DATENSCHUTZHINWEISE
BESUCHER UND MIETER

FÜR HEUTE. FÜR MORGEN. FÜR MICH.

Nach Art. 12ff. DSGVO auf dem Betriebsgelände Theodor-Heuss-Allee

1. Verantwortlich

Wenn Sie unser Betriebsgelände in der Theodor-Heuss-Allee 20, 28215 Bremen besuchen, verarbeiten wir insbesondere zur Absicherung des Standortes verschiedene personenbezogene Daten. Für die Datenverarbeitung ist die swb AG, Theodor-Heuss-Allee 20, 28215 Bremen verantwortlich. Nachfolgend informieren wir Sie über die Verarbeitungen gemäß Art. 12ff. Datenschutzgrundverordnung (DSGVO).

2. Datenverarbeitung

Wenn Sie sich auf unserem Betriebsgelände aufhalten, erfassen wir personenbezogene Daten, die sich je nach Aufenthaltszweck unterscheiden.

Für Tagesbesucher wird ein Besucherschein ausgefüllt. Dieser enthält Name, Firma, Grund des Besuchs, Datum und Uhrzeiten sowie den Namen der besuchten Person. Der Schein wird von der besuchten Person gegengezeichnet und muss bei Verlassen des Geländes an der Pforte vorgezeigt werden. Die Scheine werden 30 Tage nach dem Besuchstag ordnungsgemäß vernichtet.

In bestimmten Fällen erhalten regelmäßige Besucher (z.B. Dauergäste) sowie Mieter von Liegenschaften oder Räumen auf unserem Gelände Zutritt über mechanische, elektronische oder biometrische Systeme. Die Zugangsberechtigungen werden in den entsprechenden Systemen verwaltet.

Für die biometrische Zutrittskontrolle wird von der berechtigten Person einmalig ein Scan mit 32 relevanten Punkten des Fingers erstellt und als sog. Template (Pseudonym) im System hinterlegt. Ferner werden Stammdaten (Ausweisnummer bzw. FlexID, Rolle/Berechtigung, Vor- und Nachname, Zutrittsberechtigungsprofil und Gültigkeitszeitraum) hinterlegt. Die Person authentifiziert sich auf einem Lesegerät, auf welchem der Fingerabdruck gelesen und mit den 32 Punkten in der Datenbank abgeglichen wird. Die Daten am Lesegerät und die Stammdaten werden 90 Tage nach Ablauf der Zugangsberechtigung vollständig gelöscht.

Die Ausgabe von mechanischen Schlüsseln für bestimmte Personen erfolgt protokolliert. Dabei werden Vor- und Nachname, Schlüsselnummer, Datum der Ausgabe und des Einzugs verarbeitet und 3 Monate nach Abgabe des Schlüssels wieder gelöscht.

In bestimmten Fällen erhalten Personen auch elektronische Schlüssel. Die personenbezogenen Daten werden dann wie folgt verarbeitet:

Daten, die bei der Benutzung der App verarbeitet werden:
Externe/Dienstleister, welche durch einen Bluetooth-Schlüssel Zugang erhalten, nutzen die App-Stores der jeweiligen mobilen Endgeräte Anbieter, z.B. Apple App Store oder Google Play Store.

Nach dem Download der App auf den Smartphones der Nutzer muss die Bluetooth-Funktion eingeschaltet werden. Dem Nutzer wird dies bei der Konfiguration der App angezeigt. Ferner kann der Nutzer auswählen, ob ihm „Mitteilungen“ gesendet werden dürfen. Textmitteilungen können je nach Einstellung im Smartphone zusätzlich durch ein akustisches Signal angekündigt werden. Anschließend erhält der Nutzer eine Lizenzvereinbarung von Assa Abloy für die App, der er zustimmen muss.

