Refactored

Making GDPR Happen

Create a **3-phase plan** for managing individual data-control rights and demonstrating compliance.

Is your company prepared to comply with the European Union's General Data Protection Regulation (GDPR)? *Are you sure?* This sweeping, global regulation—in effect as of May 25, 2018— goes far beyond the double-opt-in practices that are common and familiar in the United States.

The GDPR's rules affect data capture, process, utilization, and management at a deeper level than most organizations realize. As a result, organizations that have put off taking steps toward compliance may be shocked to realize the extent of the technical and process changes that face them—and the associated potential liability.

If your organization is among those that are not yet GDPR compliant, you're not alone. However, given the potentially high costs of non-compliance, it's essential to break through any inertia you're experiencing.

You won't be able to be fully compliant overnight, but having a **realistic, manageable plan** for compliance can create momentum for the changes that need to happen.

This brief eBook isn't intended to be a comprehensive guide to compliance or replace legal advice, but it presents an overview of the types of considerations you'll want to have in mind as you **apply a phased approach** for demonstrating GDPR compliance.

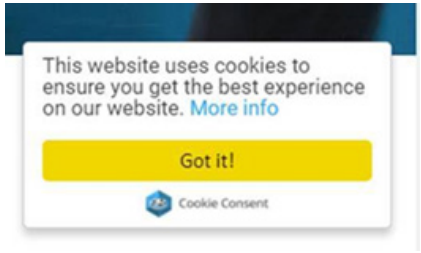
What Is the GDPR?

The General Data Protection Regulation (GDPR) is an EU regulation that creates a uniform approach to data protection. It is applicable to **any company** that offers goods or services to or monitors the behavioral activities of EU data subjects, regardless of that company's geographical location. Failure to comply with this regulation leads to a fine of €20 million or 4% of total global annual turnover, whichever is greater.

Be sure to visit the official **GDPR portal** and consult your legal counsel for clarification on the GDPR's policies and requirements.

Protecting Individual Rights

If you're like most companies in the US today, you already know the basics of data-protection, you're complying with the CAN-SPAM act, and you probably even have a notice on your website that alerts EU visitors that you may be using cookies to collect information about how they behave on your site:



Until now, that cookie-notification box was enough to let users know your organization is collecting data to track their onsite activities and for potential remarketing purposes. Under the GDPR, a simple announcement is no longer sufficient.

The GDPR is popularly supported in the EU because it gives individuals

- control over whether their data can be collected at all;
- knowledge about what data has been collected and when and how their data is used; and
- the ability to stop companies from using or even holding on to data.

Rights of Data Subjects: Some Examples

Let's take a look at some examples of how the regulation may affect your organizational processes.

Right to Data Portability

Individuals can request that you send them all the data you have about them in a portable format.

Action: You must create a form for the request and a process for fulfilling it.

Right to Notification

Individuals must be informed about when and how you're using their information.

Action: You must provide explicit opt-in notices in every place that is associated with personally identifying information, including web forms, contracts, software setup interfaces, and so on.

Right to Be Forgotten

Individuals can ask you to remove all of their personal data from every part of your data store.

Action: You have to know where every piece of data about a subject is stored in your systems and your partners' systems and be able to remove it all.

You may be required to provide proof of the processes you use for informing users and for accurately tracking and removing data. Start putting those processes in place, one step at a time.

The GDPR Is Serious Business: Know the Risks

The aim of the GDPR is to protect the rights of *data subjects*—the people who are your current and future customers. Your company is a *data controller* and is responsible for implementing appropriate technical and organizational measures to demonstrate that all data processing activities are GDPR compliant.

Do I have to worry about the GDPR? *The answer is yes.*

Regardless of where you operate, if you provide goods or services for any person residing in the EU, you must comply with GDPR requirements.

As of November 2017, only **22% of US organizations** were concerned enough about the GDPR to have a compliance plan in place. —*HyTrust*

Will people be looking for violations? *Likely.*

Development of the GDPR has been coming for a long time, and many individuals are more than ready to take back control of how and where their personal information is shared.

The penalty for non-compliance with the GDPR is a fine of **€20 million or 4% of total global revenues,** whichever is greater.

