Privacy Notice

BOX ID Platform

BOX ID Systems GmbH

Version 1.0 | Date 14 October 2026

Contents

I Name and Address of the Controller
II Contact Details of the Data Protection Officer
III Data Processing on the BOX ID Platform
IV Rights of Data Subjects
V Provision Hosting and Log Files
VI Registration and User Account
VII Cookies and Similar Technologies
VIII Location and Map Services
IX Error Analysis with Sentry
X Barcode Recognition with STRICH
XI Changelog and Feedback with Canny
XII Usage Analytics with Microsoft Clarity

I Name and Address of the Controller

The controller within the meaning of the General Data Protection Regulation and other applicable data protection legislation is:

BOX ID Systems GmbH

Lichtenbergstraße 8

85748 Garching bei München

Germany

+49 89 219097360

info@box-id.com

https://box-id.com/

II Contact Details of the Data Protection Officer

The controller's Data Protection Officer is:

DataCo GmbH

Sandstraße 33

80335 München

Germany

+49 89 7400 45840

https://www.dataguard.de/

III Data Processing on the BOX ID Platform

Scope

This Privacy Notice applies to the web-based BOX ID Platform, including the administration interface and the Scanpage. The platform provides functions for user accounts, administration, scans, maps and location determination, error analysis, and product information and feedback. Individual functions and service providers can be configured by the respective business customer or tenant.

Where BOX ID Systems GmbH determines the purposes and means of processing, BOX ID Systems GmbH is the controller. Where personal data are processed exclusively on the instructions of a business customer, the business customer is generally the controller and BOX ID Systems GmbH is the processor. The privacy notices of the respective business customer may therefore also apply.

Categories of Personal Data

- Account data such as email address, pseudonymous account ID, organisation affiliation and roles
- Authentication data such as a password or a verification value technically derived from it
- Connection and log data such as IP address, timestamp, browser, operating system and requested path

- Usage and interaction data within the platform
- Scan and location data where the respective function is used
- Feedback content, votes and profile data where Canny is used

Transmission between the end device and the platform is encrypted using HTTPS.

Purposes

- Provision and protection of the platform
- Creation and management of user accounts and permissions
- Provision of activated scan, map and location functions
- Error detection, troubleshooting and improvement of technical stability
- Analysis of usage following valid consent where non-essential analytics tools are used
- Provision of changelogs and handling of product feedback

Legal Bases

Where BOX ID Systems GmbH determines the purposes and means of processing, the following legal bases apply: Platform and account functions necessary for a contract with you, including scanning and necessary map displays, are provided on the basis of Article 6(1)(b) GDPR. Technical logging, error analysis and measures to ensure IT security and stability are based on Article 6(1)(f) GDPR; our legitimate interest is in operating a secure, stable platform protected against abusive access. Changelogs and the structured handling of product feedback are provided on the basis of Article 6(1)(f) GDPR; our legitimate interest is in transparent product communication and developing the platform in line with user needs. Usage analytics that are not technically necessary, optional location determination, and non-essential storage of or access to information on the end device take place only with consent pursuant to Article 6(1)(a) GDPR and section 25(1) of the German Telecommunications Digital Services Data Protection Act (TDDDG). Section 25(2) TDDDG applies to technically necessary storage of or access to information on the end device. Where we process data exclusively on the instructions of a business customer, that customer determines the applicable legal basis.

Deletion

Personal data are deleted or anonymised once the relevant purpose no longer applies and there are no statutory retention obligations or legitimate grounds for further storage. Server, application, security and audit logs are deleted or anonymised after 30 days. Other platform data and backups stored in AWS are deleted within 30 days after the contract ends or the customer initiates deletion. Sentry error events are deleted after 30 days. By way of exception, location history is stored without a defined time limit until deletion is requested by the customer, as described in the sections on HERE and Google location services. The 30-day period for technical logs does not apply to this location history. Further function-specific periods are stated in the sections below. Documents relevant to contracts and billing are stored for the applicable statutory retention period.

IV Rights of Data Subjects

Data subjects may exercise the following rights against BOX ID Systems GmbH in particular:

- Access Under Article 15 GDPR, you may request information about the processing of your personal data and a copy of those data.
- Rectification Under Article 16 GDPR, you may request that inaccurate data be rectified and incomplete data be completed.

