Datenschutzerklärung

BOX ID Plattform

BOX ID Systems GmbH

Version 1.0 | Stand 14.10.2026

Inhaltsverzeichnis

I Name und Anschrift des Verantwortlichen
II Kontaktdaten des Datenschutzbeauftragten
III Datenverarbeitung auf der BOX ID Plattform
IV Rechte betroffener Personen
V Bereitstellung Hosting und Logfiles
VI Registrierung und Nutzerkonto
VII Cookies und ähnliche Technologien
VIII Standort und Kartendienste
IX Fehleranalyse mit Sentry
X Barcodeerkennung mit STRICH
XI Changelog und Feedback mit Canny
XII Nutzungsanalyse mit Microsoft Clarity

I Name und Anschrift des Verantwortlichen

Verantwortlicher im Sinne der Datenschutz-Grundverordnung und anderer anwendbarer Datenschutzvorschriften ist

BOX ID Systems GmbH

Lichtenbergstraße 8

85748 Garching bei München

Deutschland

+49 89 219097360

info@box-id.com

https://box-id.com/

II Kontaktdaten des Datenschutzbeauftragten

Der Datenschutzbeauftragte des Verantwortlichen ist

DataCo GmbH

Sandstraße 33

80335 München

Deutschland

+49 89 7400 45840

https://www.dataguard.de/

III Datenverarbeitung auf der BOX ID Plattform

Geltungsbereich

Diese Datenschutzerklärung gilt für die webbasierte BOX ID Plattform einschließlich der Administrationsoberfläche und der Scanpage. Die Plattform stellt Funktionen für Benutzerkonten, Administration, Scans, Karten und Standortbestimmung, Fehleranalyse sowie Produktinformationen und Feedback bereit. Einzelne Funktionen und Dienstanbieter können durch den jeweiligen Unternehmenskunden oder Mandanten konfiguriert werden.

Soweit BOX ID Systems GmbH Zwecke und Mittel der Verarbeitung selbst festlegt, ist BOX ID Systems GmbH Verantwortlicher. Soweit personenbezogene Daten ausschließlich nach Weisung eines Unternehmenskunden verarbeitet werden, ist regelmäßig der Unternehmenskunde Verantwortlicher und BOX ID Systems GmbH Auftragsverarbeiter. Die Datenschutzhinweise des jeweiligen Unternehmenskunden können daher zusätzlich gelten.

Kategorien personenbezogener Daten

- Kontodaten wie E-Mail-Adresse, pseudonyme Konto-ID, Organisationszuordnung und Rollen
- Authentifizierungsdaten wie Passwort oder ein daraus technisch abgeleiteter Prüfwert
- Verbindungs- und Protokolldaten wie IP-Adresse, Zeitpunkt, Browser, Betriebssystem und aufgerufener Pfad
- Nutzungs und Interaktionsdaten innerhalb der Plattform

- Scan- und Standortdaten soweit die jeweilige Funktion verwendet wird
- Feedback-Inhalte Abstimmungen und Profildaten soweit Canny verwendet wird

Die Übertragung zwischen Endgerät und Plattform erfolgt verschlüsselt über HTTPS.

Zwecke

- Bereitstellung und Absicherung der Plattform
- Einrichtung und Verwaltung von Benutzerkonten und Berechtigungen
- Erbringung aktivierter Scan-, Karten- und Standortfunktionen
- Fehlererkennung, Fehlerbehebung und Verbesserung der technischen Stabilität
- Analyse der Nutzung nach wirksamer Einwilligung soweit nicht notwendige Analysewerkzeuge eingesetzt werden
- Bereitstellung von Changelogs und Bearbeitung von Produktfeedback

Rechtsgrundlagen

Soweit BOX ID Systems GmbH die Zwecke und Mittel der Verarbeitung selbst bestimmt, gelten folgende Rechtsgrundlagen: Die Bereitstellung der für einen Vertrag mit Ihnen erforderlichen Plattform- und Kontofunktionen einschließlich Scanfunktion und erforderlicher Kartendarstellung erfolgt auf Grundlage von Art. 6 Abs. 1 lit. b DSGVO. Die technische Protokollierung, Fehleranalyse sowie Maßnahmen zur IT-Sicherheit und Stabilität erfolgen auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO; unser berechtigtes Interesse besteht in einem sicheren, stabilen und vor missbräuchlichen Zugriffen geschützten Plattformbetrieb. Die Bereitstellung von Changelogs und die strukturierte Bearbeitung von Produktfeedback erfolgt auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO; unser berechtigtes Interesse besteht in transparenter Produktkommunikation und der bedarfsgerechten Weiterentwicklung der Plattform. Nicht technisch erforderliche Nutzungsanalysen sowie die optionale Standortbestimmung und nicht erforderliche Speicherungen oder Zugriffe auf Informationen im Endgerät erfolgen nur auf Grundlage einer Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO und § 25 Abs. 1 TDDDG. Für technisch erforderliche Speicherungen oder Zugriffe auf Informationen im Endgerät gilt § 25 Abs. 2 TDDDG. Soweit wir ausschließlich nach Weisung eines Unternehmenskunden verarbeiten, bestimmt dieser die einschlägige Rechtsgrundlage.

