# [Global privacy guide](https://doc.sitecore.com/xp/en/developers/102/platform-administration-and-architecture/global-privacy-guide.html)

### Warning

This Privacy Guide provides technical guidance on how your developers can choose to configure your Sitecore product implementation to support you with data privacy compliance. This guide does not provide exhaustive guidance, and should not be construed or used as legal advice about the content, interpretation, or application of any law or regulation. 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 how you process personal information. Your resulting implementation is based entirely on your own configuration choices.

This guide is aimed at developers and IT professionals. You can use it as a starting point to help you determine the way your organization stores and processes data, and the role Sitecore products play.

We know that privacy and data protection laws are constantly evolving, as are the obligations that your organization might have. This guide is intended to support those efforts and covers:

* [How individuals might be represented in your implementation](entities-that-represent-individuals-in-your-sitecore-implementation.html), how individuals and their personal information can be handled, what data is stored by default, and where it is stored.
* The Sitecore APIs and configuration options available to you as you look to comply with [privacy and individual requests](supporting-privacy-rights.html) outlined in legislation such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA).

When assessing the compliance of your Sitecore implementation with privacy regulations, start with the [privacy checklist](privacy-checklist.html).

See also:

* [Security guide](security-guide.html) for information about securing the platform.
* [Architecture and roles](architecture-overview.html) for information about how each role stores and handles personal information.
* [Data flows and processes](data-flows-and-processes.html) for information about how personal information flows through the platform.

For earlier versions of the platform, see:

* [Technical guidance for GDPR](https://doc.sitecore.com/en/developers/82/sitecore-experience-platform/technical-guidance-for-gdpr--including-exm-and-sitecore-commerce-.html) including EXM and Sitecore Commerce (Sitecore 8.2.7 and Sitecore Commerce 8.2.1 Update 3)
* [Privacy-related functionality in Sitecore 6, 7, 8, and 9](https://www.sitecore.com/en-gb/gdpr/privacy-compliance)

## Definitions

The following section defines several terms that appear in legal texts such as GDPR and/or CCPA, as they have been interpreted for the purposes of this guide only.

| Role | Definition | This is… |
| --- | --- | --- |
| Data Subject or Consumer | A Data Subject is an individual whose data is being processed and is represented by three entities: [the customer, the contact, and the user](entities-that-represent-individuals-in-your-sitecore-implementation.html). A Consumer is a California resident whose personal information is collected or processed. The term **individual** is used throughout this guide to capture both meanings unless referring to a specific entity. | The customer |
| Personal data or personal information | Any information that identifies an individual, and might include the following as applicable under relevant laws:\* Name\* Email address\* Records of products purchased\* Internet browsing history\* Fingerprints (or other biometric data)\* Social Security number\* Cookies\* IP addresses (or geolocation data)\* Contact interaction history\* Contact facets\* Contact identifiers\* Any *inferences drawn* from personal information to create a profile about a consumer reflecting the consumer’s preference, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.### ImportantYour organization is responsible for deciding what constitutes personal information in the context of your business. | The data Sitecore is processing |
| Processor or Service Provider | A Processor or Service Provider is an organization that is handling the data on behalf of another, as defined under applicable laws. | Sitecore |
| Processing | Includes:\* Tracking\* Collection\* Contact processing\* Interaction aggregation\* Personalization\* Automation processing\* Email marketing### ImportantYour organization is responsible for deciding what constitutes processing in the context of your business. | How Sitecore uses your data |
| Controller or Business | A Controller, or Business, as defined under applicable laws, is the entity or individual whose data is being handled by Sitecore. | The Sitecore customer |

# [Privacy checklist](https://doc.sitecore.com/xp/en/developers/102/platform-administration-and-architecture/privacy-checklist.html)

### Warning

This Privacy Guide provides technical guidance on how your developers can choose to configure your Sitecore product implementation to support you with data privacy compliance. This guide does not provide exhaustive guidance, and should not be construed or used as legal advice about the content, interpretation, or application of any law or regulation. 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 how you process personal information. Your resulting implementation is based entirely on your own configuration choices.

Use this privacy checklist as a starting point to assist you when assessing your Sitecore implementation’s compliance with global privacy regulations including the EU’s GDPR and California’s CCPA.

## Initial review

Consider where and how you are storing data in the platform:

* Familiarize yourself with the flow of personal information throughout the platform, and how [each role handles personal information](roles-overview.html).
* Perform an audit of all customizations that augment the contact, user, or customer entity. For example:
  + Custom contact facets.
  + Custom membership profile properties.
  + Data captured by Forms.
* Consider whether you need to [request consent to store and process personal information](consent-and-the-right-to-object.html) and plan to persist consent choices or other permissions as, for example, a contact facet.
* [Limit the exposure of personal information](limiting-exposure-of-personal-information.html) throughout the platform. You can, for example, choose not to write personal information to logs.
* Review synchronization of data between your Sitecore implementation and third-party applications, and ensure that this is included in the privacy policy.

## Individual data rights

Consider whether your implementation upholds the data rights afforded to individuals under applicable laws. For example:

* Individuals can [request that their personal information is deleted (right to erasure)](right-to-erasure.html), either by contacting the organization or using a self-service portal. This includes user, contact, and customer data, as well as any form submissions that might include personal information.
* Individuals can [request a copy of their data](right-to-data-portability.html), either by contacting the organization or using a self-service portal. This includes user, contact, and customer data, as well as any form submissions that might include personal information.
* Individuals [can update their personal information](right-to-rectification.html), either by contacting the organization or using a self-service portal. Make sure that the user, contact, and customer records are synchronized or that the individual is able to view and update each record individually.
* Individuals can [actively opt-in on all Sitecore websites](consent-and-the-right-to-object.html) or websites that use the Federated Experience Manager. You might want to avoid preselected check boxes or passive notices that do not require an active choice.
* Individuals are given [clear information about how the organization processes and stores personal information](right-to-be-informed.html). From a development point of view, ensure that it is easy for business users to update privacy policies and privacy warnings.
* You might want to review the consents or permissions in place prior to any synchronization to or from third-party applications, for example, via the Data Exchange Framework.
* Privacy policies describe the ways in which data is stored and processed across the entire platform, not just the Sitecore Experience Database (xDB). Consider the [contact, user, and customer entities, as well as form submissions](entities-that-represent-individuals-in-your-sitecore-implementation.html).
* Consider how individuals are informed of any new forms of processing as you enable them or add them to the platform.
* Determine how consent choices are persisted, for example, as a contact facet.
* Provide the ability for individuals to be able to revoke consent at any time, for example, by contacting the organization or using an online form.
* [Processing](types-of-processing.html) can be disabled for individuals who have not given consent, have revoked consent, or have objected to processing. Alternatively, if you are unable to disable processing, individuals are given the option to be forgotten.
* Prohibiting data practices that might be considered discriminatory.

## Security and access

* You have secured all application roles, storage roles, and indexes. Refer to the [Security Guide](security-guide.html) for a list of security procedures.
* You have limited [access to user interfaces](secure-access-to-applications-with-personal-information.html) to users that require access.

## Selling of personal information

* You have included the ability for the individual to opt-out from selling their personal information in accordance with the right to object or opt-out from selling personal information legislated by the CCPA.

## Storing request history

* Consider how you apply access rights to the request history and how you store these requests in a Sitecore contact report to address the CCPA right that individuals have not to be subject to discrimination.
* Review the request history to ensure that decisions around the segmentation of data does not negatively impact the user interface or customer experience.

# [Personal data in Sitecore](https://doc.sitecore.com/xp/en/developers/102/platform-administration-and-architecture/personal-data-in-sitecore.html)

This section of the Privacy Guide describes how individuals are represented in Sitecore across the different components of the platform, and how to limit the exposure of personal information.

* [Entities that represent individuals in your Sitecore implementation](entities-that-represent-individuals-in-your-sitecore-implementation.html)
* [Limiting exposure of personal information](limiting-exposure-of-personal-information.html)

For additional information about entities and data flows within Sitecore, see [Data flows and processes](data-flows-and-processes.html), and [Architecture and roles](architecture-overview.html).

