Ready, set, know: GDPR compliance with Sitecore XP 8, 7, and 6 and Sitecore XC 8 and 7*

What you need to understand for your Sitecore implementation

sitecore®
Own the experience®

* Sitecore Commerce 8 and Sitecore Commerce powered by Commerce Server 7 are herein referred to as XC 8 and XC 7, respectively, in this white paper.

Contents

Introduction

By this time, most businesspeople know of the European Union's (EU) General Data Protection Regulation (GDPR). And while the deadline may have passed, GDPR compliance is an ongoing process. You likely know that the GDPR requires global organizations to make changes when collecting and processing the personal data of your customers in EU member states from your website, CRM, and other marketing technologies. And you've probably heard the warnings about the steep fines for noncompliance—depending on the nature of infringement, fines can range between €10 million and €20 million, or between 2% and 4% of your worldwide annual revenue of the prior financial year, whichever is higher.[1]

GDPR at a glance

The General Data Protection Regulation (GDPR) is a European Union regulation (EU 2016/679) that came into effect on May 25, 2018. GDPR is intended to strengthen and unify data protection for all individuals within the EU or EEA, and it will greatly impact how companies such as yours use Sitecore and other marketing technologies to process and transfer personal data out of the EU/EEA. It replaces the prior Data Protection Directive (95/46/EC) of 1995 and, as a regulation instead of a directive, will apply immediately across all EU member states and the EEA on the enforcement date.

Despite being a European Union regulation, the GDPR has far-reaching implications for any business that has a global presence. In short, it impacts any business, EU-based or not, that has European users or customers.

Read more about the aim of GDPR at the EU Commission's website.

Even so, Gartner predicts that by the end of 2018, more than 50 percent of companies affected by the GDPR will not be in full compliance with its requirements.[2] GDPR has repercussions for how organizations collect, process, and manage personal data—an activity central to digital marketing—and transfer it out of the EU or European Economic Area (EEA).

At Sitecore, we understand the value of customer data and the importance of protecting it. After all, we built the Sitecore® Experience Platform™ (XP) and Sitecore Experience Commerce™ (XC) platform solutions on a unique architecture that supports the ability to isolate all aspects of a customer's interaction with your brand—through profile settings, implicit behaviors, and explicit interactions—at the individual level in real time and over the history of the customer–company relationship. All data is collected and connected in one singular database, the Sitecore® Experience Database™ (xDB), which debuted along with the Sitecore® Experience Profile™ as part of version 7.5 of Sitecore XP. So as a user of Sitecore technology, whether version 6, 7, or version 8 of Sitecore XP or version 7, 8 or 9 of Sitecore XC, it's imperative that you understand which areas of your configured implementation need your attention for GDPR.

That's why we've created this paper. As a Sitecore customer, only you can assess your own risks, and we recommend you seek legal counsel to understand the applicability of any law or regulation to your business, including how you process personal data. In other words:

- **Don't** construe or use this paper as an alternative to any legal advice regarding any regulation or guideline.
- **Do** consider this paper as a guide to:
  - What you should be aware of and/or look for in your current Sitecore implementation when assessing your organization's GDPR compliance needs, with or without a certified Sitecore Solution Partner.
  - Our high-level recommendations for how upgrading or migrating to the current version 9 of Sitecore XP and Sitecore XC could remediate noncompliance.

1. "Web learning resources for the EU General Data Protection Regulation, https://www.gdpreu.org/compliance/fines-and-penalties/
2. Gartner Says Organizations Are Unprepared for the 2018 European Data Protection Regulation, May 3, 2017 press release (https://www.gartner.com/newsroom/id/3701117)

Why upgrade to Sitecore XP or XC 9?

Becoming GDPR compliant becomes far simpler if your content management, digital marketing, or e-commerce platform is architected and built on a singular database that tracks all historical customer information. Customers on older versions of Sitecore would best prepare for GDPR by upgrading their platform and migrating their data to version 9.

Sitecore Experience Platform (XP) 9 and Sitecore Experience Commerce (XC) 9 facilitate GDPR compliance by incorporating 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 support for treating data as sensitive, depending on your needs and your configuration choices.

Version 9 offers capabilities that significantly expedite Sitecore users achieving GDPR compliance with their Sitecore deployment, including:

- **Extended database support:** The ability to deploy xDB on Microsoft SQL Server or Microsoft SQL Azure (in addition to MongoDB), which makes managing databases more efficient for teams already familiar with SQL Server or Azure Services, and can improve infrastructure where datasets have had to interact between different technologies.[3]
- **Sitecore xConnect™:** A new service layer and set of APIs designed to securely interact with Sitecore xDB and allow for the collection and interchange of customer data across channels—even third-party apps—and at scale. Much of how Sitecore XP 9 and XC 9 facilitate a customer configuration that supports GDPR compliance is attributable to Sitecore xConnect because it helps you more easily and effectively manage personally identifiable information.
- **Encryption:** Advanced security, with data encryption support for data that is both in motion, where data is encrypted with HTTPS and Transport Layer Security/Secure Sockets Layer (TLS/SSL), and at rest, where data in xDB can use SQL features such as Always Encrypted.

For more information on how Sitecore XP 9 and XC 9 support GDPR compliance, download our white paper "Sitecore and GDPR."

We'll outline what users of earlier Sitecore platform versions should be aware of, as well as summarize why GDPR is a key reason to consider upgrading or migrating to Sitecore XP or Sitecore XC version 9 (see box above).

What to know about GDPR compliance on earlier Sitecore versions

If upgrading or migrating is simply not an immediate option for you, you'll want at a minimum to understand what parts of your Sitecore implementation will need your attention for compliance. The table below and the rest of this paper focus on what to know and how to resolve GDPR issues if you're on Sitecore XP 8, 7, or 6 or Sitecore Commerce 8.x or Sitecore Commerce powered by Commerce Server 7 (herein this white paper referred to as XC 8.x and XC 7.x, respectively).

3. What's new in Sitecore XP 9, Oct. 24, 2017, Shout Digital's Ali Graham, https://www.shoutdigital.com/insights/blog/whats-new-in-sitecore-xp-9/

Do you know: Should I migrate or remediate?

