



EASI Control GmbH
Münsterstr. 5 59065 Hamm



02381 4673600



service@easi-control.com



www.easi-control.com

Auftragsverarbeitungsvertrag

Zwischen

Kunde
(nachfolgend „Kunde“)

Und

EASI Control GmbH | Münsterstraße 5 | 59065 Hamm
(nachfolgend „EASI Control“)

Die Parteien schließen diesen Vertrag zur Auftragsverarbeitung (AVV) zum Vertrag über die Nutzung des Systems EASI Control („Nutzungsvereinbarung“).

§ 1 Gegenstand der Verarbeitung & Dauer der Auftragsverarbeitung

Gegenstand und Dauer des Auftrags ergibt sich aus der Nutzungsvereinbarung.

§ 2 Zweck der Verarbeitung

Die Tätigkeit von EASI Control dient folgenden vereinbarten Zwecken:

Organisieren, Durchführen und Auswerten von verschiedenen Arbeitsschutzmaßnahmen wie

- Gefährdungsbeurteilungen
- Unterweisungen
- Gerätemanagement
- Standortmanagement
- Notfallpläne
- Betriebsanweisungen
- Last-Minute-Risikoabfragen
- Unfallmeldungen
- Etc.

§ 3 Kategorien personenbezogener Daten

Folgende Kategorien personenbezogener Daten sind Gegenstand des Auftrags:

- Personalstammdaten
- Nachunternehmerdaten
- Anmeldeinformationen
- Sonstige Daten, die im Zusammenhang mit der Ausführung der Arbeit entstehen, wie z.B. durchgeführte und anstehende Unterweisungen, Vorsorgeuntersuchungen, Unfälle und weiteres

§ 4 Kategorien betroffener Personen

Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst alle Personen, die der Auftraggeber mit EASI Control verwalten möchte. Das kann je nach Nutzung von EASI Control die eigenen Mitarbeiter, aber auch Personen von anderen Unternehmen beinhalten.

§ 5 Allgemeines

Dieser AVV findet auf alle unter der Nutzungsvereinbarung und möglichen individuellen Projektaufträgen stattfindenden Verarbeitungsmaßnahmen personenbezogener Daten durch EASI Control Anwendung.

Der Kunde ist im Rahmen dieser AVV für die Einhaltung der gesetzlichen Bestimmungen über die Rechtmäßigkeit der Offenlegung personenbezogener Daten gegenüber EASI Control sowie für die

Rechtmäßigkeit der Verarbeitung personenbezogener Daten allein verantwortlich.

EASI Control handelt im Rahmen der Verarbeitung personenbezogener Daten ausschließlich weisungsgebunden, es sei denn es liegt ein Ausnahmefall gemäß Art. 28 Abs. 3 lit. a) DSGVO vor. Mündliche Weisungen des Kunden hat er unverzüglich in Textform zu bestätigen. Auf Weisung des Kunden berichtigt oder löscht EASI Control die vertragsgegenständlichen Daten oder schränkt deren Verarbeitung ein (nachfolgend „Sperrung“).

EASI Control informiert den Kunden unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Vorschriften über den Datenschutz oder diese AVV verstößt. EASI Control darf die Umsetzung der Weisung solange aussetzen, bis diese vom Kunden in Textform bestätigt oder abgeändert wurde. Die Ausführung offensichtlich datenschutzrechtswidriger Weisungen darf EASI Control ablehnen.

EASI Control gewährleistet, dass die mit der Verarbeitung personenbezogener Daten beauftragten Personen die Weisungen des Kunden beachten und sich zur Vertraulichkeit verpflichtet haben. Die Vertraulichkeits- und Verschwiegenheitspflicht besteht nach Beendigung der Verarbeitung fort.

§ 6 Technische & organisatorische Maßnahmen

Die Parteien vereinbaren technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO zum angemessenen Schutz der Daten (siehe Datenschutzerklärung „Anlage TOM“).

Im Falle von Änderungen der Anlage TOM darf das vereinbarte Schutzniveau nicht unterschritten wird.