# [Entities that represent individuals in your Sitecore implementation](https://doc.sitecore.com/xp/en/developers/102/platform-administration-and-architecture/entities-that-represent-individuals-in-your-sitecore-implementation.html)

### Warning

This Privacy Guide provides technical guidance on how your developers can choose to configure your Sitecore product implementation to support you with data privacy compliance. This guide does not provide exhaustive guidance, and should not be construed or used as legal advice about the content, interpretation, or application of any law or regulation. 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 how you process personal information. Your resulting implementation is based entirely on your own configuration choices.

An [individual](global-privacy-guide.html) is represented by four separate entities across the platform:

* As **contacts** in an Experience Platform (XP) context.
* As **enrollments** in the Marketing Automation database.
* As **customers** in an Experience Commerce (XC) context.
* As **users** in an Experience Manager (XM) context.

It is also represented as form metrics data in the xDB Reporting database, which links to form submission data in the Forms database.

Each entity has the potential to store sensitive personal information and entities are linked directly or indirectly by IDs or other identifiers. When securing the platform and implementing functionality that supports the individual’s rights, you must consider all representations of the individual across the platform and how they are linked.

## Where and how data is stored

The following tables describe the purpose of each entity, where the entity is stored, and what data can be associated with each entity.

### Important

The exact data that is collected by you depends on your implementation. These tables describe the model for collecting data that is available by default. Where it is stored depends on whether you are self-hosting or hosting in the Managed Cloud environment.

### Contacts

| Purpose | Central storage for data relevant to marketing activities such as personalization, automation, and email. |
| --- | --- |
| Storage | Collection database, xDB index |
| Data | If collected, the following data is available in the Collection database and the xDB index (assuming indexing of personal information is enabled):\* Contact identifiers\* Contact facets, including personal information such as: \* First and last name \* Address \* Email address, including a historical list of emails for EXM \* Commerce-specific data such as orders and carts, including the associated address and email address \* Interactions, including: \* Events \* Outcomes \* Goals \* Page views \* Interaction facets |
| API | xConnect Client API |

#### Default facets and events

See the  [xConnect collection model reference](/xp/en/developers/93/sitecore-experience-platform/en/collection-model-reference.html) for a list of all default xConnect facets and events. Facets with personal information are marked [PIISensitive].

#### Email Experience Manager facets and events

The Email Experience Manager (EXM) EmailAddressHistory contains personal information. This facet is marked [PIISensitive].

#### Commerce Connect facets and events

Personal information associated with events is stored in contact facets marked [PIISensitive]. Events do not store personal information, but might include properties that reference contact facets. If the individual chooses to be erased, all personal information is removed and the link between an event and personal information in a contact facet is broken.

### Enrollments

| Purpose | Represents a contact’s enrollment in an automation plan or activity. |
| --- | --- |
| Storage | Marketing Automation database |
| Data | The following data is available in the Marketing Automation database:\* Contact ID\* Plans or activities that the contact is enrolled in.Plan or activity names might reveal sensitive information about the individual’s interaction with a brand or organization.### NoteYou can add custom data to enrollments. We recommend that you do not add personal information such as email addresses to an enrollment. |
| API | Marketing Automation Operations API |

### Customers

| Purpose | Receive and pay for submitted orders. |
| --- | --- |
| Storage | Shared Environments database, Customers Scope index |
| Data | The following data is available in the Shared Environments database and Customers Scope index:\* Customer details, such as name and address\* Customer ordersSee [Customer entity](/xp/en/developers/102/sitecore-experience-commerce/en/customer-service.html)### NoteThe email address and shipping address are stored as part of an order, even for anonymous customers. |
| API | [Commerce Service API](/xp/en/developers/102/sitecore-experience-commerce/en/commerce-service-api.html) |

### Users

| Purpose | Authentication and authorization. |
| --- | --- |
| Storage | The default implementation of ASP.NET Membership stores users in the Core database. There is no default provider for ASP.NET Identity. |
| Data | \* Username\* ASP.NET membership profile data |
| API | ASP.NET Membership API or ASP.NET Identity API |

### Forms

| Purpose | Metrics such as form submission successes and failures are aggregated into the xDB Reporting database. Each record includes a ContactId, InteractionId, and FieldId. Form submissions are stored in the Forms database, and include a FieldItemId.The records can be linked to a contact in the Collection database as follows. Refer to the table in the next section, [Links between individual entities](entities-that-represent-individuals-in-your-sitecore-implementation.html), for more information. |
| --- | --- |
| Storage | xDB Reporting database, specifically:\* Fact\_FormMetrics table (includes ContactID and InteractionID)\* Fact\_FormFieldMetrics table (includes InteractionID)Forms database, specifically:\* FieldData table (includes form submission data) |
| Data | Form submission data is customizable and can include personal information such as an individual’s name and email address. |
| API | Reporting API, SQL |

## Links between individual entities

The following table details how individual entities are linked in a default implementation that uses Commerce Connect to link Experience Platform and Experience Commerce.

### Links to the customer entity

| From contact to customer | There is no direct link between a contact and a customer. Indirect link via contact to user (assuming an identifier exists), user to customer. |
| --- | --- |
| From user to customer | The user entity has an ExternalId property that includes the customer’s ID and a prefix. If you are using the Sitecore Commerce Engine, the ExternalId looks like the following: Entity-Customer-6c639677c824494bbf64c1049312233e. In this case, 6c639677c824494bbf64c1049312233e is the customer ID. |
| From form submission to customer | There is no direct link between a form submission and a customer. Indirect link via form data to contact, contact to user (assuming an identifier exists), user to customer. |
| From enrollment to customer | There is no direct link between an enrollment and a customer. |

### Links to the enrollment entity

| From customer to enrollment | There is no direct link between an enrollment and a customer. |
| --- | --- |
| From contact to enrollment | Enrollments include a reference to the contact’s ID. |
| From user to enrollment | There is no direct link between an enrollment and a user. |
| From form submission to enrollment | The Fact\_FormMetrics table contains a ContactID column. You can use the xConnect Client API to retrieve a contact by ID and use that ID to look up enrollments. |

### Links to the contact entity

| From customer to contact | There is no direct link between a contact and a customer. Indirect link via customer to user, user to contact (assuming an identifier exists). |
| --- | --- |
| From user to contact | By default, there is no link between a contact entity and a user entity. To create a link, you must add a known identifier to the contact that includes an identifier string (such as the username) and a source string (such as ‘extranet’). This can be done using the  [xConnect Client API](/xp/en/developers/102/sitecore-experience-platform/en/xconnect-client-api--c--.html), or using the IdentifyAs() method in a tracking context.If you are using Commerce Connect, a known identifier is automatically added to a contact when a user is created. The identifier is the username, and the source is Sitecore.Commerce.Constants.ContactSource. If you are not using Commerce Connect, you must create this relationship yourself. A contact can have multiple identifiers that links them to different systems. You must know which identifier source your system is using for identifiers that correspond to a user entity. |
| From form submission to contact | The Fact\_FormMetrics table contains a ContactID column. You can use the xConnect Client API to retrieve a contact by ID. The Fact\_FormFieldMetricscontains an InteractionID column. You can look up the corresponding entry in the Fact\_FormMetrics table, which also contains the ContactID column. |
| From enrollment to contact | Enrollments include a reference to the contact’s ID. |

### Links to the user entity

| From customer to user | The user entity has an ExternalId property that includes the customer’s ID and a prefix. If you are using the Sitecore Commerce Engine, the ExternalId looks like the following: Entity-Customer-6c639677c824494bbf64c1049312233e. In this case, 6c639677c824494bbf64c1049312233e is the customer ID. |
| --- | --- |
| From contact to user | By default, there is no link between a contact entity and a user entity. To create a link, you must add a known identifier to the contact that includes an identifier string (such as the username) and a source string (such as ‘extranet’). This can be done using the xConnect Client API, or using the IdentifyAs() method in a tracking context.If you are using Commerce Connect, a known identifier is automatically added to a contact when a user is created. The identifier is the username, and the source is Sitecore.Commerce.Constants.ContactSource. If you are not using Commerce Connect, you must create this relationship yourself. A contact can have multiple identifiers that links them to different systems.You must know which identifier source your system is using for identifiers that correspond to a user entity. |
| From form submission to user | There is no direct link between a user and form submissions. Indirect link via user to contact (assuming an identifier exists), contact to form submission. |
| From enrollment to user | There is no direct link between a user and an enrollment. |

### Links to form submissions

| From customer to form submission | There is no direct link between a customer to a form submission. Indirect link via user to contact, contact to form submission. |
| --- | --- |
| From user to form submission | There is no direct link between a customer to a form submission. Indirect link via user to contact (assuming an identifier exists), contact to form submission |
| From contact to form submission | The Fact\_FormMetrics table contains a ContactID column. You can use the xConnect Client API to retrieve a contact by ID. The Fact\_FormFieldMetricscontains an InteractionID column. You can look up the corresponding entry in the Fact\_FormMetrics table, which also contains the ContactID column. |
| From enrollment to form submission | The Fact\_FormMetrics table contains a ContactID column. You can use the xConnect Client API to retrieve a contact by ID and use that ID to look up enrollments. |

# [Limiting exposure of personal information](https://doc.sitecore.com/xp/en/developers/102/platform-administration-and-architecture/limiting-exposure-of-personal-information.html)

### Warning

This Privacy Guide provides technical guidance on how your developers can choose to configure your Sitecore product implementation to support you with data privacy compliance. This guide does not provide exhaustive guidance, and should not be construed or used as legal advice about the content, interpretation, or application of any law or regulation. 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 how you process personal information. Your resulting implementation is based entirely on your own configuration choices.