Use this chart to determine the most effective path to your company's GDPR compliance

GDPR requirement	Sitecore 6 series	Sitecore 7 series	Sitecore XP 8 and XC 8 series	Sitecore XP and XC 9
The right to be informed, or being transparent about what you collect and how you use it (Article 12, 13, and Article 4 number 11)	As a developer you can inform end-users about data you collect through a privacy policy, cookie banner, and/or preferences page on a Sitecore 6.x website, but you have no way of auditing a history of interactions.	As a developer you can inform end-users about data you collect through a privacy policy, cookie banner, and/or preferences page on a Sitecore 7.x website, but you have no way of auditing a history of interactions.	As a developer you can inform end-users about data you collect through a privacy policy, cookie banner, and/or preferences page on a Sitecore XP 8.x website, but you have no way of auditing a history of interactions.	Yes, you or your developer can inform end-users about data you collect through a privacy policy, cookie banner, and/or preferences page on a Sitecore XP or XC 9.0 website, and can audit a history of interactions via the Sitecore xConnect™ API. For commerce data, the history of customer interactions can be audited using the Commerce journaling feature and Commerce Services API.

Table continued from page 4.

GDPR requirement	Sitecore 6 series	Sitecore 7 series	Sitecore XP 8 and XC 8 series	Sitecore XP and XC 9
The right of access, or allowing individuals to see what personal data you're processing and storing (Article 15)	Because Sitecore 6 did not include Sitecore xDB, you'll need to address this in your own database configuration.	Because Sitecore 7 did not include Sitecore xDB, you'll need to address this in your own database configuration. Users on version 7.5 (with xDB) should be aware there is no product feature support out of the box to help you configure your own compliance steps for the right to erasure or portability; you will need to customize and extend your 7.5 xDB solution to fulfill those requirements.	No product feature support out of the box for XP/XC versions prior to 8.2 Update 7. Users on prior versions will need to customize and extend their solution to fulfill the right of access requirements. Users of XP 8.2 Update 7 release can customize their solution and xDB to retrieve and delete the interaction history of a contact through a dedicated API. You will need to extend your solution to use the API and retrieve the data in a programmatic fashion. This can also be done for Sitecore XC 8 with an API.	Sitecore XP 9 and Sitecore XC 9 have dedicated features to retrieve the full interaction order history of an individual through a Sitecore API. As a developer, you will need to extend your solution to use the API and retrieve the data in a programmatic fashion.

Table continued from page 5.

GDPR requirement	Sitecore 6 series	Sitecore 7 series	Sitecore XP 8 and XC 8 series	Sitecore XP and XC 9
The right to rectification, or allowing individuals to have their personal data corrected (Article 16)	Because Sitecore 6 did not include Sitecore xDB, you'll need to address this in your own database configuration. Also see references to DMS on page 19 and OMS on page 25.	Because Sitecore 7 did not include Sitecore xDB, you'll need to address this in your own database configuration. Users on version 7.5 (with xDB) should be aware there is no product feature support out of the box to help you configure for the right to erasure or portability; you will need to customize and extend your 7.5 xDB solution to fulfill those requirements. Personal data can also be managed in Sitecore Commerce 7 with the Customer and Order Management tool.	You'll need to make changes to your Sitecore configuration (and any other systems) to edit / change / delete personal data on request. Personal data can be managed in User Security, List Management, and in XC's Customer and Order Management tool, and customized directly in MongoDB. The XC Customer and Order Management tool is a business user/ customer sales representative (CSR) focused, web-based management tool that is part of Sitecore Experience Commerce.	You need to make changes to your Sitecore configuration (and any other systems) to edit / change / delete personal data on request. Personal data can be managed in User Security, List Management, and customized directly through the Sitecore xConnect API (e.g., through a web form). Also, personal data can be managed in the Customer tool of the Commerce tool. Logs can be enabled and retrieved via the Commerce Services API.

Table continued from page 6.

GDPR requirement	Sitecore 6 series	Sitecore 7 series	Sitecore XP 8 and XC 8 series	Sitecore XP and XC 9
The right to erasure, also known as the right to be forgotten (Article 17)	Because Sitecore 6 did not include Sitecore xDB, you'll need to address this in your own database configuration.	Because Sitecore 7 did not include Sitecore xDB, you'll need to address this in your own database configuration. Users on version 7.5 (with xDB) should be aware there is no product feature support out of the box to help you configure for the right to erasure or portability; you will need to customize and extend your 7.5 xDB solution to fulfill those requirements.	No product feature support out of the box for XP versions prior to 8.2 Update 7. Users on prior versions will need to customize and extend their solution to fulfill the right of erasure requirements. Users of XP 8.2 Update 7 release can customize their solution and xDB to delete all personal data of a contact through a dedicated API. In XC 8.2.1 update 3, PII included by Commerce Connect in interactions can be erased. We recommend a review of the custom contact facets that have been extended in the xDB before using the API to ensure all personal data is removed.	Sitecore XP 9 has dedicated features for the right of erasure (or right to be forgotten). A contact's personal data can be deleted through a Sitecore API call, "Execute Right To Be Forgotten." This feature irreversibly removes the contact's personal data. XC customers are responsible for determining what data may need to be retained (i.e., for legal reasons and how long that information should be stored). The xConnect API is available to help customize what data is removed.

Table continued from page 7.

GDPR requirement	Sitecore 6 series	Sitecore 7 series	Sitecore XP 8 and XC 8 series	Sitecore XP and XC 9
The right to restrict processing, or allowing individuals to stop you from performing operations (collecting, processing, storing, etc.) on personal data (Article 18)	Because Sitecore 6 did not include Sitecore xDB, you'll need to address this in your own database configuration.	Because Sitecore 7 did not include Sitecore xDB, you'll need to address this in your own database configuration. Users on version 7.5 (with xDB) should be aware there is no product feature support out of the box to help you configure for the right to restrict processing; you will need to customize and extend your 7.5 xDB solution to fulfill those requirements.	Sitecore XP/XC 8 allows you to customize how much personal data you wish to process. Opt-in and opt-out is a customization.	Sitecore XP/XC 9 allows you to customize how much personal data you wish to process. Opt-in and opt-out is a customization.
The right to data portability, or giving individuals the personal data you have about them (Article 20)	Because Sitecore 6 did not include Sitecore xDB, you'll need to address this in your own database configuration.	Because Sitecore 7 did not include Sitecore xDB, you'll need to address this in your own database configuration. Users on version 7.5 (with xDB) should be aware there is no product feature support out of the box to help you configure for the right to data portability; you will need to customize and extend your 7.5 xDB solution to fulfill those requirements.	No product feature support out of the box for XP/XC versions prior to 8.2 Update 7. Users on prior versions will need to customize and extend their solution to fulfill the right to data portability requirements. Users of XP/XC 8.2 Update 7 release can customize their solution and xDB to retrieve/delete the interaction history of a contact through a dedicated API. The information retrieved can be exported for an end user in your chosen format.	Sitecore XP 9 ensures full interaction history is available and can be exported from the Sitecore xConnect API and provided to your end user in your chosen format. XC 9 can also export the full interaction history as well as purchase history in your end users' chosen format. The XC customer hosts these functionalities. None of this data is received by Sitecore.