Löschung

Personenbezogene Daten werden gelöscht oder anonymisiert, sobald der jeweilige Zweck entfällt und keine gesetzlichen Aufbewahrungspflichten oder berechtigten Gründe für eine weitere Speicherung bestehen. Server-, Anwendungs-, Sicherheits- und Auditlogs werden nach 30 Tagen gelöscht oder anonymisiert. Andere in AWS gespeicherte Plattformdaten und Sicherungskopien werden nach Vertragsende oder einer vom Kunden veranlassten Löschung innerhalb von 30 Tagen gelöscht. Sentry-Fehlerereignisse werden nach 30 Tagen gelöscht. Für die Standorthistorie gilt abweichend die in den Abschnitten zur HERE- und Google-Standortbestimmung beschriebene Speicherung ohne festgelegte zeitliche Begrenzung bis zur vom Kunden angeforderten Löschung. Die 30-Tage-Frist für technische Protokolle gilt nicht für diese Standorthistorie. Weitere funktionsbezogene Fristen werden in den nachfolgenden Abschnitten genannt. Vertrags- und abrechnungsrelevante Unterlagen werden für die jeweils geltende gesetzliche Aufbewahrungsfrist gespeichert.

IV Rechte betroffener Personen

Betroffene Personen können gegenüber BOX ID Systems GmbH insbesondere folgende Rechte geltend machen

- **Auskunft** Nach Art. 15 DSGVO können Sie Auskunft über die Verarbeitung Ihrer personenbezogenen Daten und eine Kopie dieser Daten verlangen.
- **Berichtigung** Nach Art. 16 DSGVO können Sie die Berichtigung unrichtiger und die Vervollständigung unvollständiger Daten verlangen.
- **Löschung** Nach Art. 17 DSGVO können Sie unter den gesetzlichen Voraussetzungen die Löschung Ihrer personenbezogenen Daten verlangen.
- **Einschränkung** Nach Art. 18 DSGVO können Sie unter den gesetzlichen Voraussetzungen die Einschränkung der Verarbeitung verlangen.
- **Datenübertragbarkeit** Nach Art. 20 DSGVO können Sie Daten die Sie bereitgestellt haben in einem strukturierten gängigen und maschinenlesbaren Format erhalten sofern die gesetzlichen Voraussetzungen erfüllt sind.
- **Widerspruch** Nach Art. 21 DSGVO können Sie aus Gründen die sich aus Ihrer besonderen Situation ergeben einer Verarbeitung auf Grundlage von Art. 6 Abs. 1 lit. e oder lit. f DSGVO widersprechen. Gegen Direktwerbung können Sie jederzeit widersprechen.
- **Widerruf** Eine erteilte Einwilligung können Sie jederzeit mit Wirkung für die Zukunft widerrufen. Die Rechtmäßigkeit der Verarbeitung bis zum Widerruf bleibt unberührt.
- **Beschwerde** Sie können sich nach Art. 77 DSGVO bei einer Datenschutzaufsichtsbehörde beschweren.

Zuständige Aufsichtsbehörde für nicht öffentliche Stellen in Bayern ist das Bayerische Landesamt für Datenschutzaufsicht (BayLDA), Promenade 18, 91522 Ansbach. Beschwerden können auch bei jeder anderen zuständigen Aufsichtsbehörde eingereicht werden.

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

Eine ausschließlich auf automatisierter Verarbeitung einschließlich Profiling beruhende Entscheidung die rechtliche Wirkung entfaltet oder eine Person ähnlich erheblich beeinträchtigt findet nicht statt.

V Bereitstellung Hosting und Logfiles

Bereitstellung und Protokollierung

Bei jedem Aufruf der Plattform werden technisch erforderliche Verbindungs- und Protokolldaten verarbeitet. Dazu können IP-Adresse, Datum und Uhrzeit des Zugriffs, aufgerufener Pfad, Referrer-URL, sofern übermittelt, Browsertyp, Browserversion, Betriebssystem, Hostname des zugreifenden Geräts sowie Status und Umfang der Serverantwort gehören. Die Verarbeitung ermöglicht die Auslieferung der Plattform, die Erkennung von Störungen und Angriffen sowie die Sicherung des Betriebs.

Zweck

Bereitstellung der Plattform Gewährleistung von Stabilität und Sicherheit Fehleranalyse sowie Abwehr missbräuchlicher Zugriffe.

Rechtsgrundlage

Art. 6 Abs. 1 lit. b DSGVO soweit die Verarbeitung für ein Vertragsverhältnis mit der betroffenen Person erforderlich ist. Im Übrigen Art. 6 Abs. 1 lit. f DSGVO aufgrund unseres berechtigten Interesses an einem sicheren funktionsfähigen Plattformbetrieb.

Speicherdauer

Daten zur unmittelbaren Bereitstellung werden grundsätzlich mit Ende der Verbindung nicht mehr benötigt. Server-, Anwendungs-, Sicherheits- und Auditlogs werden für 30 Tage gespeichert und anschließend gelöscht oder anonymisiert.

Widerspruch und Einstellungen

Die Erfassung der für die Bereitstellung und Sicherheit erforderlichen Daten ist technisch notwendig. Ein gesonderter Widerspruch ist insoweit nicht möglich. Gesetzliche Betroffenenrechte bleiben unberührt.

