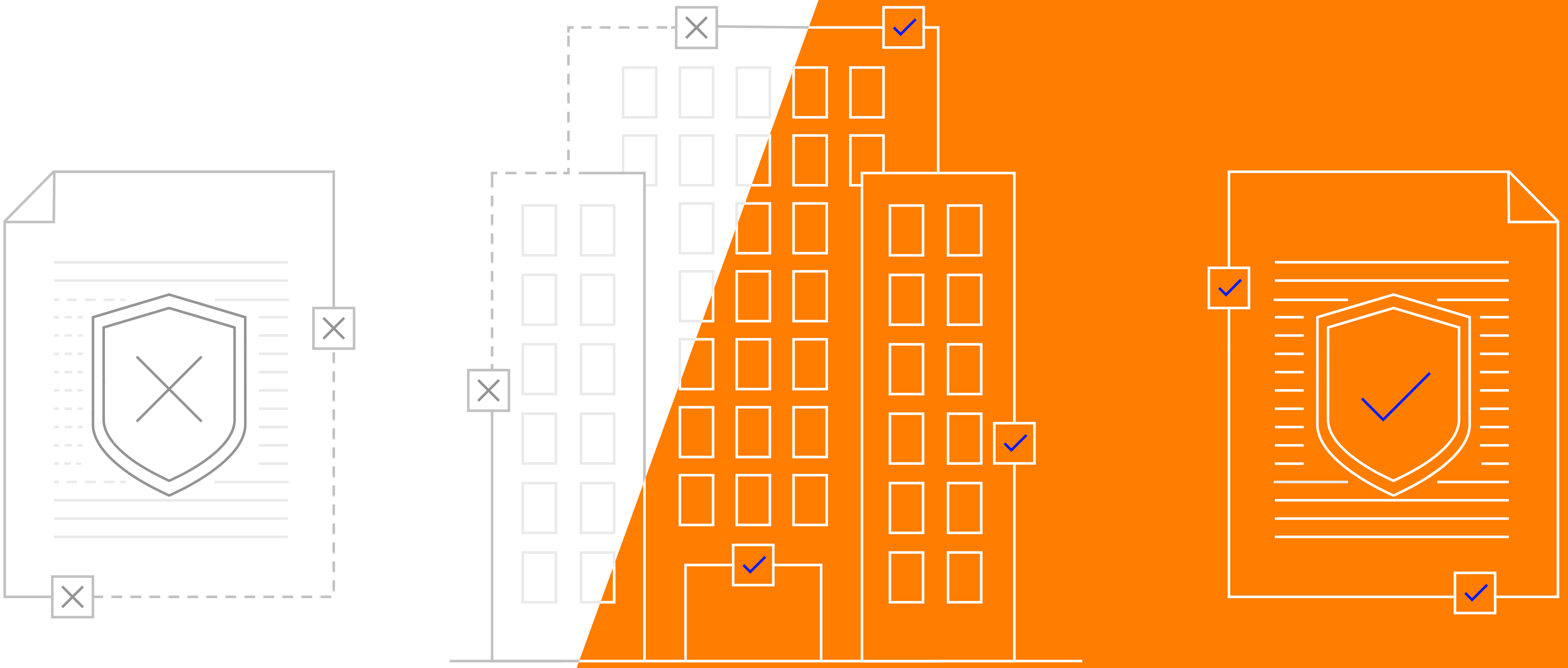
Informatica™



Turn GDPR Into an Opportunity

Become more agile, transparent, and customer-centric

Contents

Tip: Click to jump straight to any section.

GDPR: A Challenge and Opportunity

GDPR is the most disruptive data regulation to hit in decades. It's changed the way we manage, store, and process data and it's triggered a wave of national and state legislation worldwide.

For some, this disruption may be seen as a bad thing — it's created more work, upset long-standing processes, imposed fines, and introduced risk.

But the reality is that GDPR creates huge opportunities for enterprises.

It gives enterprises the chance to:

- Empower their customers.
- Break down data silos.
- Build an infrastructure that unleashes accessible, secure, and trusted.

These aren't things you should do. They're things you must do. These actions are essential if you're to compete in a world that's becoming increasingly data-driven and customer-centric.

If you're a data leader, this regulation is a catalyst — a mandate that supports your organization's data-driven digital transformation. And you'll be encouraged to deliver results, fast. After all, no one wants to get hit with regulatory fines.

This guide is about developing a nascent GDPR compliance initiative into an enterprise-wide program that delivers impactful results beyond compliance.

The six steps of successful compliance-readiness programs the critical capabilities you'll need to lay the foundation for long-term success. An exhaustive guide to compliance, contains practical advice based on our experience working with transformative data leaders.

GDPR can be a huge benefit to anyone looking to transform their business for the better. This is your chance to establish an enterprise data privacy and protection program helps accelerate and lower the risk of digital transformation programs.

In this workbook, we'll show you why.

Identifying Your GDPR Opportunity

GDPR may be a European regulation, but it applies to any organization that has personal data on European citizens.

