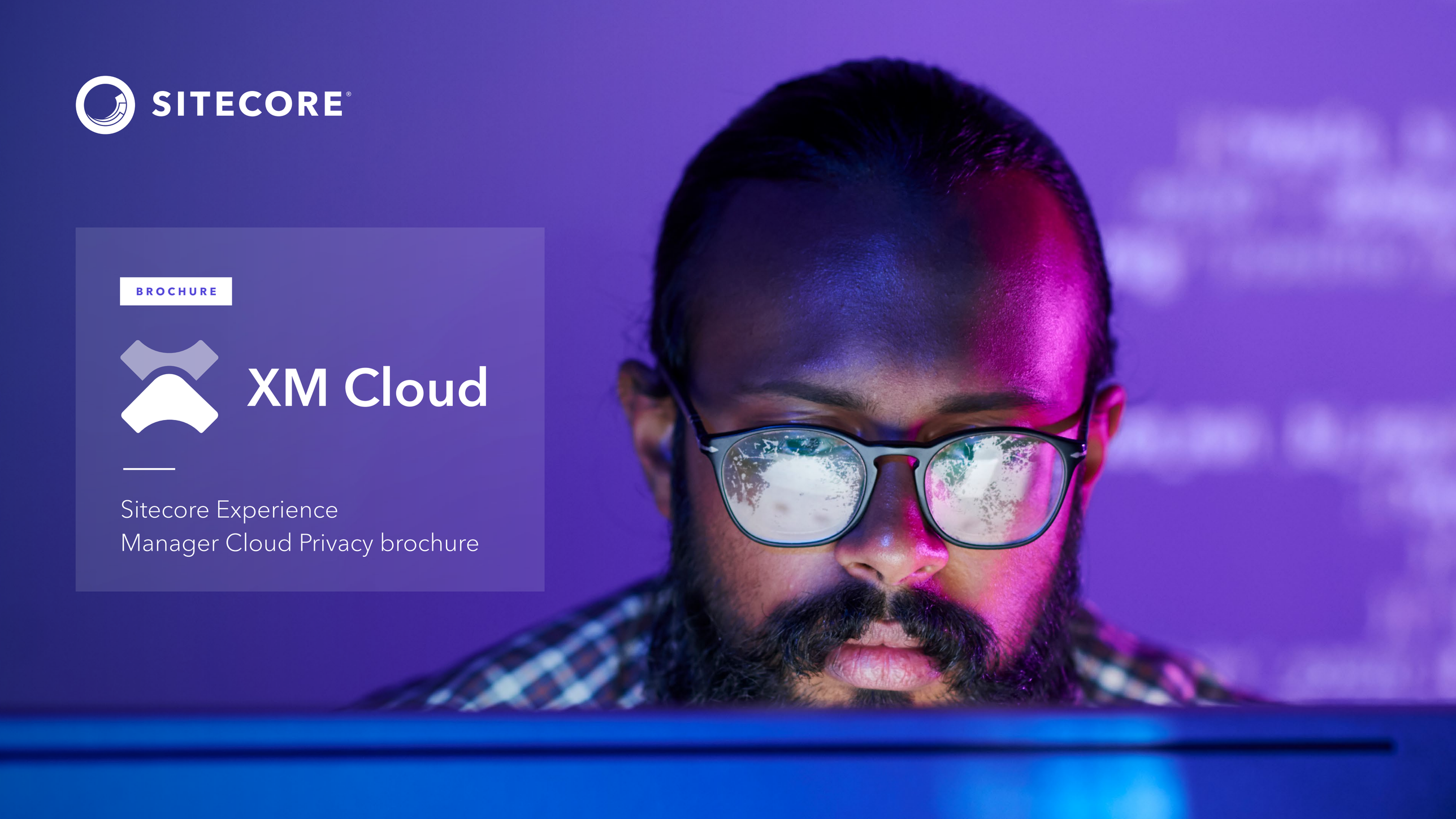
SITECORE®

BROCHURE

XM Cloud

Sitecore Experience Manager Cloud Privacy brochure



Introduction

At Sitecore, we understand the value of data and the importance of protecting it. Sitecore is committed to a security and privacy-first philosophy, following ethical data practices and emulating that in our own internal compliance framework, as well as implementing privacy-by-design features and security-as-default in our products and services.

Sitecore understands the challenges faced by brands. We want to be a helpful partner in your compliance journey. As a provider of the leading digital experience platform, it is important for us to share how we are managing data privacy in our solutions and services.