Amazon Web Services

Für Betrieb Verarbeitung und Speicherung der Plattform nutzen wir Amazon Web Services AWS. Nach den vorliegenden Angaben werden die primären Workloads in der AWS Region Frankfurt betrieben. Anbieter für Kunden im Europäischen Wirtschaftsraum ist regelmäßig Amazon Web Services EMEA SARL 38 Avenue John F Kennedy L 1855 Luxemburg.

Je nach Plattformfunktion verarbeitet AWS insbesondere Kontodaten, E-Mail-Adressen, Authentifizierungsdaten, IP-Adressen, Protokolldaten sowie die von Unternehmenskunden in der Plattform gespeicherten Inhalte. AWS verarbeitet diese Daten in unserem Auftrag. Mit AWS besteht eine Vereinbarung zur Auftragsverarbeitung. Für mögliche Zugriffe oder Übermittlungen außerhalb des Europäischen Wirtschaftsraums sieht AWS vertragliche Schutzmechanismen einschließlich der Standardvertragsklauseln vor.

Zweck

Technischer Betrieb, Speicherung, Datensicherung, Skalierung und Absicherung der BOX ID Plattform.

Rechtsgrundlage

Art. 6 Abs. 1 lit. b und lit. f DSGVO entsprechend dem Zweck der jeweiligen Plattformverarbeitung.

Speicherdauer

Personenbezogene Daten in aktiven Datenbanken und Objektspeichern werden bis zur Löschung durch den Kunden, bis zur Deaktivierung oder Löschung des betreffenden Kontos oder bis zum Ende des Kundenvertrags gespeichert. Nach einer Löschung oder Vertragsbeendigung werden die betroffenen Daten einschließlich Sicherungskopien innerhalb von 30 Tagen gelöscht oder anonymisiert, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Protokolldaten bei AWS werden für 30 Tage gespeichert und anschließend gelöscht oder anonymisiert. Abweichend hiervon wird die Standorthistorie ohne festgelegte zeitliche Begrenzung bis zur vom Kunden angeforderten Löschung gespeichert; hierzu gelten die Angaben in den Abschnitten zur HERE- und Google-Standortbestimmung. Sie ist nicht von der 30-Tage-Frist für technische Protokolle erfasst.

Widerspruch und Einstellungen

Soweit Daten zur Vertragserfüllung oder zum sicheren Plattformbetrieb erforderlich sind besteht keine gesonderte Widerspruchsmöglichkeit. Lösch und Berichtigungsanfragen können über die oben genannten Kontaktwege gestellt werden.

AWS Datenschutzhinweis https://aws.amazon.com/privacy/

AWS Informationen zur Auftragsverarbeitung
https://docs.aws.amazon.com/whitepapers/latest/navigating-gdpr-compliance/aws-data-processing-addendum-dpa.html

VI Registrierung und Nutzerkonto

Umfang der Verarbeitung

Benutzer erhalten regelmäßig über den Administrator ihres Unternehmens Zugang zu einem organisationsbezogenen Konto. Dabei werden insbesondere E-Mail-Adresse, Organisationszuordnung, Rollen und Berechtigungen, eine interne Konto-ID, Authentifizierungsdaten sowie Zeitpunkte und technische Angaben zu Anmeldungen verarbeitet. Ein Passwort sollte ausschließlich in technisch gesicherter, abgeleiteter Form und nicht im Klartext gespeichert werden.

Zweck

Einrichtung Authentifizierung und Verwaltung des Nutzerkontos Zuordnung zu einem Mandanten sowie Durchsetzung von Zugriffsrechten.

Rechtsgrundlage

Soweit das Nutzerkonto zur Erfüllung eines Vertrags mit Ihnen erforderlich ist, ist Art. 6 Abs. 1 lit. b DSGVO die Rechtsgrundlage.

Erhalten Sie Ihren Zugang über einen Unternehmenskunden (z. B. als Beschäftigte oder Beschäftigter), verarbeiten wir Ihre Kontodaten ausschließlich nach dessen Weisung als Auftragsverarbeiter. Verantwortlich ist in diesem Fall der jeweilige Unternehmenskunde; die Rechtsgrundlage richtet sich nach dessen Datenschutzhinweisen.

Für die Protokollierung von Anmeldevorgängen sowie die Durchsetzung von Zugriffsrechten verarbeiten wir Daten auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO. Unser berechtigtes Interesse besteht in der Absicherung der Konten gegen unbefugten Zugriff und dem Nachweis sicherheitsrelevanter Vorgänge.

Speicherdauer

Kontodaten werden grundsätzlich bis zur Deaktivierung oder Löschung des Kontos beziehungsweise bis zum Ende des Kundenvertrags gespeichert. Gesetzliche Aufbewahrungspflichten und erforderliche Sicherheitsnachweise bleiben unberührt.

Widerspruch und Einstellungen

Kontodaten können über den zuständigen Unternehmensadministrator berichtigt oder gelöscht werden. Soweit Daten für die laufende Bereitstellung des Kontos erforderlich sind kann die Löschung zur Beendigung der Nutzung führen.