We’re not just talking about data in your CRM or marketing automation platform, either. GDPR applies to employee, supplier, partner, and customer data.

That’s why the regulation has had such an impact, it applies to every enterprise. Prioritizing European divisions won’t actually help if everyone’s working from centralized data stores.

The good news is the requirements of the regulation set the tone for a lot of crucial digital transformation work.

Here's how meeting core requirements will benefit bigger, more strategic initiatives.

GDPR requirements	Technical requirements	Bigger initiatives that will benefit
Right to access, correction, portability	Visibility into where all customer data lives	Customer & HR analytics, customer experience, personalization
Data protection by default and design	Visibility into all sensitive data, data lineage, and proliferation	Security, operational analytics, compliance
Data accuracy	Ability to collect profile, clean, and standardize data	Analytics, CRM, HR planning, financial reporting
Accountability	Clearly defined roles and responsibilities	Data governance, operational excellence
Notification of breach	Ability to identify and report on breaches when they happen	Data privacy and protection
Limits on purpose for which data is processed	Visibility into data use and consents given	Data governance, intelligent security, commercial programs
Data minimization	Archiving and purging	Customer and HR analytics, personalization
Pseudonymization	Data masking	Intelligent security, personalization, analytics

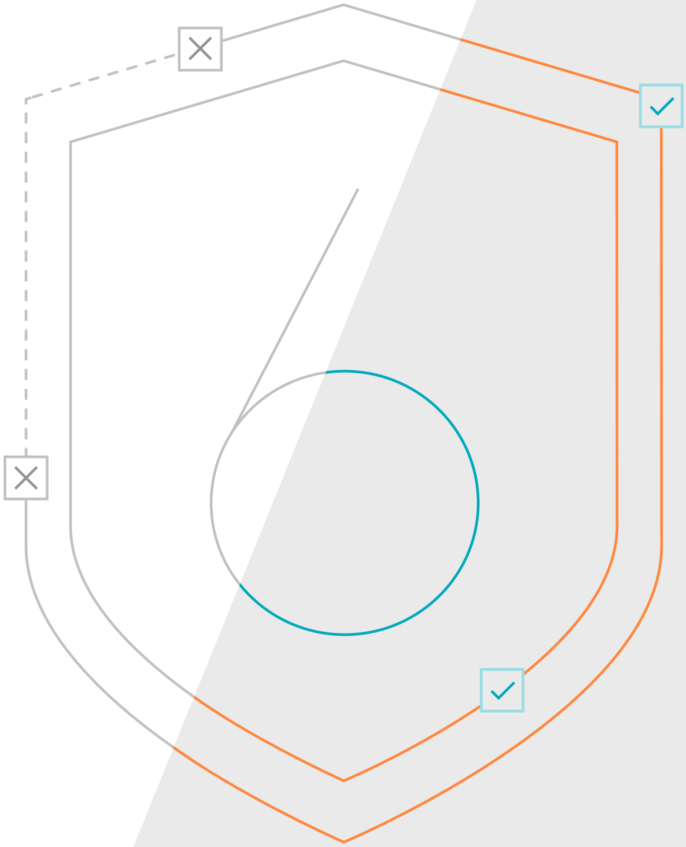
Six Steps to GDPR Readiness — and a Whole Lot More

GDPR readiness is an exercise in data management. You need to collect, clean, govern, and master your data to gain tight control over the critical assets that fall under the scope of the regulation.

This process has six crucial steps:

1. Define and Manage Governance Policies.
2. Discover and Classify.
3. Link Identities.
4. Analyze Privacy Risk and Plan Remediation.
5. Protect Data and Manage Subject Rights.
6. Measure and Communicate.

Let's examine each one and the crucial actions you'll need to take to deliver long-term business value.



Practical checklists

Some chapters in this section include a short checklist of the most important questions to ask yourself at critical steps of your compliance journey. Use them to focus your thinking and track your progress.

↑ ⌂ ↓

1. Define and Manage Governance Policies

To extend your GDPR program across the enterprise, you'll need to embrace data governance—it's the only way to standardize how data is used, moved, and stored. It will also bring everyone in your business onto the same page.

In practice, this means defining policies, identifying key stakeholders, and taking a more granular approach to the data management.

Setting standards

Step one is critical — defining what "good" looks like. You'll need to document data definitions, policies, standards, and processes. You'll also need to assign roles and responsibilities, as well as establish success metrics and KPIs.

A lot of businesses get bogged down documenting rules and forget to invest in the technology and processes that turn into action. Avoid this by empowering your stewards to document policies, standards etc., and create processes that operationalize these rules.

Assigning roles can be another stumbling block. Everyone wants a say on the way their data is governed so establishing a clear decision-making framework is critical. Traditional project management tools like DACIs and RACIs can help here. They can help you map stakeholders into a hierarchy and establish clear lines of communication. That way, everyone can have their say, but only critical stakeholders make decisions.