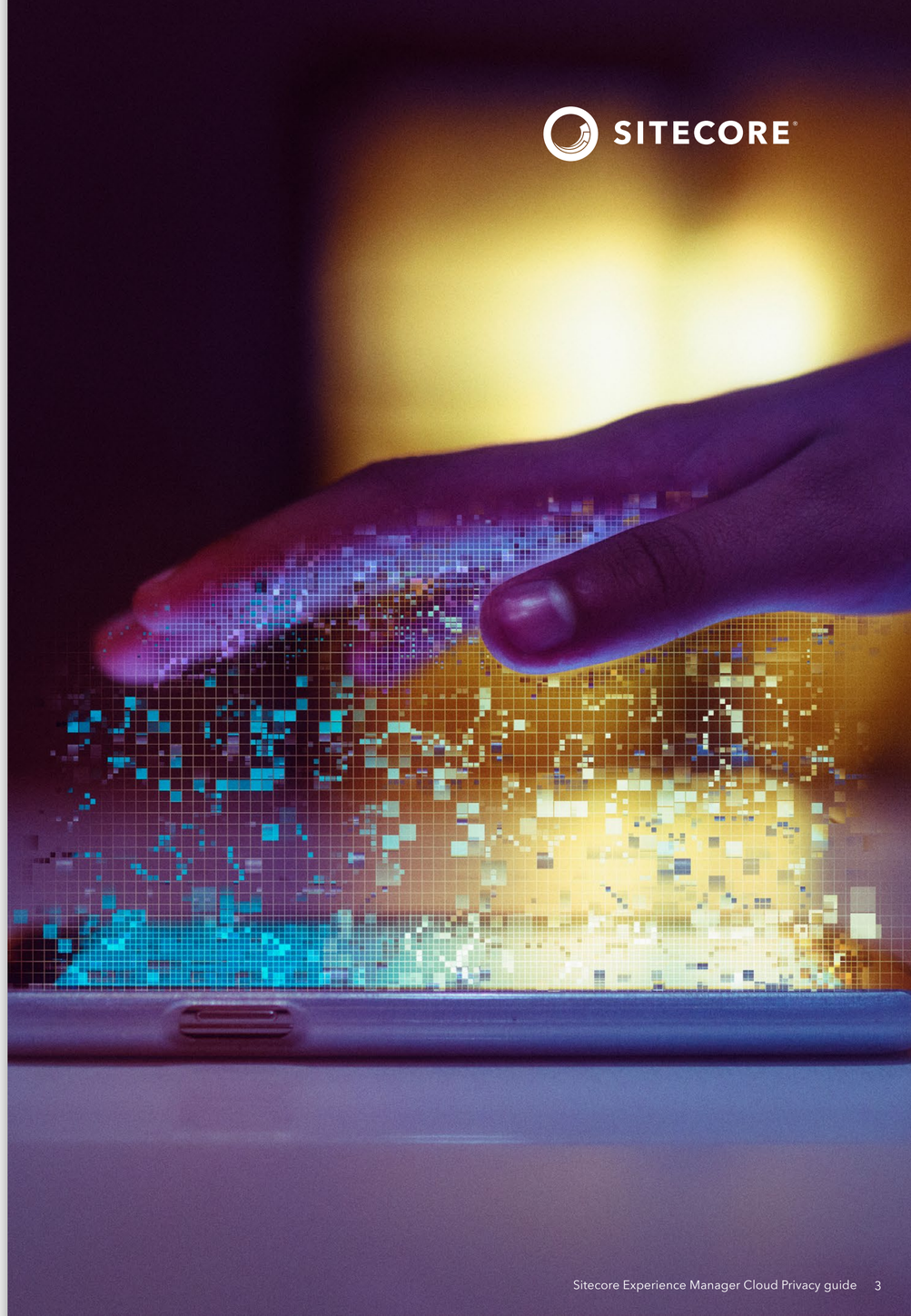
Sitecore Experience Manager Cloud ("XMC") is a modern, cloud-native, headless CMS delivered as SaaS that enables customers to achieve greater agility in the delivery of fast, contextual digital experiences to achieve business outcomes.

This XMC Privacy brochure provides a high-level outline of the processes that are applicable when purchasing this product offering. Further details on the specific data protection obligations relating to this product are available in our Data Processing Addendum available here.