§ 7 Mitteilungspflichten bei Datenschutzverletzungen

EASI Control unterrichtet den Kunden unverzüglich, wenn Verletzungen des Schutzes der von EASI Control verarbeiteten personenbezogenen Daten im Sinne des Art. 4 Nr. 12 DSGVO im Hoheitsbereich von EASI Control bekannt werden bzw. falls ein konkreter Verdacht einer solchen Datenschutzverletzung bei EASI Control besteht.

EASI Control und der Kunde werden unverzüglich die erforderlichen Maßnahmen zur Behebung der Datenschutzverletzung treffen.

§ 8 Drittlandübermittlung

Die Übermittlung von Daten an einen Empfänger in einem anderen Land in der EU oder in einem Drittland außerhalb der EU und des EWR findet nicht statt.

§ 9 Unterauftragsverarbeiter

EASI Control darf die Verarbeitung personenbezogener Daten ganz oder teilweise durch weitere Auftragsverarbeiter erbringen lassen. Unterauftragsverarbeiter von EASI Control sind:

Name, Anschrift	Auftragsinhalt
-----------------	----------------

IONOS SE Elgendorfer Str. 57, 56410 Montabaur	Anbieter der Cloud
--	--------------------

Der Kunde kann der Unterbeauftragung bei Vorliegen eines wichtigen Grundes der Unterbeauftragung in Textform widersprechen. Ein wichtiger Grund liegt insbesondere vor, wenn ein begründeter Anlass zu Zweifeln an der Integrität des Unterauftragsverarbeiters besteht. EASI Control wird mit dem Unterauftragsverarbeiter die in diesem AVV getroffenen Regelungen vereinbaren. Leistungen, die EASI Control als reine Nebenleistung zur Unterstützung der geschäftlichen Tätigkeit außerhalb der Auftragsverarbeitung in Anspruch nimmt sind keine Unterbeauftragung.

EASI Control hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Kunde und EASI Control auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten von EASI Control und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Kunde berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

Der Auftragnehmer informiert den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DSGVO).

§ 10 Betroffenenrechte und Unterstützung des Kunden

Macht eine betroffene Person seine Betroffenenrechte aus der DSGVO bei einer der Parteien geltend, so hat sie die jeweils andere Partei darüber unverzüglich zu informieren. EASI Control unterstützt den Kunden im Rahmen der Möglichkeiten bei der Bearbeitung solcher Anträge sowie bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten.

§ 11 Kontrollrechte des Kunden

Der Kunde überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen von EASI Control. Hierfür kann er z. B. Auskünfte von EASI Control einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen von EASI Control nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zu EASI Control steht. Der Kunde wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe von EASI Control dabei nicht unverhältnismäßig stören.

EASI Control verpflichtet sich, dem Kunden auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen von EASI Control erforderlich sind.

EASI Control stellt dem Kunden auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und

Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

§ 12 Haftung und Schadenersatz

Kunde und EASI Control haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

Die Parteien unterstützen sich wechselseitig bei der Abwehr von Schadenersatzansprüchen betroffener Personen.

§ 13 Laufzeit

Die Laufzeit der AVV orientiert sich an der Laufzeit der Nutzungsvereinbarung.

§ 14 Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags

Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen. Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

§ 15 Schlussbestimmungen

Mündliche Nebenabreden wurden nicht getroffen. Änderungen und Ergänzungen der AVV bedürfen zu ihrer Wirksamkeit der Textform. Dies gilt auch für Änderungen dieser Klausel.

Sollte eine Bestimmung dieser AVV ganz oder teilweise unwirksam sein, bleibt diese AVV im Übrigen unberührt. Anstelle der unwirksamen Bestimmung gilt das Gesetz.

Es gilt deutsches Recht unter Ausschluss des Kollisionsrechts; Art. 3 Abs. 3, Abs. 4 ROM-I-VO bleiben unberührt.