VII Cookies und ähnliche Technologien

Technisch erforderliche Technologien

Die Plattform kann Cookies sowie Browser Speicher wie Local Storage einsetzen um Anmeldesitzungen Spracheinstellungen Sicherheitsmerkmale und Funktionszustände zu speichern. Diese Technologien sind erforderlich soweit die angeforderte Plattformfunktion ohne sie nicht bereitgestellt werden kann.

Rechtsgrundlage für eine nachfolgende Verarbeitung personenbezogener Daten ist je nach Funktion Art. 6 Abs. 1 lit. b oder lit. f DSGVO. Das Speichern oder Auslesen auf dem Endgerät ist bei technisch erforderlichen Vorgängen nach § 25 Abs. 2 TDDDG zulässig.

Analyse Technologien

Nicht technisch erforderliche Analyse Technologien werden nur nach Einwilligung eingesetzt. Rechtsgrundlage ist Art. 6 Abs. 1 lit. a DSGVO in Verbindung mit § 25 Abs. 1 TDDDG. Die Einwilligung kann jederzeit über die Einwilligungseinstellungen mit Wirkung für die Zukunft geändert oder widerrufen werden.

VIII Standort und Kartendienste

Allgemeine Hinweise

Die Plattform verarbeitet je nach freigeschalteter Funktion Standortinformationen und stellt Karten dar. Ein Mandant kann teilweise zwischen verschiedenen Anbietern wählen. Standortdaten WLAN-Zugangspunktkennungen und die daraus ermittelten Koordinaten können personenbezogen sein wenn sie einer Person einem Endgerät oder einem Nutzungsvorgang zugeordnet werden können. Wir behandeln diese Informationen deshalb als schutzbedürftige Daten auch wenn kein Name an den jeweiligen Dienst übermittelt wird.

Bei direkt im Browser geladenen Karteninhalten stellt das Endgerät eine Verbindung zum jeweiligen Anbieter her. Dabei wird mindestens die IP-Adresse übertragen. Je nach Dienst können Browser- und Geräteinformationen Referrer Zeitstempel Kartenbereich Koordinaten und Interaktionsdaten hinzukommen.

HERE Standortbestimmung

Standardmäßig kann die Plattform den HERE-Dienst zur Bestimmung eines Standorts anhand in der Umgebung erfasster WLAN-Zugangspunkte nutzen. Hierfür werden Kennungen der WLAN-Zugangspunkte, insbesondere BSSID oder MAC-Adresse, und je nach Implementierung weitere Messwerte wie Signalstärke, Kanal und Alter der Messung an HERE übermittelt. HERE gibt daraus abgeleitete Koordinaten und eine Genauigkeitsangabe zurück.

Zweck

Ermittlung eines ungefähren Gerätestandorts aus WLAN Signalen zur Bereitstellung der aktivierten Standortfunktion.

Rechtsgrundlage

Das Auslesen der Kennungen erreichbarer WLAN-Zugangspunkte aus Ihrem Endgerät erfolgt auf Grundlage Ihrer Einwilligung nach § 25 Abs. 1 TDDDG. Die anschließende Verarbeitung der Standortdaten stützen wir auf Art. 6 Abs. 1 lit. a DSGVO. Die Einwilligung ist freiwillig und jederzeit mit Wirkung für die Zukunft über die Einwilligungseinstellungen widerrufbar; ohne Einwilligung steht die Standortfunktion nicht zur Verfügung.

Nutzen Sie die Plattform über einen Unternehmenskunden, der die Standortfunktion aktiviert hat, ist dieser für die Verarbeitung verantwortlich. Die Rechtsgrundlage ergibt sich in diesem Fall aus dessen Datenschutzhinweisen; wir verarbeiten die Daten insoweit als Auftragsverarbeiter nach Art. 28 DSGVO.

Speicherdauer

BOX ID speichert die von HERE gelieferten Standortergebnisse für 24 Stunden in einem temporären Cache. Die Standortergebnisse werden daneben als historische Plattformdaten ohne festgelegte zeitliche Begrenzung gespeichert und auf Anforderung des Kunden gelöscht. Diese Standorthistorie wird nicht für spätere WLAN-Positionsabfragen verwendet und ist von dem

temporären Cache sowie von technischen Protokollen mit einer Aufbewahrungsfrist von 30 Tagen zu unterscheiden. Für die Speicherung von Anfrage- und Protokolldaten durch HERE gelten die für den eingesetzten Dienst maßgeblichen Vertrags- und Datenschutzbestimmungen des Anbieters.

Widerspruch und Einstellungen

Die Funktion kann durch den Mandanten beziehungsweise Administrator deaktiviert oder auf einen anderen Anbieter umgestellt werden. Ohne Standortdienst steht die entsprechende Funktion gegebenenfalls nicht zur Verfügung.

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

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

Google Cloud Standortbestimmung

Ein Mandant kann die Google Geolocation API als alternative Standortbestimmung konfigurieren. Die API ermittelt einen Standort aus WLAN-Zugangspunkten und gegebenenfalls Mobilfunkinformationen. Bei einer WLAN-Abfrage ist die MAC-Adresse des Zugangspunkts ein erforderliches Feld. Optional können insbesondere Signalstärke, Kanal, Signal-Rausch-Verhältnis und Alter der Messung übertragen werden. Wenn die IP-basierte Rückfallfunktion aktiviert ist, kann auch die anfragende IP-Adresse zur Standortbestimmung verwendet werden.

