

Technische und organisatorische Maßnahmen nach Art.32 DSGVO

Bird Home Automation GmbH verpflichtet sich gegenüber dem Kunden zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

Zum Zeitpunkt des Vertragsschlusses bestehender Stand der technischen und organisatorischen Maßnahmen ist in dieser Anlage ersichtlich. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird Bird Home Automation GmbH im Voraus mit dem Kunden abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können von Bird Home Automation GmbH ohne Abstimmung mit dem Kunden umgesetzt werden. Der Kunde kann jederzeit eine aktuelle Fassung der von Bird Home Automation GmbH getroffenen technischen und organisatorischen Maßnahmen anfordern.

Bird Home Automation GmbH wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird Bird Home Automation GmbH den Kunden informieren.

Bird Home Automation GmbH trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

1. Vertraulichkeit

- (1) Zutrittskontrolle: Um den Zutritt Unbefugter zu den Datenverarbeitungsanlagen, mit denen Daten verarbeitet oder genutzt werden, zu verhindern hat Bird Home Automation GmbH umfangreiche formale Zutrittskontrollprozesse implementiert.

Der Standort Uhlandstr. 165 beherbergt neben den Büros der Bird Home Automation GmbH einen Serverraum. Für den Zutritt zu Büroräumen werden an ausgewählte Mitarbeiter elektronische Schlüssel vergeben. Die Schlüssel berechtigen den jeweiligen Mitarbeiter nur zur Öffnung/Schließung einzelner dafür zugelassener Türen. Alle Öffnungs- und Schließvorgänge eines Schlüssels werden gemeinsam mit der eindeutigen ID des Schlüssels elektronisch protokolliert. Für die Verwaltung der Schlüssel sind ausschließlich durch die Geschäftsleitung direkt autorisierte Mitarbeiter zuständig. Der Serverraum ist jederzeit verschlossen und kann nur von ausgewählten Mitarbeitern betreten werden. Innerhalb des Gebäudes sind die Zutrittsrechte der Mitarbeiter – auch solcher die über einen Schlüssel verfügen – auf das zur konkreten Aufgabenerfüllung notwendige Maß beschränkt. Ausgewählte Räume werden videoüberwacht. Innerhalb der Geschäftszeiten wird beim Betreten des Gebäudes am ständig besetzten Empfang des Gebäudes eine Personenkontrolle durchgeführt. Außerhalb der Geschäftszeiten sind alle Zugänge zum Gebäude verschlossen und alarmgesichert. Das Gebäude wird zusätzlich durch einen Wachdienst gesichert. Alle Alarmer der Alarmanlage werden direkt an einen Wachdienst gemeldet. In allen Rechenzentren kommen die standardmäßigen Sicherheitsmaßnahmen zur Anwendung. Diese entsprechen dem Stand der Technik und den best practices der IT-Branche. Es handelt sich unter anderem um elektronische Zugangskontrollsysteme mit Protokollierung, wobei nur autorisierte Personen das Gebäude betreten dürfen, Alarmsysteme, Videoüberwachung Innen/Außen, 24/7 anwesendes Sicherheitspersonal, Alarmanlagen, Sicherung des Gebäudes mit Stacheldraht, Absicherung durch externe Wachdienste, die im Alarmfall über eine dezidierte Alarmleitung automatisch informiert werden.

Die Schlüssel zu den einzelnen Räumen und Cages im Rechenzentrum müssen stets beim Sicherheitspersonal abgeholt werden.