Read "How to Govern Your Data as a Business Asset" for more detail on the value of these frameworks and practical advice on establishing them.

Laying the foundation for bigger things

Enterprise-wide data governance programs can deliver very real business benefits. Beyond liberating data from silos, they bring people together and create a forum for important discussions.

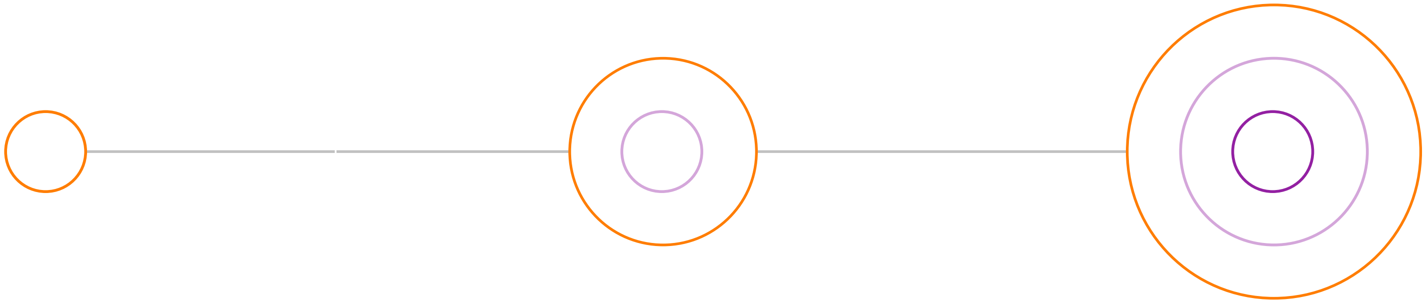
Most importantly, they lay the foundation for almost every major data-driven initiative — from streamlining analytics to building a single view of the customer.

The problem is, they're notoriously difficult to get off the ground.

At least that used to be the case. GDPR presents an opportunity to change this.

It stipulates that every enterprise tackles data governance on an enterprise-wide scale. It must apply to every department and become a strategic initiative, rather than an isolated project.

Data governance is now a business priority and everyone — from analysts to executives — needs to take it seriously.



Scaling data governance

There's no question that scaling data governance is a challenge. The more data that falls under the scope of your program, the harder it becomes to collect, manage, and control it.

Broader programs also involve more people. And aligning disconnected teams around a single goal can be difficult, especially when they each have different (and sometimes conflicting) agendas.

There's no silver bullet solution to these problems. But there are tried-and-tested steps you can take to create a robust and adaptable technical platform that scales seamlessly.

The easiest way to do this is to give datasets a score based on pre-defined criteria. Consider the following when you draw up your list:

Enable collaboration

Data governance is a team sport and sharing knowledge will become more important as you try and scale your program.

Your job is to find key stakeholders and enable them to share their insight into policies, rules, standards, and processes. That way, you can create a single source of truth about your business and data lineage.

Part of the challenge here is to convince people to share their knowledge, but you'll also need to give them the tools to do this. An easy-to-use collaboration tool that unites workflows, policies, definitions, and rules will be a major asset in creating a complete picture of your business.

Look for a solution that will help business stakeholders:

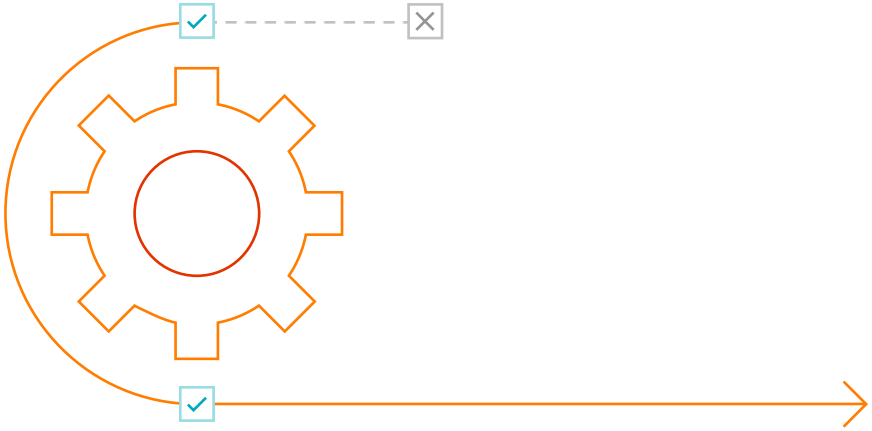
- Define what success means for the program at a policy, rule, and quantitative level.
- Align with their technical counterparts to implement their data management operations accordingly.
- Assess and monitor the state of data on an ongoing basis.

Automate with artificial intelligence (AI)

Data governance involves a lot of repetitive tasks, like data discovery, rule verification, and reporting. You can tackle these tasks manually when your program is small but they can become an issue when you try and broaden your remit. Costs start to spiral, and the sheer volume of work means progress slows to a crawl.