Anbieter ist Google Ireland Limited Gordon House Barrow Street Dublin 4 Irland. Je nach Support Unterauftragnehmern und technischer Bereitstellung kann eine Verarbeitung außerhalb des Europäischen Wirtschaftsraums stattfinden. Google stellt hierfür vertragliche Datenschutzregelungen und Übermittlungsmechanismen bereit.

Zweck

Optionale Ermittlung eines Gerätestandorts aus WLAN und gegebenenfalls Mobilfunksignalen.

Rechtsgrundlage

Das Auslesen der Kennungen erreichbarer WLAN-Zugangspunkte aus Ihrem Endgerät erfolgt auf Grundlage Ihrer Einwilligung nach § 25 Abs. 1 TDDDG. Die anschließende Verarbeitung der Standortdaten stützen wir auf Art. 6 Abs. 1 lit. a DSGVO. Die Einwilligung ist freiwillig und jederzeit mit Wirkung für die Zukunft über die Einwilligungseinstellungen widerrufbar; ohne Einwilligung steht die Standortfunktion nicht zur Verfügung.

Nutzen Sie die Plattform über einen Unternehmenskunden, der die Standortfunktion aktiviert hat, ist dieser für die Verarbeitung verantwortlich. Die Rechtsgrundlage ergibt sich in diesem Fall aus dessen Datenschutzhinweisen; wir verarbeiten die Daten insoweit als Auftragsverarbeiter nach Art. 28 DSGVO.

Speicherdauer

BOX ID speichert die von Google gelieferten Standortergebnisse für 24 Stunden in einem temporären Cache. Die Standortergebnisse werden daneben als historische Plattformdaten ohne festgelegte zeitliche Begrenzung gespeichert und auf Anforderung des Kunden gelöscht. Diese Standorthistorie wird nicht für spätere WLAN-Positionsabfragen verwendet und ist von dem temporären Cache sowie von technischen Protokollen mit einer Aufbewahrungsfrist von 30 Tagen zu unterscheiden. Für die Speicherung von Anfrage- und Protokolldaten durch Google gelten die für den eingesetzten Dienst maßgeblichen Vertrags- und Datenschutzbestimmungen des Anbieters.

Widerspruch und Einstellungen

Die Auswahl erfolgt durch den Mandanten beziehungsweise Administrator. Ohne aktivierten Dienst werden keine WLAN Messdaten an Google übermittelt.

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

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

Google Maps

Ein Mandant kann Google Maps zur Anzeige von Karten in der Administrationsoberfläche aktivieren. Beim Laden der Karte baut der Browser eine direkte Verbindung zu Google auf. Dabei werden insbesondere IP-Adresse, Browser- und Geräteinformationen, Zeitpunkt, Referrer, aufgerufener Kartenbereich und Nutzungsdaten verarbeitet. Google kann je nach Konfiguration Cookies oder vergleichbare Technologien einsetzen.

Zweck

Darstellung interaktiver Karten in der Administrationsoberfläche.

Rechtsgrundlage

Für das Setzen oder Auslesen nicht erforderlicher Cookies und die damit verbundene Verarbeitung ist eine Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO und § 25 Abs. 1 TDDDG erforderlich.

Speicherdauer

Die Speicherdauer bei Google richtet sich nach den Einstellungen und Datenschutzbestimmungen von Google. BOX ID speichert Kartenabrufe nur soweit dies für die Plattformfunktion oder Sicherheitsprotokollierung erforderlich ist.

Widerspruch und Einstellungen

Die Aktivierung erfolgt mandantenbezogen. Erforderliche Einwilligungen können über die Einwilligungseinstellungen widerrufen werden. Ohne Aktivierung oder nach Widerruf kann die Google Karte nicht geladen werden.

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

Esri ArcGIS Karten

In der Scanpage werden Basemaps von Esri ArcGIS zur Kartendarstellung abgerufen. In der Administrationsoberfläche werden diese außerdem für Satellitenbilder genutzt, wenn OpenStreetMap als Kartenanbieter ausgewählt ist. Bei einem direkten Abruf durch den Browser werden insbesondere IP-Adresse, Browser- und Geräteinformationen, Zeitpunkt, Referrer sowie die angeforderten Kartenkacheln und damit der dargestellte Kartenbereich an den Anbieter übertragen. Anbieter ist Environmental Systems Research Institute, Inc. (Esri), 380 New York Street, Redlands, California 92373, USA.

Zweck

Darstellung von Basiskarten innerhalb der Scanpage sowie von Satellitenbildern in der Administrationsoberfläche bei Auswahl von OpenStreetMap als Kartenanbieter.

Rechtsgrundlage

Die Kartendarstellung ist Bestandteil der Scanpage und der genannten Satellitenansicht in der Administrationsoberfläche. Soweit sie für die von Ihnen angeforderte Funktion erforderlich ist, stützen wir die Übermittlung der Verbindungsdaten an Esri auf Art. 6 Abs. 1 lit. b DSGVO. Im Übrigen verarbeiten wir diese Daten auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO; unser berechtigtes Interesse besteht in der verständlichen räumlichen Darstellung der Scanergebnisse ohne Aufbau einer eigenen Kartendatenbank.