Will I be affected? *Probably.*

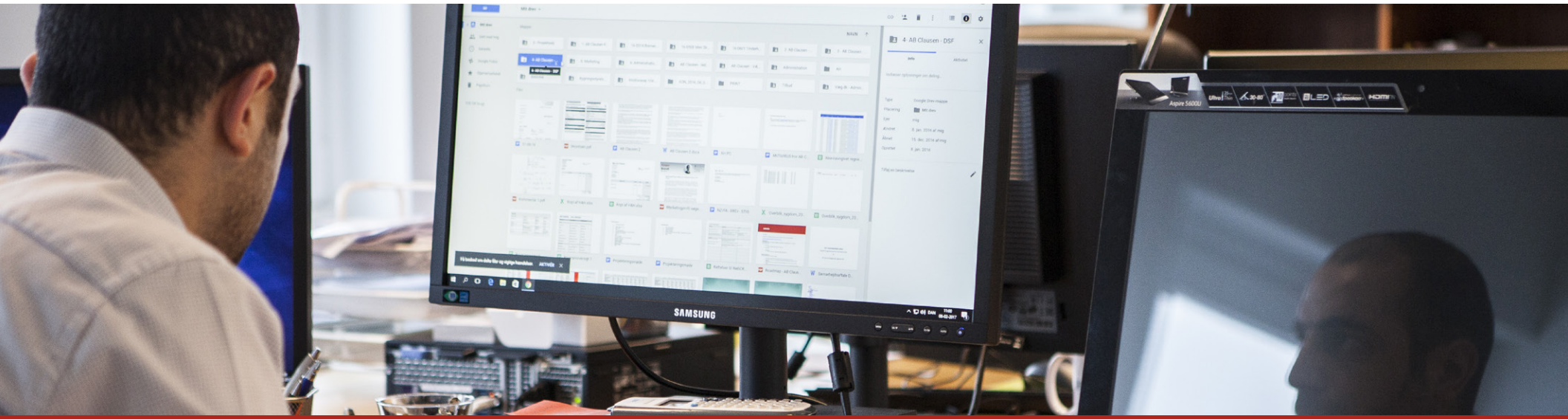
Consequences of non-compliance are serious. In addition to fines, loss of trust and reputation can do substantial damage.

91% of EU consumers expect companies to be 100% transparent about how and when they use personal data. —*Hubspot*

What can I do? *Start where you are—and start now.*

If you're behind on your timeline, it's important to take steps to get into compliance as quickly as possible.

Forrester predicts that **80%** of firms affected by the GDPR will not comply by May 2018.



3-Phase Approach: Break Requirements into Manageable Chunks

What's the rule about how to eat an elephant? One bite at a time.

That's the advice you'll get for almost any large project or goal: break it down into manageable tasks.

For your GDPR-compliance project, use the checklists on the following pages as a guide to help you focus on understanding the changes you're going to have to deal with and setting up a phased plan for making those changes happen.

- **Phase 1: Start at the Front Door**—Review your entire online presence to understand which sites and pages are presented to EU customers and prospects. Set up the appropriate notifications and consent forms online.
- **Phase 2: Optimize Back-Office Data Handling**—Adjust website, marketing, and sales systems to ensure accurate tracking of consent to use personal data. Identify which of your customers are in the EU and conduct a consent campaign. Enable timely notifications about data changes and use, and enable data removal upon request.
- **Phase 3: Formalize Partner Processes**—Extend compliant, two-way data-handling processes to vendors, suppliers, distributors, and channel sales partners.

Because the GDPR requires companies to be able to prove that data has been audited and scrubbed throughout **all** systems that the company uses, full compliance requires a large effort and coordination among all your teams who touch customer data.