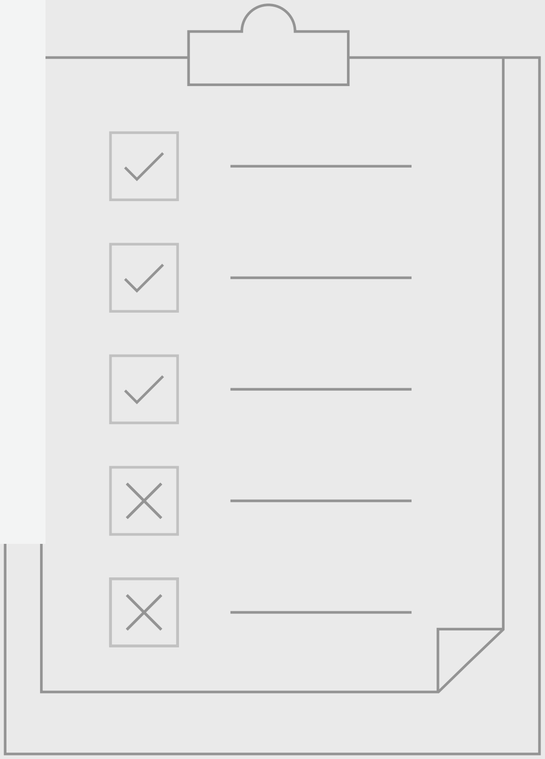
The good news is that machine learning can solve many of these problems. AI tools can now automate data categorization and tagging, as well as link data sets based on shared context. They can even provide users with intelligent recommendations based on previous rule-setting practices.

All of these capabilities add up to huge savings. And when stewards don't have to bother with admin tasks, they can focus on more meaningful projects.



Checklist: Define and Manage Governance Policies

- □ Have you defined what you mean by personal data?
- □ Have you defined policies, standards, and processes?
- □ Do you have the tools to track this as it changes?
- □ Do you have the tools to support ongoing collaboration around policies, processes, etc.?
- □ Can you attach business context to this data?
- □ Have you automated the manual tasks that can hamper your ability to scale your program?



2. Discover and Classify

The deadline for GDPR has come and gone, so it's likely you've tackled the most fundamental step of any GDPR program: discovering the data you'll need to manage. If you haven't, it's time to get started!

To meet GDPR requirements, it's critical that you understand what data you hold, where it's located, how it's used, how it's protected, and how it moves across or outside your organization.

An essential starting point — and an action you should repeat on an ongoing basis — is to discover and classify the personal and sensitive data of EU data subjects.

This isn't a case of building a simple inventory, you'll need intelligence on this data. Consider the following when you draw up your list:

– **Location**
Is the data located or used in a regulated territory?

– **Proliferation**
How does this data move across geographies, departments, and data stores?

– **Data volume**
How many sensitive or personal data records are in this set?

– **Department**
Who uses the data?

– **Sensitivity level**
Is the data considered confidential? Is it only for internal use?

– **Protection**
What controls are presently in place to secure this data?

Checklist: Discover and Classify

Starting from scratch? These are the critical questions to ask yourself:

□ Have you defined what data falls under the scope of GDPR?

□ Have you mapped the internal systems that store this data?

□ Do you know where your partners and suppliers store it?

□ Do you know where this data is coming from?

□ Have you validated the sources of this data?

□ Have you defined the purpose of this data?

↑
⌂
↓

3. Link Identities

☑ ☑ ☑ ☒ ☒ ☒

Identity is central to GDPR and other privacy regulations. Personal and sensitive data must be accurately and holistically linked to the individuals it represents in various systems. This helps you address data subject access rights, and data breach notification requirements.

You'll need to develop a clear understanding of what personal and sensitive data belongs to which individuals. This involves:

- Mapping the geographic location of subjects and the data stores that hold their personal data.
- Measuring an individual's data footprint and risk profile.
- Providing support for a subject's right to be forgotten (RTBF).
- Enabling subjects to submit data portability and access requests.
- Supporting consent management and data breach notifications.

↑ ⌂ ↓

Linking Identities

□ Have you discovered where you're storing personal information?

□ Do you have an understanding of the personally identifying attributes contained in these stores?

□ Do you have a way to match and link records into a common registry for data subjects' identities?

□ Is that registry identifying data subjects in a reliable and timely way?

□ Is this registry searchable, so you can find data subjects when needed?

□ Is this registry secure?

4. Analyze Privacy Risk and Plan Remediation

☑ ☑ ☑ ☑ ☒ ☒

As you analyze risk associated with personal and sensitive data, you'll have multiple scenarios to consider. A framework that reflects your data protection priorities can help you pinpoint a suitable starting point for your remediation efforts. It's also worth considering simulation tools. When you can test security strategies ahead of time it becomes far easier to make critical decisions.

To calculate data privacy risk you'll need to consider what's important to the safety and security of the data itself:

- Is the data personal and/or controlled by GDPR?
- How much is there?
- Is it protected?
- What is the value to the organization?
- Who uses the data, and how does it move around the organization?