Table continued from page 8.

GDPR requirement	Sitecore 6 series	Sitecore 7 series	Sitecore XP 8 and XC 8 series	Sitecore XP and XC 9
The right to object, or prevent you from processing their personal data (Article 21)	Because Sitecore 6 did not include Sitecore xDB, you'll need to address this in your own database configuration.	Because Sitecore 7 did not include Sitecore xDB, you'll need to address this in your own database configuration. Users on version 7.5 (with xDB) should be aware there is no product feature support out of the box to help you configure for the right to object; you will need to customize and extend your 7.5 xDB solution to fulfill those requirements.	No product feature support out of the box. Customization is required, dependent on your implementation.	No product feature support out of the box. Customization is required, dependent on your implementation.

Sitecore XP 8.x and XC 8 and GDPR compliance: Challenges and opportunities

Users on Sitecore XP 8.x and XC 8.x, will need to carefully review their deployment for security, and will likely need to extend and customize their implementation to meet GDPR compliance. The result will not be on par with what Sitecore XP 9 and XC 9 offer because, for example, security support for features like Microsoft SQL's Always Encrypted are not available in MongoDB, XP/XC 8's host database for xDB.

XP 9 and XC 9 use SQL Server and support Always Encrypted. For internal connections that handle PII, the default is TLS. And the XC Storefront is encrypted at the access layer.

It is important that XP and XC customers assess the data they are retaining and its legal basis.

Support and maintenance: *Self-assessment is key*

Sitecore XP 8.x and XC 8.x are still in mainstream support, and depending on which version you're using, Sitecore support will address security-related questions that customers or partners raise. But security is all about risk management: you will still need to examine and understand the security risks and concrete threats to your Sitecore installation and mitigate them for GDPR compliance.

Sitecore XP 9 and XC 9 are in mainstream support longer. Sitecore will provide support and fixes for any issues discovered on the platform or with underlying software.

Secure website access: *Add encryption to your access layer*

Sitecore products are based on the .NET framework and the Windows web technology platform; it is hosted on the Windows Server Operating System software and relies on Internet Information Services (or IIS) server features for website hosting. If end users are accessing your Sitecore XP 8 website(s) through a web browser, you should determine whether the connection is secure.

With Sitecore XP 8, you can secure the connection from the browser to the website through the HTTP transport layer, which can be made HTTPS-secure by using certificates with Transport Layer Security (TLS). Certificates are based on your website domain, and provide both certainty that the website is yours and that the connection is securely encrypted.

You can configure HTTPS for individual sites in IIS. However, due to the age of the IIS product in Sitecore XP 8, we strongly recommend that you install every available service pack, and update for all software products in use within your enterprise.

On the other hand, Sitecore XP 9 uses HTTPS by default for all connections, making it more secure due to TLS encryption. It supports HTTPS and still requires IIS for managing website security (certificates and encryption). In Sitecore XP 9 and Sitecore XC 9, with the introduction of the Sitecore xConnect service layer, we require HTTPS for all connections to Sitecore xDB through xConnect.

Similarly for XC, HTTPS is required for connections, and IIS manages all certificates for security. HTTPS is also required for all connections to Sitecore Commerce Services.

Latest compatible Windows versions

Various versions of Sitecore XP 8 run on various Microsoft Windows Server versions: for example, Sitecore XP 8.0, 8.1, and all 8.x versions run on Windows Server 2008 or 2008 R2, but Sitecore XP 8.2 u3 and higher and Sitecore XP 9 run on Windows Server 2016. Sitecore XP 8 will be under Sitecore mainstream support until year-end 2018 to 2019, depending on your version. Sitecore XP 9 runs on either Windows Server 2016—which is still in active mainstream Microsoft support until Jan. 2022—or the 64-bit 2012 R2, which is in active mainstream Microsoft support until Oct. 2018 for any new vulnerabilities that may appear.

For database support, if you are currently using Sitecore XP 8 with SQL Server 2008 or 2012 or MongoDB, we recommend that you consider an upgrade to Sitecore XP 9, which is under mainstream support until Dec. 31, 2020, and supports SQL Server 2016.

Built-in user authentication: *WAF recommended*

Sitecore XP 8 allows secure logons to websites through the .NET membership provider, with users' personal data stored in your Sitecore Core Database configuration. The authentication is secured between your configuration of the Content Delivery server and your configuration of the Content Management server, where user details are held.

For security, we recommend that Sitecore XP 8 enterprises install a Web Application Firewall (WAF), which only allows traffic to arrive from specific ports of your Content Delivery server. User authentication is an area in XP 8 where it may benefit you to schedule a technical review of your solution from your Sitecore Solution Partner.

In Sitecore XP 9, secure logons are still supported through the .NET membership provider. But Sitecore XP 9 also provides improved support for centralized security management with the new Federated Authentication feature, which allows you to configure data security to go through a trusted third-party solution. This is a highly secure approach that enables multi-factor authentication. You can also integrate into third-party services such as Microsoft Azure Active Directory, which itself integrates into wider multi-factor security systems.

xDB: *A security review is essential*

Your Sitecore xDB configuration can collect all customer interactions from all channel sources into a real-time big data repository. It can connect all interaction data to create a unified view of each individual, making the data available to marketers to manage the customer experience in real time.

As a core component of your GDPR compliance plan, Sitecore recommends a security review of your xDB installation. In doing so, you will need to ensure that any access to xDB is restricted and that data-at-rest encryption is active. Data-at-rest encryption is supported on all MongoDB versions. Sitecore xDB security is an area in XP 8 where it may benefit you to schedule a technical review of your solution from your Sitecore Solution Partner.

In Sitecore XP 9 implementations, xDB holds all data in the Microsoft SQL server database. Sitecore xConnect, our new secure service API layer, allows you to safely contact and update your xDB configuration, and ensures that HTTPS is used throughout the communication of personal data into and out of xDB. HTTPS can be secured by following standard certificate and encryption security practices.

Web Forms for Marketers (WFFM): *Ensure a secure connection*

In Sitecore XP/XC 8, end users' personal data from a web form can be saved to both a separate database and your xDB configuration. In instances where xDB is not running (e.g., in installations running Sitecore Experience Management [XM] only), you can use WFFM and save data to a separate SQL database. If you are running xDB and save user data to it, the captured personal data will be in MongoDB.

In either scenario, you must ensure a secure connection from the Content Delivery server to the server hosting the web forms database (SQL or MongoDB). If the web forms database is not secured or encrypted, you are at a higher risk of exposing personal data. If you are saving web forms data to a custom database, you will need to add customized code to pull required data out of the database to comply with the numerous rights articulated in GDPR.