- Erasure Under Article 17 GDPR, you may request the erasure of your personal data where the statutory conditions are met.
- Restriction Under Article 18 GDPR, you may request restriction of processing where the statutory conditions are met.
- Data portability Under Article 20 GDPR, you may receive data you have provided in a structured, commonly used and machine-readable format where the statutory conditions are met.
- Objection Under Article 21 GDPR, you may object, on grounds relating to your particular situation, to processing based on Article 6(1)(e) or (f) GDPR. You may object to direct marketing at any time.
- Withdrawal You may withdraw consent at any time with effect for the future. This does not affect the lawfulness of processing carried out before withdrawal.
- Complaint Under Article 77 GDPR, you may lodge a complaint with a data protection supervisory authority.

The competent supervisory authority for private-sector bodies in Bavaria is the Bavarian State Office for Data Protection Supervision (BayLDA), Promenade 18, 91522 Ansbach, Germany. Complaints may also be lodged with any other competent supervisory authority.

https://www.lda.bayern.de/de/beschwerde.html

No decision based solely on automated processing, including profiling, that produces legal effects or similarly significantly affects a person is made.

V Provision Hosting and Log Files

Provision and Logging

Each time the platform is accessed, technically necessary connection and log data are processed. These may include the IP address, date and time of access, requested path, referrer URL where transmitted, browser type and version, operating system, hostname of the accessing device, and the status and size of the server response. This processing enables delivery of the platform, detection of faults and attacks, and secure operation.

Purpose

Provision of the platform, ensuring stability and security, error analysis and prevention of abusive access.

Legal Basis

Article 6(1)(b) GDPR where processing is necessary for a contractual relationship with the data subject. Otherwise, Article 6(1)(f) GDPR applies on the basis of our legitimate interest in operating a secure and functional platform.

Retention Period

Data needed for immediate delivery are generally no longer required once the connection ends. Server, application, security and audit logs are stored for 30 days and then deleted or anonymised.

Objections and Settings

Collection of the data required for provision and security is technically necessary. A separate objection is not possible in this respect. Statutory data subject rights remain unaffected.

Amazon Web Services

We use Amazon Web Services (AWS) to operate the platform and to process and store data. According to the information available, the primary workloads run in the AWS Frankfurt region. The provider for customers in the European Economic Area is generally Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxembourg.

Depending on the platform function, AWS processes account data, email addresses, authentication data, IP addresses, log data and content stored on the platform by business customers in particular. AWS processes these data on our behalf. A data processing agreement is in place with AWS. For potential access or transfers outside the European Economic Area, AWS provides contractual safeguards, including Standard Contractual Clauses.

Purpose

Technical operation, storage, backup, scaling and protection of the BOX ID Platform.

Legal Basis

Article 6(1)(b) and (f) GDPR, depending on the purpose of the respective platform processing.

Retention Period

Personal data in active databases and object storage are retained until deletion by the customer, deactivation or deletion of the relevant account, or the end of the customer contract. Following deletion or termination of the contract, the relevant data, including backups, are deleted or anonymised within 30 days, unless statutory retention obligations prevent this. Log data at AWS are stored for 30 days and then deleted or anonymised. By way of exception, location history is stored without a defined time limit until deletion is requested by the customer; the information in the sections on HERE and Google location services applies. Location history is not subject to the 30-day period for technical logs.

Objections and Settings

Where data are required to perform the contract or to operate the platform securely, there is no separate option to object. Requests for deletion or rectification may be submitted using the contact details above.

AWS Privacy Notice https://aws.amazon.com/privacy/

AWS Data Processing Information https://docs.aws.amazon.com/whitepapers/latest/navigating-gdpr-compliance/aws-data-processing-addendum-dpa.html

VI Registration and User Account

Scope of Processing

Users generally obtain access to an organisation-related account through their company administrator. In particular, email addresses, organisation affiliation, roles and permissions, an internal account ID, authentication data, and login timestamps and technical details are processed. Passwords should be stored only in a technically secured, derived form, not in plain text.

Purpose

Creation, authentication and management of the user account, assignment to a tenant and enforcement of access rights.

Legal Basis

Where the user account is necessary to perform a contract with you, Article 6(1)(b) GDPR is the legal basis.

If you obtain access through a business customer (for example, as an employee), we process your account data exclusively on that customer's instructions as a processor. In this case, the respective business customer is the controller; the legal basis is set out in its privacy notices.