Information collected

When using XMC, Sitecore may collect and retain the information in the table below. Within Sitecore applications, Sitecore customers (or their partner) may implement capabilities that collect information from their customers and users. This data is managed and used completely by customer organizations. Sitecore personnel do not have access or directly manage these data other than at the aggregate resource level, e.g. managing the database that house these data.

Data Type	Description	Purpose
Product usage data	Sitecore XM Cloud and its services collect product usage data. This data includes: • Number of builds • Number of deployments • Number of publishing jobs • Number of indexing jobs • Actions performed by the Sitecore Management Services	Used to get a better understanding of how Customers use our products, which allows us to optimize and evolve future versions of XMC.
Resource usage data	Data about XMC resource usage such as # of environments, entitlements, VMs, network transfer, storage, etc.	Used for billing purposes and to help Sitecore optimize service delivery to Customers.
Performance data	Data about service response time, latency, etc.	Used by Sitecore to optimize service delivery to Customers.
XMC customer data	Data requested from the Customer representing the number of Customer visitors who access the web applications built with Sitecore XMC, e.g. website visits	Used for billing purposes.
Support tickets	Sitecore will receive whatever information customers choose to submit to Sitecore as part of a support ticket.	Data is used to diagnose and reproduce problems encountered by a Sitecore customer to develop a solution to fix the problem reported by customer.



Information storage

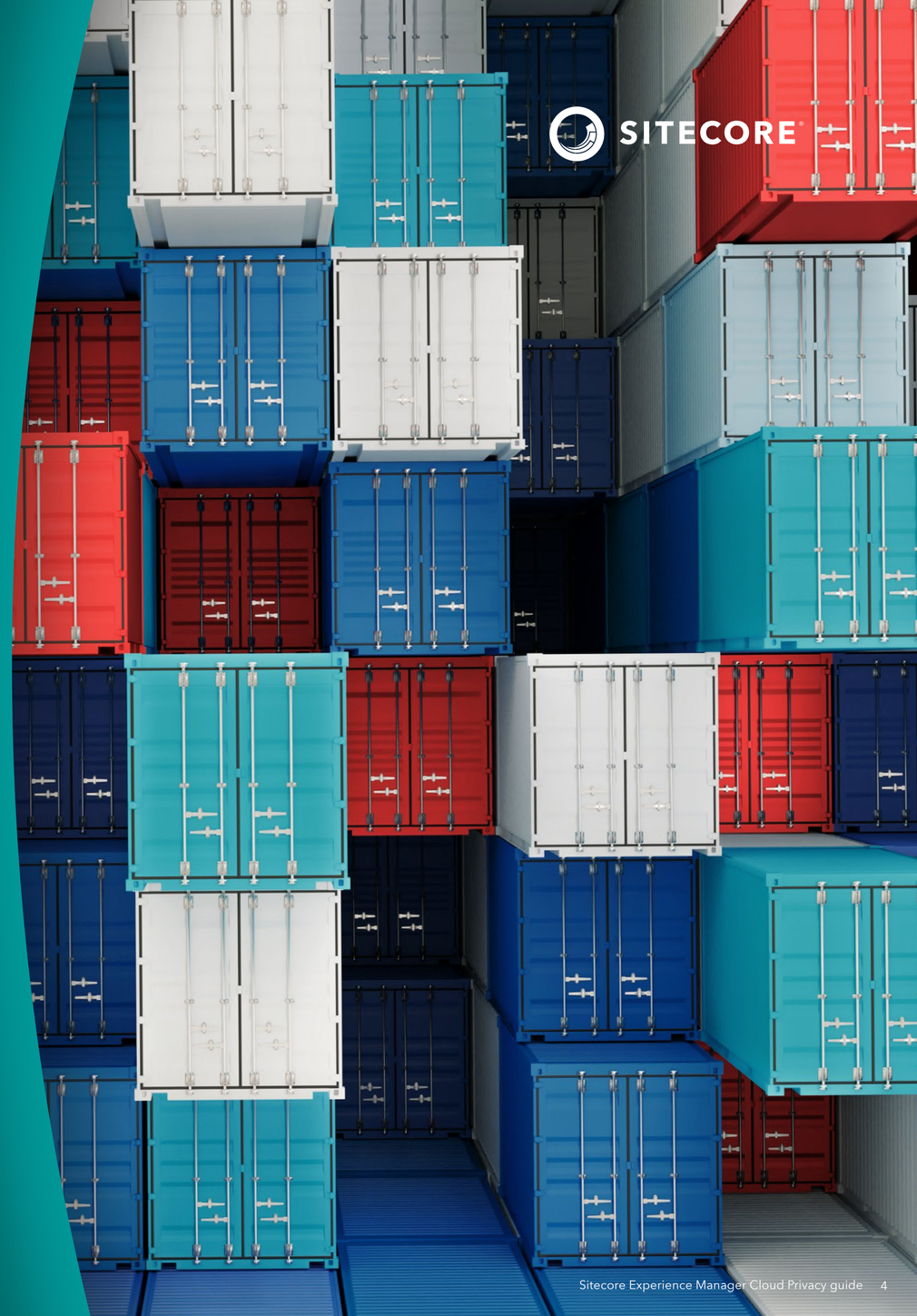
Sitecore deploys XMC using Microsoft Azure, with its Embedded Personalization capability delivered through Amazon Web Services (AWS). Data created and used in XMC is stored in datacenters within the country or region selected by customers. The following table shows available data centers where data is stored "at rest":