In Sitecore XP/XC 9, end users' personal data from a website form can be saved to both a separate database and xDB. In instances in which xDB is not running (e.g., you've only implemented Sitecore XM), you can use WFFM and save data to a separate SQL database. In either use case, we encourage you to apply encryption to any database storing personal data. Saving personal data to xDB allows for centralized auditing, security, and review. Again, if you are saving web forms data to a custom database, you will need to add customized code to pull required data out of the database to comply with the numerous rights articulated in GDPR.

Geo-IP integration: *Regain it with Sitecore XP 9*

In older versions of Sitecore products, geo-IP integration was provided by a third-party vendor called Maxmind, but this service was discontinued on August 31, 2015, and replaced with Sitecore® IP Geolocation Service, available directly from Sitecore. We recommend that you review your implementation and ensure that any personal data is secured within the environment.

Sitecore XP 9 supports and hosts IP location detection through its own IP geolocation service, if configured. It does not send any data to Maxmind; Sitecore XP 9 interprets IP addresses for details on their location, including country, city, postal code, time zone, latitude, and longitude.

Sitecore XP 9 stores this data on memory caches in the Content Delivery server. IP interaction data is added to xDB for both anonymous and known contact records. Sitecore XP 9 supports the encryption of IP addresses in the xDB through "hashing," which means the data is stored in a way that the system can understand, but humans can't read.

For further help with Sitecore 8 remediation to enhance your organization's GDPR compliance, please contact your Sitecore implementation partner or Sitecore Account Manager to schedule a technical review of your solution.

Sitecore XP 8.x and XC 8.x and security: What to know

If you're using this on Sitecore XP 8.x or XC 8.x	Be aware that...	How to resolve in Sitecore XP 8.x and XC 8.x	How Sitecore XP and XC 9 help
Support and maintenance	Because Sitecore XP/XC is still in mainstream support, you should be aware that Sitecore support will try to resolve any questions about security raised by customers or partners..	Security is risk management: it is about understanding the risks and concrete threats to your environment and taking action to mitigate them. You must analyze the threats and risks your installation faces, and then do your utmost to secure your installation against these threats.	Sitecore XP and XC 9 are in mainstream support longer. Sitecore will provide support and fixes for any issues discovered on the platform or with underlying software.

Table continued from page 11.

If you're using this on Sitecore XP 8.x or XC 8.x	Be aware that...	How to resolve in Sitecore XP 8.x and XC 8.x	How Sitecore XP and XC 9 help
Secure website access	If your end user is accessing a Sitecore XP 8 website through a web browser, then a review of whether the connection is secure is in order. Sitecore products are based on the .NET framework and the Windows web technology platform. That includes the host Windows Server Operating System (OS) software that it is installed into, and it relies on the IIS (Internet Information Services) server features for website hosting.	You are able to secure the connection from the browser to the website through the HTTP transport layer. The HTTP transport layer can be encrypted using certificates with TLS (Transport Layer Security), enabling the connection to be HTTPS. You are able to configure HTTPS for individual sites in IIS. Certificates are based on your website domain, and provide both certainty to your end user that the website is in fact yours, and that the connection is securely encrypted. Due to the age of the IIS product in Sitecore XP 8, we strongly recommend that you install every available service pack and update for all of the software products you use.	Sitecore XP 9 supports HTTPS and still requires IIS for managing website security (certificates and encryption). In Sitecore XP 9, with the introduction of the xConnect service layer, we require HTTPS for all connections to xDB through xConnect. For Sitecore XC 9, HTTPS and IIS are required for all Commerce Services connections.
Latest compatible Windows version	Sitecore XP/XC 8.0 and 8.1 use Windows Server 2012 R2, the mainstream support for which expires Oct. 2018. Both also support SQL Server 2012, for which mainstream support expired in July 2018. Sitecore XP/XC 8 also supports MongoDB 3.2.1, for which mainstream support ended Sept. 2018.	Sitecore XP/XC 8.2 uses Windows Server 2016, supported until Jan. 2021, and supports SQL Server 2016 SP1, for which mainstream support ends Sept. 2018, as well as MongoDB 3.2.1, for which mainstream support ends September 2018. We recommend that you start to review an upgrade to Sitecore XP/XC 9, which supports the latest versions of technologies used.	Sitecore XP/XC 9 uses Windows Server 2016, for which mainstream support expires Jan. 2021, and which is actively supported by Microsoft against any new vulnerabilities that may appear. Sitecore XP/XC 9 supports SQL Server 2016 SP1, for which mainstream support ends July 2021.

Table continued from page 12.

If you're using this on Sitecore XP 8.x or XC 8.x	Be aware that...	How to resolve in Sitecore XP 8.x and XC 8.x	How Sitecore XP and XC 9 help
User authentication	Sitecore XP 8 has features for secure logons to your Sitecore configuration website. This feature is driven through the .NET membership provider, and the user's personal data is stored in the Sitecore Core Database. The authentication is secured between the Content Delivery server and the Content Management server, where user details are held.	We recommend that you ensure that you have a Web Application Firewall (WAF), which only allows traffic to arrive from specific ports of your Content Delivery server. For further assistance, please contact your Sitecore implementation partner or Sitecore Account Manager to schedule a technical review of your solution.	We still support secure logons through the .NET membership provider in Sitecore XP 9. In addition, we have improved support for centralized security management with the introduction of the Federated Authentication feature. Federated Authentication allows you to configure data security to go through a trusted third-party solution, which is highly secure and enables multi-factor authentication. You can integrate into third-party services like Microsoft Azure Active Directory, which integrates into wider multi-factor (e.g., user name, password, and mobile phone login code) security systems.

Table continued from page 13.

If you're using this on Sitecore XP 8.x or XC 8.x	Be aware that...	How to resolve in Sitecore XP 8.x and XC 8.x	How Sitecore XP and XC 9 help
xDB	The Sitecore Experience Database (xDB) can be configured to collect all your customer interactions from all channel sources in a real-time big data repository. It can connect interaction data to create a comprehensive, unified view of each individual customer and makes the data available to marketers to manage the customer experience in real time.	As a core part of your solution, and to help you meet GDPR requirements, Sitecore recommends that you review your solution's security controls. To do so, you need to ensure that any access to xDB is restricted, and that data-at-rest encryption is active. Data-at-rest encryption is supported on all MongoDB versions. For further assistance, please contact your Sitecore implementation partner or Sitecore Account Manager to schedule for a technical review of your solution.	In Sitecore XP and XC 9, xDB holds all data in the Microsoft SQL Server database. We have also implemented a new Service API layer, called Sitecore xConnect, that securely lets you contact and update xDB. xConnect is a secure service layer that ensures that HTTPS is used throughout the communication of personal data into and out of xDB. HTTPS can be secured following standard certificate and encryption security practices.

