Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO

Präambel

Diese Vereinbarung konkretisiert die Verpflichtung der Vertragsparteien zum Datenschutz, die sich aus dem Vertrag in ihren Einzelheiten beschriebenen Beauftragung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers (der Bosch Sicherheitssysteme GmbH) oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten („Daten“) des Auftraggebers (Kunde gemäß Vertrag) in Berührung kommen können.
Dies kann im Zuge von Wartungen, Updates, etc. oder eines eventl. Fernzugriff der Fall sein.

Sollte bereits eine unbefristete Vereinbarung zur Auftragsdaten-Verarbeitung zwischen dem Auftraggeber und Bosch Sicherheitssysteme existieren, dann gilt dies unverändert fort.

1. Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

1.1 Der Gegenstand der Auftragsverarbeitung ist im Vertrag beschrieben. Im Wesentlichen handelt es sich um folgende Aufgaben durch den Auftragnehmer:

- ☒ Software-Reparaturen
- ☒ Software-Updates bzw. Software-Pflege
- ☒ ggf. Software-Anpassungen

1.2 Art und Zweck der Auftragsverarbeitung sind im Vertrag beschrieben und umfassen insbesondere Kontrolle und Anpassungen der Systeme und Workflows für Systeme des Auftraggebers.

1.3 Die Verarbeitung umfasst die nachfolgend genannten Arten von Daten:

Datenart bei Produktsparte Video:

- ☒ Bildaufnahmen von Kunden und Mitarbeitern, Besuchern
- ☒ Personenstammdaten (insb. Name, Kennung, Kennzeichen)
- ☒ Datums-, Zeit- und Zeitraum-Angaben
- ☒ Bewegungsdaten
- ☒ ggf. Kommunikationsdaten

Datenart bei Produktsparte Zeitwirtschaft:

- ☒ ggf. Bildaufnahmen von Kunden und Mitarbeitern
- ☒ Personenstammdaten (insb. Name, Kennung, Kennzeichen)
- ☒ Datums-, Zeit- und Zeitraum-Angaben
- ☒ ggf. Bewegungsdaten
- ☒ ggf. Kommunikationsdaten

Datenart bei Produktsparte Zutrittskontrolle:

- ☒ ggf. Bildaufnahmen von Kunden und Mitarbeitern, Besuchern
- ☒ Personenstammdaten (insb. Name, Kennung, Kennzeichen)
- ☒ Datums-, Zeit- und Zeitraum-Angaben
- ☒ Bewegungsdaten
- ☒ ggf. Kommunikationsdaten

Datenart bei Produktsparte BIS:

- ☒ ggf. Personenstammdaten (insb. Name, Kennung, Kennzeichen)
- ☒ ggf. Datums-, Zeit- und Zeitraum-Angaben
- ☒ ggf. Bewegungsdaten
- ☒ ggf. Kommunikationsdaten

Datenart bei Produktsparte Dienstleistungen, Aufschaltungen sonstige:

- ☒ Personenstammdaten (insb. Name, Kennung, Kennzeichen)

☒ Datums-, Zeit- und Zeitraum-Angaben
☒ ggf. Bewegungsdaten
☒ ggf. Kommunikationsdaten

Datenart bei Produktsparte FSA:
☒ Personenstammdaten (insb. Name, Kennung, Kennzeichen)
☒ Datums-, Zeit- und Zeitraum-Angaben
☒ Bewegungsdaten
☒ ggf. Kommunikationsdaten

Datenart bei Produktsparte Infotainment:
☒ Personenstammdaten (insb. Name, Kennung, Kennzeichen)
☒ Datums-, Zeit- und Zeitraum-Angaben
☒ Bewegungsdaten
☒ ggf. Kommunikationsdaten

Datenart bei Produktsparte Energy Manager:
☒ Personenstammdaten (insb. Name, Kennung, Kennzeichen)
☒ Datums-, Zeit- und Zeitraum-Angaben
☒ ggf. Kommunikationsdaten

1.4 Folgende **Kategorien von Personen** können von der Verarbeitung betroffen sein:

☒ Geschäftsführung, Leitende Ange stellte des Auftraggebers
☒ Beschäftigte aller Art des Auftraggebers
☒ Kunden des Auftraggebers
☒ ggf. Lieferanten des Auftraggebers (insbes. Subunternehmer)
☒ ggf. Besucher des Auftraggebers
☒ Ansprechpartner des Auftraggebers

1.5 Die Laufzeit dieser Vereinbarung und die Dauer der Verarbeitung richtet sich nach der Laufzeit des Vertrags, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüberhinausgehende Verpflichtungen ergeben.