We process data for logging login events and enforcing access rights on the basis of Article 6(1)(f) GDPR. Our legitimate interest is in protecting accounts against unauthorised access and maintaining evidence of security-related events.

Retention Period

Account data are generally stored until the account is deactivated or deleted, or until the customer contract ends. Statutory retention obligations and necessary security records remain unaffected.

Objections and Settings

Account data can be rectified or deleted through the responsible company administrator. Where data are required for the ongoing provision of the account, deletion may result in termination of use.

VII Cookies and Similar Technologies

Technically Necessary Technologies

The platform may use cookies and browser storage, such as Local Storage, to store login sessions, language settings, security attributes and function states. These technologies are necessary where the requested platform function cannot be provided without them.

The legal basis for subsequent processing of personal data is Article 6(1)(b) or (f) GDPR, depending on the function. Storage of or access to information on the end device is permitted under section 25(2) TDDDG where technically necessary.

Analytics Technologies

Analytics technologies that are not technically necessary are used only with consent. The legal basis is Article 6(1)(a) GDPR in conjunction with section 25(1) TDDDG. Consent may be changed or withdrawn at any time through the consent settings with effect for the future.

VIII Location and Map Services

General Information

Depending on the enabled function, the platform processes location information and displays maps. In some cases, a tenant can choose between different providers. Location data, Wi-Fi access point identifiers and the coordinates derived from them may constitute personal data if they can be linked to a person, an end device or a usage event. We therefore treat this information as data requiring protection even if no name is transmitted to the respective service.

When map content is loaded directly in the browser, the end device connects to the respective provider. At least the IP address is transmitted. Depending on the service, browser and device information, referrer, timestamps, map area, coordinates and interaction data may also be transmitted.

HERE Location Services

By default, the platform can use the HERE service to determine a location from Wi-Fi access points detected nearby. Wi-Fi access point identifiers, particularly the BSSID or MAC address, and, depending on the implementation, additional measurements such as signal strength, channel and age of the measurement are transmitted to HERE. HERE returns derived coordinates and an accuracy estimate.

Purpose

Determination of an approximate device location from Wi-Fi signals to provide the activated location function.

Legal Basis

Access to the identifiers of reachable Wi-Fi access points from your end device is based on your consent pursuant to section 25(1) TDDDG. Subsequent processing of location data is based on Article 6(1)(a) GDPR. Consent is voluntary and may be withdrawn at any time with effect for the future through the consent settings; without consent, the location function is unavailable.

If you use the platform through a business customer that has activated the location function, that customer is the controller for the processing. In this case, the legal basis is set out in its privacy notices; we process the data as a processor pursuant to Article 28 GDPR.

Retention Period

BOX ID stores location results supplied by HERE in a temporary cache for 24 hours. Location results are also stored as historical platform data without a defined time limit and are deleted at the customer's request. This location history is not used for subsequent Wi-Fi positioning queries and is separate from the temporary cache and from technical logs with a retention period of 30 days. Storage of request and log data by HERE is governed by the provider's contractual terms and privacy provisions applicable to the service used.

Objections and Settings

The tenant or administrator can deactivate the function or switch to another provider. Without a location service, the corresponding function may be unavailable.

HERE Privacy Notice https://legal.here.com/en-gb/privacy

HERE Data Processing https://legal.here.com/en-gb/data-protection-addendum

Google Cloud Location Services

A tenant can configure the Google Geolocation API as an alternative location service. The API determines a location from Wi-Fi access points and, where applicable, mobile network information. For a Wi-Fi query, the access point's MAC address is a required field. Optional data may include signal strength, channel, signal-to-noise ratio and age of the measurement. If IP-based fallback is enabled, the requesting IP address may also be used to determine the location.

The provider is Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland. Depending on support, subprocessors and technical provision, processing may take place outside the European Economic Area. Google provides contractual data protection provisions and transfer mechanisms for this purpose.

Purpose

Optional determination of a device's location from Wi-Fi signals and, where applicable, mobile network signals.

Legal Basis

Access to the identifiers of reachable Wi-Fi access points from your end device is based on your consent pursuant to section 25(1) TDDDG. Subsequent processing of location data is based on Article 6(1)(a) GDPR. Consent is voluntary and may be withdrawn at any time with effect for the future through the consent settings; without consent, the location function is unavailable.