Datenschutzerklärung nach Art. 13 und 21 DSGVO für den Service der EASI Control GmbH

1. Allgemeines

Der Schutz Ihrer personenbezogenen Daten ist für uns, die EASI Control GmbH, von zentraler Bedeutung. Deshalb möchten wir Ihnen umfassende Transparenz bezüglich der Verarbeitung Ihrer Daten bieten. Denn nur, wenn die Verarbeitung für Sie als betroffene Person nachvollziehbar ist, sind sie ausreichend über den Umfang, die Zwecke und den Nutzen der Verarbeitung informiert.

Verantwortlicher im Sinne der Datenschutz-Grundverordnung (DSGVO), des Bundesdatenschutzgesetzes (BDSG) sowie sonstiger datenschutzrechtlicher Vorgaben ist die

EASI Control GmbH
Münsterstraße 5
59065 Hamm
+49 2381 4673600
service@easi-control.com
www.easi-control.com

Im Folgenden „Verantwortlicher“ oder „wir“ genannt.

2. Allgemeine Informationen zur Datenverarbeitung

Wir verarbeiten personenbezogene Daten innerhalb der rechtlich zulässigen Grenzen. Das bedeutet, dass Datenverarbeitungsvorgänge auf einer rechtlichen Grundlage basieren müssen. Diese sind in Art. 6 Abs. 1 DSGVO normiert. Die meisten Datenverarbeitungen basieren auf einem berechtigten Interesse unsererseits (Art. 6 Abs. 1 lit. f DSGVO), auf zur Vertragsdurchführung notwendigen Verarbeitungsvorgängen (Art. 6 Abs. 1 lit. b DSGVO) oder aufgrund einer von Ihnen erteilten Einwilligung (Art. 6 Abs. 1 lit. a DSGVO). In diesen Fällen werden Sie separat auf den Einwilligungsvorgang hingewiesen und erhalten zusätzliche Informationen. Eine Weitergabe personenbezogener Daten findet vorbehaltlich nur in den unten beschriebenen Fällen (siehe Nr. 4.) statt.

Personenbezogene Daten müssen auch für eindeutige Zwecke verarbeitet werden (Art. 5 Abs. 1 lit. b DSGVO). Sobald der Zweck der Verarbeitung wegfällt, werden Ihre personenbezogenen Daten gelöscht oder durch technische sowie organisatorische Maßnahmen geschützt (z.B. durch Pseudonymisierung oder Anonymisierung). Gleiches gilt für den Ablauf einer vorgeschriebenen Speicherfrist, vorbehaltlich der Fälle, in denen eine weitere Speicherung für einen Vertragsabschluss oder Vertragserfüllung notwendig ist.

Darüber hinaus kann sich eine gesetzliche Pflicht zu einer längeren Speicherung oder einer Weitergabe an Dritte (insb. an Strafverfolgungsbehörden) ergeben. In sonstigen Fällen hängt die Speicherdauer und Art der erhobenen Daten sowie die Art der Datenverarbeitung davon ab, welche Funktionen von EASI Control Sie im Einzelfall nutzen. Gerne geben wir Ihnen darüber auch im Einzelfall Auskunft, gemäß Art.

3. Datenverarbeitung im Zusammenhang mit der Nutzung von EASI Control

Durch die Nutzung von EASI Control mit allen ihren Funktionen ist eine Verarbeitung von bestimmten personenbezogenen Daten erforderlich.

3.1 Informatrische Nutzung der Plattform von EASI Control

Das rein informatrische Aufrufen von EASI Control erfordert eine Verarbeitung von folgenden personenbezogenen Daten und Informationen: Browsertyp und Browserversion, verwendetes Betriebssystem, Adresse von zuvor besuchten Internetseiten, Adresse des Endgeräts, mit dem Sie auf EASI Control zugreifen (IP-Adresse) sowie die Uhrzeit des Abrufs von EASI Control. All diese Informationen werden automatisch von Ihrem Browser übermittelt, sollten die diesen nicht derart konfiguriert haben, dass eine Übermittlung der Informationen unterdrückt wird. Dies gilt sowohl für die Nutzer der Webapp, als auch Mobile App.