- (2) Zugangskontrolle: Um zu gewährleisten, dass Datenverarbeitungssysteme nur durch berechtigte genutzt werden können setzt Bird Home Automation GmbH zur Verwaltung der Zugangsberechtigungen ein zentrales System ein. Die Zugangsberechtigungen werden durch den technischen Leiter der Bird Home Automation GmbH vergeben. Die Verwaltung dieser Zugangsberechtigungen erfolgt durch autorisierte Administratoren. Ein Fernzugriff auf Server der Bird Home Automation GmbH zu administrativen Zwecken, z.B. zur Wartung der Systeme, ist nur über verschlüsselte Verbindungen und nach vorheriger Authentifizierung möglich.
- (3) Zugriffskontrolle: Um zu gewährleisten, dass die zur Benutzung eines Systems zur Verarbeitung von Daten Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass gespeicherte oder in Verarbeitung befindliche Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, setzt Bird Home Automation GmbH ein zentrales System zur Verwaltung der Zugriffsberechtigungen ein. Alle Zugriffe werden lokal und im zentralen Logserver gespeichert. Administrative Rechte sind nur über ein zentrales Verwaltungsprogramm ausführbar. Der Zugriff auf alle Daten ist bei allen Berechtigten auf das zur konkreten Aufgabenerfüllung notwendige Maß beschränkt. Hierbei werden die gesetzlichen Datenschutzanforderungen, insbesondere solche der Datenschutzgrundverordnung (DSGVO) und des TKG eingehalten.
- (4) Trennung: Bird Home Automation GmbH verarbeitet die Daten auf Serversystemen, die durch ein System logischer und physischer Zugriffskontrollen im Netzwerk logisch getrennt sind.

2. Integrität

- (1) Eingabekontrolle: Um zu gewährleisten, dass Bird Home Automation GmbH nachträglich überprüfen und feststellen kann, ob und von wem Daten in den Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind, werden alle Zugriffe auf die gespeicherten Daten des Kunden lokal und im zentralen Logserver protokolliert.
- (2) Weitergabekontrolle: Um zu gewährleisten, dass Daten bei der elektronischen Übertragung, während des Transportes oder ihrer Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft werden kann, an welchen Stellen die Übertragung von Daten durch Systeme zur Datenübertragung vorgesehen sind, unterliegt der Zugriff auf sämtliche Systeme, die Kundendaten verarbeiten, wirksamen Zugriffskontrollen. Diese Mechanismen zur Zugriffskontrolle sind bereits oben unter 3. näher beschrieben.

3. Verfügbarkeit und Belastbarkeit

- (1) Bird Home Automation GmbH verwendet in allen Systemen eine Kombination aus redundanten Systemen und Backup-Lösungen, um die gespeicherten Daten zu schützen und ggf. wiederherstellen zu können. Diese Systeme werden ausschließlich in nach dem aktuellen Stand der Technik gesicherten und ausgestatteten Räumlichkeiten betrieben, die über die notwendige Klimatisierung, Feuer- und Rauchmeldeanlagen verfügen und für die detaillierte Notfallpläne bestehen.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- (1) Alle Mitarbeiter werden regelmäßig zu Themen des Datenschutzes geschult. Diese Schulungen werden komplett inhouse realisiert, sodass eine genaue Abstimmung auf die bei Bird Home Automation GmbH maßgeblichen Fragen möglich ist. Es werden im Rahmen dieser Schulungen werden auch individuelle Fragen eingehend behandelt.
- (2) Alle Mitarbeiter der Bird Home Automation GmbH, die im Rahmen ihrer Tätigkeit mit der Verarbeitung personenbezogener Daten in Berührung kommen sind auf den vertraulichen Umgang mit personenbezogenen Daten verpflichtet. Dies geschieht regelmäßig bereits bei der Einstellung neuer Mitarbeiter mittels einer vertraglichen Verpflichtungserklärung, die jeder Mitarbeiter abzugeben hat.

- (3) Bird Home Automation GmbH hat einen Beauftragten für den Datenschutz bestellt. Dieser trägt gemeinsam mit seinen Stellvertretern Sorge für die fristgemäße Beantwortung von Anfragen Betroffener.
- (4) Bird Home Automation GmbH unterhält ein Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 und 2 DSGVO. Dieses Verarbeitungsverzeichnis ist nicht öffentlich.