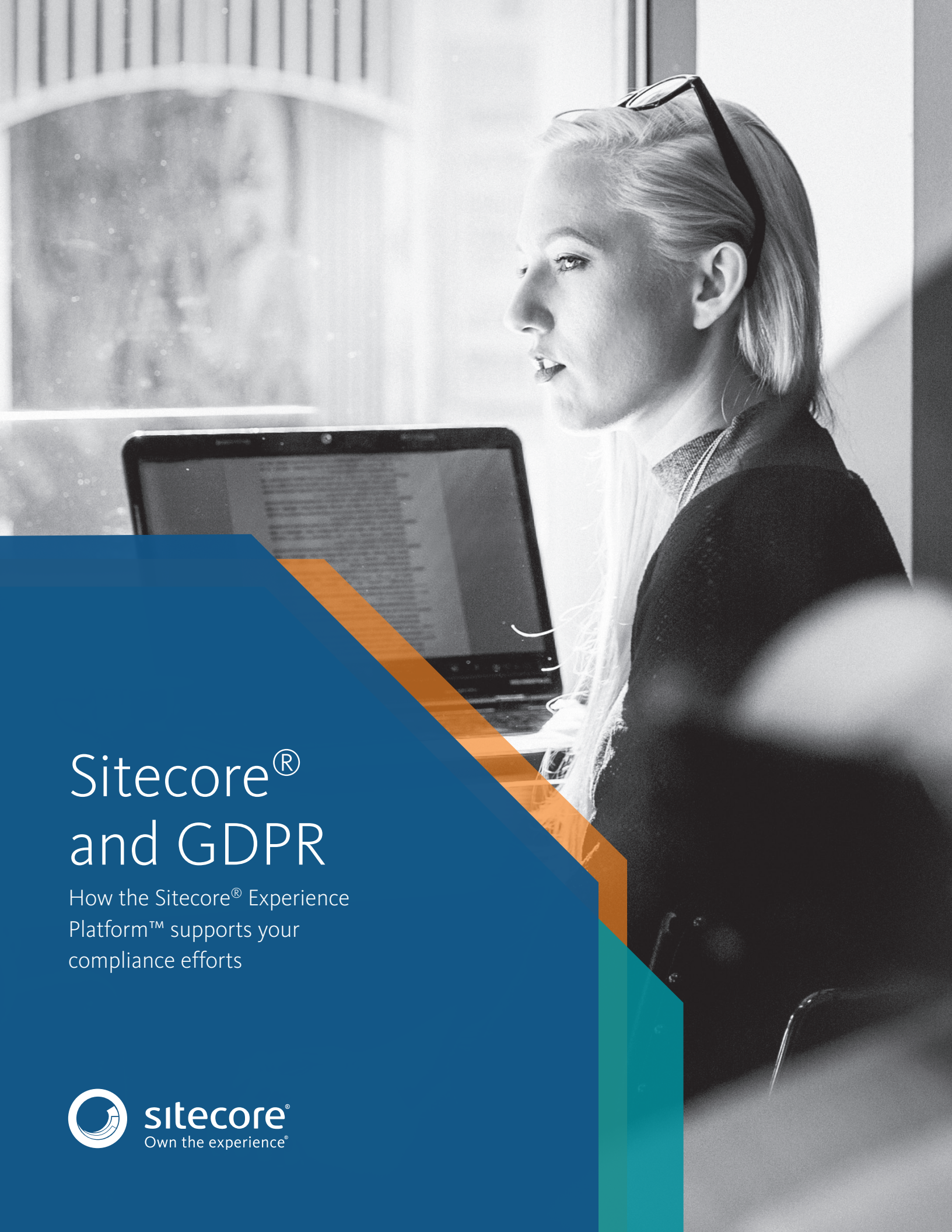

Sitecore® and GDPR

How the Sitecore® Experience Platform™ supports your compliance efforts

sitecore®
Own the experience®

Table of contents

Introduction 2

Sitecore XP 9 privacy features 2

GDPR data privacy rights and Sitecore XP 3

Sitecore and privacy by design 5

What's next 5

About Sitecore 5

Introduction

As a digital marketer, you may need to prepare for compliance with the European Union's General Data Protection Regulation (GDPR) by May 2018. The GDPR is intended to strengthen and unify data protection for all individuals within the European Union (EU) or European Economic Area (EEA), and it has repercussions for how you process and transfer out of the EU/EEA personally identifiable information (PII).

As this paper summarizes, the GDPR asks you to recognize and respect each of your end customer's data contribution to your business. The key to complying with evolving global data privacy regulations, including the GDPR, is transparency and accessibility. The Sitecore® Experience Platform™ (XP) can provide a consolidated view on the totality of every interaction your end customers have with your brand, accessible in one place, and can provide you a full, granular audit trail of what, where, how, and when you collected and stored all end-customer-related data, down to the individual level. Since Sitecore XP is an extensible framework, it's important to know that GDPR compliance may require changes to existing Sitecore XP implementations, which can only be determined through your own assessment of any PII you may have gathered and processed, or intend to gather and process, as a result of your implementation.

We've created this document to summarize how features in Sitecore XP support your compliance efforts. The guidance we've outlined applies to Sitecore XP 9, though some of the principles and features may apply to XP 8.2 and other previous Sitecore product versions as well. This guidance should not be construed or used as legal advice about the content, interpretation, or application of any law, regulation, or regulatory guideline. You, the customer, will always be in the best position to assess your own risks, and must seek your own legal counsel to understand the applicability of any law or regulation to your business, including processing of PII, whether you collect and process it independently or through using any vendor's products or services.

Sitecore XP 9 privacy features

Sitecore XP 9 incorporates a number of privacy-by-design and privacy-by-default principles and new features. These include support for anonymizing data, the ability to annotate data and treat data as sensitive, depending on your needs and your configuration choices.