Phase 1: Start at the Front Door

Operational layers to address: Digital marketing and initial website visit

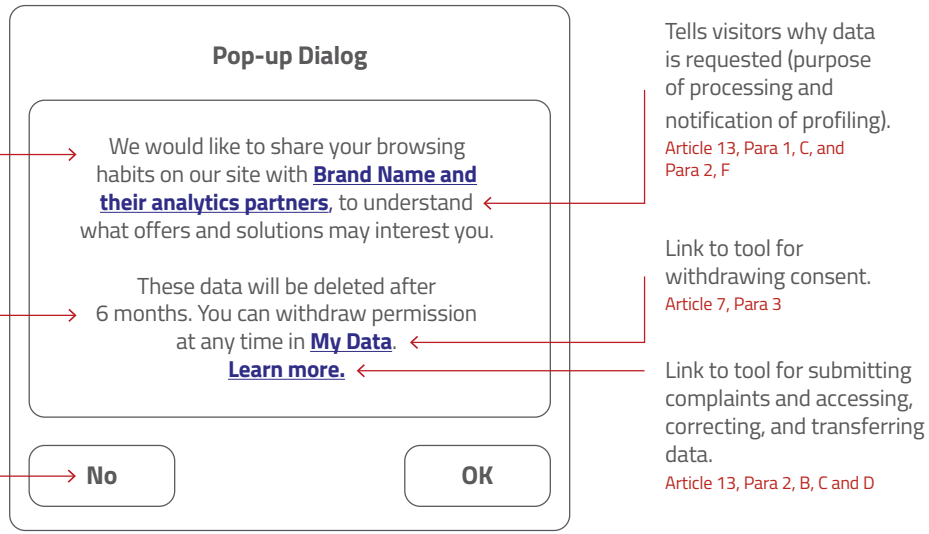
Start by taking immediate steps to show your site visitors that you are working to ensure their data is protected and used appropriately.

Conduct a thorough site review to understand where you are collecting EU subjects' personal data and where you will need to gain consent. Then, you must show visitors how to communicate any request for changing or removing that data.

- As visitors enter from the public internet, are they are being tracked via codes and cookies anonymously? Create an **updated, GDPR-compliant notice that allows people to opt in OR opt out** of any data collection and tracking.
- **Opt in and opt out must have equal weight** and be equally clear and simple.
- **Update your privacy policy** to include information about how and when you will use the data you collect, how long you will keep data, and how data subjects can request to have their data exported to them or removed.
- Create a form and process to **allow data subjects to request their information** in all the places their data may exist.
- Create a form and process to **allow data subjects to request deletion** of all data.
- Add notices and **explicit opt-in/opt-out forms** throughout your website, in contracts, and in any setup for software or other products (web-based or installed at customer sites) that contain personally identifiable information.
- Establish **processes for responding to data-related requests.** Any contact- or data-change requests must be handled within 30 days.

Example of a GDPR Consent Request

Request for consent to share data with a brand for product offers.



How to Revise Your Privacy Policy

Forms and notifications on your site should refer visitors to a privacy policy that tells them:

- That you are collecting data and how to contact you or your European representative
- What you'll use the data for, how you process it, and the legitimate interest you have for collecting it
- Who you might share the data with
- If you might share the data with partners in another country, whether the EU considers that country's protections adequate and what alternative protection you have in place
- How long you'll hold the data
- That the user has the right to request corrections to errors in personal information
- That the user has the right to withdraw consent and any potential consequences
- How the user can lodge a complaint with the supervisory authority
- Whether you use any automated decision-making process, why you use it, and what the outcomes may be

Phase 2: Optimize Your Back Office

Operational layers to address: Website CMS; marketing automation software; sales management software; corporate ERP

When an anonymous prospect converts to a marketing or sales lead, you probably hold their contact information and associated visitor-tracking data in several systems, all of which will need a mitigation plan. Adjust your website, marketing, and sales systems to ensure accurate tracking of personal data, enable removal of data on request, and provide reporting to verify compliance. Work through how you will track and manage data through all your back-office systems.

- **Who are your EU contacts?** Determine how many of your contacts are in the EU and who they are. Create a notification campaign telling them you are working on GDPR compliance and requesting permission to stay in contact.
- **Where are you tracking site visitor activity?** Likely you're tracking with Google Analytics, in your CMS, or with other tracking code (e.g., Hotjar, CrazyEgg, Mouseflow). You must track GDPR consent and denials through all levels.
- **How are you storing contact records?** This may be happening in your CMS, marketing software, sales software, or in multiple systems.
- **Where are you creating and storing forms?** Are they in your CMS or your marketing or sales software?
- **Have you updated all your forms?** Remember to include forms in which it might seem obvious that you'll be collecting data, such as Contact Us, Support Request, Open a Service Ticket, Request a Demo, Request a Quote, Make an Appointment, and so on.
- **Create and document policies and procedures for** collecting, tracking, and using personal data.
- **Create reporting** so that you can see all permissions and all areas where a person's data is being used and so that you can demonstrate your methods for finding, updating, using, and removing data.