XMC datacenters (Azure)	Corresponding XMC embedded personalization datacenters (AWS)
Western Europe (Netherlands)	eu-west-1 (Ireland)
East US 2 (Virginia)	us-east-1 (N. Virginia)
West US 2 (Washington)	us-east-1 (N. Virginia)
Australia East (New South Wales)	ap-southeast-2 (Sydney)
Japan East (Tokyo)	ap-southeast-2 (Sydney)

Data access

Within any Sitecore XMC environment, only Sitecore personnel who are responsible for supporting the specific customer environment will have access to telemetry metric data, resource usage data, performance data, and customer data of that environment. Role-based access to Sitecore XMC data is restricted to the SaaS Ops team, based on business-need-to-know policy to maintain privacy and protect confidentiality. Time-limited, temporary access may be granted to developers for the purposes of troubleshooting, solving issues, and improving the effectiveness of security protections. Online access controls are managed following standard protocols and standards. Physical access controls to datacenters are managed by Microsoft Azure and AWS.

To demonstrate our commitment to protecting customer data, and to assure our Sitecore community that Sitecore's security framework is aligned with industry-recognized best practices, Sitecore maintains a number of compliance programs and certifications in accordance with strict regulatory and industry standards.



Security

At Sitecore, we understand the value of data and the importance of protecting it. We aim to be transparent with our customers, partners, service providers, and web visitors about how we handle data in every interaction with Sitecore, so you know your information is safe and secure.

Sitecore is committed to security and a privacy-first philosophy. We act on this philosophy through our internal compliance framework, as well as by implementing privacy-by-design features and security-as-default across our products and services such as XMC.

Since January 2019 Sitecore has received certifications and attestations for ISO27001, ISO 27017, ISO27018, CSA Star and SOC2 (Type 2) for a number of its product offerings.

For details of our current security certifications, see here.

