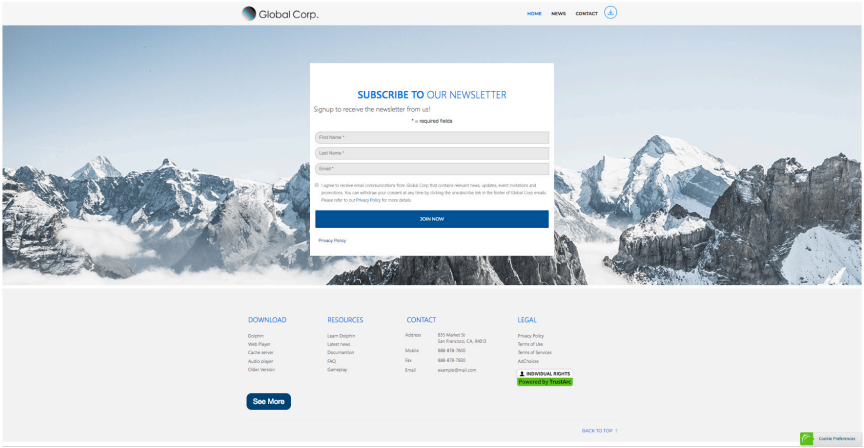
Where it becomes apparent that EU personal data that was collected or received on the basis of consent that does not meet the GDPR's standard for consent, the company should consider with legal counsel whether another legal processing basis applies, or whether data subject consent should be newly requested that meets the GDPR's level.

Best Practices and Tips -- Accountability on Demand

Companies must be prepared to provide records of data subject consent for various possible reasons: per request from the board of directors; to respond to inquiries from regulators; to know what processing purpose was offered at the time consent was given; to confirm whether a request to withdraw consent is valid; to provide to a data subject upon request; and to be able to show a business partner that request was duly obtained to information that an organization seeks to permissively sell to third parties. These are just a few possible uses cases for where consent may need to be evidenced, if it is going to be relied upon as a legal processing basis.

Accordingly, and in keeping with Article 25's Data Protection by Design and by Default requirements, companies should seek to build data subject-respecting consent mechanisms from the idea stage through to the deployment (and ongoing monitoring) stages of any product, service, or form of data collection.

Embedding within digital properties and webforms a mechanism for providing notice, setting forth processing purposes, and then capturing consent, is one scalable way of creating a record of consent for both the data subject and the organization. This consent could then be tied to overall individual rights management for data subjects. For instance, whether requesting permission to drop cookies and other tracking technologies, or asking for consent in the direct marketing context while someone wishes to purchase a product, describing the processing purpose and capturing consent is both respectful of consumers and business-enabling by furthering accountability on demand.



TrustArc Direct Marketing Consent Manager implemented on sample website

Individual Rights Management

While Chapter III of the GDPR has multiple requirements, many companies will already have controls in place which address some of these articles. However, the GDPR expands upon some of the existing individual rights, creating what may seem like "new" requirements. Three Articles that will seem like new requirements for many companies are:

- the right to erasure ('right to be forgotten'), Article 17
- the right to restriction of processing, Article 18
- the right to data portability, Article 20

While most companies will have a process in place, we are providing two case study examples of what companies can do if they have not operationalized a process yet.

Case Study

Global Corp. received over 500 data subject access requests on May 26th, but they do not have a data subject access request / individual rights management process in place yet.

One of the major challenges that Global Corp. faces is authenticating the data subject while also understanding the nature of the request to get some assurance that the need of that person is being fulfilled. Authentication is a responsibility that has to be handled delicately because of the conflicting pressure of ensuring that the individual is authenticated while not feeling like their privacy is violated.

To meet this challenge, Global Corp. should have a process documented that lists which kinds of authentication are required in common situations. Global Corp. can come up with novel ways to authenticate the individual that don't involve that person providing more information, but rather validating information the company has already obtained. Global Corp. also needs to document a process for keeping or disposing of that new information after the individual's identity is validated.

Best Practice Tip

TIP

Think through how diligent you need to be, given the nature of the request, and the risk to the data subject if you get it wrong.

Case Study

Regional Corp. has a technology solution in place, but no process to address individual rights requests. Last week Regional Corp. was bombarded with requests and was not prepared.

To fulfill these requests Regional Corp. will need to do some triage first, then make some initial decisions whether they will honor requests if they are not legally required to. Answering these questions will help them make that determination:

(1) are we going to handle all of these in the same way?