In addition to securing the platform and complying with GDPR [data rights](supporting-privacy-rights.html), we recommend that you review the spread of personal information throughout your implementation. Use the following list as a starting point.

## Marking facets as [PIISensitive]

Make sure that any custom contact facets with personal information are marked [PIISensitive] - these facets are cleared when the [right to erasure](/xp/en/developers/93/sitecore-experience-platform/en/execute-right-to-be-forgotten.html) is executed.

## Indexing of data marked PIISensitive

By default, contact facets marked [PIISensitive] are not indexed. This means that sensitive personal information is not stored in the xDB index. Be wary of [enabling the indexing of PII sensitive data](/xp/en/developers/102/sitecore-experience-platform/en/enable-indexing-of-pii-sensitive-data-in-the-xdb-index.html), unless it is absolutely necessary.

## Personal information in logs

You might choose to exclude personal information from logging that you perform in your code - for example, when a visitor logs in or registers, you might exclude their email address or other personal information from the log entry.

### Note

If you must log a reference to a contact for debugging reasons, you might consider using the alias identifier rather than the contact ID. The alias identifier is deleted when the right to erasure is executed, thereby severing the link between contact and log entry. This assumes that the storage and lifetime of your logs comply with legislation.

### Excluding personal information from EXM logs

In Sitecore 9.0 Update-1 and later, you can use the following configuration setting to include or exclude personal information in the EXM logs:

Copy <setting name=“EXM.IncludePIIinLogFiles” value=“false”/>

Personal information is excluded from the logs by default.

## Limiting personal information loaded into session

Use configuration to [limit which facets containing personal information are loaded into session](/xp/en/developers/102/sitecore-experience-platform/en/load-facets-into-session.html). This reduces the amount of personal information that is stored in the Shared Session State Store for the duration of a contact’s session.

## Contact IDs in external systems

You might choose not to expose contact IDs in external systems or expose them in interfaces or URLs.

Contact IDs in the [Collection database](xdb-collection-database.html) are sequentially generated by the xConnect service layer. This means that it is technically possible for an application with access to the  [xConnect API](/xp/en/developers/93/sitecore-experience-platform/en/xconnect-client-api-overview.html) to guess a contact ID and retrieve a contact that it should not have access to.

If you want to store an anonymous reference to a contact in an external system, consider using the [alias identifier](/xp/en/developers/102/sitecore-experience-platform/en/contact-identifiers.html). Identifiers are removed when the right to erasure is executed against a contact, and any link between the alias identifier and a third-party system will be broken.

## Hashing or redacting IPs

IP addresses are [hashed by default](/xp/en/developers/102/sitecore-experience-platform/en/configure-the-tracker.html), and can be redacted. IP addresses are stored in IpInfo interaction facet and are not cleared when the right to erasure is executed.

## The LocaleInfo facet

You might choose not to populate the GeoCoordinate property of the LocaleInfo interaction facet. Interaction facets are not cleared when the right to erasure is executed.

### Note

In the tracker, these properties are populated automatically if you are using Sitecore’s [IP Geolocation Service](/xp/en/developers/90/sitecore-experience-manager/en/set-up-sitecore-ip-geolocation.html). You can disable the service to prevent sensitive data from being stored in interactions.

## Sensitive data in interactions or events

You can create custom event models and extend interactions with facets. You might choose not to store personal information in interaction facets and events, as interaction data is not cleared when the right to erasure is executed.

Email Experience Manager’s EmailEvent does not store an email address. Instead, the EmailAddressHistoryEntryId property of each event references an entry in the EmailAddressHistory facet on the contact. This facet is marked [PIISensitive] and is cleared when the right to erasure is executed against the contact.

## Disabling analytics for a particular page

If a page does not need to be tracked, you might choose to [disable analytics](/xp/en/users/102/sitecore-experience-platform/en/disable-analytics-on-an-item.html) to reduce the amount of behavioral data that you are collecting.

## Sensitive information in URL query strings

If tracking is enabled, the complete URL of a page - including the query string - is persisted in session and mapped to the Url property of the PageViewEvent before being submitted to xConnect. You might choose not to include contact IDs, email addresses, usernames, or any other data that can be linked back to a contact, user, or customer entity.

### Tip

Disable analytics for any page that exposes sensitive data in the URL.

## Personal data in the xDB Reporting database

[Processing and aggregation](processing-and-aggregation.html) produces aggregate data that is stored in the xDB Reporting database. To avoid creating a link between data in the xDB Reporting database and a specific contact, you might choose not to store contact IDs, interaction IDs, or any other data that can be linked back to a contact, user, or customer entity.

## Limiting the use of personal information in Marketing Automation activities

Be aware of any custom Marketing Automation activities that store personal information in an activity’s [custom values](/xp/en/developers/102/sitecore-experience-platform/en/custom-values.html). This data is stored in the Marketing Automation database.

## Limiting use of List Manager CSV export

The [List Manager](/xp/en/users/91/sitecore-experience-platform/en/the-list-manager.html), which enables you to manage contact lists, also allows you to export lists of contacts to a CSV. Use [role-based authorization to lock down this interface](secure-access-to-applications-with-personal-information.html) and make sure that the organization is aware that personal information can be exported in this manner.

## Search events

If you are  [triggering the search event from the tracker](/xp/en/developers/102/sitecore-experience-platform/en/triggering-built-in-events.html), consider the type of data that might be included in the search text. For example, if you raise the search event as part of map search, the search text might include an individual’s home address. The search event is saved to the xDB Collection database as a SearchEvent, and cannot be edited once it has been saved.

### Note

Sitecore Experience Accelerator (SXA) components that use search automatically trigger the search event.

## Serialized xConnect data

Make sure that any custom cache or custom storage role that contains [serialized contacts or interactions](/xp/en/developers/102/sitecore-experience-platform/en/serialize-xconnect-entities-using-json-net.html) is secure and addresses the recommendations in this guide. Alternatively, you can choose not to serialize personal information.

## Cookie lifetime

Consider whether the default lifetime of the SC\_ANALYTICS\_GLOBAL\_COOKIE needs to be changed. See [Tracker configuration](/xp/en/developers/102/sitecore-experience-platform/en/configure-the-tracker.html) for more information.

# [Securing personal information](https://doc.sitecore.com/xp/en/developers/102/platform-administration-and-architecture/securing-personal-information.html)

This section describes the steps you can take to [secure access to applications with personal information.](secure-access-to-applications-with-personal-information.html)

For additional information on securing personal information, see:

* [Security Guide](security-guide.html)
* [Managed cloud policies](https://kb.sitecore.net/articles/133931)

# [Secure access to applications with personal information](https://doc.sitecore.com/xp/en/developers/102/platform-administration-and-architecture/secure-access-to-applications-with-personal-information.html)

### Warning

This Privacy Guide provides technical guidance on how your developers can choose to configure your Sitecore product implementation to support you with data privacy compliance. This guide does not provide exhaustive guidance, and should not be construed or used as legal advice about the content, interpretation, or application of any law or regulation. 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 how you process personal information. Your resulting implementation is based entirely on your own configuration choices.