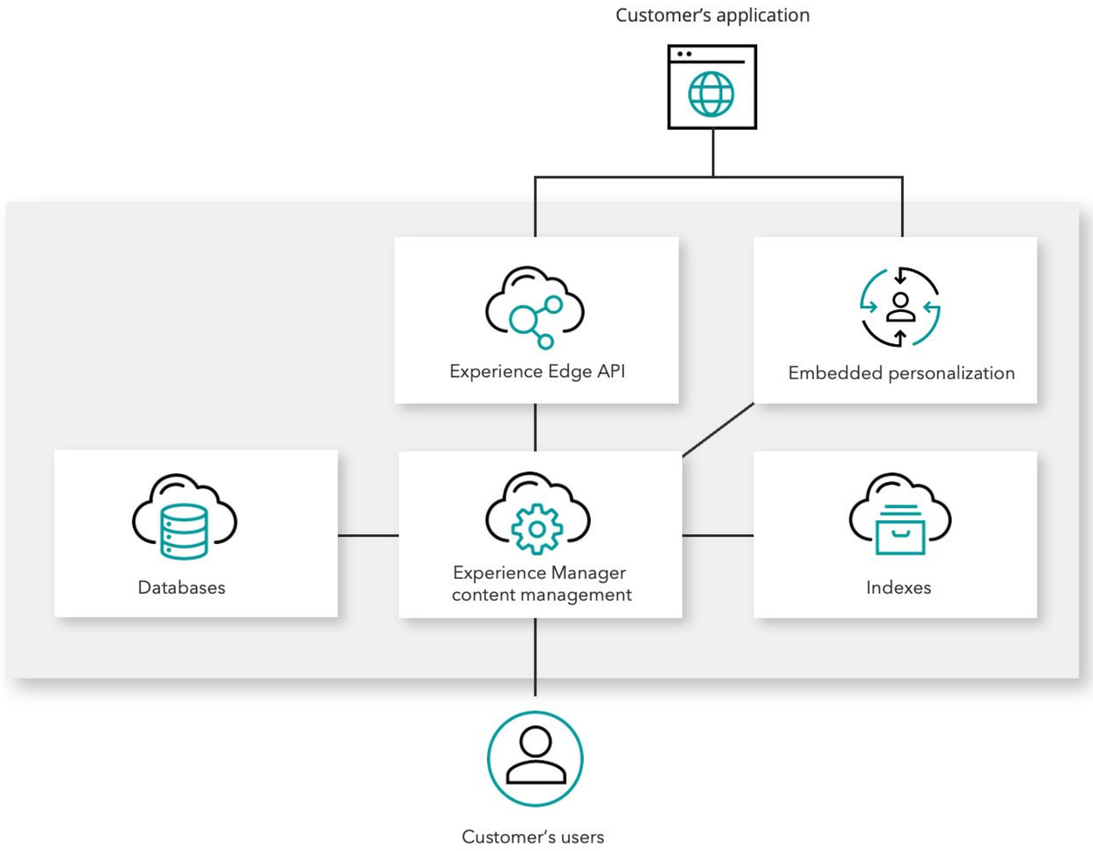
Retention

Data owned and managed by Sitecore customers (end-user data) are managed in accordance with XMC data retention policies. Sitecore personnel will only assist customers, upon request, in executing processes that implement these policies. For data managed by Sitecore (product usage, resource consumption, performance data), Sitecore maintains a record retention and disposal policy that addresses how long we store these data. When a customer terminates, we can return or delete their data within 30 days upon customer request.

Data transfers

For operations of Sitecore XMC, Sitecore transfers Customer Data only in accordance with the measures described in the Sitecore Data Processing Addendum (DPA). In its DPA, Sitecore has provided its customers two levels of protection for data transfers: both the Standard Contractual Clauses (SCCs) and Privacy Shield frameworks.

Data access flow



Subprocessors

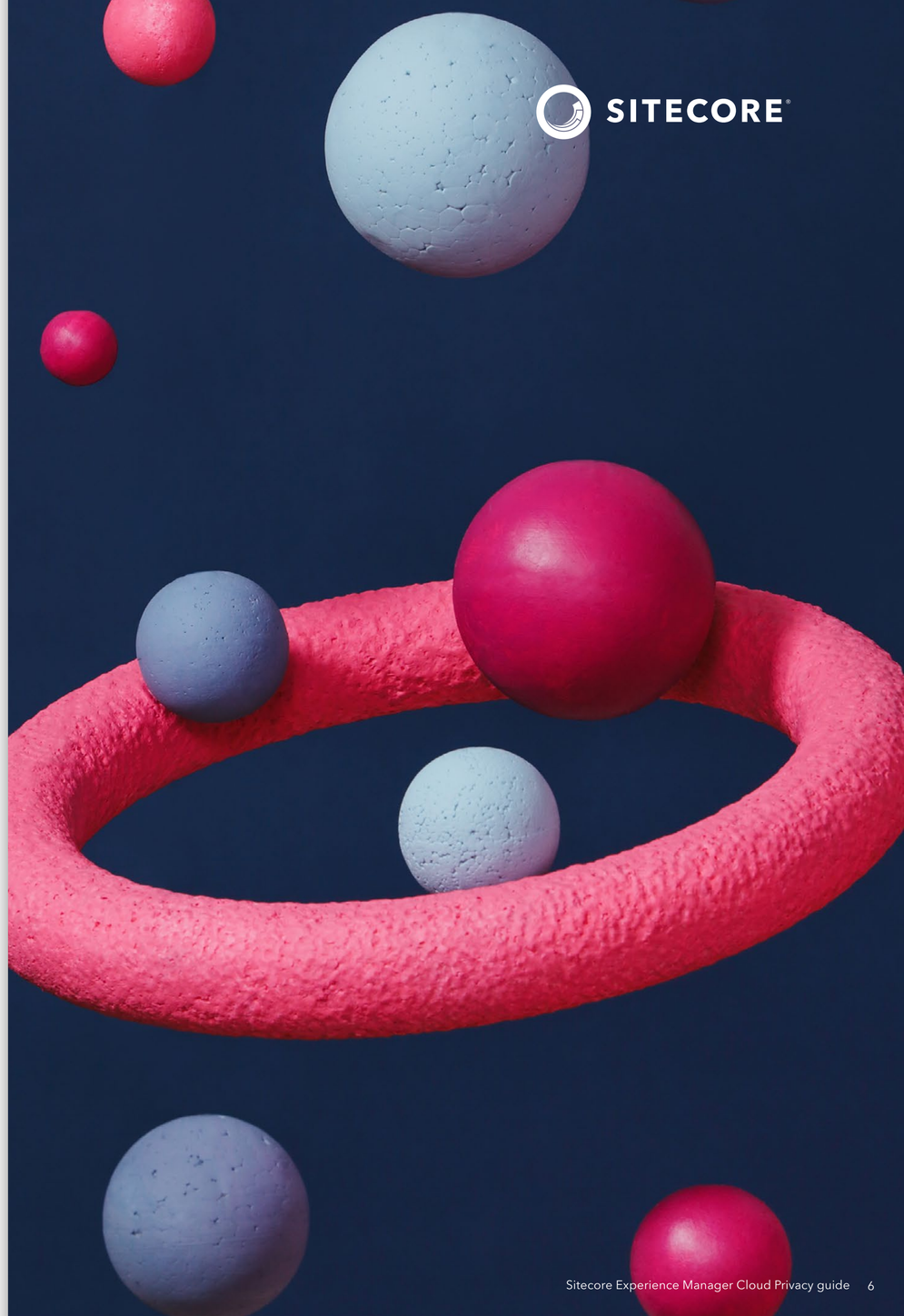
Sitecore XMC (if applicable)		
Entity Name	**Description of the performance**	**Corporate Location**
Microsoft	Cloud Service Provider	Redmond, Washington
AWS	Cloud Service Provider	Seattle, Washington
Vercel*	Cloud platform	San Francisco, California
Auth0	Authentication tool	Seattle, Washington
SearchStax	Search Services	Manhattan Beach, California
Confluent	Real-time data management	Mountainview, California