(2) how many requests do we have from "required countries" (EU and Canada)?

After answering those questions, Regional Corp. should use the first one as a test case, and document the process. Once that documentation is in place, Regional Corp. should be able to follow that process.

TrustArc Individual Rights Manager

Best Practice Tips

TIP

- Respond to people without making promises of how you're handling the request by letting them know you've received their request and are working on it. Take the time to understand and work out the processes and document them so that multiple resources are trained to manage requests.
- Take time for each request so that you can understand what jurisdictions are impacted, and what rules apply.
- Don't be afraid to reach out to that individual directly so that you can better understand and authenticate them, or to better understand the nature of their request if it's not clear.

Meeting the requirements for providing the protections for individual rights (data subject rights) may require new processes and technological capabilities within your company to receive, escalate, and accommodate requests pertaining to these rights. The key to having a successful process will be communicating it throughout the company, documenting it, and incorporating it into your overall privacy program.

Chapter III Summary

Maintaining compliance requires diligent planning and training for teams on their roles in helping to sustain GDPR compliance. Technology can help teams automate some of the otherwise manual processes, which will save time and help promote consistency. Technology can also assist teams to keep careful records - both for implementing programs that pertain to requirements such as responding to data subject access requests; and, for demonstrating compliance.

Chapter IV: Ongoing Compliance

Phase 5 - Demonstrate Ongoing Compliance

See Articles 30-31

The final steps on your roadmap should include ways to demonstrate ongoing compliance. Set up methods to regularly review your compliance activities, and keep records that can be used for both internal and external reporting. As you build out your privacy program, identify the way or ways you can prove to internal stakeholders and external regulators your company's compliance with each GDPR requirement. Remember that documentation of privacy notices and records of privacy-related escalation handling activities form an important part of this "demonstrable compliance."

Maintain Ongoing Reporting / Audit Trail

Once all components are implemented, circle back to the GDPR Readiness Assessment and ensure all gaps are closed. In order to ensure a solid audit trail, take the following steps:

- Keep detailed records of any processing performed on personal data
- Schedule periodic audits and ongoing DPIAs, ensuring they reflect any evolving requirements
- Have a Findings Report ready that shows that all GDPR requirements have been met and that you have accountability-on-demand in the event of an inquiry
- House all DPIAs with supporting documentation in a central repository

Maintain Overall Compliance

The GDPR is a complex regulatory regime. Some companies may feel comfortable with their resources available in-house to maintain their GDPR program, whereas others may want to consult an expert or work with a team of professionals to help with certain pieces of the ongoing assessment plan, implementation, and maintenance. Law firms and consulting firms can be hired to provide recommendations.

Full service privacy companies have the staff needed to provide recommendations and the technology needed to leave your company with the tools to manage ongoing compliance. Regardless of how you choose to approach your GDPR assessment, implementation, and maintenance, take the time to assess the nature of your current program status.

Chapter V: How TrustArc Can Help

Solutions

TrustArc has a comprehensive set of privacy management solutions to help you manage all phases of GDPR compliance. Our solutions are powered by the TrustArc Platform along with our team of privacy experts and proven methodology. A summary of our solutions mapped into the five implementation phases is provided below. Note that many of these activities can be conducted in parallel depending on your organization's requirements and resources.

GDPR Compliance Roadmap - 5 Phases

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

Phase 1 Solutions - Build Program and Team

Identifying the right people, aligning everyone on a common set of goals, and providing them with the right tools and resources to accomplish those goals are the first critical steps in developing your GDPR compliance program.

GDPR Maturity Assessment — Comprehensive solution which includes a GDPR readiness assessment, detailed implementation plan, and communications program to build internal awareness and help secure resources and funding.

Phase 2 Solutions - Assess Risks and Create Awareness

Data Inventory and Business Process Mapping — Comprehensive inventory of your data, classification by risk and type, and data flows. Our Data Flow Manager can help meet Article 30 requirements while mapping business processes. Our consulting team is available to help if needed.

Privacy Risk Assessments — Detailed review of privacy risks across your organization and a findings report summarizing gaps and remediation recommendations.

GDPR Policies and Procedures — Develop customized privacy policies and procedures that address GDPR requirements.

Privacy Governance Committee & Employee Training — Develop the policies, procedures, and processes necessary to execute your GDPR roadmap. This can also include customized employee training to address a wide variety of subjects.