Sodann muss der Nutzer in der App ein zugelassenes „CLIQ-Gerät“ hinzufügen. Dies sind die zu verwendenden Bluetooth-Schlüssel oder mobile Programmiergeräte, siehe hierzu die hochgeladene Datei Bedienungsanleitung-Schlüssel-N110-Bluetooth gekürzt.pdf

Der Nutzer erhält über die CLIQ Connect App z.B. einen Überblick über die für ihn hinterlegten Bluetooth-Schlüssel mit System-ID, Schlüssel-ID, dem Batterie-Ladezustand und Versionsstände der Bluetooth Schnittstelle sowie der eigentlichen Firmware des eCLIQ-Schlüssels. Der Nutzer kann hier den „Cache“ (Pufferspeicher) auf dem Gerät (nicht aber im System selbst) bereinigen. Die App selbst fungiert nicht als Schlüssel. Sie dient lediglich der Validierung der Schlüssel (Übertragung von Schließberechtigungen) und zur Übersicht über den Status der Schlüssel. Weitere personenbezogene Daten werden mittels der App nicht verarbeitet. Insbesondere enthält die App keine Namen der Nutzer, keine Personalnummern und auch keine Ereignisdaten über Schließungen/Öffnungen und Fehlversuche an den Schließzylindern. Die Daten auf der App werden gelöscht, sobald die App auf dem Gerät gelöscht wird.

Datenverarbeitungen im elektronischen Schlüssel und an den Zylindern:

Alle durch den Nutzer vorgenommen Steckvorgänge und die damit verbundene Berechtigungsprüfung werden im Zylinder und im Schlüssel gespeichert. Bei jeder Validierung werden die Daten aus dem Schlüssel an das System als Ereignisliste (Steckvorgänge, abgelehnte Schließversuche, Schließzylinder und Schlüssel-ID sowie Datum und Uhrzeit) übertragen. Laufwege der Schlüsselnutzer können somit im geregelten Bedarfsfall über die an ASSA ABLOY angeschlossenen Zylinder rekonstruiert werden. Die im Zylinder gespeicherten Daten können nur über einen speziellen Programmierschlüssel ausgelesen und in das System übertragen werden. Dieser Auslesevorgang muss im Vorfeld durch den zuständigen Betriebsrat freigegeben werden. Die in der Ereignisliste hinterlegten Vorgänge können nur durch einen Administrator eingesehen werden. Alle Abrufe von Ereignislisten von Zylindern werden im System protokolliert.

Ereignislisten werden im System für 366 Tage vorgehalten, um im Bedarfsfall eine optimale Nachvollziehbarkeit der Öffnungen/Steckvorgänge/Fehlversuche zu erreichen. In der Ereignisliste werden hierzu die Namen des Schlüsselinhabers sowie die Schlüssel-ID in der .log Datei nach 366 Tagen gelöscht.

Datenverarbeitung bei der Verwaltung von elektronischen Schlüsseln und Berechtigungen, Administration - Webmanager:

ID (Identity), FirstName (Vorname), Surname (Nachname), MobilePhone (Mobiltelefon), E-Mail, Phone (Telefon), Company (Organisation), Department (Abteilung), Street (Straße), ZipCode (Postleitzahl), Job, City (Ort), Zusatztext (Ansprechpartner bei swb). Die Löschfrist beträgt 3 Monate.

Bei Zutritt von bestimmten Personen prüft der Werkschutz, ob standortspezifische und aktuelle Nachweise für Unterweisungen in ein sicherheits- und umweltgerechtes Verhalten vorliegen. Diese Daten werden auf dem ASIP – Arbeitssicherheitsportal hinterlegt. Nach einer auf dem Webportal online durchgeführten Unterweisung wird ein Zertifikat über die erfolgreiche Teilnahme generiert und hinterlegt. Der Werkschutz kann dieses abrufen und feststellen, ob die Unterweisung vorliegt und aktuell ist. Ist dies der Fall, wird ein entsprechender Betriebsausweis ausgegeben. Der Werkschutz ruft dabei folgende Daten ab: Titel, Vor- und Nachname, Firmenname, geschäftliche Kontaktdaten (E-Mail, Telefon- und Faxnummer), das Zertifikat, den Einsatzort und die Pass-ID (Ausweis-ID) mit Erstellungs- und Ablaufdatum. Alle Daten werden 2 Jahre nach Durchführung der jeweiligen Unterweisung gelöscht.