*Used for Sitecore XM Cloud where purchased under the relevant Order for Services.
The latest list of sub processors can be found here

Security incident management

Upon becoming aware of a Security Incident, Sitecore will notify Customer without undue delay (and no later than 48 hours after becoming aware of the Security Incident) and will provide information relating to the Security Incident as it becomes known or as is reasonably requested by Customer including the following:

- Details of the Customer Data compromised, including whether the Customer Data had been encrypted, hashed or otherwise rendered incomprehensible, inaccessible or unintelligible for unauthorized persons
- Information on the Data Subjects affected, such as categories and the number of Data Subjects affected
- Categories and number of information data records affected
- Description of the nature of the unlawful disclosure
- Identity and contact details of Sitecore's Privacy contact



- When the Security Incident took place (date or time period) and suspected cause
- Likely consequences of the security incident
- Recommendations to minimize harm

Sitecore will also take reasonable steps to mitigate and, where possible, to remedy the effects of, any Security Incident. Sitecore shall provide reasonable assistance to Customer, at Customer's expense, in the event Customer is required under Data Protection Laws to notify a supervisory authority or any Data Subjects of a Security Incident.

Additional information on Sitecore's use of customer information

Locations of Sitecore Personnel

Sitecore Cloud Operations teams are located globally in the following regions:

- North America
- Europe
- Asia-Pacific

Additionally, Sitecore adopts a "follow the sun" approach with a global development and support team to ensure that Sitecore customers benefit from robust response times. Support team members are located in these locations. Support tickets submitted by a Customer might be accessed by personnel in any one of these locations.

Customer confidential information

Global access is granted on a need-to-know basis (e.g., legal staff, CSMs and finance in any region can see contracts; sales can access CRM data; finance can access POs, invoices, etc.)

Further Information about Sitecore's privacy and security efforts can be found in the Sitecore Trust Center.

SITECORE

About Sitecore

Sitecore is a global leader of end-to-end digital experience software. Unifying data, content, commerce, and experiences, our SaaS-enabled, composable platform empowers brands like L'Oreal, Microsoft, United Airlines, and PUMA to deliver unforgettable interactions across every touchpoint. Our solution provides the cutting-edge tools brands need to build stronger connections with customers, while creating content efficiencies to stand out as transformation and innovation leaders.

Experience more at Sitecore.com.