If you use the platform through a business customer that has activated the location function, that customer is the controller for the processing. In this case, the legal basis is set out in its privacy notices; we process the data as a processor pursuant to Article 28 GDPR.

Retention Period

BOX ID stores location results supplied by Google in a temporary cache for 24 hours. Location results are also stored as historical platform data without a defined time limit and are deleted at the customer's request. This location history is not used for subsequent Wi-Fi positioning queries and is separate from the temporary cache and from technical logs with a retention period of 30 days. Storage of request and log data by Google is governed by the provider's contractual terms and privacy provisions applicable to the service used.

Objections and Settings

The tenant or administrator makes the selection. No Wi-Fi measurement data are transmitted to Google unless the service is activated.

Google Geolocation API https://developers.google.com/maps/documentation/geolocation/requests-geolocation

Google Cloud Data Processing https://cloud.google.com/terms/data-processing-addendum

Google Maps

A tenant can activate Google Maps to display maps in the administration interface. When a map loads, the browser establishes a direct connection to Google. In particular, the IP address, browser and device information, timestamp, referrer, requested map area and usage data are processed. Depending on the configuration, Google may use cookies or comparable technologies.

Purpose

Display of interactive maps in the administration interface.

Legal Basis

Consent pursuant to Article 6(1)(a) GDPR and section 25(1) TDDDG is required for setting or reading non-essential cookies and the associated processing.

Retention Period

Retention by Google is governed by Google's settings and privacy provisions. BOX ID stores map requests only to the extent necessary for the platform function or security logging.

Objections and Settings

Activation is tenant-specific. Required consent can be withdrawn through the consent settings. Without activation or following withdrawal, the Google map cannot be loaded.

Google Privacy Policy https://policies.google.com/privacy?hl=de

Esri ArcGIS Maps

The Scanpage retrieves Esri ArcGIS basemaps to display maps. They are also used for satellite imagery in the administration interface when OpenStreetMap is selected as the map provider. When the browser retrieves content directly, the IP address, browser and device information, timestamp, referrer and requested map tiles, and therefore the displayed map area, are transmitted to the provider in particular. The provider is Environmental Systems Research Institute, Inc. (Esri), 380 New York Street, Redlands, California 92373, USA.

Purpose

Display of basemaps within the Scanpage and satellite imagery in the administration interface when OpenStreetMap is selected as the map provider.

Legal Basis

The map display forms part of the Scanpage and the satellite view in the administration interface described above. Where it is necessary for the function you request, transmission of connection data to Esri is based on Article 6(1)(b) GDPR. Otherwise, we process these data on the basis of Article 6(1)(f) GDPR; our legitimate interest is in providing an understandable spatial presentation of scan results without building our own map database.

If cookies or comparable technologies that are not necessary for the function are used, this takes place only with your consent pursuant to Article 6(1)(a) GDPR and section 25(1) TDDDG. You may withdraw consent at any time with effect for the future through the consent settings.

Transfers to third countries: Esri is based in the USA. The company is certified under the EU-U.S. Data Privacy Framework. Transfers therefore take place on the basis of the European Commission’s adequacy decision (Article 45 GDPR).

Retention Period

BOX ID does not store or cache Esri map tiles. Browser caching is governed by the cache instructions provided by Esri and the browser settings. Where BOX ID generates technically necessary logs of map requests, these are stored for 30 days in accordance with section V and then deleted or anonymised. Storage of access and log data by Esri is governed by the provider’s contractual terms and privacy provisions applicable to the basemap service used.

Objections and Settings

Where the map service is optional, the tenant can deactivate it. Where a map function is technically necessary, use without transmission to the provider may not be possible.

Esri Privacy https://www.esri.com/en-us/privacy/privacy-statements/privacy-statement

Esri Data Processing https://content.esri.com/resources/trustcenter/data_process_addend.pdf

OpenStreetMap Maps

By default, map tiles from OpenStreetMap are loaded in the administration interface. When services of the OpenStreetMap Foundation (OSMF) are accessed directly, the IP address, browser and device type, operating system, referrer, date and time, and requested map resources may be processed. OSMF processes the resulting connection data as an independent controller. There is neither a controller-processor relationship nor a contract between BOX ID and OSMF. Map tiles are delivered through a global network of cache servers. Data may be processed in the United Kingdom, the European Union and, depending on the cache location, other countries.

