TrustArc

Essential Guide to the GDPR

Practical Steps to Address EU General Data Protection Regulation Compliance

Over 200 Pages of Legal Text Translated into Practical Implementation Steps

Table of Contents

This guide distills the 200+ page GDPR into five discrete phases to help a business develop a plan for 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.

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 replaces the 20 year old Directive (95/46/EC).

The deadline for compliance is 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.

TIP

Am I a Data Processor or Controller?

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

Under the GDPR, companies will be subject to new requirements. For most companies, the new requirements will raise the bar above current privacy practices. Despite its complexity and new requirements, complying with the GDPR can be accomplished by following the five step 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, 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 Matrix

Level of Effort

Risk Level	HIGH	MODERATE	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

- 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.
- Genetic data.
- Personal data relating to criminal convictions.
- Political opinions.
- Racial or ethnic origin.
- Religious or philosophical beliefs.
- Trade union membership.

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.

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.

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

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.

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 – Maintain and Enhance Controls

Develop DPIA Program

See Article 35

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

TIP

Processes Involving Risk & "High Risk"

See Article 35, Section 3:

- Conversions & System Changes
- Database Changes
- International Data Transfers
- Large Scale Processing
- Mergers & Acquisitions
- New Products / Processes
- Security / Data Protection
- Sensitive Data, Genetic and Biometric Data
- Vendor Management

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, now is the time to 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.

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

Chapter II Summary

By taking the time to diligently step through all of the activities in the plan, you will have successfully secured GDPR compliance and protected the company's hard-earned brand reputation, goodwill, and business valuation.

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

Full service privacy firms 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 III: 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

Sample Timeline

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.

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 Priorities 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 so you can access and store data on a consumer's computer or other device after obtaining informed consent.

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 help you 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 — We provides a 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.

Dispute Resolution — Efficiently manage privacy inquiries from customers, and addresses dispute handling requirements for programs like Privacy Shield.

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

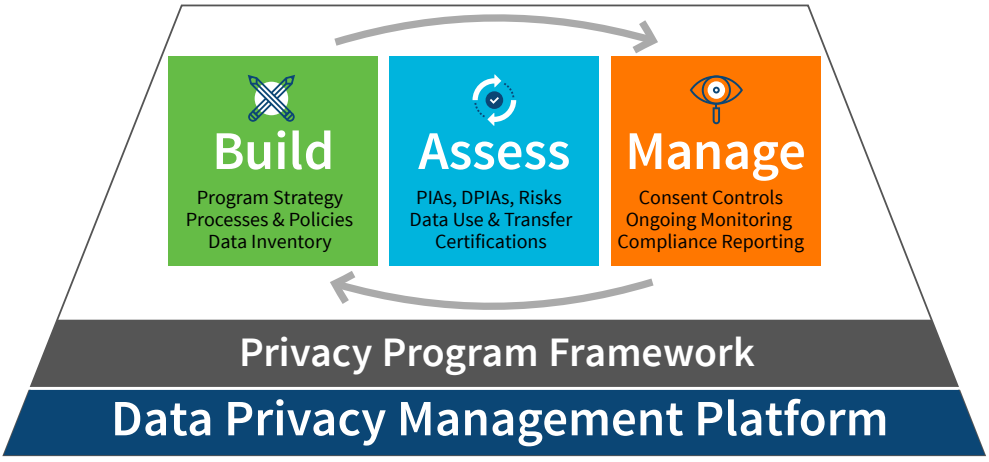
The TrustArc team, located at both our headquarters in San Francisco and offices throughout the US, EU, and Asia, is dedicated to developing and delivering best in class data privacy management solutions. The TrustArc team has helped companies of all sizes across all industries develop and implement privacy programs by using it's 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

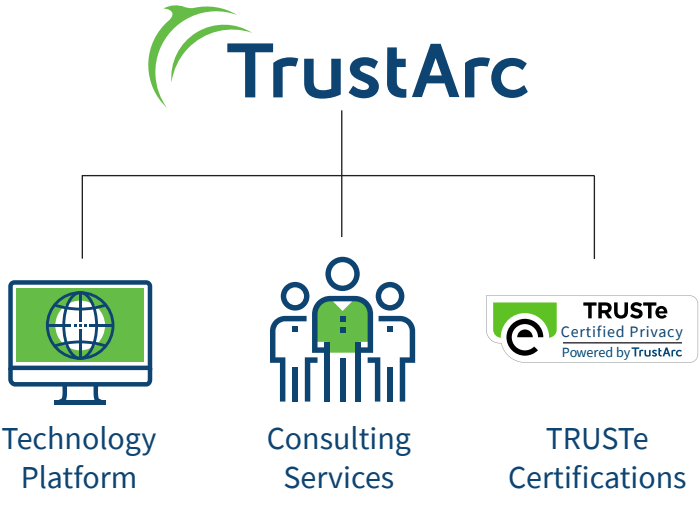
TrustArc powers privacy compliance and risk management with integrated technology, consulting and TRUSTe certification solutions – addressing all phases of privacy program management. The foundation for these solutions is our SaaS-based TrustArc Data Privacy Management Platform which provides powerful, 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. Headquartered in San Francisco, and with offices around the globe, we help over 1,000 clients worldwide demonstrate compliance, minimize risk, and build trust.

Contact

To learn more about TrustArc solutions visit www.TrustArc.com/gdpr or call 888-878-7830 (US) or +44 (0) 203 078 6495 (EU).

TrustArc
the new TRUSTe

TrustArc offers an unrivaled combination of people, process, and technology



US: 1 (888) 878 - 7830 | EU: +44 (0) 203 078 6495

www.trustarc.com/GDPR