1.6 Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraus-setzungen der Art. 44 ff. DSGVO erfüllt sind.
Das angemessene Schutzniveau im Drittland:
☒ ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DSGVO);
☒ wird hergestellt durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b) i.V.m. Art. 47 DSGVO);
☒ wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c) und d) DSGVO);

2. Anwendungsbereich und Verantwortlichkeit

2.1 Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist hinsichtlich der Verarbeitung der Daten für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Datenverarbeitung verantwortlich.

2.2 Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform an, die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Einzelweisungen, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt und der Auftragnehmer darf hierfür eine angemessene Vergütung verlangen.

2.3 Mündliche Weisungen bestätigt der Auftraggeber unverzüglich mindestens in Textform.

2.4 Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, wenn er der Meinung ist, eine Weisung verstößt gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

3. Pflichten des Auftragnehmers

3.1 Der Auftragnehmer darf personenbezogene Daten von betroffenen Personen nur im Rahmen des Auftrages und der dokumentierten Weisungen des Auftraggebers verarbeiten. Sofern der Auftragnehmer durch nationales oder europäisches Recht zu einer hiervon abweichenden Verarbeitung verpflichtet ist, weist er den Auftraggeber vor Beginn der Verarbeitung auf diesen Umstand hin, soweit das betreffende Recht einen Hinweis nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3.2 Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird die in **Anhang 1** beschriebenen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der personenbezogenen Daten des Auftraggebers treffen. Die Maßnahmen sollen die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogenen Daten auf Dauer gewährleisten. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt. Er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden personenbezogenen Daten ein angemessenes Schutzniveau bieten.

3.3 Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch gewährleistet sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

3.4 Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten und der vertraglich geschuldeten Leistung bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gemäß Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten. Hierfür kann der Auftragnehmer eine angemessene Vergütung verlangen.

3.5 Der Auftragnehmer gewährleistet, dass es die mit der Verarbeitung der personenbezogenen Daten des Auftraggebers befassten Mitarbeiter und anderen für den Auftragnehmer tätigen Personen untersagt ist, die personenbezogenen Daten außerhalb der Weisungen des Auftraggebers zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits- oder Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

3.6 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der personenbezogenen Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

3.7 Der Auftragnehmer ist verpflichtet, einen fachkundigen und zuverlässigen Datenschutzbeauftragten nach Art. 37 DSGVO zu bestellen, sofern und so-

lange die gesetzlichen Voraussetzungen für eine Bestellpflicht gegeben sind. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

Sofern der Auftragnehmer nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet ist, nennt er dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

Erster Ansprechpartner in Datenschutzfragen
Abteilung: BT/DSO
Anschrift: Robert-Bosch-Ring 5, 85630 Grasbrunn
E-Mail: GDPR.ST@de.bosch.com

Kontaktdaten des Datenschutzbeauftragten des Auftragsnehmer:
Robert Bosch GmbH,
Konzernbeauftragter für den Datenschutz
Postfach 30 02 20, 70442 Stuttgart
Mail: DPO@bosch.com

3.8 Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DSGVO nachzukommen und ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

3.9 Die Berichtigung und Löschung von personenbezogenen Daten obliegt dem Auftraggeber. Gleiches gilt für die Einschränkung der Verarbeitung von personenbezogenen Daten (Sperrung).

3.10 Die personenbezogenen Daten werden nach dem Ende des jeweiligen Vertrags gelöscht. Es obliegt dem Auftraggeber, Sicherungskopien von seinen personenbezogenen Daten anzufertigen und die personenbezogenen Daten vor Vertragsende umzuziehen. Die Pflicht des Auftragnehmers zur Herausgabe von personenbezogenen Daten, auf die der Auftraggeber selbst Zugriff hat, besteht nicht.

3.11 Der Auftragnehmer verpflichtet sich zur Führung eines Verzeichnisses von Verarbeitungs-tätigkeiten gemäß Art. 30 Abs. 2 DSGVO.

4. Pflichten des Auftraggebers

4.1 Dem Auftraggeber obliegt es, dem Auftragnehmer die personenbezogenen Daten rechtzeitig zur Leistungserbringung nach dem Vertrag zur Verfügung zu stellen. Er ist für die Qualität der personenbezogenen Daten verantwortlich. Der Auftraggeber hat dem Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Leistungen feststellt.