Purpose

Display of the map in the administration interface.

Legal Basis

We process connection data generated by the integration on the basis of Article 6(1)(f) GDPR. Our legitimate interest is in providing a map view within the platform without building our own map database. Cookies or comparable technologies that are not technically necessary are used only with your consent pursuant to Article 6(1)(a) GDPR and section 25(1) TDDDG.

Transfers to third countries: The OpenStreetMap Foundation is based in the United Kingdom; transfers take place on the basis of the European Commission's adequacy decision for the United Kingdom (Article 45 GDPR). Map tiles are delivered through a network of cache servers, so connection data may also be processed in other countries depending on the server location.

Retention Period

BOX ID generally stores map requests only in technically necessary logs. OSMF describes its own retention and logging practices in its privacy policy.

Objections and Settings

If the map function is optional, the tenant can deactivate it. When the OSM service is used directly, transmission of the IP address cannot be avoided.

OpenStreetMap Foundation Privacy https://osmfoundation.org/wiki/Privacy_Policy

IX Error Analysis with Sentry

Scope of Processing

We use Sentry for automated detection and analysis of errors in the user interface. If an error occurs, the error message, stack trace, requested path, timestamp, browser, operating system, device information, release and environment data, and the technical context of the error may be transmitted. A pseudonymous BOX ID account ID is also transmitted. The IP address is transmitted to and processed by Sentry. Error contexts may inadvertently contain additional personal information if it is not technically filtered out.

The provider is Functional Software Inc. d/b/a Sentry, 45 Fremont Street, 8th Floor, San Francisco, California 94105, USA. Sentry processes customer data as a processor under its data processing agreement. The agreement includes provisions for international transfers, including Standard Contractual Clauses.

Purpose

Detection, analysis and resolution of software errors, and improvement of platform stability and security.

Legal Basis

Article 6(1)(f) GDPR, on the basis of our legitimate interest in operating a secure and stable platform. Sentry is used as a processor pursuant to Article 28 GDPR.

Retention Period

Sentry error events are stored for 30 days and then deleted.

Objections and Settings

Error analysis forms part of secure platform operation. Data subjects may object on grounds relating to their particular situation pursuant to Article 21 GDPR where the statutory conditions are met.

Sentry Data Processing https://sentry.io/legal/dpa/

Sentry Security and Privacy https://docs.sentry.io/security-legal-pii/security/

X Barcode Recognition with STRICH

Scope of Processing

An advanced barcode scanner based on the STRICH SDK can be used in Scanpage v2. Scanning requires access to the end device's camera after permission has been granted by the user. According to the manufacturer, camera images are analysed exclusively locally on the end device and are not transmitted to STRICH. The recognised barcode content is returned to the BOX ID application and processed as part of the selected platform function.

During an online licence check, the SDK transmits the licence key, origin URL, user agent, SDK version and a randomly generated device ID to the licensing service. According to the manufacturer, the IP address transmitted for technical reasons is discarded immediately. Under certain usage-based licensing models, the timestamp, number and type of scans, and an integration identifier may also be transmitted. According to the manufacturer, barcode content is not transmitted to STRICH. A random device ID and a token for licence verification are stored locally in the browser.

STRICH is a product of Pixelverse GmbH.

Purpose

Local recognition of one-dimensional and two-dimensional barcodes, verification of the software licence and, depending on the licensing model, usage billing.

Legal Basis

Where scanning is necessary to perform a contract with you, Article 6(1)(b) GDPR is the legal basis. If you obtain access through a business customer, we process scan data on that customer's instructions as a processor; in this case, the legal basis is set out in its privacy notices. Processing of technical connection data required for licence verification is based on Article 6(1)(f) GDPR. Our legitimate interest is in proper licensing and protection against unauthorised use of the SDK. Camera access takes place only after you grant permission on your device. Local storage of the randomly generated device ID and the licence token is technically necessary for licence verification and takes place pursuant to section 25(2), point 2, TDDDG.

Retention Period

Camera images are not transmitted to STRICH. Following a successful online licence check, the locally stored licence token remains on the end device for a maximum of 48 hours. The randomly generated device ID remains in the browser's Local Storage until you delete the website data or clear the browser storage.