Ensure that business users with access to back office interfaces such as the Commerce Business Tools or the User Manager on the Content Management role have the appropriate levels of access. Other recommendations include:

* Use security roles to limit access to Sitecore interfaces. You can use [default security roles](the-security-roles.html) or create your own.
* Disable or remove unused user accounts.
* Limit the number of administrator accounts.
* Configure a [strong password policy](configure-the-password-policy.html).

## Applications that expose personal information

The following table lists the business user applications that access and display personal information, and the role that is required to access the application:

| Application | Personal information exposed by the application | Role required to access application |
| --- | --- | --- |
| User Manager | User name, user email, and potentially other personal information. | sitecore\Sitecore Client Account Managing |
| Federated authentication | User name, user email, and potentially other personal information. | sitecore\Sitecore Client Account Managing |
| All SPEAK applications | User name. Name is displayed in the SPEAK ribbon. | Any logged-in user |
| List Manager | User email address, user name. | sitecore\List Manager Editors |
| Content Editor | Fields with user name in Created By and Edited By fields. | sitecore\Sitecore Client Authoring |
| Experience Profile | User name, email, location, and other personal information. | sitecore\Analytics Reportingsitecore\EXM Advanced Userssitecore\EXM Users |
| Experience Analytics | Reports by Location, reports by IP, reports by User Agent/Device. | sitecore\Analytics Reporting |
| Email Experience Manager | Accesses recipient lists created by List Manager. | See [EXM security roles](/xp/en/developers/exm/102/email-experience-manager/en/exm-security-roles.html) |
| Marketing automation | User names, email addresses. | sitecore\Marketing Automation Editors### NoteYou can export contacts currently enrolled in a campaign to CSV. The CSV includes personal information such as the contact’s name and email address. |
| Commerce Business Tools | Customer name, address, email, order history. | See [User roles and permissions](/xp/en/developers/102/sitecore-experience-commerce/en/user-roles-and-permissions.html) for information about Commerce roles |
| Forms | Form submission data. | See [The security roles in Sitecore Forms](/xp/en/developers/92/sitecore-experience-manager/en/the-security-roles-in-sitecore-forms.html) |

# [Supporting privacy rights](https://doc.sitecore.com/xp/en/developers/102/platform-administration-and-architecture/supporting-privacy-rights.html)

### Warning

This Privacy Guide provides technical guidance on how your developers can choose to configure your Sitecore product implementation to support you with data privacy compliance. This guide does not provide exhaustive guidance, and should not be construed or used as legal advice about the content, interpretation, or application of any law or regulation. 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 how you process personal information. Your resulting implementation is based entirely on your own configuration choices.

Privacy legislation such as the [EU General Data Protection Regulation (GDPR)](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN) and [California Consumer Protection Act (CCPA)](https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375) afford various rights to individuals including:

* [The right to erasure](right-to-erasure.html)
* [The right of access](right-of-access-by-the-individual.html)
* [The right to object or opt-out of selling of personal information](right-to-object-or-opt-out-of-selling-of-personal-information.html)
* [The right to data portability](right-to-data-portability.html)
* [The right to rectification](right-to-rectification.html)
* [The right to be informed](right-to-be-informed.html)
* [The right to restrict processing](right-to-restrict-processing.html)
* [The right not to be subject to discrimination](right-not-to-be-subject-to-discrimination.html)
* [The right to opt out of automated decision making and profiling](profiling-and-automated-decision-making.html)

The following section describes each data right as it relates to the contact, user, and customer entities, and lists the features, APIs, and configuration options available to you: [Entities that represent individuals in your Sitecore installation](entities-that-represent-individuals-in-your-sitecore-implementation.html).

See also:

* [Types of processing](types-of-processing.html)
* [Privacy functionality by feature](privacy-functionality-by-feature.html)

# [Right to erasure](https://doc.sitecore.com/xp/en/developers/102/platform-administration-and-architecture/right-to-erasure.html)

| Applies to | GDPR, CCPA |
| --- | --- |
| Applies to | GDPR, CCPA |

### Warning

This Privacy Guide provides technical guidance on how your developers can choose to configure your Sitecore product implementation to support you with data privacy compliance. This guide does not provide exhaustive guidance, and should not be construed or used as legal advice about the content, interpretation, or application of any law or regulation. 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 how you process personal information. Your resulting implementation is based entirely on your own configuration choices.

The right to erasure (also known as the right to be forgotten) concerns the individual’s right to request the deletion of personal information. This topic describes how Sitecore facilitates the ability to remove an individual’s personal information.

## Erasing personal contact data

Within your Sitecore implementation, you can:

* Use the [xConnect Client API](/xp/en/developers/102/sitecore-experience-platform/en/xconnect-client-api--c--.html) to erase data marked [PIISensitive] by calling the ExecuteRightToBeForgotten() method. The ClearSupressionListWhenExecutingRightToBeForgotten handler automatically clears the contact’s past and current email addresses from the suppression list.

### Note

* The ExecuteRightToBeForgotten() method [does not delete the entire contact record](/xp/en/developers/93/sitecore-experience-platform/en/execute-right-to-be-forgotten.html).
* Execute the right to erasure from the Experience Profile interface.

The organization is responsible for the following:

* Implementing a process or interface that allows individuals to request deletion of personal information.
* Ensuring that personal information in custom contact facets is marked [PIISensitive]. Any facet or facet property marked [PIISensitive] is deleted when the right to erasure is executed.

### Important

Interaction facets cannot be marked [PIISensitive] and are not deleted when the right to erasure is executed.

### Removing all contact data

In Sitecore 9.2 and later, you can [delete a contact and all of its interactions](/xp/en/developers/93/sitecore-experience-platform/en/deleting-contacts-and-interactions-from-the-xdb.html). Keep the following in mind if you choose to delete contacts and interactions instead of using the ExcuteRightToBeForgotten() method:

* If a contact is deleted during an active session, that contact might be partially recreated on session end - including known identifiers that were loaded into session.
* Aggregated data in the xDB Reporting database are affected if you choose to rebuild all reporting data.

## Erasing personal user data

Within your Sitecore implementation, you can:

* Use the [Security API](http:///legacy-docs/SC75/security-api-cookbook-sc60-and-later-a4.pdf) to clear profile properties that contain personal information.
* [Edit a user in the User Manager interface](edit-and-manage-a-user-account.html).

The organization is responsible for the following:

* Implementing a process or interface that allows individuals to request that their data is deleted.
* Ensuring all user profile properties that contain personal information are identified and cleared.

## Erasing personal customer data

Within your Sitecore implementation, you can:

* Use the [Commerce Service API](/xp/en/developers/102/sitecore-experience-commerce/en/commerce-service-api.html) to delete a customer. You must set the ForgetCustomer property to true in the CustomersRemovePolicy. This ensures that the customer entity is deleted rather than marked as inactive.
* [Manage a customer’s data in the Customers dashboard](/xp/en/users/102/sitecore-experience-commerce/en/work-with-customer-accounts.html)

The organization is responsible for the following:

* Configuring the CustomersRemovePolicy correctly.
* Implementing a process or interface that allows individuals to request that their data is deleted.
* Ensuring all customer profile properties that contain personal information are identified and cleared.

### Note

Deleting a customer does not delete the shipping address and email address associated with the order. This data also exists for anonymous orders.

## Erasing active session data

If a contact requests that their data be erased, consider clearing session data and removing cookies to ensure that all connections between the device and the contact are severed:

* Call Session.Clear().
* Call Session.Abandon().
* Remove the SITECORE\_GLOBAL\_ANALYTICS\_COOKIE (although tracking does not resume after the right to erasure has been executed, xConnect Client API can be used to link a cookie to a device profile, and then to an anonymized contact record).

## Erasing forms submission data

By default, form submission data is stored in the [Forms database](forms-database.html). If the xDB is enabled, all form submissions are associated with a contact ID. To facilitate Sitecore and its partners in complying with data privacy obligations, Sitecore Forms provides a redact API to anonymize database records of users’ personal information. You need to expose a mechanism by which the individual can trigger a query to erase their data, for example, by [implementing a custom submit action](/xp/en/developers/102/sitecore-experience-manager/en/walkthrough--create-a-submit-action-that-redacts-form-submissions.html) that redacts form submissions.