4.2 Im Falle einer Inanspruchnahme durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichten sich Auftraggeber und Auftragnehmer bei der Abwehr des Anspruches sich gegenseitig zu unterstützen.

4.3 Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

5. Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung, Einschränkung der Verarbeitung oder Auskunft über die personenbezogenen Daten an den Auftragnehmer, wird der Auftragnehmer die betroffenen Personen an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach den Angaben der betroffenen Person möglich ist.

6. Nachweismöglichkeiten

6.1 Der Auftragnehmer weist dem Auftraggeber auf Anfrage die Einhaltung der in Art. 28 DSGVO und diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach. Zum Nachweis der Einhaltung der vereinbarten Pflichten kann der Auftragnehmer, dem Auftraggeber Zertifikate und Prüfergebnisse Dritter (z.B. nach Art. 42 DSGVO oder ISO 27001) zur Verfügung stellen oder Prüfberichte des betrieblichen Datenschutzbeauftragten oder von diesen beauftragten Personen.

6.2 Sollten im Einzelfall Kontrollen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten Montag – Freitag zwischen 08:00 Uhr und 17:00 Uhr ohne Störung des Betriebsablaufs und nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit von mind. 4 Arbeitstagen durchgeführt. Der Auftragnehmer darf diese von der Unterzeichnung einer angemessenen Verschwiegenheitserklärung durch den Auftraggeber oder den von diesem beauftragen Prüfer abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Widerspruchsrecht. Der Widerspruch ist in Textform gegenüber dem Auftraggeber zu erklären.

6.3 Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Kontrolle vornehmen, gilt grundsätzlich 6.2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

6.4 Für die Unterstützung bei der Durchführung einer Kontrolle nach 6.2 oder 6.3 darf der Auftragnehmer eine angemessene Vergütung verlangen, sofern nicht Anlass der Kontrolle der dringende Verdacht eines Datenschutzvorfalls im Verantwortungsbereich des Auftragnehmers ist. In diesem Fall sind die Verdachtsmomente mit der Ankündigung der Kontrolle vom Auftraggeber vorzutragen.

7. Subunternehmer (weitere Auftragsverarbeiter)

7.1 Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Vor der Hinzuziehung oder Ersetzung von Subunternehmern informiert der Auftragnehmer den Auftraggeber mit einer Frist von vier Wochen vorab in Textform. Der Auftraggeber kann der Hinzuziehung oder Ersetzung nur aus wichtigem Grund widersprechen. Der Widerspruch hat binnen 14 Tagen zu erfolgen und alle wichtigen Gründe ausdrücklich zu benennen. Erfolgt innerhalb der Frist kein Widerspruch, gilt die Zustimmung zur Hinzuziehung oder Ersetzung als gegeben. Liegt ein wichtiger Grund vor, der vom Auftragnehmer nicht durch Anpassung des Auftrages beseitigt werden kann, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt. Über die in **Anhang 2** aufgeführten, bei Vertragsschluss bereits bestehenden, Subunternehmer und deren Teilleistungen erfolgt keine gesonderte Information. Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

7.2 Auf schriftliche Aufforderung des Auftraggebers hat der Auftragnehmer jederzeit Auskunft über die datenschutzrelevanten Verpflichtungen seiner Subunternehmer zu erteilen.

7.3 Die Regelungen in dieser Ziffer 7 gelten auch, wenn – unter Wahrung der Grundsätze von Kapitel 5 der DSGVO – ein Subunternehmer in einem Drittstaat eingeschaltet wird. Der Auftragnehmer erklärt sich bereit, an der Erfüllung der Voraussetzungen nach

Kapitel 5 der DSGVO im erforderlichen Maße mitzuwirken.

8. Haftung

8.1 Neben den gesetzlichen Haftungsbeschränkungen gelten die Haftungsbeschränkungen aus dem Vertrag.

8.2 Der Auftraggeber stellt den Auftragnehmer von sämtlichen Ansprüchen frei, die Dritte wegen der Verletzung ihrer Rechte gegen den Auftragnehmer aufgrund der vom Aufraggeber beauftragten Verarbeitung personenbezogener Daten geltend machen, sofern nicht der Anspruch des Dritten auf einer weisungswidrigen Verarbeitung der personenbezogenen Daten durch den Auftragnehmer beruht.