5. Protect Data and Manage Subject Rights

The security requirements of GDPR can be boiled down to access. You have to make sure only certain people can see certain types of data as it flows throughout your business.

This applies to personal data used in internal processes, customer services, sales, marketing, order processing, analytics, reporting, and more. Crucially, it applies to data involved in testing and development initiatives. So, even if personal data never leaves the confines of your office, it must be protected.

Practically speaking, you'll need the following capabilities to comply with these requirements:

- **Dynamic data masking**
  Some personal data will touch a huge range of people within your business — though only some of them will be authorized to use it. That means you need dynamic data masking that can intelligently adapt to reveal only the right information to the right individuals.

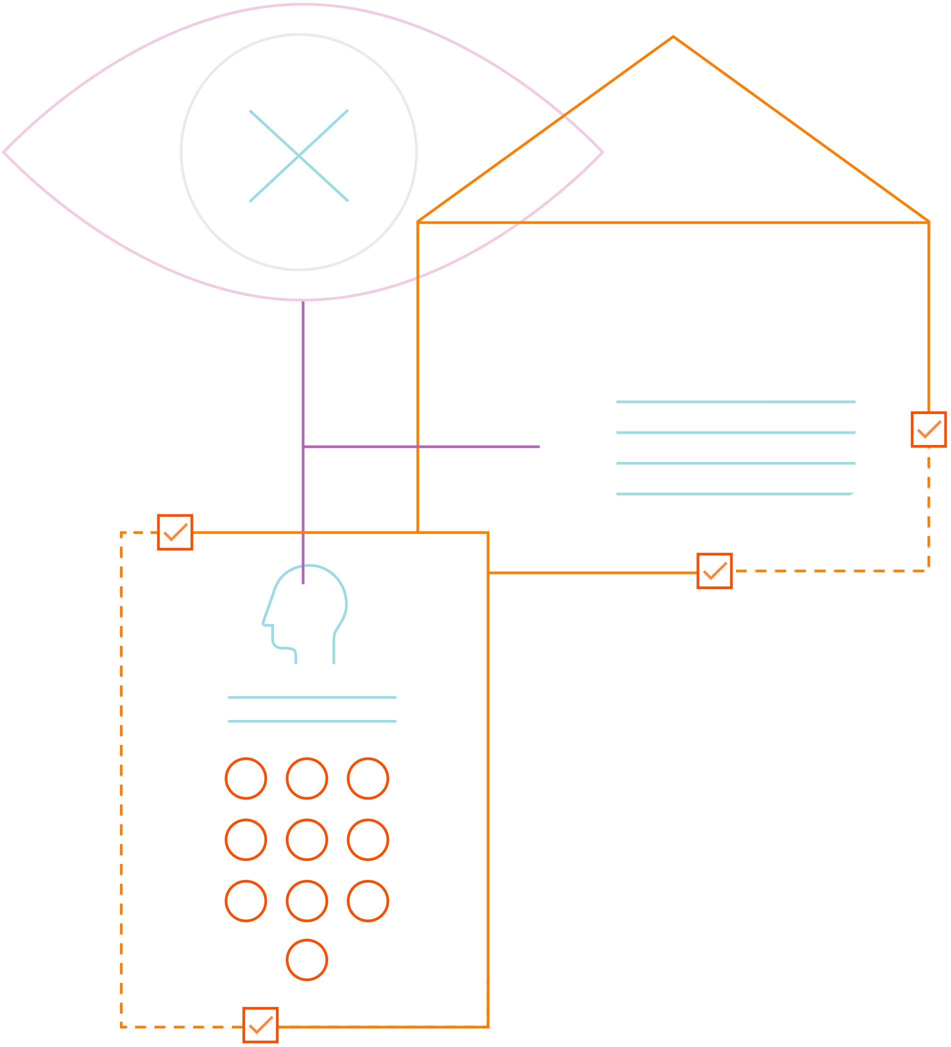
- **Persistent data masking**
  Equally, some of your personal data will touch a lot of people who aren't authorized to access it at all. For example, if you're sending personal details to analysts working on a model, they shouldn't be able to read individuals' email addresses and telephone numbers. This is where persistent data masking comes in. It masks your data wherever it resides, regardless of who accesses it.

- **Data archiving**
  GDPR gives everyone the right to access, request, correct, and erase their data at any moment. If you archive all personal data post-use and take it offline, it'll be much easier to find when a request comes in. It will also protect you against accidental access or usage.

- **Orchestration**
  Access rules change all the time, so you need the ability to adapt security practices on the fly. Orchestration is the ability to coordinate and schedule data protection tasks in accordance with risk. It's critical to staying agile.