The Forms redact API is responsible for the following:

* Searches for all form entries associated with a specific contact ID and anonymizes these entries by erasing the contact ID value and marking the entries as [IsRedacted].
* Erases all submitted data associated to these entries by setting their value to [~REDACTED~].
* Deletes all the uploaded files associated with the contact ID.

In CMS-only mode, form submissions are not associated with a contact ID (the contact ID is NULL). However, if form submissions are linked to another identifier such as an email address, you can use SQL to access and update a specific individual’s personal information.

### Important

If you create a custom submit action that stores personal information in a third-party system such as a CRM, you are responsible for ensuring that individuals can access their data in that system.

# [Right of access by the individual](https://doc.sitecore.com/xp/en/developers/102/platform-administration-and-architecture/right-of-access-by-the-individual.html)

| Applies to | GDPR, CCPA |
| --- | --- |
| Applies to | GDPR, CCPA |

### Warning

This Privacy Guide provides technical guidance on how your developers can choose to configure your Sitecore product implementation to support you with data privacy compliance. This guide does not provide exhaustive guidance, and should not be construed or used as legal advice about the content, interpretation, or application of any law or regulation. 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 how you process personal information. Your resulting implementation is based entirely on your own configuration choices.

The right of access concerns the individual’s right to access their personal information and obtain information about how their data is being processed. This topic describes how the Sitecore product facilitates the ability to access and [update](right-to-rectification.html) the individual’s personal information.

## Accessing contact data

Within your Sitecore implementation, you can:

* Use the [xConnect API](/xp/en/developers/102/sitecore-experience-platform/en/xconnect-client-api--c--.html) to [access and update a single contact’s person details and interaction history](/xp/en/developers/93/sitecore-experience-platform/en/get-contacts.html).

The organization is responsible for the following:

* Implementing a process or an interface that allows individuals to access their contact data.

## Accessing user data

Within your Sitecore implementation, you can:

* Use the [Security API](http:///legacy-docs/SC75/security-api-cookbook-sc60-and-later-a4.pdf) to access and edit a user’s profile.
* Allow members of your organization to respond to requests for data by [using the User Manager interface to view an individual’s personal information](edit-and-manage-a-user-account.html).

The organization is responsible for the following:

* Implementing a process or an interface that allows individuals to access their user data.

## Accessing customer data

Within your Sitecore implementation, you can:

* Use the [Commerce Service API](/xp/en/developers/102/sitecore-experience-commerce/en/commerce-service-api.html) to access customer and order data.

The organization is responsible for the following:

* Implementing a process or an interface that allows individuals to access their customer data.

## Accessing form submission data

By default, form submission data is stored in the [Forms database](forms-database.html). If a form submission is linked to an identifier such as a contact identifier or an email address, you can use SQL to access and update a specific individual’s personal information.

The organization is responsible for:

* If relevant, implementing a process or an interface that allows individuals to access their form submission data. The following example assumes that you know which form field (represented by FieldItemID) contains sensitive data. Forms and form fields are created by business users. For more information, see [Create a form](/xp/en/users/100/sitecore-experience-platform/en/design-a-form.html).
* CopyUSE [sample\_Sitecore.ExperienceForms]
* GO
* SELECT [ID], [FormEntryID], [FieldItemID], [FieldName], [Value], [ValueType] FROM [dbo].[FieldData] WHERE [FieldItemID] = ‘7d00533b-1cf2-4597-aaa0-01e09a01b7cc’ AND [Value] = ‘youremail’
* GO

### Important

If you create a custom submit action that stores personal information in a third-party system such as a CRM, you are responsible for ensuring that individuals can access their data in that system.

# [Consent and the right to object](https://doc.sitecore.com/xp/en/developers/102/platform-administration-and-architecture/consent-and-the-right-to-object.html)

| Applies to | GDPR, CCPA |
| --- | --- |
| Applies to | GDPR, CCPA |

### Warning

This Privacy Guide provides technical guidance on how your developers can choose to configure your Sitecore product implementation to support you with data privacy compliance. This guide does not provide exhaustive guidance, and should not be construed or used as legal advice about the content, interpretation, or application of any law or regulation. 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 how you process personal information. Your resulting implementation is based entirely on your own configuration choices.

The right to object concerns the individual’s right to object to processing, direct marketing, and automated profiling. This topic describes how the Sitecore product supports the individual’s ability to give and revoke consent, including:

* Existing interfaces and API calls for opting in/out of processing.
* Options for storing consent choices.

For information about processing, see [Types of processing](types-of-processing.html).

## Opting in and out of processing

The Sitecore product provides the following functionality by default:

* The Email Experience Manager supports [double opt-in](/xp/en/developers/exm/102/email-experience-manager/en/the-exm-double-opt-in-process.html).
* The Email Experience Manager API supports [unsubscribing from one or all mailing lists](/xp/en/developers/exm/102/email-experience-manager/en/the-email-experience-manager-client-api.html).
* Every email message sent by the Email Experience Manager includes links to unsubscribe from the context email message or all email messages.
* Sitecore 10.0 and later provides API calls and configuration options that make it easier to [enforce explicit consent for tracking a contact’s activity on your websites](/xp/en/developers/102/sitecore-experience-platform/en/enable-or-disable-web-tracking-based-on-visitor-consent.html).

The organization is responsible for:

* Supporting active opt-in for all forms of processing.
  + See [Right to be informed](right-to-be-informed.html) for information about implementing privacy notices or cookie consent banners.
  + See [Types of processing](types-of-processing.html) for a list of processing activities.
* Implementing interfaces (such as cookie consent banners) or processes that allow contacts to update consent choices.
* Implementing active opt-in on websites that use the Federated Experience Manager.
* Requesting consent for any additional collection or processing of personal information, including any data collected using [forms](entities-that-represent-individuals-in-your-sitecore-implementation.html).
* Implementing an interface or process that allows individuals to revoke consent at any time.

## Storing consent

Sitecore provides the following functionality by default:

* [Explicit consent for tracking](/xp/en/developers/102/sitecore-experience-platform/en/walkthrough--configuring-a-website-to-require-explicit-consent-for-tracking.html) is configured per website using the explicitConsentForTrackingIsRequired attribute in the Sitecore.config file (<siteroot>/App\_Config/Sitecore.config). The default value is false.
* The ConsentInformation facet, which is used by the Email Experience Manager and the [web tracker](/xp/en/developers/102/sitecore-experience-platform/en/enable-or-disable-web-tracking-based-on-visitor-consent.html) by default. Consent options are stored as a dictionary (Dictionary<string, ConsentItem>). You can choose to use the ConsentInformation facet to store consent choices if it meets your requirements for storing consent.
* Email Experience Manager global opt-out list.
* Email Experience Manager suppression list (available for customers that use the Email Cloud Service).
* Marketing automation plan Update consent settings [marketing action](/xp/en/users/90/sitecore-experience-platform/en/the-elements-in-a-marketing-automation-campaign.html).

The organization is responsible for:

* If necessary, implementing additional contact facets that store consent choices for specific types of processing.
* Storing consent for personal information collected via custom Forms - for example, by including a consent check box on each form.
* Persisting consent choices for individuals that do not want to be tracked or stored at all - for example, by storing a value in session or issuing a cookie.

## Disabling processing

See [Types of processing](types-of-processing.html) for an overview of processing activities in the platform and the options available for disabling processing.

# [Right to data portability](https://doc.sitecore.com/xp/en/developers/102/platform-administration-and-architecture/right-to-data-portability.html)

| Applies to | GDPR, CCPA |
| --- | --- |
| Applies to | GDPR, CCPA |

### Warning

This Privacy Guide provides technical guidance on how your developers can choose to configure your Sitecore product implementation to support you with data privacy compliance. This guide does not provide exhaustive guidance, and should not be construed or used as legal advice about the content, interpretation, or application of any law or regulation. 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 how you process personal information. Your resulting implementation is based entirely on your own configuration choices.

The right to data portability concerns the individual’s right to obtain and reuse their personal information. This topic describes how the Sitecore product facilitates the ability to export the individual’s data to a machine-readable format.

## Exporting contact data

Within your Sitecore implementation, you can:

* Use the [xConnect API](/xp/en/developers/93/sitecore-experience-platform/en/xconnect-client-api-overview.html) to export a contact’s data and interaction history to JSON.