Table continued from page 14.

If you're using this on Sitecore XP 8.x or XC 8.x	Be aware that...	How to resolve in Sitecore XP 8.x and XC 8.x	How Sitecore XP and XC 9 help
Web Forms for Marketers (WFFM)	You can configure both xDB and a separate database to save an end user's personal data from WFFM. In instances where you do not have xDB running, you can use WFFM and save its data to a separate SQL database. If you are running xDB and you have selected to save user data to xDB, personal data captured will be stored in MongoDB. For either avenue, you must ensure that you have security from the Content Delivery server to the server hosting the forms database (whether SQL or MongoDB). If your database is not secured or encrypted, you are at risk of exposing personal data.	If you are saving WFFM data to a custom database, you need to add customized code that pulls required data out of the database to comply with the numerous rights from GDPR regulation.	An end user's personal data from WFFM can be saved to both a separate database and Sitecore xDB. In instances where you do not have xDB running, you can use WFFM and save its data to a separate SQL database. We encourage you to apply database encryption to either database solution where you are storing personal data. Please refer to the relevant vendor documentation for SQL to secure your solution. Saving personal data to xDB allows for a centralized location for auditing, security, and review. If you are saving WFFM data to a custom database, you need to add customized code that pulls required data out of the database to comply with the numerous rights from GDPR regulation.

Table continued from page 15.

If you're using this on Sitecore XP 8.x or XC 8.x	Be aware that...	How to resolve in Sitecore XP 8.x and XC 8.x	How Sitecore XP and XC 9 help
Geo-IP integration	Sitecore XP 8 supported a direct connector to the third-party vendor Maxmind, which provided a service that interpreted an IP address and provided details on its location, such as country, city, postal code, time zone, latitude, and longitude. Sitecore XP 8 stored this data on memory caches on the Content Delivery server and the Content Management server (Analytics SQL database).	The Maxmind service was discontinued on August 31, 2015. If you are still using Sitecore XP 8, we recommend that you review the implementation and ensure that this personal data is secured within the environment. Sitecore XP versions 8.1 and later support IP location detection features through a service that Sitecore offers directly to customers.	Sitecore XP 9 supports IP location detection through the IP geolocation service that Sitecore offers. It is hosted by Sitecore in Azure and does not send any data to Maxmind. It provides the same service of interpreting IP addresses and providing details on their location, including elements such as country, city, postal code, time zone, latitude, and longitude. Sitecore XP 9 stores this data on memory caches on the Content Delivery server, and IP interaction data is added to xDB for both anonymous and known contact records. In Sitecore XP 9, we support hashing of IP addresses in xDB for encryption or redaction.

Sitecore XP 7.x and XC 7.x and GDPR compliance: Issues and remedies

Organizations using Sitecore XP 7 or XC 7 face many of the same challenges in achieving GDPR compliance as those on Sitecore XP 8 and XC 8. The points below reflect the differences in GDPR-related upgrades between Sitecore XP and XC 8 and Sitecore XP and XC 7. All issues can effectively be addressed by upgrading Sitecore 7 environments to Sitecore XP/XC 9 or configuring your Sitecore 7 environments, using the table on previous pages to assist, in accordance with your own needs and legal counsel.

- ***Support and maintenance:*** Sitecore version 7 is now out of mainstream support. As such, Sitecore recommends that customers review their implementation and plan to upgrade at their earliest convenience.
- ***Secure website access:*** The issues and remedies for secure website access are the same for Sitecore 7 and Sitecore 8.
- ***Latest compatible Windows version:*** Many Sitecore 7 implementations run on Windows 2008 or older versions, which Microsoft does not actively support. To achieve the maximum level of GDPR compliance with your Sitecore IT investments, we recommend upgrading from Windows Server 2008 to a later, supported version of Windows Server, as well as to Sitecore XP/XC 9.
- ***Built-in user authentication:*** The issues and remedies for built-in user authentication are the same for Sitecore 7 and Sitecore 8.
- ***xDB:*** In Sitecore XP 7.5, the only 7 version that supported xDB, all data is held in a MongoDB database provided by Sitecore technology partner MongoDB. As with Sitecore XP 8, Sitecore recommends a security review of your Sitecore 7.5 xDB solution to ensure that any access to it is restricted and that data-at-rest encryption in MongoDB is active.
- ***Web Forms for Marketers:*** WFFM with xDB is available only on Sitecore XP 7.5. As with Sitecore XP 8, you must ensure a secure connection from the Content Delivery server to the server hosting the Web Forms MongoDB database. If the Web Forms database is not secured or encrypted, you are at a higher risk of exposing personal data.
- ***Geo-IP integration:*** If you are still using Sitecore 7, we recommend that you review the implementation and ensure that associated personal data is secured within the geo-location environment.

The xDB turning point

The Sitecore Experience Platform version 7.5 marked an important turning point. This release introduced the Sitecore Experience Database (xDB) and the Sitecore Experience Profile (or xProfile™), Sitecore's two cornerstones for modern digital marketing.

Built on an open-source NoSQL database, xDB is a big data repository that, depending on how you have configured it, collects and connects all customer data from Sitecore and other external services and applications. xDB is the foundation upon which all Sitecore experiences are built today. Depending on how you have configured it, xDB feeds data into Sitecore xProfile, a customizable view of each individual customer and their interaction with your brand across channels—versus an aggregated view of a target segment.

While xDB stores all customer data, xProfile provides immediate insights at the individual level and enables you to act in real time, ensuring a highly relevant and contextual experience for each customer as they are interacting with you on any device.

What's important to recognize about Sitecore 7.x is that it let you move beyond tracking traffic, clicks, and stats to embracing experience management fully, delivering a highly personalized experience for each customer.

Sitecore XP and XC 7.x and security: What to know

If you're using this on Sitecore XP and XC 7.x	Be aware that...	How to resolve in Sitecore XP and XC 7.x	How Sitecore XP and XC 9 help
Support and maintenance	Sitecore version 7 is now currently out of mainstream support, and therefore Sitecore recommends that you review your implementation and start to plan an upgrade at your earliest convenience.	Security is risk management: it is about understanding the risks and concrete threats to your environment and mitigating them. You must analyze the threats and risks your installation faces, and then do your utmost to secure your installation against these threats.	Sitecore XP and XC 9 are in mainstream support. Sitecore will provide support and fixes for any issues discovered on the platform or with underlying software.
Secure website access	If your end users are accessing a Sitecore 7 website through a web browser, then a review of whether the connection is secure is in order. Sitecore products are based on the .NET framework and the Windows web technology platform. That includes the host Windows Server Operating System (OS) software that it is installed into, and it relies on the IIS (Internet Information Services) server features for website hosting.	You are able to secure the connection from the browser to the website through the HTTP transport layer. The HTTP transport layer can be encrypted using certificates with TLS (Transport Layer Security), enabling the connection to be HTTPS. You are able to configure HTTPS for individual sites in IIS. Certificates are based on your website domain, and provide both certainty to your end user that the website is in fact yours, and that the connection is securely encrypted. Due to the age of the IIS product in Sitecore 7, we strongly recommend that you install every available service pack and update for all of the software products that you use.	Sitecore XP 9 is secure by default and requires HTTPS for all connections to the website. Sitecore XP 9 supports HTTPS and still requires IIS for managing website security (certificates and encryption). In Sitecore XP 9, with the introduction of the Sitecore xConnect service layer, we require HTTPS for all connections to xDB through xConnect.