A Data Flow Audit Reveals Essential Information About Data You Hold

PURPOSE	WHOSE DATA	WHAT			WHEN		WHERE
		Type	Source	Legal basis	Updated	Retention Period	
Digital Marketing	Existing customers	Name Address Email Mobile Phone	Individual	Contract	As required	End of relationship	Marketing provider
	Potential customers	Name Email	Third party list	Consent of individual		Consent withdrawn	CRM locally stored
HR	Employee	Name Address Contact details Health details CV	Individual	Contract	As required As required Regularly As required No	Five years after termination	HR manual records in CRM

Is Your CMS GDPR Ready?

Kentico 11 provides the tools you need to achieve and maintain GDPR compliance.

Conducting a **data flow audit** will reveal the flow of data around your business. **Data mapping** enables you to prove that you are obtaining, using, and storing data legally. The map also helps you show that data subjects' requests for updates, erasure, and portability can be fulfilled effectively and in a timely manner.

Once data mapping is completed, Refactored can make recommendations for simplifying data flow and even limiting the spread of submitted data to only the uses intended.

Whether you are using Kentico or another website platform, Refactored is here to provide guidance on developing your GDPR-compliant tools and processes.

Phase 3: Formalize Partner Processes

Operational layers to address: Sales management software; corporate ERP; product/application data; supplier, vendor, and partner portals and integrations

Control data flow and extend your compliant, two-way data-handling and monitoring processes to vendors, suppliers, distributors, and channel sales partners.

- Collaborate with suppliers, vendors, and sales partners to ensure they all have GDPR compliance measures in place.
- Ensure you have the ability to manage data coming and going:
  - From your systems to suppliers, vendors, and partners
  - From vendors, suppliers, and partners to your systems
  - From your systems to your products/applications at customer sites
  - From customer sites back to your internal systems

As you work through these steps, you'll become highly aware of the siloes in your organization and you'll see where you need coordination between departments. It's essential to have everyone on the same page.

Do We Need a DPO?

A Data Protection Officer (DPO) is responsible for overseeing your organization's strategy for compliance with GDPR requirements. You need to add this centralized, security-leadership role if your organization:

- Is a public authority
- Engages in large-scale, systematic monitoring
- Conducts large-scale processing of sensitive personal data

Typically, enterprise-scale organizations do need a DPO. Some very large enterprises have created Data Protection **Offices** to house entire DPO teams.

An Issue or an Opportunity?

Naturally, marketers and sales people are concerned about how the GDPR will affect their ability to track and market to EU customers and prospects. It will. Significantly. And lurking on the horizon is the question of whether similar regulations may make their way to the US and other parts of the world.

But savvy marketing leaders may also see the GDPR as just the next evolution in personalized, customer-centered marketing.

The steps you take to comply may yield hidden benefits:

- With clear data mapping, you can streamline your approach to collecting and using data. Any time you can simplify data flow, you make your own job easier.
- When you include only the most essential information on your forms, you may find that visitors are more likely to complete them.
- And of course, the better you target your messaging and offerings, the more qualified our leads are—and more qualified leads turn into more paying customers.

Demonstrating compliance with the GDPR also builds trust that your company is being transparent in its dealings and that it's treating data securely and responsibly. And for modern organizations, that trust is essential.

As you dig into each phase of your implementation, you'll want to work with a qualified partner who knows your business and your internal systems. That partner will help you ensure that you're completing the requirements, integrating changes into your systems effectively, and creating efficient processes for maintaining compliance going forward.

Are you ready for the GDPR?

If you're not sure—or not sure how you'll get there—

contact **Refactored.**

Refactored

About us

Refactored is a full-service B2B digital agency helping brands navigate the complexities of modern marketing by aligning people, process, and technology. Our goals are to showcase your brand's unique value and generate results that matter to your business. We help you find your voice, tell your story, and outperform your competition. Through engaging online and offline experiences that align with your customers' needs, we help you educate stakeholders and motivate them to positive action. Refactored serves national and international corporate clients from its home offices in Colorado. Let us show you how to demonstrate your compelling purpose—and strengthen your brand from the inside out. Connect with us at www.refactoredmedia.com.

Contact Information

hello@refactoredmedia.com
970.545.4171

For more information, visit
www.refactoredmedia.com.