Objections and Settings

Camera access can be revoked in the browser or device settings. Scanning is unavailable without camera access.

STRICH Privacy and Security Statement https://strich.io/docs/STRICH%20-%20SDK%20Privacy%20and%20Security%20Statement%20V2.pdf

XI Changelog and Feedback with Canny

Scope of Processing

We may use Canny to publish changelogs and allow logged-in users to submit and vote on feature requests. Depending on the configuration, Canny processes the following data in particular: full name, email address, profile picture, IP address, an internal user or account ID, browser and operating system, and posts, comments, votes and other voluntarily entered content. Additional data may be transmitted through custom fields where this is explicitly configured.

The provider is Canny Inc., 800 N King Street, Suite 304 1121, Wilmington, Delaware 19801, USA. Canny states that it stores data in the USA and uses AWS and MongoDB, among other services. A data processing agreement is in place. Canny provides Standard Contractual Clauses for transfers to third countries.

Purpose

Information about product changes, collection, handling and prioritisation of feedback, and voting on feature requests.

Legal Basis

Article 6(1)(f) GDPR, on the basis of our legitimate interest in transparent product communication and structured product improvement. Where the function forms part of a contract with the data subject, Article 6(1)(b) GDPR may also apply.

Retention Period

Profile, feedback and voting data are retained for as long as the user account or respective post exists and the data are needed for the stated purposes. Retention for contractual or security reasons remains unaffected.

Objections and Settings

Users can edit or delete posts using the available functions and contact BOX ID or their company administrator for further requests.

Canny Privacy https://canny.io/privacy

Data Collected by Canny https://help.canny.io/en/articles/4299733-what-personal-information-does-canny-collect

Canny GDPR Information https://help.canny.io/en/articles/1876821-is-canny-gdpr-compliant

XII Usage Analytics with Microsoft Clarity

Scope of Processing

We use Microsoft Clarity to understand platform usage through behavioural metrics, heatmaps and session replays, and to identify usability issues. Clarity can capture interactions such as clicks, scrolling, mouse movements, selections, resizing and page changes. It also collects technical diagnostic and performance data, information about the page and the Document Object Model, pseudonymous user, session and page identifiers, browser, device and operating system data, the IP address and approximate location data derived from it.

According to the provider, input fields and drop-down lists are masked. We also configure masking so that confidential content is not transmitted to Clarity. A session replay reconstructs technical changes to the page; it is not a camera video recording.

Where consent has been given, Clarity uses first-party cookies including _clck and _clsk, and may use Microsoft third-party cookies such as CLID, MUID, ANONCHK, MR and SM. The cookies contain pseudonymous identifiers and are used to link page views and sessions. We use Clarity only after valid consent has been obtained and transmit consent status to Clarity. Sharing with Microsoft Advertising is enabled only where separate valid consent and documented approval are in place.

The provider for users in the European Economic Area is Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland. Processing outside the European Economic Area is possible. According to Microsoft, European Commission Standard Contractual Clauses pursuant to Article 46(2)(c) GDPR are in place for transfers from Microsoft Ireland Operations Limited to Microsoft Corporation in the USA.

Purpose

Usage analysis, identification of usability issues, improvement of user navigation and technical optimisation of the platform.

Legal Basis

Article 6(1)(a) GDPR and section 25(1) TDDDG, on the basis of your consent. Consent is voluntary and may be withdrawn at any time with effect for the future.

Retention Period

Microsoft specifies a retention period of 30 days for replay data. Flagged or favourited sessions, click data and heatmap data may be retained for up to 9 months. According to the provider, the data, including backups, are deleted after the respective retention period expires.

Objections and Settings

You may change or withdraw your consent at any time through the consent settings. If consent is withdrawn, Clarity cookies are deleted in accordance with the implemented consent management mechanism and future analysis stops.

Microsoft Clarity Data Collection https://learn.microsoft.com/en-us/clarity/setup-and-installation/clarity-data

Microsoft Clarity Cookies https://learn.microsoft.com/en-us/clarity/setup-and-installation/clarity-cookies

Microsoft Clarity Consent https://learn.microsoft.com/en-us/clarity/setup-and-installation/consent-management

Microsoft Clarity Retention Period https://learn.microsoft.com/en-us/clarity/setup-and-installation/data-retention

Microsoft Privacy Statement https://privacy.microsoft.com/de-de/privacystatement