Bestimmte externe Personen erhalten von uns auch einen Betriebsausweis, welcher der Identifizierung und Zutrittskontrolle, sowie der Freigabe von Druckaufträgen dient. Die Ausweise bestehen aus der I-Card, worauf Name, Vorname und Ausweisnummer abgebildet sind sowie dem integrierten Legic-Chip, worauf die Ausweisnummer, der Kundencode, die Stammdatennummer sowie Schnittstellen zu angeschlossenen Systemen und Berechtigungen hinterlegt sind. An den entsprechenden Lesegeräten werden per RFID-technik Ausweisnummer, Datum und Uhrzeit erfasst und nach 90 Tage gelöscht. Mit Rückgabe des Ausweises wird dieser sowie alle Daten darauf unverzüglich gelöscht. In den jeweils angeschlossenen Systemen werden die Daten der Lieferanten und zutrittsberechtigten Personen grundsätzlich 10 Jahre nach Ende des Vertragsverhältnisses gelöscht.

Bestimmte Personen können auf elektronische Schlüsseltresore (z.B. Kemas Schlüsselschränke) zugreifen und dort Schlüssel entnehmen. Dabei wird mit dem Betriebsausweis das Fach geöffnet und der Name mit der Schließzeit und dem geöffneten Schlüsselfach protokolliert. Die Protokolle werden nach 90 Tagen gelöscht.

Wenn Sie unser Gelände mit einem Fahrzeug befahren, wird das Kennzeichen durch Kameras an den Ein- und Ausfahrten erfasst und mit den reservierten Tickets für eine Zufahrt und den Daten für zugelassene Fahrzeuge und Personen abgeglichen. Dies dient nicht nur der Zutrittskontrolle, sondern auch der Zuweisung und Verwaltung von Parkplätzen. Stammdaten (Firmenname, Vor- und Nachname, dienstliche Telefonnummer, Fahrzeug-Kennzeichnen) sind in unserem System als Berechtigungsticket hinterlegt. Die Telefonnummer wird dabei benötigt, um in Notsituationen (z.B. Falschparker, Beschädigungen) schnellstmöglich informieren zu können. Die Stammdaten werden 7 Tage nach Ablauf der Zufahrtsberechtigung gelöscht. Die Bildaufnahmen der Kennzeichen werden nach 72h nach der Ausfahrt gelöscht.

Unsere Betriebsgelände sind per Video überwacht. Auf dem Gelände sowie an der Peripherie werden Bilddaten von den sich dort aufhaltenden Personen erfasst und auf Monitoren des Sicherheitspersonals aufgeschaltet. Eine Speicherung der Bilddaten findet nicht statt. Die Kameras dienen der Zutrittskontrolle, der Überwachung der Sicherheit von Personen auf dem Gelände, der Durchsetzung unseres Hausrechts, sowie der Verhinderung und Aufklärung von Schadensfällen und Straftaten. Sie haben das Recht, dieser Datenverarbeitung zu widersprechen. Näheres erfahren Sie unter „Ihre Datenschutzrechte“.

3. Rechtsgrundlagen der Datenverarbeitung

Die oben genannten Datenverarbeitungen dienen gemäß Art. 6 Abs. 1 S. 1 lit. f DSGVO der Zutrittskontrolle, der Überwachung der Sicherheit von Personen auf dem Gelände, der Durchsetzung unseres Hausrechts, sowie der Verhinderung und Aufklärung von Schadensfällen und Straftaten. Sie haben das Recht, dieser Datenverarbeitung zu widersprechen. Näheres erfahren Sie unter „Ihre Datenschutzrechte“.

Sofern Sie Mieter von Liegenschaften oder Räumen auf unseren Betriebsgeländen sind, ist die Ausgabe von Schlüsseln ein vertraglicher Bestandteil gemäß Art. 6 Abs. 1 S. 1 lit. b DSGVO.