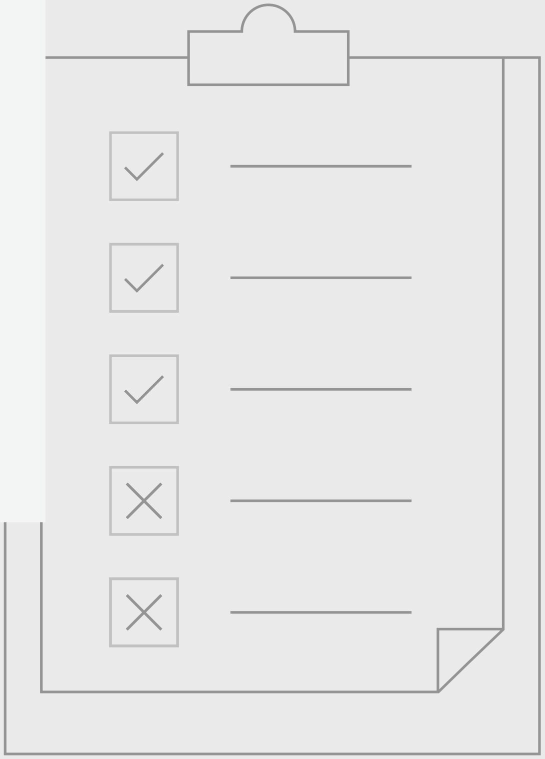
- **Encryption, tokenization, and pseudonymization**
  GDPR specifies instances where encryption and tokenization are necessary, and it encourages pseudonymization. You won't achieve compliance without these capabilities.

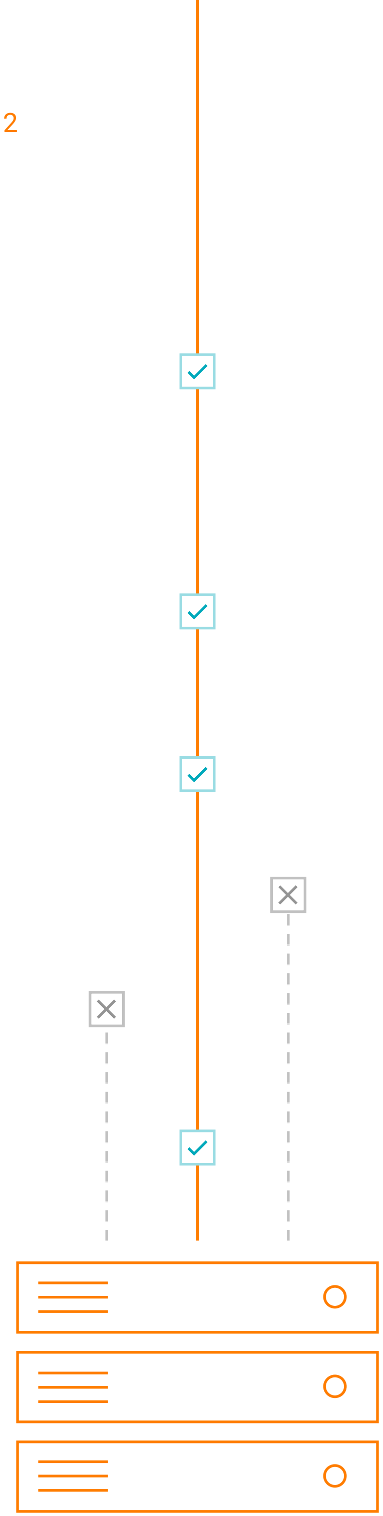
- **Change/Update history**
  To demonstrate GDPR readiness to your internal stakeholders and external regulators you'll need to keep a record of the actions you've taken to meet requirements. For example, every time you compare applications against source systems, you'll need to create an audit trail that can be shared with regulators. Look for a data management tool that does this automatically. It'll save you a lot of hassle in the long run.



Checklist: Protect Data and Manage Subject Rights

- □ Have you applied persistent and dynamic data masking?
- □ Have you used encryption, tokenization, and pseudonymization where appropriate?
- □ Can you coordinate and schedule data protection tasks automatically?
- □ Have you applied risk analysis scores to these tools?
- □ Can you archive sensitive data post-usage?
- □ Have you determined which processes need to be audited and tracked?
- □ Do you have the tools to do this?
- □ What needs to be tracked?
- □ How will you track it?





Some of the most daunting requirements of GDPR are the new rules around subject access requests and consent. You need the ability to provide or remove all of a subject's data when requested, be clear on what explicit consents have been given, and change consent status on demand.

Centralizing this data makes sense and delivers huge benefits beyond compliance. A centralized repository of reliable, current subject data is an invaluable asset for any business that wants to become more customer-centric, transparent, and agile. Suddenly it becomes much easier to enact rights when requested, meanwhile you can accelerate customer experience programs, improve analytics, enhance security, and make personalization a reality.