9. Informationspflichten, Schriftformklausel, Rechtswahl

9.1 Sollten die personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle Dritten in diesem Zusammenhang unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den personenbezogenen Daten ausschließlich beim Auftraggeber als »Verantwortlicher « im Sinne der DSGVO liegt.

9.2 Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in elektronischer Form erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

9.3 Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen des Vertrags vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

9.4 Die Vereinbarung unterliegt deutschem Recht. Als Gerichtsstand wird Stuttgart (Deutschland) vereinbart.

Grasbrunn, 15.12.2022

Anhang 1

Technisch–organisatorische Maßnahmen / Sicherheits-konzept Bosch Sicherheitssysteme GmbH, Grasbrunn

Allgemein
Die Unternehmen des Geschäftsbereichs Sicherheitssysteme und somit auch die Bosch Sicherheitssysteme GmbH nehmen ihre Verpflichtung zur Schaffung und Wahrung eines hohen Datenschutz- und Datensicherheitsniveaus sehr ernst. Aus diesem Grund dürfen wir Ihnen versichern, dass im Hinblick auf die Einhaltung der gesetzlichen Bestimmungen alle erforderlichen Maßnahmen getroffen werden. Als Unternehmen der Bosch-Gruppe haben wir dabei nicht nur unsere eigenen Interessen im Fokus, sondern auch diejenigen unserer Kunden und Vertragspartner.

Gerne geben wir Ihnen einige Informationen zur Datenschutzorganisation innerhalb der Bosch-Gruppe, des Geschäftsbereichs Sicherheitssysteme und der Bosch Sicherheitssysteme GmbH.

Zum Beauftragten für den Datenschutz der Unternehmen der Bosch-Gruppe ist gem. Art. 37 DSGVO.

Konzernbeauftragter für den Datenschutz Informationssicherheit und Datenschutz Bosch-Gruppe
(C/ISP) Robert Bosch GmbH
Postfach 30 02 20
70442 Stuttgart
E-Mail: DPO@bosch.com

bestellt. Der Konzerndatenschutzbeauftragter ist in seiner Funktion der Geschäftsleitung unmittelbar unterstellt und in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei.

Im Auftrag des Konzerndatenschutzbeauftragten sind in den einzelnen Geschäftsbereichen für deren Unternehmen so genannte Data Security Officer (DSO) als Bereichsbeauftragte für Informationssicherheit und Datenschutz in Vollzeit tätig. Diese sind in Belangen des Datenschutzes und der Datensicherheit - auch für unsere Kunden - erste Ansprechpartner.

Für die Bosch Sicherheitssysteme GmbH sind als Bereichsbeauftragte Ihre Ansprechpartner:

Bosch Sicherheitssysteme GmbH
BT/DSO
Robert-Bosch-Ring 5
85630 Grasbrunn Tel.: 089/6290-0
E-Mail: GDPR.ST@de.bosch.com

Unser Umgang mit personenbezogenen Daten
Unsere Mitarbeiter werden zu Beginn ihrer Tätigkeit nicht nur auf das Datengeheimnis gemäß Art. 5 Abs. 1 f. DSGVO verpflichtet. Zugleich wird die Pflicht zur Verschwiegenheit bzw. Geheimhaltung vertraglich vereinbart. Sofern es die besondere Aufgabenstellung des einzelnen Mitarbeiters mit sich bringt, erfolgen zusätzliche Verpflichtungen nach einschlägigen Bestimmungen.

Auch im Interesse unserer Kunden sorgen wir mit einer weitreichenden Datenschutzorganisation dafür, dass den spezifischen Vorgaben zu Datenschutz und Informationssicherheit Rechnung getragen wird. Mit verschiedensten Richtlinien, Zentralanweisungen und Standards wird hierfür eine tragfähige Basis geschaffen. Zugleich werden die Beschäftigten bedarfsgerecht beispielsweise mit Broschüren, Awareness-Kampagnen, Präsenzschulungen oder Modulen unseres Web-based- Trainings mit den besonderen Anforderungen vertraut gemacht. Ferner stellen wir mittels geeigneter Maßnahmen sicher, dass den gesetzlichen Anforderungen an den sogenannten technisch- organisatorischen Datenschutz im Sinne von Art. 32 DSGVO und diesbezüglicher Anlage entsprochen wird.