Table continued from page 18.

If you're using this on Sitecore XP and XC 7.x	Be aware that...	How to resolve in Sitecore XP and XC 7.x	How Sitecore XP and XC 9 help
User authentication (built-in)	Sitecore 7 has features for secure logons to your Sitecore configuration website that are driven through the .NET membership provider. The user's personal data is stored in the Sitecore Core Database. Authentication is secured between the Content Delivery server and the Content Management server, where user details are held.	We recommend that you ensure that you have a Web Application Firewall (WAF), which only allows traffic to arrive from specific ports of your Content Delivery server. For further assistance, please contact your Sitecore implementation partner or Sitecore Account Manager to schedule a technical review of your solution.	We still support secure logons through the .NET membership provider in Sitecore XP 9. In addition, we have improved support for centralized security management with the introduction of the Federated Authentication feature. Federated Authentication allows you to configure data security to go through a trusted third-party solution that is highly secure and enables multi-factor authentication. You can integrate into third-party services such as Microsoft Azure Active Directory, which integrates into wider multi-factor (e.g., user name, password, and mobile phone login code) security systems.
Digital Marketing System (DMS) (on Sitecore 7.0 - 7.2 only)	The Analytics Database in Sitecore's DMS was used to collect visitor behavior and enable reporting. Built on SQL, it was the precursor to the xDB collection database, and if still in use may contain personal data. You'll need to address this in your own database configuration.	Sitecore recommends that you cease capturing analytics data in DMS and move to Sitecore XP/XC 9 with xDB.	In Sitecore XP 9, xDB is included by default and is designed to be a secure personal data store.

Table continued from page 19.

If you're using this on Sitecore XP and XC 7.x	Be aware that...	How to resolve in Sitecore XP and XC 7.x	How Sitecore XP and XC 9 help
xDB (version 7.5 only)	The Sitecore Experience Database can be configured to collect all your customer interactions from all channel sources in a real-time, big data repository. It can connect interaction data to create a comprehensive, unified view of each individual customer, and makes the data available to marketers to manage the customer experience in real time. In Sitecore XP 7.5 (the only 7 version that supports xDB), xDB holds all data in a MongoDB database.	As a core part of your solution, and to ensure that you meet GDPR requirements, Sitecore recommends that you review your solution for security. To do so, you need to ensure that any access to xDB is restricted, and that data-at-rest encryption is active. Data-at-rest encryption is supported on all MongoDB versions. For further assistance, please contact your Sitecore implementation partner or Sitecore Account Manager to schedule a technical review of your solution.	In Sitecore XP and XC 9, xDB holds all data in the Microsoft SQL server database. We have also implemented a new Service API layer, called Sitecore xConnect, that securely lets you contact and update xDB. xConnect is a secure service layer that ensures that HTTPS is used throughout the communication of personal data into xDB. HTTPS can be secured following standard certificate and encryption security practices.

Table continued from page 20.

If you're using this on Sitecore XP and XC 7.x	Be aware that...	How to resolve in Sitecore XP and XC 7.x	How Sitecore XP and XC 9 help
Web Forms for Marketers (WFFM)	An end user's personal data from WFFM can be saved to both a separate database and xDB (in version 7.5 only). In instances where you do not have xDB running, you are able to use WFFM and save data to a separate SQL database. If you are running xDB and you have selected to save user data to xDB, personal data captured will be stored in MongoDB. For either avenue, you must ensure that you have security from the Content Delivery server to the server hosting the WFFM database (SQL or MongoDB). If your database is not secured or encrypted, you are at risk of exposing personal data.	Sitecore recommends that you move away from WFFM on this version of Sitecore, and move to a later release that has improved underlying security and encryption in both the database and transport (HTTPS). If you are saving WFFM data to a custom database, you need to customize a way of pulling required data out of the database to comply with the numerous rights from the new regulation.	An end user's personal data from WFFM can be saved to both a separate database and xDB. In instances where you do not have xDB running, you are able to use WFFM and save data to a separate SQL database. We encourage you to apply database encryption to either database solution where you are storing personal data. Please refer to the relevant vendor documentation for SQL to secure your solution. Saving personal data to xDB allows for a centralized location for auditing, security, and review. If you are saving WFFM data to a custom database, you need to customize a way of pulling required data out of the database to comply with the numerous rights from the new regulation.

Table continued from page 21.

If you're using this on Sitecore XP and XC 7.x	Be aware that...	How to resolve in Sitecore XP and XC 7.x	How Sitecore XP and XC 9 help
Geo-IP integration	Sitecore 7 supported a direct connector to the third-party vendor Maxmind, which provided a service of interpreting an IP address for details on its location, including country, city, postal code, time zone, latitude, and longitude. Sitecore 7 stored this data on memory caches on the Content Delivery server and the Content Management server (Analytics SQL) database.	The service was discontinued on August 31, 2015. If you are still using Sitecore 7, we recommend that you review the implementation and ensure that this personal data is secured within the environment.	Sitecore XP 9 supports IP location detection through Sitecore's IP Geolocation service, which is hosted by Sitecore in Azure and does not send any data to Maxmind. It provides the same service of interpreting IP addresses for details on their location, including country, city, postal code, time zone, latitude, and longitude. Sitecore XP 9 stores this data on memory caches on the Content Delivery server, and IP interaction data is added to xDB for both anonymous and known contact records. In Sitecore XP 9, we support hashing of IP addresses in xDB for encryption or redaction.

Sitecore 6.x and GDPR compliance: Time for a fresh start

As indicated in the table on p.4, "Do you know: Should I migrate or remediate?" both Sitecore 7.x and Sitecore 6.x have limited support out of the box for helping you with configuring to comply with the General Data Protection Regulation. Many organizations will find the complexities of upgrading Sitecore 6 environments to achieve greater GDPR compliance to be time-consuming and potentially costly.