Diese personenbezogenen Daten werden zum Zwecke der Funktionsfähigkeit und Optimierung von EASI Control, sowie zur Gewährleistung der Sicherheit unserer informationstechnischen Systeme verarbeitet. Diese Zwecke sind zugleich berechtigte Interessen nach Art. 6 Abs. 1 lit. f DSGVO, die Verarbeitung erfolgt somit mit Rechtsgrund.

Die Speicherdauer dieser personenbezogenen Daten beträgt maximal 14 Tage. Diese personenbezogenen Daten werden nicht mit anderen Datenquellen zusammengeführt. Eine Datenweitergabe an Dritte findet ausschließlich in erforderlichen Fällen statt. Eine Übermittlung in Drittstaaten oder an internationale Organisationen ist nicht beabsichtigt oder vorgesehen. Sie findet vorbehaltlich weiterer Bestimmungen der vorliegenden Datenschutzerklärung nicht statt.

3.2 Nutzung nach Registrierung für unsere Software-as-a-Service (SaaS) Anwendung

Über die rein informatrische Nutzung von EASI Control hinaus haben Sie die Möglichkeit, sich für unsere Plattform zu registrieren (siehe Nr. 3.4) und unser gesamtes Angebot zu nutzen.

Diese Nutzung erfordert eine Verarbeitung von folgenden personenbezogenen Daten und Informationen:

- Accountdaten (Name des Administrators und weiterer Benutzer; Unternehmensname, Mailadresse des Administrators und weiterer Benutzer);
- Eingepflegte Daten (sofern diese ausgefüllt werden: Telefonnummern, Mailadressen, Anschrift)
- Nutzungsdaten (ergeben sich aus der Nutzung unserer Funktionen, wie zugeordnete Unterweisungen, Gefährdungsbeurteilungen, Gerätezuständigkeiten, Beauftragungen, Teamzugehörigkeit, (Beinahe-) Unfallmeldungen etc.).
- Nutzungsdaten (Zeitpunkt und Dauer der Nutzung; Ansichten und Bearbeitungsreihenfolge).

Die Nutzung nach erfolgtem Login und die damit verbundenen Datenverarbeitungsvorgänge können von der rein informatrischen Nutzung abweichen. Das Erheben dieser, mit Ihrem Profil in Verbindung stehenden Daten, erfolgt zum Zwecke der Optimierung und zu Zwecken der Gewährleistung der Funktionsfähigkeit unseres Angebots. Dies sind legitime Zwecke nach Art. 6 Abs. 1 lit. f DSGVO. Bei

weiteren Fragen stehen wir Ihnen gerne im Rahmen Ihres Auskunftsrechts nach Art. 15 Abs. 1 DSGVO zur Verfügung.

3.3 Kontaktformular / Kontaktaufnahme per E-Mail

Durch die Nutzung des Kontaktformulars in EASI Control (wie zum Beispiel über den „Kontakt“ oder „Verbesserungs-Anfragen“-Button) oder die Kontaktaufnahme via E-Mail, werden die von Ihnen angegebenen personenbezogenen Daten zunächst verarbeitet und zur weiteren Verarbeitung durch uns zur Verfügung gestellt. Die Speicherung erfolgt nach der Übermittlung in unseren informationstechnischen Systemen. Die Verarbeitung erfolgt zum Zwecke der Beantwortung Ihrer Anfrage. Zur Zuordnung werden zusätzlich das Datum, die Uhrzeit der Kontaktanfrage und Ihre IP-Adresse gespeichert. Dies erfolgt zu Zwecken der Missbrauchsprävention und der Gewährleistung der Sicherheit unserer informationstechnischen Systeme. Diese Zwecke sind berechtigte Interessen im Sinne des Art. 6 Abs. 1 lit. f DSGVO.