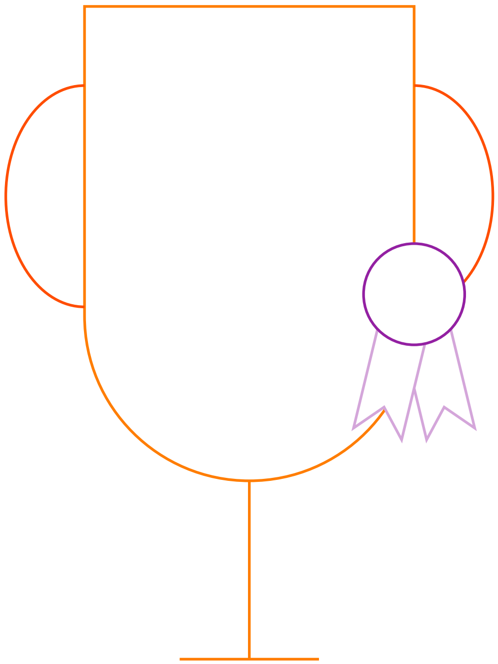
To create this repository, you'll need to master your subject data — collect it, reconcile it, relate it, and standardize it. You'll also need to master consents, including where consent was given, when a consent is revoked, and what data can be used for which purposes. Under GDPR, ignoring changes to consent isn't an option. And if you can't link consent status to specific individuals, you'll open yourself up to huge amounts of risk.

In practice, mastering consents and enacting rights mean matching and merging multiple data sets. Different systems have different pieces of the customer profile. The ultimate goal is to create a single, complete view by matching and merging records across all systems, and then share this trusted information securely across the company.

From a technical perspective, you'll need to:

- Gather and connect to all in-scope data found across systems, sources, and channels.
- Employ algorithms to match and merge all the data you've found.
- Manage the information proactively across its lifecycle so it's always up-to-date.
- Synchronize the data with all required applications.
- Make data subject information and consent status searchable and available when required, on-demand, in all the business process contexts where it's required.

It's possible your existing master data management tools are already fit for purpose, but you need to be sure. You'll also need to determine if the consent-tracking practices of the past match the standards demanded by GDPR. If not, you'll need new solutions to meet them.



Here are the key capabilities to look for when you're vetting your solution:

Discovery

This is the ability to profile data and extract it from source systems. You can leverage the discovery capabilities used in step 1 to do this.

Modeling

GDPR doesn't just apply to your customers so you'll need the ability to model and manage other domains, including prospects, employees, and suppliers.

Data quality processing

Before you can act on data, you need to know that it's high-quality. That requires assessing data completeness and validity. Then, you'll need to apply manual or automatic remediation and establish reporting metrics.

Matching and merging

You'll need the ability to define and apply matching rules based on business process definitions. Then, you'll need to merge the records based on a trusted framework that evaluates the sources, completeness, and accuracy of the data you're combining.

Attributing consent

Once both the subject and consent are mastered, then they can be linked together at an individual level. This way, you can manage, share, and curate data. The result? You get a single, reliable view of the consent status of any data subject your organization interacts with.

Delivering a trusted view of data

This is the big one. This repository should include information on consent status, how and where it was obtained, and how it's managed and governed. And this information needs to be available for any business process where using subject's data depends on an accurate and timely assessment of the subject's consent grants.

Checklist: Protect Data and Manage Subject Rights

□ Have you identified the sources and channels that capture consents and subject data?

□ Have you evaluated the quality, completeness, and validity of this data?

□ Have you found a way to automate and fix problems in your data?

□ Do you know if you have conflicting and multiple versions of the same information? If so, can you efficiently create a single, trusted view?

□ Are you able to link consents and preferences to the subjects that provided them?

□ Do you have a way to ensure the data remains accurate on an ongoing basis with little or no manual effort?

□ Have you considered which other data domains (beyond customer) will be affected by GDPR?

□ Have you looked at how you can extend the benefits of a single, trusted view to other initiatives?

6. Measure and Communicate

Managing data privacy is an ongoing process and you must continually measure the performance of your programs and policies to gauge success and satisfy auditors.

You'll need tools that can generate accurate quarterly and on-demand reports, as well as forecasts. Visualization software will also help you track progress on a day-to-day basis. That way you can stay agile, adapt to shifting priorities and redirect resources when necessary.

Your data privacy dashboards will need to meet the requirements of every business function stakeholder that tracks data privacy and protection KPIs. These include:

- **IT leads:**
  Audit/compliance support, asset value and risk, DevOps privacy.
- **Security leads:**
  Compliance, security decisions, data protection.
- **Privacy leads:**
  GDPR, DPIAs, data subject risk, subject access requests, privacy readiness measurement/tracking.
- **Business/Risk leads:**
  Risk reduction, data governance, regulatory compliance.