Specifically, in addition to the issues identified for Sitecore 7 deployments in the previous section, Sitecore 6 presents challenges with:

- ***xDB:*** Sitecore 6 does not support the Sitecore Experience Database. xDB provides critical functionality for compliance with numerous consumer rights that GDPR specifies.
- ***Web Forms for Marketers:*** GDPR compliance issues in Sitecore 6 are the same as in Sitecore 7, although the WFFM database in 6 could only be configured on either a SQL or a SQL Lite database, whereas Sitecore 7 installations running xDB store WFFM data in MongoDB.

Given the host of remediation issues in Sitecore 6, as well as this version being no longer supported, it is highly recommended that organizations using it migrate to Sitecore XP 9.

Sitecore XP 6.x and security: What to know

If you're using this on Sitecore XP 6.x	Be aware that...	How to resolve in Sitecore XP 6.x	How Sitecore XP 9 helps
Support and maintenance	Sitecore version 6 is now currently out of mainstream support, and therefore Sitecore recommends that you review your implementation and start to plan an upgrade at your earliest convenience.	Security is risk management: it is about understanding the risks and concrete threats to your environment and mitigating them. You must analyze the threats and risks your installation faces, and then do your utmost to secure your installation against these threats.	Sitecore XP 9 is in mainstream support until 2020. Sitecore will provide support and fixes for any issues discovered on the platform or with underlying software.
Secure website access	If your end users are accessing a Sitecore 6 website through a web browser, then a review of whether the connection is secure is in order. Sitecore products are based on the .NET framework and the Windows web technology platform. That includes the host Windows Server Operating System (OS) software that it is installed into, and it relies on the IIS (Internet Information Services) server features for website hosting.	You are able to secure the connection from the browser to the website through the HTTP transport layer. The HTTP transport layer can be encrypted using certificates with TLS (Transport Layer Security), enabling the connection to be HTTPS. You are able to configure HTTPS for individual sites in IIS. Certificates are based on your website domain, and provide both certainty to your end user that the website is in fact yours, and that the connection is securely encrypted. Due to the age of the IIS product in Sitecore 6, we strongly recommend that you install every available service pack and update for all of the software products that you use.	Sitecore XP 9 is secure by default and requires HTTPS for all connections to the website. Sitecore XP 9 supports HTTPS and still requires IIS for managing website security (certificates and encryption). In Sitecore XP 9, with the introduction of the Sitecore xConnect service layer, we require HTTPS for all connections to xDB through xConnect.

Table continued from page 23.

If you're using this on Sitecore XP 6.x	Be aware that...	How to resolve in Sitecore XP 6.x	How Sitecore XP 9 helps
Latest compatible Windows version	Sitecore 6 uses Windows Server 2008 R2 SP1, for which mainstream support ended Jan. 2015. Vulnerabilities in older versions of software are not actively supported by Microsoft, and should be migrated and upgraded to the latest versions of the required software.	We recommend that you upgrade from Windows Server 2008 to a later supported version of Sitecore and Windows Server.	Sitecore XP 9 supports Windows Server 2016, for which mainstream support expires January 2021.
User authentication (built-in)	Sitecore 6 has features for secure logons to your Sitecore configuration website that are driven through the .NET membership provider. The user's personal data is stored in the Sitecore Core Database. Authentication is secured between the Content Delivery server and the Content Management server, where user details are held.	We recommend that you ensure that you have a Web Application Firewall (WAF), which only allows traffic to arrive from specific ports of your Content Delivery server. For further assistance, please contact your Sitecore implementation partner or Sitecore Account Manager to schedule a technical review of your solution.	The product still supports secure logons through the .NET membership provider in Sitecore XP 9. In addition, we have improved support for centralized security management with the introduction of the Federated Authentication feature. Federated Authentication allows you to configure data security to go through a trusted third-party solution that is highly secure and enables multi-factor authentication. You can integrate into third-party services such as Microsoft Azure Active Directory, which integrates into wider multi-factor (e.g., user name, password, and mobile phone login code) security systems.

Table continued from page 24.

If you're using this on Sitecore XP 6.x	Be aware that...	How to resolve in Sitecore XP 6.x	How Sitecore XP 9 helps
Online Marketing Suite (OMS) / Digital Marketing System (DMS) in Sitecore 6.x	The Analytics Database was used with OMS (and later DMS) to collect visitor behavior and enable reporting. Built on SQL, it was the precursor to the xDB collection database, and if still in use may contain personal data.	You'll need to address this in your own database configuration. Sitecore recommends that you cease capturing analytics data in OMS/DMS and move to Sitecore XP 9 with xDB.	In Sitecore XP 9, xDB is included by default and is designed to be a secure personal data store.
xDB	Sitecore xDB is not supported in Sitecore 6.	Not applicable.	In Sitecore XP 9, xDB is included by default and is designed to be a secure personal data store.

Table continued from page 25.

If you're using this on Sitecore XP 6.x	Be aware that...	How to resolve in Sitecore XP 6.x	How Sitecore XP 9 helps
Web Forms for Marketers (WFFM)	An end user's personal data from WFFM can be saved to a separate database configured to run on either SQL or SQL Lite. If your database is not secured or encrypted, you are at risk of exposing personal data.	Sitecore recommends that you move away from WFFM on this version of Sitecore to a later release that has improved underlying security and encryption in both the database and transport (HTTPS). If you are saving WFFM data to a custom database, you need to customize a way of pulling required data out of the database to comply with the numerous rights from the new regulation.	An end user's personal data from WFFM can be saved to both a separate database and xDB. In instances where you do not have xDB running, you are able to use WFFM and save data to a separate SQL database. We encourage you to apply database encryption to either database solution where you are storing personal data. Please refer to the relevant vendor documentation for SQL to secure your solution. Saving personal data to xDB allows for a centralized location for auditing, security, and review. If you are saving WFFM data to a custom database, you need to customize a way of pulling required data out of the database to comply with the numerous rights from the new regulation.

Table continued from page 26.

If you're using this on Sitecore XP 6.x	Be aware that...	How to resolve in Sitecore XP 6.x	How Sitecore XP 9 helps
Geo-IP integration	Sitecore 6 supported a direct connector to the third-party vendor Maxmind, which provided a service of interpreting an IP address for details on its location, including country, city, postal code, time zone, latitude, and longitude. Sitecore 6 stored this data on memory caches on the Content Delivery server and the Content Management server (Analytics SQL) database.	The service was discontinued on August 31, 2015. If you are still using Sitecore 6, we recommend that you review the implementation and ensure that this personal data is secured within the environment.	Sitecore XP 9 supports IP location detection through Sitecore's IP Geolocation service, which is hosted by Sitecore in Azure and does not send any data to Maxmind. It provides the same service of interpreting IP addresses for details on their location, including country, city, postal code, time zone, latitude, and longitude. Sitecore XP 9 stores this data on memory caches on the Content Delivery server, and IP interaction data is added to xDB for both anonymous and known contact records. In Sitecore XP 9, we support hashing of IP addresses in xDB for encryption or redaction.