Die Speicherung Ihrer personenbezogenen Daten erfolgt grundsätzlich bis zum Abschluss des Verfahrens, das Ihrem Anliegen zugrunde lag. Eine Weitergabe an Dritte erfolgt nicht. Eine Übermittlung in einen Drittstaat oder eine internationale Organisation ist nicht beabsichtigt.

Die Nutzung des Kontaktformulars und die Einspeisung Ihrer Daten sind freiwillig. Bitte beachten Sie jedoch, dass eine Nutzung des Formulars oder eine Bearbeitung Ihrer Anfrage ohne Zurverfügungstellung Ihrer Daten nicht möglich ist.

3.4 Einrichtung und Verwendung eines Nutzerkontos

Sie können ein Nutzerkonto (im Folgenden auch „Profil“) auf unserer Plattform anlegen, um die Plattform EASI Control und Ihre Dienstleistungen in Anspruch zu nehmen. Wenn Sie dies tun, werden die von Ihnen dort angegebenen personenbezogenen Daten durch Ihren Browser an uns übermittelt und in unseren informationstechnischen Systemen gespeichert. Gespeichert werden außerdem Ihre IP-Adresse und Zeitpunkt der Registrierung. Wenn Sie sich in Ihr Profil einloggen, legt EASI Control auf Ihrem Endgerät Cookies ab, um zu ermöglichen, dass Sie eingeloggt bleiben – auch wenn Sie die Website zwischenzeitlich neu laden müssen. Durch das Anlegen des Profils können sie die Funktionen der EASI Control Plattform nutzen.

Die mit dem Anlegen eines Profils zusammenhängenden Verarbeitungsvorgänge dienen dem Zweck, künftige Nutzungsvorgänge zuordnen zu können und das gesamte Angebot der EASI Control Plattform abrufen zu können. Bei der Bestellung etwaiger Ergänzungen und Produkte der Plattform dient die Verarbeitung Ihrer Daten ferner der Vertragsdurchführung, ist somit zweckgebunden und erforderlich gemäß Art. 6 Abs. 1 lit. b DSGVO.

Die Speicherung von IP-Adresse und Zeitpunkt der Registrierung ist erforderlich zur Gewährleistung der Sicherheit unserer informationstechnischen Systeme. Hierin liegt zugleich unser berechtigtes Interesse, weshalb die Verarbeitung auch nach Art. 6 Abs. 1 lit. F DSGVO rechtmäßig ist.

Die Speicherung der von Ihnen eingegebenen personenbezogenen Daten erfolgt bis zum Zeitpunkt der Löschung Ihres Profils bei EASI Control, darüber hinaus nur solange wie die Verarbeitung zu etwaiger Vertragserfüllung erforderlich ist.

Eine Datenweitergabe an Dritte ist nicht beabsichtigt.

4. Auftragsverarbeitung

Teilweise bedienen wir uns zur Verarbeitung Ihrer Daten externer Dienstleister, wie z.B. IONIS SE. Diese Dienstleister wurden von uns sorgfältig ausgewählt und beauftragt. Sie sind an unsere Weisungen gebunden und werden regelmäßig kontrolliert. Dabei entsprechen unsere Auftragsverarbeitungsverträge den strengen Voraussetzungen des Art. 28 DSGVO sowie den Vorgaben der deutschen Datenschutzbehörden.

5. Betroffenenrechte

Die gesetzlichen Datenschutzrechtlichen Bestimmungen gewähren Ihnen als betroffene Person folgende Rechte:

Das Recht auf Auskunft nach Art. 15 DSGVO, das Recht auf Berichtigung Ihrer Daten gemäß Art. 16 DSGVO, das Recht auf Löschung und Vergessenwerden gemäß Art. 17 DSGVO, das Recht auf Einschränkung der Verarbeitung Ihrer Daten gemäß Art. 18 DSGVO und das Recht auf Datenübertragbarkeit gemäß Art. 20 DSGVO. Das Löschungs- sowie das Auskunftsrecht unterliegen den Beschränkungen der §§ 34, 35 BDSG. Ferner steht Ihnen ein Beschwerderecht bei einer Datenschutzbehörde, gemäß Art. 77 DSGVO in Verbindung mit § 19 BDSG, zu. Ihre Betroffenenrechte sind sowohl bei der Nutzung von EASI Control als auch bei der Nutzung der SaaS (siehe Nr. 3.2) gewahrt.

6. Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

Automatisierte Entscheidungen im Einzelfall einschließlich Profiling erfolgen nicht.

7. Mitteilungspflichten des Verantwortlichen

Sollten anderen Empfängern (Dritte) Ihre personenbezogenen Daten mit Rechtsgrund offengelegt worden sein, teilen wir jenen jede Berichtigung, Löschung oder Einschränkung der Verarbeitung Ihrer personenbezogenen Daten mit (Art. 16, Art 17 Abs. 1 und Art. 18 DSGVO). Die Mitteilungspflicht entfällt, wenn sie mit einem unverhältnismäßigen Aufwand verbunden ist oder unmöglich ist. Wir unterrichten Sie ferner auf Verlangen über die Empfänger.

8. Widerspruchsrecht

Aus Art. 21 DSGVO steht Ihnen ein Widerspruchsrecht zu: Das bedeutet, dass Sie jederzeit das Recht haben, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, gegen die Verarbeitung von Sie betreffenden personenbezogenen Daten Widerspruch einzulegen. Die Verarbeitung dieser Daten muss dafür gemäß Art. 6 Abs. 1 lit. e oder f erfolgt sein. Ein besonderer Verarbeitungsgrund muss dann nicht vorliegen, wenn sie gegen die Verarbeitung von Daten widersprechen, die für Direktwerbung genutzt werden. Dies gilt auch für Profiling, soweit es mit Direktwerbung in Verbindung steht.

9. Recht auf Widerruf der Einwilligung in die Verarbeitung der personenbezogenen Daten

Basiert die Verarbeitung Ihrer personenbezogenen Daten auf Ihrer Einwilligung (Art. 6 Abs. 1 lit. a DSGVO) können sie diese jederzeit gemäß Art. 7 Abs. 3 DSGVO widerrufen. Die Verarbeitung ist bis zu Ihrem Widerruf rechtmäßig – der Widerruf wirkt somit erst auf die Verarbeitung nach Zugang Ihres Widerrufs. Sie können den Widerruf formlos per Post oder E-Mail erklären. Die Verarbeitung Ihrer personenbezogenen Daten erfolgt dann nicht mehr, vorbehaltlich der Gestattung durch eine anderweitige gesetzliche Grundlage. Ist dies nicht der Fall, müssen Ihre Daten nach dem Widerruf gemäß Art. 17 Abs. 2 DSGVO unverzüglich gelöscht werden. Ihr Recht, Ihre Einwilligung vorbehaltlich der oben genannten Voraussetzungen zu widerrufen wird gewährleistet.

Ihr Widerruf ist zu richten an:

EASI Control GmbH
Münsterstraße 5
59065 Hamm
service@easi-control.com

Anlage TOM

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

EASI Control nimmt die besondere Verantwortung im Umgang mit den Daten ihrer Kunden sehr ernst. Aus diesem Grund hat EASI Control die erforderlichen technischen und organisatorischen Maßnahmen getroffen, um die Daten nach dem aktuellen Stand der Technik zu schützen.

Diese Dokumentation beschreibt diese technischen und organisatorischen Maßnahmen zur Einhaltung und Umsetzung der Datenschutzanforderungen gemäß Art. 32 DSGVO.

Unterauftragnehmer

EASI Control betreibt keine eigenen Server sondern nutzt für den Serverbetrieb den Unterauftragnehmer IONOS SE. Die Datenverarbeitung erfolgt in Europa und die Datenspeicherung am Serverstandort Frankfurt in deutschen Rechenzentren. IONOS SE garantiert für den Serverbetrieb alle technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO unter anderem in den Bereichen Zutrittskontrollen, Zugangskontrollen, Verfügbarkeit und Belastbarkeit.