Werden dabei Cookies oder vergleichbare Technologien eingesetzt, die für die Funktion nicht erforderlich sind, erfolgt dies nur nach Ihrer Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO und § 25 Abs. 1 TDDDG. Sie können die Einwilligung jederzeit mit Wirkung für die Zukunft über die Einwilligungseinstellungen widerrufen.

Übermittlung in Drittländer: Esri hat seinen Sitz in den USA. Das Unternehmen ist nach dem EU-U.S. Data Privacy Framework zertifiziert. Die Übermittlung erfolgt daher auf Grundlage des Angemessenheitsbeschlusses der Europäischen Kommission (Art. 45 DSGVO).

Speicherdauer

BOX ID speichert oder zwischenspeichert keine Kartenkacheln von Esri. Eine Zwischenspeicherung im Browser richtet sich nach den von Esri übermittelten Cache-Vorgaben und den Browsereinstellungen. Soweit bei BOX ID technisch erforderliche Protokolle zu Kartenabrufen anfallen, werden diese entsprechend Abschnitt V für 30 Tage gespeichert und anschließend gelöscht oder anonymisiert. Für die Speicherung von Zugriffs- und Protokolldaten durch Esri gelten die für den eingesetzten Basemap-Dienst maßgeblichen Vertrags- und Datenschutzbestimmungen des Anbieters.

Widerspruch und Einstellungen

Soweit der Kartendienst optional ist kann er durch den Mandanten deaktiviert werden. Bei einer technisch erforderlichen Kartenfunktion ist die Nutzung ohne Übertragung an den Anbieter gegebenenfalls nicht möglich.

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

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

OpenStreetMap Karten

In der Administrationsoberfläche werden standardmäßig Kartenkacheln aus OpenStreetMap geladen. Bei direktem Abruf von Diensten der OpenStreetMap Foundation (OSMF) können IP-Adresse, Browser- und Gerätetyp, Betriebssystem, Referrer, Datum und Uhrzeit sowie die abgerufenen Kartenressourcen verarbeitet werden. Die OSMF verarbeitet die dabei anfallenden Verbindungsdaten als eigenständig Verantwortliche. Zwischen BOX ID und der OSMF besteht weder ein Auftragsverarbeitungsverhältnis noch ein Vertrag. Kartenkacheln werden über ein globales Netz von Cache-Servern bereitgestellt. Daten können dabei im Vereinigten Königreich, in der Europäischen Union und abhängig vom Cache-Standort in weiteren Ländern verarbeitet werden.

Zweck

Darstellung der Karte in der Administrationsoberfläche.

Rechtsgrundlage

Wir verarbeiten die bei der Einbindung anfallenden Verbindungsdaten auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO. Unser berechtigtes Interesse besteht in der Bereitstellung einer Kartenansicht innerhalb der Plattform ohne Aufbau einer eigenen Kartendatenbank. Werden nicht technisch erforderliche Cookies oder vergleichbare Technologien eingesetzt, erfolgt dies nur nach Ihrer Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO und § 25 Abs. 1 TDDDG.

Übermittlung in Drittländer: Die OpenStreetMap Foundation hat ihren Sitz im Vereinigten Königreich; die Übermittlung erfolgt auf Grundlage des Angemessenheitsbeschlusses der Europäischen Kommission für das Vereinigte Königreich (Art. 45 DSGVO). Die Auslieferung der Kartenkacheln erfolgt über ein Netz von Cache-Servern, sodass Verbindungsdaten je nach Serverstandort auch in weiteren Ländern verarbeitet werden können.

Speicherdauer

BOX ID speichert die reinen Kartenabrufe grundsätzlich nur in technisch erforderlichen Protokollen. Die OSMF beschreibt eigene Aufbewahrungs und Protokollierungspraktiken in ihrer Datenschutzerklärung.

Widerspruch und Einstellungen

Ist die Kartenfunktion optional kann sie durch den Mandanten deaktiviert werden. Bei direkter Nutzung des OSM Dienstes lässt sich die Übertragung der IP-Adresse nicht vermeiden.

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

IX Fehleranalyse mit Sentry

Umfang der Verarbeitung

Zur automatisierten Erkennung und Analyse von Fehlern in der Benutzeroberfläche verwenden wir Sentry. Bei einem Fehler können Fehlermeldung, Stack-Trace, aufgerufener Pfad, Zeitpunkt, Browser, Betriebssystem, Geräteinformationen, Release- und Umgebungsdaten sowie der technische Kontext des Fehlers übertragen werden. Zusätzlich wird eine pseudonyme BOX ID Konto-ID übermittelt. Die IP-Adresse wird an Sentry übertragen und verarbeitet. Fehlerkontexte können unbeabsichtigt weitere personenbezogene Inhalte enthalten, wenn diese nicht technisch herausgefiltert werden.

Anbieter ist Functional Software Inc d/b/a Sentry 45 Fremont Street 8th Floor San Francisco California 94105 USA. Sentry verarbeitet Kundendaten nach seiner Vereinbarung zur Auftragsverarbeitung als Auftragsverarbeiter. Die Vereinbarung enthält Regelungen für internationale Übermittlungen einschließlich Standardvertragsklauseln.