The organization is responsible for:

* Implementing an interface or a process that allows individuals to export their contact data.
* Ensuring a user is authorized to access requested data.

## Exporting user data

Within your Sitecore implementation, you can:

* Use the [Security API](http:///legacy-docs/SC75/security-api-cookbook-sc60-and-later-a4.pdf) to access a user’s profile.

The organization is responsible for:

* Converting profile data to JSON or another machine-readable format.
* Implementing an interface or a process that allows individuals to export their user data.
* Ensuring a user is authorized to access requested data.

## Exporting customer data

Within your Sitecore implementation, you can:

* Use the [Commerce Service API](/xp/en/developers/102/sitecore-experience-commerce/en/commerce-service-api.html) to access customer and order data.

The organization is responsible for the following:

* Converting customer information to JavaScript Object Notation (JSON) or another machine-readable format. The final product must have a simple data structure and associative arrays where the information must be language and machine independent.
* Implementing an interface or a process that allows individuals to export their customer data.
* Ensuring a user is authorized to access requested data.

## Exporting form data

By default, form submission data is stored in the [Forms database](forms-database.html). If a form submission is linked to an identifier such as a contact identifier or an email address, you can use SQL to access and export a specific individual’s personal information.

### Important

If you create a custom submit action that stores personal information in a third-party system such as a CRM, you are responsible for ensuring that individuals can access their data in that system.

# [Right to rectification](https://doc.sitecore.com/xp/en/developers/102/platform-administration-and-architecture/right-to-rectification.html)

| Applies to | GDPR |
| --- | --- |
| Applies to | GDPR |

### Warning

This Privacy Guide provides technical guidance on how your developers can choose to configure your Sitecore product implementation to support you with data privacy compliance. This guide does not provide exhaustive guidance, and should not be construed or used as legal advice about the content, interpretation, or application of any law or regulation. 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 how you process personal information. Your resulting implementation is based entirely on your own configuration choices.

The right to rectification concerns the individual’s right to have their data rectified if it is inaccurate or incomplete. This topic describes how to update [contact, user, and customer](entities-that-represent-individuals-in-your-sitecore-implementation.html) data.

Some data is automatically synchronized between entities. For example, if a customer’s first or last name is updated from the BizFX role, that data is copied to the associated contact entity. Refer [Links between individual entities](entities-that-represent-individuals-in-your-sitecore-implementation.html) for more information.

## Updating personal information for a contact

Within your Sitecore implementation, you can:

* Use the [xConnect API](/xp/en/developers/93/sitecore-experience-platform/en/xconnect-client-api-overview.html) to update a contact’s personal information.

The organization is responsible for:

* Implementing a process or an interface that allows individuals to access and update their data.

### Tip

You can [create a custom submit action](/xp/en/developers/102/sitecore-experience-manager/en/walkthrough--creating-a-custom-submit-action.html) for Sitecore Forms that updates a contact’s personal details.

## Updating personal information for a user

Within your Sitecore implementation, you can:

* Use the [Security API](http:///legacy-docs/SC75/security-api-cookbook-sc60-and-later-a4.pdf) to update a user’s personal information.

The organization is responsible for:

* Implementing a process or an interface that allow users to access and update their data.

## Updating personal information for a customer

Within your Sitecore implementation, you can:

* Use the [Commerce Service API](/xp/en/developers/102/sitecore-experience-commerce/en/commerce-service-api.html) to update a customer’s personal information.

The organization is responsible for:

* Implementing a process or an interface that allows customers to access and update their data.

## Updating form data

By default, form submission data is stored in the [Forms database](forms-database.html). If the xDB is enabled, all form submissions are associated with a contact ID. By default, there is no API to update submitted data in the Forms database but you can extend the FormDataProvider to implement a new API that uses SQL to access and update personal information based on Contact Id. You also need to expose a mechanism by which the individual can trigger a query to erase their data, for example, by implementing a custom submit action that updates the contact information.

You can do this in a fashion similar to what is detailed in the topic [Walkthrough: Creating a custom submit action that updates contact details](/xp/en/developers/102/sitecore-experience-manager/en/walkthrough--creating-a-custom-submit-action-that-updates-contact-details.html) except the submit action updates contact information stored in the Forms database instead of updating contact details stored in xConnect.

In CMS-Only mode, form submissions are not associated with a Contact id (the Contact id is NULL). Therefore, if you store email addresses or other personal information that can be used to identify an individual, you can use SQL to access and update a specific individual’s personal information.

### Important

If you create a custom submit action that stores personal information in a third-party system such as a CRM, you are responsible for ensuring that individuals can access their data in that system.

# [Right to be informed](https://doc.sitecore.com/xp/en/developers/102/platform-administration-and-architecture/right-to-be-informed.html)

| Applies to | GDPR, CCPA |
| --- | --- |
| Applies to | GDPR, CCPA |

### Warning

This Privacy Guide provides technical guidance on how your developers can choose to configure your Sitecore product implementation to support you with data privacy compliance. This guide does not provide exhaustive guidance, and should not be construed or used as legal advice about the content, interpretation, or application of any law or regulation. 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 how you process personal information. Your resulting implementation is based entirely on your own configuration choices.

The right to be informed concerns the individual’s right to fair processing of information. In the context of a website, fairness means handling an individual’s personal information in ways that they would reasonably expect. This is typically accomplished through a privacy notice or cookie consent banner. This topic describes how the Sitecore product facilitates adding a privacy notice or cookie consent banner to your website.

For more information about storing and acting on customer consent see:

* [Consent and the right to object](consent-and-the-right-to-object.html)
* [Types of processing](types-of-processing.html)

Within your Sitecore implementation, you can:

* Use the layout engine to implement a custom rendering to display a privacy notice or cookie consent banner on a Sitecore website. You control the rendering logic.
* Customize and extend the basic privacy notice available with [Sitecore Experience Accelerator (SXA)](/xp/en/users/sxa/102/sitecore-experience-accelerator/en/introducing-sitecore-experience-accelerator.html).

The organization is responsible for the following:

* Implementing a privacy notice or cookie consent banner that complies with privacy laws, including active opt-in. This includes websites that use the Federated Experience Manager.

### Note

* Sitecore 10.0 and later provides API calls and configuration options that make it easier to [enforce explicit consent for tracking a contact’s activity on your websites](/xp/en/developers/102/sitecore-experience-platform/en/enable-or-disable-web-tracking-based-on-visitor-consent.html).
* Storing customer [consent choices](consent-and-the-right-to-object.html).
* Acting on an individual’s choice to [opt out of certain processing activities](types-of-processing.html).
* Ensuring that all [processing](types-of-processing.html) - including personalization and tracking - is disabled until [consent](consent-and-the-right-to-object.html) is given.

### Note

If you are creating a form that captures personal information, you can use a [Checkbox element](/xp/en/users/92/sitecore-experience-platform/en/the-basic-elements.html) to request consent for collection and processing of that data. To comply with privacy guidelines, the Field Importance setting for the check box must be set to Mandatory and the Checked setting must be set to No.

# [Right to restrict processing](https://doc.sitecore.com/xp/en/developers/102/platform-administration-and-architecture/right-to-restrict-processing.html)

| Applies to | GDPR |
| --- | --- |
| Applies to | GDPR |

### Warning

This Privacy Guide provides technical guidance on how your developers can choose to configure your Sitecore product implementation to support you with data privacy compliance. This guide does not provide exhaustive guidance, and should not be construed or used as legal advice about the content, interpretation, or application of any law or regulation. 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 how you process personal information. Your resulting implementation is based entirely on your own configuration choices.

The right to restriction of processing concerns the individual’s right to restrict the use of personal information by the controller without necessarily invoking the [right to erasure](right-to-erasure.html). Depending on how your organization chooses to interpret the right to restriction of processing, the Sitecore product offers the following options:

* [Export all personal information](right-to-data-portability.html) for storage in a non-Sitecore database.
* Customize the platform to [disable all forms of processing](types-of-processing.html) for an individual.

# [Right not to be subject to discrimination](https://doc.sitecore.com/xp/en/developers/102/platform-administration-and-architecture/right-not-to-be-subject-to-discrimination.html)

| Applies to | CCPA |
| --- | --- |
| Applies to | CCPA |

### Warning

This Privacy Guide provides technical guidance on how your developers can choose to configure your Sitecore product implementation to support you with data privacy compliance. This guide does not provide exhaustive guidance, and should not be construed or used as legal advice about the content, interpretation, or application of any law or regulation. 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 how you process personal information. Your resulting implementation is based entirely on your own configuration choices.