A 'lift and shift' approach to Sitecore XP 9 migration

The path to migrate from older Sitecore versions to Sitecore XP 9 isn't always the same. However, regardless of which Sitecore version your organization currently uses, the Sitecore Express Migration tools make it easy to migrate older instances to the latest version of Sitecore XP 9—without the need to gradually upgrade from version to version.

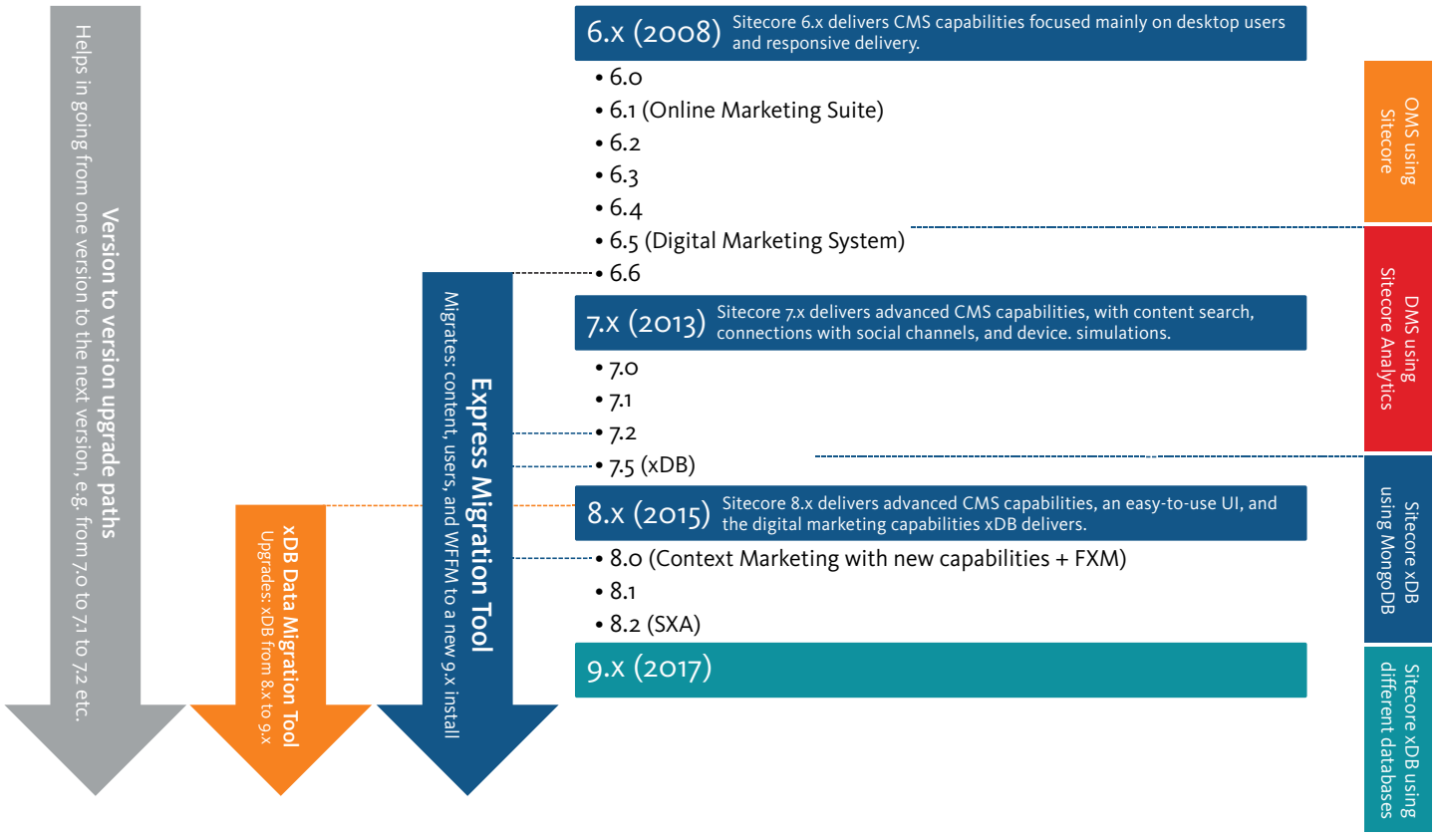
In this way, you can "lift and shift" your content from the old instance to the new one.

If you're moving from Sitecore XP 8.1 or higher, the upgrade is simple, and you can upgrade directly. If you're moving from a lower version, there are two other paths:

1. If you are using Sitecore 6.6, 7.2, XP 7.5, or XP 8.0, you could start with a clean Sitecore XP 9 install and migrate your content using the Express Migration Tool. In addition, you can use the xDB Data Migration Tool to migrate data from the xDB Mongo database in Sitecore XP 8 to either a Mongo or Microsoft SQL Server xDB database in Sitecore XP 9.
2. If you are on Sitecore 6.5 (or lower), 7.0, or 7.1, you can run through each upgrade version to one supported by the Express Migration Tool.

The arrows on the left of the diagram below illustrate these migration paths for various Sitecore and xDB instances. Note: While content can easily be migrated to Sitecore XP 9 in a "lift and shift" fashion, additional tuning of the new Sitecore XP 9 environment will be necessary. These services are widely available from Sitecore partners.

Sitecore version summary and upgrade paths



Summary: Now you know

Achieving GDPR compliance is a major catalyst for all organizations running Sitecore XP 8.x, 7.x, and 6.x and Sitecore XC 8.x and 7.x to take stock and assess whether their current configuration meets their data governance and security compliance needs. Even for those who are not immediately prepared for an upgrade, we recommend a close review of your configuration to assess the security of your data and connections, among other issues that GDPR covers. Migrating to Sitecore XP/XC 9 presents the fastest, most cost-effective path for your organization's GDPR compliance efforts. As a Sitecore customer, only you can assess your own risks, and we recommend you seek legal counsel to understand the applicability of any law or regulation to your business, including how you process personal data.

Next steps

For more details on how Sitecore XP/XC 9 supports your compliance efforts, read our white paper "Sitecore and GDPR."

Further information on Sitecore's GDPR compliance plans will be made available on our Trust center as they develop. However, if you have any specific queries in the meantime, please contact us at privacy@sitecore.com.

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. For more information, visit www.sitecore.com.