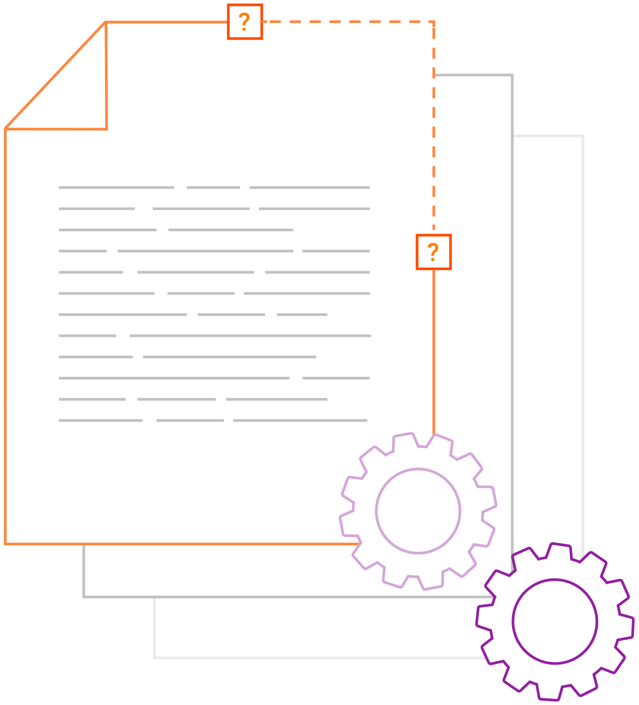
Policy Interpretation – Where IT and the Business Meet

GDPR is a complex regulation that's open to interpretation. Unravelling this complexity is partly a job for legal but it's also up to the business and IT to translate requirements into actual policies and processes.

This is one of the biggest opportunities created by the regulation. Agreement on policy definition, responsibilities, and processes and you can minimize inefficiency and streamline workflows for the long run.

The upshot? Programs move faster, and you can focus on critical initiatives ahead of schedule. More importantly, you create a platform for ongoing collaboration and discussion between some of the most important leaders in your business.

That's a level of alignment that few data leaders have achieved (and many have only ever dreamed of).



GDPR: a Catalyst for Transformation

GDPR compliance isn't just about avoiding fines. It's the basis for a more transparent, collaborative, and customer-centric approach to data management.

It's your chance to:

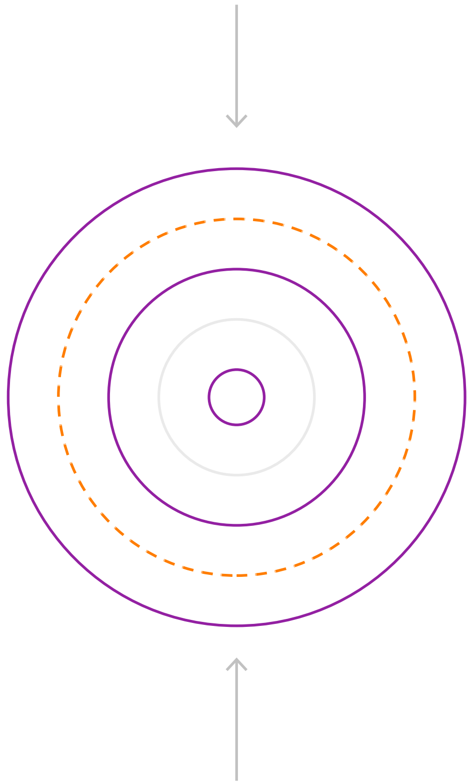
- Create a single view of your customers based on accurate data.
- Build trust with customers.
- Improve data security and tighten privacy controls.
- Connect disconnected departments and unite the business with IT.

Most importantly, it's a golden opportunity to lay the foundations for data-driven digital transformation.

With complete control over your data it becomes far easier to launch, sustain and accelerate critical initiatives like customer and HR analytics, and personalization.

And you can get started right away. The urgency around compliance means executives *must* commit support (and budget) to your cause and it's in everyone's interest to become compliant as soon as possible.

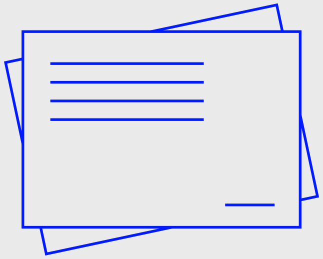
GDPR isn't just a disruptive compliance headache. It can also be the catalyst for data-driven transformation — around the world and within your business. And that's good news for any ambitious data leader.



Further Reading

Ready to get started?

Our GDPR solution can help you tackle every major challenge along the compliance journey — from cataloging data and unifying stakeholders, to understanding customers and linking consents, assessing risk and automating protections. For a full breakdown of key features and benefits, download your copy of the Informatica GDPR Solution Brief today.



DOWNLOAD NOW

About Informatica

Digital transformation is changing our world. As the leader in Enterprise Cloud Data Management, we're prepared to help you intelligently lead the way and provide you with the foresight to become more agile, realize new growth opportunities or even create new inventions. We invite you to explore all that Informatica has to offer — and unleash the power of data to drive your next intelligent disruption. Not just once, but again and again.

Worldwide Headquarters
2100 Seaport Blvd, Redwood City, CA 94063, USA
Phone: 650.385.5000
Fax: 650.385.5500
Toll-free in the US: 1.800.653.3871

informatica.com
linkedin.com/company/informatica
twitter.com/Informatica

CONTACT US

Informatica™