Die sich so ergebende Datenschutzstrategie wird stets fortgeschrieben und nicht nur den sich ändernden Anforderungen, sondern auch den sich in einer verändernden Welt ergebenden Herausforderungen, angepasst. Die Einhaltung der konzernweit geltenden Regelungen zu Datenschutz und Datensicherheit wird in den einzelnen Abteilungen durch so genannte Data Security Partner (DSP) dokumentiert. Eine Überprüfung erfolgt im Rahmen verschiedener interner Audits durch den Konzerndatenschutzbeauftragten, die Datenschutzbereichsbeauftragten der Geschäftsbereiche und die interne Unternehmensrevision. Im Bedarfsfall greifen wir in diesem Zusammenhang auf die Expertise namhafter externer Beratungshäuser zurück.

Werden uns von Ihrem Unternehmen Daten zur Verfügung gestellt, damit Ihr Unternehmen beispielsweise eine vertragliche Leistung gegenüber seinen Kunden erbringen kann oder ist nicht auszuschließen, dass wir beispielsweise im Zusammenhang mit Installations- oder Wartungsarbeiten personenbezogene Daten Ihres Unternehmens bzw. Ihrer Kunden oder Mitarbeiter zur Kenntnis nehmen müssen, so werten wir diese Daten als solche, die einer spezifischen Zweckbindung unterliegen. Das bedeutet, dass eine außerhalb des vorgegebenen Zwecks liegende Verarbeitung oder Nutzung durch uns nicht erfolgt. Insbesondere werden die von Ihrem Unternehmen zur Verfügung gestellten Daten nicht an Dritte offenbart, übermittelt oder weitergeben, es sei denn dies ist für die Erbringung der Dienstleistung zwingend erforderlich und wird von einer Rechtsgrundlage gestattet.

Mit dem Wegfall des Zwecks der Erhebung, Verarbeitung oder Nutzung erhält Ihr Unternehmen - sofern technisch möglich - das zur Verfügung gestellte Datenmaterial zurück. Ist eine Rückgabe nicht möglich, kommen wir unserer Verpflichtung zur Löschung beziehungsweise Vernichtung gemäß Art. 17 DSGVO nach.

Auswahl einschlägiger interner Regelungen zu Datenschutz, Informationssicherheit und Persönlichkeitsrecht
Der Umgang mit Daten und Informationstechnologie ist in der Bosch-Gruppe und damit auch für die Bosch Sicherheitssysteme GmbH in zahlreichen Vorschriften verbindlich geregelt. Dazu zählen beispielsweise:

Richtlinien der Bosch-Gruppe
- Unternehmensschutz und Sicherheit für Mitarbeiter und Eigentum
- Informationsverarbeitung (IV)

Zentralanweisung der Bosch-Gruppe
- Informationssicherheit und Datenschutz

Standards der Bosch-Gruppe
- Interne-Audits
- Sicherheit von SAP-Systemen

Dabei werden insbesondere die folgenden Themenbereiche abgedeckt:
- Informationssicherheit und Datenschutz
- CERT (Computer Emergency Response Team)
- Sicherheit bei IV-Endgeräten
- Server-Sicherheit
- Sicherheitsanforderungen an IV-Räume
- Sicherheit Netze und TK-Anlagen
- Sicherheit von SAP-Systemen
- Informationssicherheit und Datenschutz in E-Business-Anwendungen
- Umgang mit Schriftgut und elektronischen Datenträgern
- Authentisierung
- Kryptographie
- Anbindung an das Bosch-Corporate-Network
- Audits im Bereich Informationssicherheit und Datenschutz
- Regelungen, Konzepte zur Informationssicherheit und Datenschutz auf Standort-/Abteilungsbasis
- Schutzklassen

A) Technische und organisatorische Schutzmaßnahmen im Sinne des Art. 32 DS-GVO

Bosch Sicherheitssysteme GmbH hat seine betriebliche Organisation so gestaltet, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Hierzu wurden im Hinblick den Ort der Verarbeitung und Nutzung personenbezogener Daten geeignete und angemessene technische und organisatorische Maßnahmen ergriffen.

Zutrittskontrolle
Maßnahmen, die verhindern sollen, dass Unbefugte Zutritt zu Datenverarbeitungsanlagen erhalten, mit denen personenbezogene Daten verarbeitet oder genutzt werden.