Zweck

Erkennen Analysieren und Beheben von Softwarefehlern sowie Verbesserung von Stabilität und Sicherheit der Plattform.

Rechtsgrundlage

Art. 6 Abs. 1 lit. f DSGVO aufgrund unseres berechtigten Interesses an einem sicheren und stabilen Plattformbetrieb. Sentry wird als Auftragsverarbeiter nach Art. 28 DSGVO eingesetzt.

Speicherdauer

Sentry-Fehlerereignisse werden für 30 Tage gespeichert und anschließend gelöscht.

Widerspruch und Einstellungen

Die Fehleranalyse ist Bestandteil des sicheren Plattformbetriebs. Betroffene Personen können aus Gründen ihrer besonderen Situation nach Art. 21 DSGVO widersprechen soweit die gesetzlichen Voraussetzungen erfüllt sind.

Sentry Auftragsverarbeitung https://sentry.io/legal/dpa/

Sentry Sicherheit und Datenschutz https://docs.sentry.io/security-legal-pii/security/

X Barcodeerkennung mit STRICH

Umfang der Verarbeitung

In der Scanpage v2 kann ein erweiterter Barcode-Scanner auf Grundlage des STRICH SDK eingesetzt werden. Für den Scan ist nach Freigabe durch den Nutzer ein Zugriff auf die Kamera des Endgeräts erforderlich. Die Kamerabilder werden nach Angaben des Herstellers ausschließlich lokal auf dem Endgerät ausgewertet und nicht an STRICH übertragen. Der erkannte Barcode-Inhalt wird an die BOX ID Anwendung zurückgegeben und im Rahmen der jeweils gewählten Plattformfunktion verarbeitet.

Bei einer Online Lizenzprüfung übermittelt das SDK den Lizenzschlüssel, die Herkunfts-URL, den User-Agent, die SDK-Version und eine zufällig erzeugte Geräte-ID an den Lizenzdienst. Die technisch übermittelte IP-Adresse wird nach Herstellerangaben unmittelbar verworfen. Bei bestimmten nutzungsabhängigen Lizenzmodellen können zusätzlich Zeitpunkt, Anzahl und Typ der Scans sowie ein Integrationskennzeichen übermittelt werden. Der Barcode Inhalt wird nach Herstellerangaben nicht an STRICH übertragen. Eine zufällige Geräte-ID und ein Token zur Lizenzprüfung werden lokal im Browser gespeichert.

STRICH ist ein Produkt der Pixelverse GmbH.

Zweck

Lokale Erkennung von ein- und zweidimensionalen Barcodes sowie Prüfung der Softwarelizenz und je nach Lizenzmodell Abrechnung der Nutzung.

Rechtsgrundlage

Soweit die Scanfunktion zur Erfüllung eines Vertrags mit Ihnen erforderlich ist, ist Art. 6 Abs. 1 lit. b DSGVO die Rechtsgrundlage. Erhalten Sie Ihren Zugang über einen Unternehmenskunden, verarbeiten wir die Scandaten nach dessen Weisung als Auftragsverarbeiter; die Rechtsgrundlage richtet sich in diesem Fall nach dessen Datenschutzhinweisen. Für die zur Lizenzprüfung erforderliche Verarbeitung technischer Verbindungsdaten stützen wir uns auf Art. 6 Abs. 1 lit. f DSGVO. Unser berechtigtes Interesse besteht in der ordnungsgemäßen Lizenzierung und dem Schutz vor unberechtigter Nutzung des SDK. Der Kamerazugriff erfolgt erst nach Ihrer Gerätefreigabe. Die lokale Speicherung der zufällig erzeugten Geräte-ID und des Lizenz-Tokens ist für die Lizenzprüfung technisch erforderlich und erfolgt nach § 25 Abs. 2 Nr. 2 TDDDG.

Speicherdauer

Kamerabilder werden nicht an STRICH übertragen. Das lokal gespeicherte Lizenz-Token bleibt nach einer erfolgreichen Online-Lizenzprüfung für höchstens 48 Stunden auf dem Endgerät gespeichert. Die zufällig erzeugte Geräte-ID bleibt im lokalen Speicher des Browsers (Local Storage) gespeichert, bis Sie die Website-Daten beziehungsweise den Browser-Speicher löschen.

Widerspruch und Einstellungen

Der Kamerazugriff kann in den Browser oder Geräteeinstellungen entzogen werden. Ohne Kamerazugriff steht die Scanfunktion nicht zur Verfügung.

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

XI Changelog und Feedback mit Canny

Umfang der Verarbeitung

Wir können Canny verwenden, um Changelogs zu veröffentlichen und angemeldeten Nutzern das Einreichen und Bewerten von Funktionswünschen zu ermöglichen. Abhängig von der Konfiguration verarbeitet Canny insbesondere folgende Daten: vollständiger Name, E-Mail-Adresse, Profilbild, IP-Adresse, eine interne Nutzer- oder Konto-ID, Browser und Betriebssystem sowie Beiträge, Kommentare, Abstimmungen und sonstige freiwillig eingegebene Inhalte. Über benutzerdefinierte Felder können weitere Daten übertragen werden, wenn dies ausdrücklich konfiguriert wird.