Phase 3 Solutions - Design and Implement Operational Controls

Cookie Consent Compliance — Manage user consent regarding the use of cookies.

Direct Marketing Consent Compliance — Comply with GDPR consent requirements for activities such as promoting products and services, surveys, newsletter subscriptions and other marketing activities.

Online & Offline Notice and Consent — Create Fair Processing Statements for employees, vendors, and customers.

Ads Compliance — Manage user preferences regarding interest-based advertising to meet the DAA, EDAA, and DAAC self-regulatory programs.

Privacy Shield Assessment and Verification — Address cross-border data transfers between the EU or Switzerland and the US in alignment with Privacy Shield requirements.

BCR Readiness Assessment — Assessment of the process changes and investments required to pursue BCRs and recommendations to help determine if BCRs are right for your organization.

Model Contract Clause Review — Review of your program to assess privacy risks associated with your Model Contract Clauses.

Third Party Management — Manage third party vendor risk by creating policies and procedures along with training, technology implementation and ongoing management.

Phase 4 Solutions - Maintain and Enhance Controls

DPIA Program Development — Define the assessment processes, create customized assessment templates, train personnel, and implement the technology required to manage a sustainable DPIA program.

DPIA Management — Automate the management of DPIAs via a secure, centrally accessible solution that will enable you to assess privacy risk across your company.

Data Breach Incident Response Plan — Develop a customized incident response process flow, retention schedule, and record keeping procedures along with the tools required to manage them on an ongoing basis.

Phase 5 Solutions - Demonstrate Ongoing Compliance

Certifications — Comprehensive certification & verification program, encompassing standards including FIPPs, OECD, Privacy Shield, and APEC.

Reporting — Generate a variety of reports to help you meet GDPR compliance requirements, including Article 30, and other audit requirements.

GDPR Validation — Demonstrate GDPR compliance efforts and status, using intelligent technology-powered assessments, TrustArc managed services and an independent TRUSTe GDPR compliance validation. GDPR Validation is offered at Practices and Program levels.

Training — Train your teams with either computer-based training or customized computer-based training packages and workshops that can be delivered to certain groups within the Company.

Individual Rights Management — Respond to individual requests with a proven methodology and streamlined workflow.

Why TrustArc

TrustArc provides a unique combination of deep privacy expertise, proven methodology, and powerful technology to solve complex compliance challenges like the GDPR.

Our People

The TrustArc team, located at both our headquarters in San Francisco and offices throughout the US, EU, and Asia, is dedicated to developing and delivering best in class data privacy management solutions. The TrustArc team has helped companies of all sizes across all industries develop and implement privacy programs by using its extensive privacy, legal, technology, business, and project management experience. TrustArc Privacy Consultants and Analysts are recognized data privacy leaders with significant experience using the TrustArc methodology and Data Privacy Management platform at every stage of privacy maturity.

Our Methodology

For two decades TrustArc has continuously refined its methodology to address new and existing laws, regulations, and standards. Additionally, our best practice standards are based upon helping thousands of clients at all levels of privacy maturity. Our processes are powered by our technology solutions to provide an unparalleled level of service.

Our Technology

The TrustArc Platform was purpose-built to address complex privacy compliance and risk management challenges. The award winning SaaS solution was initially launched in 2011 and has been continuously expanded to address automated compliance reviews, cookie consent management, website tracker scanning, advertising compliance, data mapping, and much more. This proven technology solution is backed by an expert team of engineers, used by over 1,000 clients and available in flexible self-service and managed-service delivery options.

About TrustArc

TrustArc powers privacy compliance and risk management with integrated technology, consulting and TRUSTe certification solutions – addressing all phases of privacy program management. The foundation for these solutions is our SaaS-based TrustArc Data Privacy Management Platform which provides powerful, easy to use technologies – and is backed by over six years of large scale operating experience across all industries and client use cases. The technology platform, along with our services, leverage deep privacy expertise and proven methodologies which we have continuously enhanced through tens of thousands of client projects over the past two decades.

Contact

To learn more about TrustArc solutions
visit www.TrustArc.com/gdpr

or call **US** +1 888 878 7830 | **UK** +44 203 078 6495
FR +33 420 102 065 | **DE** +49 221 569 4412

TrustArc
the new TRUSTe

Fall 2018

www.trustarc.com/GDPR