Die Verarbeitung von biometrischen Daten erfolgt gemäß Art. 9 Abs. 2 DSGVO mit Ihrer freiwilligen Einwilligung. Diese können Sie jederzeit bei uns widerrufen, z.B. per E-Mail an eingangspost_liegenschaften@swb-gruppe.de. Wir stellen Ihnen dann alternative Zugangskontrollsysteme zur Verfügung.

4. Datenempfänger

Wir setzen verschiedene Dienstleister ein, die uns bei den Sicherheitskontrollen und dem Support und Betrieb von IT-Systemen im Rahmen einer Auftragsverarbeitung streng weisungsgebunden unterstützen.

Eine Datenverarbeitung außerhalb der EU findet nicht statt.

5. Ihre Datenschutzrechte

Betroffene Personen haben das Recht auf Auskunft seitens des Verantwortlichen über die sie betreffenden personenbezogenen Daten sowie auf Berichtigung unrichtiger Daten oder auf Löschung, sofern einer der in Art. 17 DSGVO genannten Gründe vorliegt, z.B. wenn die Daten für die verfolgten Zwecke nicht mehr benötigt werden. Es besteht zudem das Recht auf Einschränkung der Verarbeitung, wenn eine der in Art. 18 DSGVO genannten Voraussetzungen vorliegt und in den Fällen des Art. 20 DSGVO das Recht auf Datenübertragbarkeit. Werden Daten auf Grundlage von Art. 6 Abs. 1 S. 1 lit. e

(Datenverarbeitung zur behördlichen Aufgabenerfüllung bzw. zum Schutz des öffentlichen Interesses) oder lit. f DSGVO erhoben (Datenverarbeitung zur Wahrung berechtigter Interessen), steht der betroffenen Person das Recht zu, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung Widerspruch einzu-legen. Wir verarbeiten die personenbezogenen Daten dann nicht mehr, es sei denn, es liegen nachweisbar zwingende schutzwürdige Gründe für die Verarbeitung vor, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. Jede betroffene Person hat das Recht auf Beschwerde bei einer Aufsichtsbehörde, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden Daten gegen datenschutzrechtliche Bestimmungen verstößt. Das Beschwerderecht kann insbesondere bei einer Aufsichtsbehörde in dem Mitgliedstaat des Aufenthaltsorts der betroffenen Person oder des Orts des mutmaßlichen Verstoßes geltend gemacht werden.

6. Hinweis auf ein Widerspruchsrecht nach Art. 21 DSGVO

Werden Daten auf Grundlage von Art. 6 Abs. 1 S. 1 lit. e (Datenverarbeitung zur behörd-lichen Aufgabenerfüllung bzw. zum Schutz des öffentlichen Interesses) oder lit. f DSGVO erhoben (Datenverarbeitung zur Wahrung berechtigter Interessen), steht Ihnen das Recht zu, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung Widerspruch einzulegen. Wir verarbeiten die personenbezogenen Daten dann nicht mehr, es sei denn, es liegen nachweisbar zwingende schutzwürdige Gründe für die Verarbeitung vor, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. Bitte richten Sie den Widerspruch möglichst an: eingangspost_liegenschaften@swb-gruppe.de.

7. Beschwerderecht bei einer Aufsichtsbehörde

Jede betroffene Person hat das Recht auf Beschwerde bei einer Aufsichtsbehörde, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden Daten gegen datenschutzrechtliche Bestimmungen verstößt. Das Beschwerderecht kann insbe-sondere bei einer Aufsichtsbehörde in dem Mitgliedstaat des Aufenthaltsorts der betroffenen Person oder des Orts des mutmaßlichen Verstoßes geltend gemacht werden.

Ihre Datenschutzrechte können Sie hier geltend machen:
Datenschutzbeauftragte der swb AG
Theodor-Heuss-Allee 20
28215 Bremen
T 0421 359-2117
datenschutz@swb-gruppe.de