The right to not be subject to discrimination directs certain California Businesses to avoid denying goods or services, charge individuals a different price, or provide a different level or quality of goods or services just because an individual exercised their rights.

Your management approach and workflow for subject rights requests determines how you apply access rights to request history. If you choose to store these requests in a Sitecore Contact record, you can extend the xDB data model to do so; however, you are responsible for applying a governance model that restricts access to view this data.

# [Right to object or opt-out of selling of personal information](https://doc.sitecore.com/xp/en/developers/102/platform-administration-and-architecture/right-to-object-or-opt-out-of-selling-of-personal-information.html)

| Applies to | CCPA |
| --- | --- |
| Applies to | CCPA |

### Warning

This Privacy Guide provides technical guidance on how your developers can choose to configure your Sitecore product implementation to support you with data privacy compliance. This guide does not provide exhaustive guidance, and should not be construed or used as legal advice about the content, interpretation, or application of any law or regulation. 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 how you process personal information. Your resulting implementation is based entirely on your own configuration choices.

The right to object or opt-out of selling personal information gives Individuals the ability to direct a Business not to sell their personal information to a third party. This provision does not stop a Business from distributing the data within the organization that collected it (even to different business units). It also does not stop all transfers to third parties as businesses can continue to provide personal information to their Service Providers pursuant to a written contract that meets the law’s requirements. Further, they can continue to provide data that does not meet the definition of personal information. Businesses must wait at least 12 months before asking consumers to opt back in.

Sitecore XP is a framework that lets you build websites using any front-end technologies that fulfill your requirements. Using the desired web technology and the Sitecore Content Editor, you can define and manage privacy policies, as content, and present these to the end customer as part of your solution. Sitecore recommends capturing and storing your end-customer’s affirmative action and consent choices in the 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™.

### Note

To protect the confidentiality, integrity, and availability of personal information, Sitecore Content Hub takes important security measures associated with [user activity monitoring](https://docs.stylelabs.com/content/3.4.x/integrations/security/personal-data.html?q=UAM) (UAM). UAM is the monitoring and recording of user actions. UAM captures user actions and is recorded in User logs. The User logs document all activities by users. The User logs match up with a playback of concurrent actions or events of all the users.

# [Profiling and automated decision-making](https://doc.sitecore.com/xp/en/developers/102/platform-administration-and-architecture/profiling-and-automated-decision-making.html)

| Applies to | GDPR |
| --- | --- |
| Applies to | GDPR |

### Warning

This Privacy Guide provides technical guidance on how your developers can choose to configure your Sitecore product implementation to support you with data privacy compliance. This guide does not provide exhaustive guidance, and should not be construed or used as legal advice about the content, interpretation, or application of any law or regulation. 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 how you process personal information. Your resulting implementation is based entirely on your own configuration choices.

The following features can use data such as IP address or past behavior to determine content that is presented to an individual. For example, an individual’s IP address might be used to personalize the offers that are included in a marketing email message. Make sure individuals are aware of and have actively consented to automated decision-making based on their personal information.

| Feature | Description |
| --- | --- |
| [Personalization](tracking-and-personalization.html) | Personalized components can show different content depending on an individual’s behavior or data that has been collected about the individuals, such as location. Email messages can also be personalized.Sitecore 9.1 and later uses the Sitecore Cortex™ Processing Engine to [suggest personalization rules](/xp/en/users/102/sitecore-experience-platform/en/personalization-suggestions.html) based on data gathered during component testing. |
| [Automation](marketing-automation.html) | Automation plans can contain conditional activities that make decisions about an individual’s progress through a plan based on behavior or data collected about the individuals. Automation plans can be customized to exclude individuals who do not want to be enrolled, and plans can be extended with conditional activities that use a default path for individuals who have opted out of personalized automation. |
| [Segmentation](indexing-and-segmentation.html) | The segmentation engine can be used to organize contacts into lists based on behavior or data collected about the contact. The List Manager uses the segmentation engine to build mailing lists for the Email Experience Manager. Segmentation conditions can be customized to exclude individuals that have opted out of personalized email messages. |
| [Content Testing](/xp/en/users/102/sitecore-experience-platform/en/experience-optimization.html) | Content testing might result in visitors to your website seeing different variations of the same content. Variations are randomly assigned, but persist across multiple sessions and might affect a visitor’s behavior on your website. Emails can also contain content tests.Sitecore 9.1 and later uses the Sitecore Cortex™ Processing Engine to [suggest personalization rules](/xp/en/users/102/sitecore-experience-platform/en/personalization-suggestions.html) based on data gathered during component testing. |
| [Sitecore Cortex™ Processing Engine](/xp/en/developers/91/platform-administration-and-architecture/en/sitecore-cortex-processing-engine.html) | You can use the Sitecore Cortex Processing Engine to integrate with external machine learning platforms. |

See [Types of processing](types-of-processing.html) for a list of all processing activities and options for disabling processing.

# [Types of processing](https://doc.sitecore.com/xp/en/developers/102/platform-administration-and-architecture/types-of-processing.html)

### Warning

This Privacy Guide provides technical guidance on how your developers can choose to configure your Sitecore product implementation to support you with data privacy compliance. This guide does not provide exhaustive guidance, and should not be construed or used as legal advice about the content, interpretation, or application of any law or regulation. 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 how you process personal information. Your resulting implementation is based entirely on your own configuration choices.

This topic lists the types of processing that happens in the platform and describes the options for disabling processing for individuals who [opt out](consent-and-the-right-to-object.html) or invoke their [right to restriction of processing](right-to-restrict-processing.html). The following features of the Experience Platform access or handle personal information in the context of marketing activities:

* [Web tracking](tracking-and-personalization.html)
* [Collection](collecting-experience-data.html)
* [Contact processing](processing-and-aggregation.html)
* [Interaction aggregation](processing-and-aggregation.html)
* [Personalization and behavior profiling](tracking-and-personalization.html)
* [Automation processing](marketing-automation.html)
* [Email marketing](email-marketing.html)
* [Content testing](/xp/en/users/102/sitecore-experience-platform/en/experience-optimization.html) (accesses a contact facet during session)

Refer to the [Data flows and processing documentation](data-flows-and-processes.html) for descriptions of all processing activities, including [checkout](checkout.html).

## Disabling processing

Individuals can [opt out](consent-and-the-right-to-object.html) of processing or invoke the [right to restriction of processing](right-to-restrict-processing.html). The Sitecore platform provides the following functionality:

* The Email Experience Manager excludes contacts from email campaigns if any of the following conditions is true:
  + The DoNotMarket property on the ConsentInformation facet is set to true.
  + The ConsentRevoked property on the ConsentInformation facet is set to true.
  + The contact’s email address is on the suppression list.
  + The contact belongs to the global opt-out list.
* Sitecore 10.0 and later provides API calls and configuration options that make it easier to [enforce explicit consent for tracking a contact’s activity on your websites](/xp/en/developers/102/sitecore-experience-platform/en/enable-or-disable-web-tracking-based-on-visitor-consent.html).

The organization is responsible for the following:

* Implementing processes or interfaces that allow customers to opt out of processing. See [Right to object](consent-and-the-right-to-object.html).
* Storing an individual’s consent choices as it relates to processing. See [Right to object](consent-and-the-right-to-object.html).
* Disabling processing for individuals who have revoked consent.

# [Privacy functionality by feature](https://doc.sitecore.com/xp/en/developers/102/platform-administration-and-architecture/privacy-functionality-by-feature.html)

### Warning

This Privacy Guide provides technical guidance on how your developers can choose to configure your Sitecore product implementation to support you with data privacy compliance. This guide does not provide exhaustive guidance, and should not be construed or used as legal advice about the content, interpretation, or application of any law or regulation. 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 how you process personal information. Your resulting implementation is based entirely on your own configuration choices.

The platform includes features that were specifically created to support responsible processing and storage of personal information. Refer to the data rights section for features organized by data right.