Anbieter ist Canny Inc 800 N King Street Suite 304 1121 Wilmington Delaware 19801 USA. Canny gibt an Daten in den USA zu speichern und unter anderem AWS und MongoDB einzusetzen. Es besteht eine Vereinbarung zur Auftragsverarbeitung. Canny stellt Standardvertragsklauseln für Übermittlungen in Drittländer bereit.

Zweck

Information über Produktänderungen Sammlung Bearbeitung und Priorisierung von Feedback sowie Abstimmung über Funktionswünsche.

Rechtsgrundlage

Art. 6 Abs. 1 lit. f DSGVO aufgrund unseres berechtigten Interesses an transparenter Produktkommunikation und strukturierter Produktverbesserung. Soweit die Funktion Teil eines Vertrags mit der betroffenen Person ist kann zusätzlich Art. 6 Abs. 1 lit. b DSGVO gelten.

Speicherdauer

Profil Feedback und Abstimmungsdaten werden gespeichert solange das Nutzerkonto oder der jeweilige Beitrag besteht und die Daten für die genannten Zwecke benötigt werden. Vertrags und sicherheitsbedingte Aufbewahrungen bleiben unberührt.

Widerspruch und Einstellungen

Nutzer können Beiträge im Rahmen der verfügbaren Funktionen bearbeiten oder löschen und sich für weitergehende Anfragen an BOX ID oder ihren Unternehmensadministrator wenden.

Canny Datenschutz https://canny.io/privacy

Canny erhobene Daten https://help.canny.io/en/articles/4299733-what-personal-information-does-canny-collect

Canny DSGVO Informationen https://help.canny.io/en/articles/1876821-is-canny-gdpr-compliant

XII Nutzungsanalyse mit Microsoft Clarity

Umfang der Verarbeitung

Wir verwenden Microsoft Clarity, um die Nutzung der Plattform anhand von Verhaltensmetriken, Heatmaps und Sitzungswiedergaben zu verstehen und Bedienungsprobleme zu erkennen. Clarity kann Interaktionen wie Klicks, Scrollbewegungen, Mausbewegungen, Auswahlhandlungen, Größenänderungen und Seitenwechsel erfassen. Hinzu kommen technische Diagnose- und Leistungsdaten, Informationen zur Seite und zum Document Object Model sowie pseudonyme Nutzer-, Sitzungs- und Seitenkennungen, Browser-, Geräte- und Betriebssystemdaten, IP-Adresse und daraus abgeleitete ungefähre Standortdaten.

Eingabefelder und Auswahllisten werden nach Herstellerangaben maskiert. Darüber hinaus konfigurieren wir die Maskierung so dass vertrauliche Inhalte nicht an Clarity übertragen werden. Eine Sitzungswiedergabe bildet technische Änderungen der Seite nach und ist keine Videoaufnahme durch die Kamera.

Clarity verwendet bei erteilter Einwilligung unter anderem die First-Party-Cookies _clck und _clsk sowie mögliche Microsoft Third-Party-Cookies wie CLID, MUID, ANONCHK, MR und SM. Die Cookies enthalten pseudonyme Kennungen und dienen der Zuordnung von Seitenaufrufen und Sitzungen. Wir verwenden Clarity erst nach einer wirksamen Einwilligung und übermitteln den Einwilligungsstatus an Clarity. Eine Weitergabe an Microsoft Advertising wird nur aktiviert, wenn hierfür eine gesonderte gültige Einwilligung und eine dokumentierte Freigabe vorliegen.

Anbieter für Nutzer im Europäischen Wirtschaftsraum ist Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland. Eine Verarbeitung außerhalb des Europäischen Wirtschaftsraums ist möglich. Für Übermittlungen von Microsoft Ireland Operations Limited an Microsoft Corporation in den USA bestehen nach Angaben von Microsoft Standardvertragsklauseln der Europäischen Kommission gemäß Art. 46 Abs. 2 lit. c DSGVO.

Zweck

Analyse der Nutzung Erkennung von Bedienungsproblemen Verbesserung der Benutzerführung und technische Optimierung der Plattform.

Rechtsgrundlage

Art. 6 Abs. 1 lit. a DSGVO und § 25 Abs. 1 TDDDG auf Grundlage Ihrer Einwilligung. Die Einwilligung ist freiwillig und kann jederzeit mit Wirkung für die Zukunft widerrufen werden.

Speicherdauer

Microsoft nennt für Wiedergabedaten eine Aufbewahrung von 30 Tagen. Markierte oder favorisierte Sitzungen Klickdaten und Heatmap Daten können bis zu 9 Monate gespeichert werden. Nach Ablauf der jeweiligen Frist werden die Daten einschließlich Sicherungskopien nach Herstellerangaben gelöscht.

Widerspruch und Einstellungen

Sie können Ihre Einwilligung jederzeit über die Einwilligungseinstellungen ändern oder widerrufen. Bei Widerruf werden Clarity Cookies nach der implementierten Einwilligungssteuerung gelöscht und die zukünftige Analyse beendet.

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

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

Microsoft Datenschutzerklärung https://privacy.microsoft.com/de-de/privacystatement