IONOS SE ist mehrfach zertifiziert unter anderem für die Bereiche Sicherheitsmanagement, Schutz personenbezogener Daten und Betriebssicherheit. Für eine umfassende Übersicht siehe die Online-Auskunft von IONOS SE.

EASI Control verwendet im Wesentlichen die folgenden Services:

- AMD-Server
- Strato Hosting
- Strato Email
- Strato Domains

Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO) Zugriffskontrolle

Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

EASI Control stellt durch verschiedene Maßnahmen sicher, dass Personen nur entsprechend der ihnen eingeräumten Zugriffsberechtigung auf IT-Systeme und die darauf gespeicherten Daten zugreifen können. Dies wird durch folgende Maßnahmen erreicht:

- Benutzer und ihre Zugriffsrechte werden zentral verwaltet, aktiviert und gesperrt
- Die Verwaltung der Nutzer für die sicherheits- und datenschutzrelevante Systeme ist nur durch Geschäftsführung und einen leitenden Angestellten möglich
- Für den Zugriff auf die verwendeten Systeme werden, sofern technisch möglich, Passwortrichtlinien

inkl. Passwortlänge und –änderungsintervallen vorgegeben

- Ein Datenverarbeitungskonzept für sensible Daten regelt die Plattformen, Dienste und Geräte, die personenbezogene Daten verarbeiten dürfen
- Die Büros von EASI Control über ein elektronisches Schlüsselsystem, welches Zugangsrechte auf Personenebene verwaltet und Zugänge protokolliert
- Jegliche Hardware ist bei Nichtbenutzung gesperrt und mit Passwörtern gemäß den Empfehlungen des Bundesamts für Sicherheit und Informationstechnik geschützt

Trennungskontrolle

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Mit den folgenden Maßnahmen realisiert EASI Control die Trennung der Daten verschiedener Kunden:

- Produktiv- und Testsysteme werden getrennt betrieben.
- Die Daten der Mandanten werden logisch getrennt verarbeitet.

Pseudonymisierung

Sobald keine (gesetzliche oder vertragliche) Notwendigkeit der Aufbewahrung mehr besteht, werden alle personenbezogenen Daten gelöscht und durch Pseudonyme (Codierung) ersetzt.

Integrität (Art. 32 Abs. 1 lit. b DSGVO) Weitergabekontrolle

Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Es werden folgende Maßnahmen zur Sicherung der personenbezogenen Daten bei der elektronischen Übertragung vorgenommen:

- Daten werden ausschließlich verschlüsselt (per SSH-, TLS- oder VPN-Verbindung) übertragen.

Eingabekontrolle

Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Folgende Maßnahmen gewährleisten die Überprüfung und Feststellung, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind:

- Das Löschen von Datensicherungsdateien im Rahmen des Betriebs erfolgt nach der vom Auftraggeber festgelegten Frist.
- Maßnahmen innerhalb der Anwendung, die Lösch- und Sperrfristen umsetzen, sind durch den Auftraggeber im Rahmen der Zusammenarbeit zu beauftragen.

Verfügbarkeit und Belastbarkeit

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Die Verarbeitung personenbezogener Daten erfolgt im Rechenzentrum des Unterauftragnehmers. Der Unterauftragnehmer für den Serverbetrieb im Rechenzentrum ist vertraglich verpflichtet, mindestens mit den folgenden Maßnahmen die Verfügbarkeit sicherzustellen:

- Betrieb einer unterbrechungsfreien Stromversorgung
- Temperatur- Feuchtigkeits- und Klimaüberwachung
- Feuer- und Rauchmeldeanlagen
- Automatische Löschanlagen

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. D DSGVO; Art. 25 Abs. 1 DSGVO)

Datenschutz-Management

Es ist zu gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist. Dazu werden Schulungen der Mitarbeitenden im Thema Datenschutz vorgenommen und die Mitarbeitenden zur Vertraulichkeit verpflichtet.