The following table summarizes information available to the public regarding how the GDPR prioritizes the data privacy rights for individuals, along with the corresponding Sitecore solutions that you can use to help you protect the PII you may choose to collect and process.

GDPR data privacy rights and Sitecore XP

Individual right	GDPR reference	High-level description	XP features
The right to be informed	Article 12 Article 13 Article 4 (11)	If you process personal information, you must be transparent about what you collect and how you use it. Transparency is typically achieved through a privacy notice, but also through other interactions with your end customer (e.g., a user-friendly preferences page, custom privacy settings, etc.)	Sitecore XP is a framework that lets the customer build websites using any front-end technologies that suit their needs. Using your desired web technology (for example MVC or HTML and JavaScript) and Sitecore Content Editor, you can define and manage your privacy policies, as content, and present these to your end customers as part of your solution. Article 4 (11) of the GDPR defines "consent" as an affirmative action by the user. Sitecore recommends capturing and storing your end customer's affirmative action in the Sitecore® Experience Database™ (xDB). This action can be stored as a facet on the end customer's contact record in xDB. Once stored in xDB it is possible to display the contact's information in the Sitecore® Experience Profile™.
The right of access	Article 15	Individuals have a right to obtain confirmation that their data is being processed and a right to access their personal data that you're processing and storing.	Sitecore xConnect™ provides an API "GetContactAsync" that allows you to retrieve a full contact profile for your end customer. With this API call, you can specify whether you wish to retrieve all known data about the contact. This includes their full profile and historical behavior.
The right to rectification	Article 16	Individuals are entitled to have their personal information corrected if it is inaccurate or incomplete.	We recommend that you build a preferences form, which displays and allows end customers to edit their PII profile data, making it easier for you to maintain accurate data you choose to store in xDB.
The right to erasure	Article 17	Also known as the "right to be forgotten," individuals may request you delete or remove their personal data under certain circumstances.	To support your response to your end customer's erasure request, Sitecore provides the Sitecore xConnect feature "ExecuteRightToBeForgotten." This feature irreversibly anonymizes the individual's data so that the data is no longer identifiable.

The right to restrict processing	Article 18	Individuals have a right to restrict processing of their personal data.	We recommend that you define the appropriate level of opt-in / opt-out required, based on the type of data you collect, and ensure your end customers have control of these settings and that your application respects the settings. The Sitecore® Email Experience Manager (EXM) offers a global opt-out list setting, which you can use to disable all direct marketing activities to your end customer.
The right to data portability	Article 20	Individuals have a right to obtain and reuse their personal data for either their own use or for a different service.	Sitecore's xConnect provides an API "GetContactAsync" that allows you to retrieve a full contact profile for your end customer. With this API call, you can choose to specify whether you wish to retrieve all known data about the contact. This includes their full profile and historical behavior. This profile, in a JSON format, can be provided to your end customer in whatever format you choose to provide.
The right to object	Article 21	Individuals have a right to object, at any time, to the processing of personal data concerning them.	We recommend that you define the appropriate level of opt-in / opt-out required, based on the type of data you collect, and ensure your end customers have control of these settings, and that your application respects the settings. Sitecore's EXM offers a global opt-out list setting.
Rights in relation to automated decision making and profiling	Article 22	Individuals have a right to not be subject to decisions made based upon automated processing, unless they provide explicit consent.	As an extensible platform, XP allows you to personalize experiences for your end customers, based on the information you choose to collect. Sitecore and industry best practices can recommend steps for being transparent in your privacy statements and consent language, and Sitecore products can help you track and store information, but data processing decisions will always be yours to make.

Sitecore and privacy by design

The design and development process for Sitecore XP 9 follows a privacy-by-design approach. This incorporates the following foundational principles that embed data protection controls into Sitecore products for customers to leverage.

- **Proactive and preventative:** Out of the box, Sitecore products provide features to help you choose how to identify PII, configure your collection and processing choices, and protect your end customer's PII.
- **Privacy by default:** Sitecore XP 9 is built on a privacy-by-default foundation that helps you protect PII out-of-the-box, and XP 9 provides facilities for you to identify and secure PII that may be introduced via installing extensions.
- **Embedded privacy:** Sitecore's development process includes an exercise in identifying potential PII data. Sitecore products include resources exemplifying this exercise.
- **Positive sum:** Sitecore products are designed to help you strike the right balance between privacy, security controls, and usability.
- **Ensure end-to-end security:** Sitecore supports the use of strong security measures to protect personal data throughout the product lifecycle. This includes encryption of data at rest (data storage) and in motion (data transport).
- **Visibility, transparency, and respect for end-customer privacy:** Sitecore and industry best practices recommend that you create a clear privacy policy stating what data you gather, how you process it, and that you clearly justify your collection and processing practices.

With ongoing releases, Sitecore is committed to providing additional privacy controls and features out-of-the-box that can assist you in planning for GDPR compliance using Sitecore products.

What's next

We'd welcome the opportunity to hear more about how you're readying your company for GDPR—there are lots of ways to get in touch. Besides giving your account manager a call, you can contact us by:

- Email: sitecore.net/contact-us
- Phone: sitecore.net/phone
- Chat: sitecore.net/chat
- Or request a demo here.

About Sitecore

Sitecore is the global leader in experience management software that combines content management, commerce, and customer insights. The Sitecore Experience Cloud™ empowers marketers to deliver personalized content in real time and at scale across every channel—before, during, and after a sale. More than 5,200 brands—including American Express, Carnival Cruise Lines, Dow Chemical, and L'Oréal—have trusted Sitecore to deliver the personalized interactions that delight audiences, build loyalty, and drive revenue.