## xConnect and data privacy

xConnect provides the following features:

* Allows you to mark contact facets or facet properties that contain personal information as [PIISensitive]. See  [Facets](/xp/en/developers/93/sitecore-experience-platform/en/facets.html) for more information.
  + Facets marked [PIISensitive] are cleared when the [right to erasure](/xp/en/developers/93/sitecore-experience-platform/en/execute-right-to-be-forgotten.html) is executed.
  + By default, facets marked [PIISensitive] are not [indexed by the xConnect Search Indexer](/xp/en/developers/102/sitecore-experience-platform/en/enable-indexing-of-pii-sensitive-data-in-the-xdb-index.html).
* Allows you to clear a contact’s personal information by executing the right to erasure.
* Allows you to [export a contact’s facets and interaction history](/xp/en/developers/93/sitecore-experience-platform/en/export-all-contact-data.html).
* Includes a generic ConsentInformation facet that is set when the right to erasure is executed.

## Web tracking and data privacy

Sitecore 10.0 and later provides API calls and configuration options that make it easier to [enforce explicit consent for tracking a contact’s activity on your websites](/xp/en/developers/102/sitecore-experience-platform/en/enable-or-disable-web-tracking-based-on-visitor-consent.html).

## Email Experience Manager and data privacy

The Email Experience Manager (EXM) provides the following features:

* Extends xConnect with a ClearSupressionListWhenExecutingRightToBeForgotten service plugin. This plugins removes email addresses from the suppression list (where relevant) and executes each time the right to erasure is executed.
* Extends xConnect with a EmailAddressHistory facet that contains every email that a contact has ever used. This facet is marked [PIISensitive], which means that it is cleared when the right to erasure is executed. Events such as EmailEvent have a EmailAddressHistoryEntryId property that matches an ID of an email address in the EmailAddressHistory facet. This ensures that email addresses are never stored as event data, which is not cleared when the right to erasure is executed.
* Includes a [double opt-in process](/xp/en/developers/exm/102/email-experience-manager/en/the-exm-double-opt-in-process.html) that cannot be disabled or changed to single opt-in.
* Includes default campaign templates with the option to [unsubscribe from current or all email campaigns](/xp/en/developers/exm/102/email-experience-manager/en/the-unsubscribe-options.html).
* Respects properties of the ConsentInformation revoked facet. See QueueMessage processor in the [EXM pipelines documentation](/xp/en/developers/exm/102/email-experience-manager/en/the-exm-pipelines.html).

# [Cookies used by Sitecore](https://doc.sitecore.com/xp/en/developers/102/platform-administration-and-architecture/cookies-used-by-sitecore.html)

Sitecore Experience Platform issues cookies to website visitors and client users. The following tables describe the purpose of each cookie and link to configuration options where applicable.

### Note

For a list of the cookies used by the Sitecore Content Hub, see [Cookie usage](https://docs.stylelabs.com/content/3.3.x/user-documentation/administration/security/cookie-usage.html).

## Sitecore visitor cookies

The following cookies can be issued to website visitors:

| Cookie name | Description | Configuration options |
| --- | --- | --- |
| sxa\_site | Functional cookie. Stores the name of the context site. Used by the Sitecore Experience Accellerator for wireframe images.Sample value: docsite |  |
| privacy-notification | Used by the Sitecore Experience Accelerator only. Expiry is set to 1 year.Used by SXA [privacy component](https://doc.sitecore.com/developers/sxa/19/sitecore-experience-accelerator/en/add-a-cookie-warning-message-to-your-site.html).### NoteThe privacy component only sets a cookie - it does not disable tracking or any other forms of processing if consent is revoked. |  |
| sc\_test\_combination | Used by the Experience Optimization feature to store information about the test variant used on the current page. |  |
| SC\_ANALYTICS\_GLOBAL\_COOKIE | Sitecore’s analytics cookie. Stores an ID that represents the device (issued by Sitecore) and a true/false value indicating whether visitor classification was guessed (robot or not robot). Used by the tracker to [identify a returning contact](https://doc.sitecore.com/developers/93/sitecore-experience-platform/en/tracking-contacts.html). Only issued if [tracking is enabled](/xp/en/developers/102/sitecore-experience-platform/en/enable-the-web-analytics-tracking-feature.html).Sample value: 26c532a61c5247719cc8b68b0c41f7e4\|False### NoteCustomization is required to [disable tracking on a per-visitor basis](types-of-processing.html) and prevent Sitecore from creating the cookie. | [Configure cookie lifetime](configure-the-analytics-cookie-lifetime.html) |
| SC\_TRACKING\_CONSENT | Sitecore’s tracking consent cookie. Available in Sitecore 10 and later. | [Enable or disable web tracking based on visitor consent](/xp/en/developers/102/sitecore-experience-platform/en/enable-or-disable-web-tracking-based-on-visitor-consent.html) |
| ASP.NET\_SessionId | The default [ASP.NET session ID cookie](https://docs.microsoft.com/en-us/dotnet/api/system.web.sessionstate.sessionidmanager?view=netframework-4.8). | Configured on the [sessionState element in web.config](https://docs.microsoft.com/en-us/previous-versions/dotnet/netframework-4.0/h6bb9cz9(v=vs.100)?redirectedfrom=MSDN). |
| \_\_RequestVerificationToken | The [default ASP.NET anti-XSRF cookie](https://docs.microsoft.com/en-us/aspnet/mvc/overview/security/xsrfcsrf-prevention-in-aspnet-mvc-and-web-pages). |  |
| {website}#lang | Stores context language of the current site.Sample value: docsite#en |  |

### SXA Storefront cookies

See [Privacy and consent with SXA Storefront](/xp/en/developers/102/sitecore-experience-commerce/en/privacy-and-consent-with-sxa-storefront.html).

## Sitecore client user cookies

The following cookies are issued to users of the Sitecore client interfaces (for example, the Experience Editor):

| Cookie name | Description |
| --- | --- |
| .aspnet.cookies | Authentication cookie. Set for Sitecore client users if you use Sitecore.Owin.Authentication. |
| .aspnet.cookies.preview | Authentication cookie. Set for Sitecore client users in Preview mode if you use Sitecore.Owin.Authentication. |
| sc\_rotated\_simulator\_id | Used by device preview mode. |
| sc\_simulator\_id | Used by device preview mode. |
| sc\_date | Used by Experience Editor for previewing and setting date and time in Editor Mode. |
| sc\_pview\_shuser | Preview Shell User Cookie used when accessing the shell site during preview. |
| sc\_rte\_shuser | RTE Shell User Cookie used to set up Editor. |
| scContentEditorFolders | State of the “Content tree” option (check box), located on the ribbon of Content Editor. |
| scContentEditorFoldersWidth | Width of the content tree panel in the Content Editor. Appears after resizing by a user. |
| lang | Usually refers to Sitecore item’s language or Sitecore client language. |
| fileDownloadToken{...} | Used for the file upload/download interface. For internal use only. |
| messageLanguage | Preserves the selected language for a message. For internal use only. |
| {website}#lang | Sitecore’s client language. |
| {website}#sc\_mode | Used by Experience Editor to indicate Edit, Preview, or Normal mode. |
| {website}#sc\_date | Used by Experience Editor to set or get the value from the Date or DateTime field. |
| {website}#sc\_debug | Used by Experience Editor to indicate Debug mode. |
| {website}#sc\_prof | Used by Experience Editor to enable or disable profiling. |
| {website}#sc\_rb | Used by Experience Editor to enable or disable borders. |
| {website}#sc\_ri | Used by Experience Editor to enable or disable Sitecore Information. |
| {website}#sc\_trace | Used by Experience Editor to enable or disable Sitecore Trace. |
| .ASPXAUTH | Default authentication cookie if you do not use Sitecore.Owin.Authentication. |
| sitecore\_userticket | Sitecore license assumes a limited number of concurrent users (tickets). Sitecore keeps track of every user logged in to the system and assigns a Sitecore user ticket to each. |
| sitecore\_starturl | Start page URL for the Shell site. |
| \_\_CSRFCOOKIE | Protection against cross-site request forgery (CSRF) attacks. |
| sc\_fv | Shockwave Flash version. |
| sc\_last\_page\_mode\_command | Used by Experience Editor to indicate last page mode. |
| experienceeditor\_deviceId | Used by Experience Editor, Cookie for Device Id- |
| sitecore\_floatie\_state | Position preferences of the Floatie form. |
| utcOffset | For internal use only. |