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Datenschutzfreundliche Voreinstellungen sind sowohl bei den standardisierten Voreinstellungen von Systemen und Apps als auch bei der Einrichtung der Verarbeitungen zu berücksichtigen. In dieser Phase werden Funktionen und Rechte konkret konfiguriert, wird im Hinblick auf Datenminimierung die Zulässigkeit bzw. Unzulässigkeit bestimmter Eingaben oder Eingabemöglichkeiten festgelegt und über die Verfügbarkeit von Nutzungsfunktionen entschieden. Ebenso werden die Art und der Umfang des Personenbezugs bzw. der Anonymisierung (z. B. bei Selektions-, Export- und Auswertungsfunktionen, die festgelegt und voreingestellt oder frei gestaltbar zur Verfügung gestellt werden) oder die Verfügbarkeit bestimmter Verarbeitungen, Funktionen oder Protokollierungen bestimmt.

Schulungen

Alle Mitarbeitenden werden mindestens halbjährlich zu dem Thema Datenschutz geschult. Die Schulung kann in Form von Webinaren, Trainings oder Workshops stattfinden.

Auftragskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Kunden verarbeitet werden können.

Um zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend der Weisungen des Kunden verarbeitet werden, unternimmt EASI Control u.a. die folgenden Maßnahmen:

- Überprüfung vorhandener Zertifizierungen von Unterauftragnehmern (speziell gemäß ISO

9001, ISO 27001 und ISO 27018)

- Abschluss einer Vereinbarung zur Auftragsdatenverarbeitung oder von EU-Standard-Vertragsklauseln
- Überprüfen von sonstigen Dokumentationen und Rechercheergebnissen, die eine Beurteilung der Zuverlässigkeit eines Anbieters ermöglichen
- Kontrolle der Vertragsausführung

Rollenkonzept Einleitung

Dieses Rollenkonzept wird regelmäßig überprüft und Rollenkonflikte werden bei der Rollenzuordnung beachtet. Zudem werden Rollenzuordnungen bei Projekten zeitlich befristet. Grundlegende Regeln dieser Rollenverteilung sind:

- Ausscheidende Mitarbeitende, Altgeräte und zu löschende Anwendungen werden von ihren Rollen getrennt.
- System- und Fachaufgaben bei der Zuweisung von Rollen werden getrennt.
- Rollen werden grundsätzlich immer nach dem Vier-Augen-Prinzip definiert.
- Neue Mitarbeitende werden entsprechend ihrer Rollenzuweisung und Stellenbeschreibung in die Organisation eingeführt. Der Freigabe-Workflow wird laufend überprüft.

Need-to-know Prinzip

Bei EASI Control wird der Daten-Zugriff nach dem Prinzip der Datensparsamkeit und des Datenschutzes nach dem need-to-know Prinzip gestaltet.

Stellenbeschreibung

Mitarbeitende im Bereich Produkt & Prozesse sind für die Entwicklung des Produktes zuständig. Das heißt zum Aufgabenbereich gehören die Zusammenfassung von Anforderungen, Priorisierung von Anforderungen und daraus bedingt die Unterstützung bei der Produktentwicklung.

Mitarbeitende im Bereich IT & Entwicklung sind für die technische Umsetzung der Anforderungen zuständig. Hierzu gehört primär die Softwareentwicklung sowie Datenmanagement und die Bereitstellung des Produktivsystems.

Mitarbeitende im Bereich Marketing & Operatives sind für die Vermarktung des Produktes zuständig. Zudem kümmern sie sich um den operativen Betrieb der Organisation. Dazu gehören insbesondere Kundengespräche, das Beantworten von Support-Anfragen und allgemeines Stakeholder-Management.

Mitarbeitende im Bereich Finanzen & Strategie sind für Einkaufsprozesse und Rechnungsabwicklung sowie Kooperationsthemen zuständig.

Nur Mitarbeitende der Bereiche Produkt & IT haben Zugriff auf Geräte und Anwendungen in denen oder mit denen personenbezogene Daten verarbeitet werden.