- Festlegung zutrittsberechtigter Personen
- Zutrittskontrolleinrichtungen unter Einsatz personalisierter und codierter Ausweiskarten mit Lichtbild
- Zutrittsregelung für betriebsfremde Personen
- Einrichtung verschiedener Sicherheitszonen mit verschiedenen Zutrittsberechtigungen
- Dokumentation der Vergabe und des Entzugs von Zutrittsberechtigungen
- Videoüberwachung
- Einbruchmeldeanlage mit Alarmübertragung zur ununterbrochen besetzten Sicherheitsleitstelle bzw. zur Polizei
- Zusätzliche Zutrittskontrollmaßnahmen sowie Türzustandsüberwachung für Serverräume
- Fluchttürüberwachung
- Restriktive Schlüsselregelungen
- Besucheraufenthalte nur in Begleitung von Beschäftigten des Geschäftsbereichs Sicherheitssysteme
- Ausweistragepflicht

Zugangskontrolle
Maßnahmen, die sicherstellen sollen, dass nur befugte Personen Zugang zu Datenverarbeitungsanlagen erhalten, mit denen personenbezogene Daten verarbeitet werden.

- Kennwortverfahren (u.a. Festlegungen hinsichtlich Verwendung Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
- Verbot der Weitergabe von Kennwörtern
- Automatische Sperrung des Bildschirms bei Inaktivität nach Zeit
- Sperren von Arbeitsplätzen und/oder Benutzernamen bei mehrfachen fehlerhaften Zugriffsversuchen
- Regelmäßige Zugangsberechtigungsprüfungen
- Protokollierung der Nutzung von Zugangsberechtigungen
- Abschottung interner Netzwerke durch Einrichtung von Firewall-Systemen
- Verschlüsselung von Daten und Festplatten gemäß Schutzklassenkonzept

Zugriffskontrolle
Maßnahmen, um sicherzustellen, dass berechtigte Personen nur auf solche personenbezogene Daten Zugriff erhalten, für die sie die Befugnis zur Einsichtnahme und zur Verarbeitung besitzen.

- Verwendung von benutzerbezogenen und individualisierten Anmeldeinformationen
- Vorgaben zur Festlegung von Passwörtern (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
- Verbot der Weitergabe von Passwörtern
- Berechtigungskonzepte auf Applikations- und Datenebene mit differenzierten Berechtigungsstufen (Profile, Rollen, Transaktionen und Objekte)
- Protokollierung der vergebenen Zugriffsberechtigungen
- Einsatz von Signaturen und Zertifikaten zur Sicherstellung von Urheberschaft und Berechtigung zur Kenntnisnahme (Bosch Trustcenter)
- Verschlüsselung von Daten und Datenträgern in Abhängigkeit von deren Schutzbedürftigkeit
- Datenschutzkonforme Vernichtung von Daten, Datenträgern und Ausdrucken entsprechend Schutzklassenkonzept

Weitergabekontrolle
Maßnahmen, die verhindern, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger unbefugt gelesen, kopiert, verändert oder

entfernt werden können. Zudem soll überprüft und festgestellt werden können, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen der Datenübertragung vorgesehen ist.

- Verschlüsselung von Daten und Datenträgern in Abhängigkeit von deren Schutzbedürftigkeit insbesondere mittels Datei- und Festplattenverschlüsselung auf Hard- oder Softwarebasis (z.B. Secude Secure File, SecureDoc Disk Encryption, Truecrypt, Bitlocker)
- Verwendung von Virtual Private Networks (VPN)
- Benutzung verschließbarer Transportbehälter
- Datenschutzkonforme Vernichtung von Daten, Datenträgern und Ausdrucken entsprechend Schutzklassenkonzept

Eingabekontrolle
Maßnahmen, die gewährleisten, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Protokollierung der Nutzer, welche Eingaben tätigen
- Sicherung der Protokolldateien gegen unbefugte Nutzung und Veränderung

Auftragskontrolle
Maßnahmen, damit personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Gesetzeskonforme Vertragsgestaltung
- Kontrolle der Umsetzung
- Einholung von Selbstauskünften bei Dienstleistern bezüglich deren Maßnahmen zur Umsetzung datenschutzrechtlicher Anforderungen
- Schriftliche Bestätigung von mündlichen Weisungen

Verfügbarkeitskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Zentrale Beschaffung von Hard- und Software
- Einsatz zentral geprüfter und freigegebener Standardsoftware aus sicheren Quellen
- Regelmäßige Durchführung von Datensicherungen bzw. Einsatz von Spiegelungsverfahren
- Unterbrechungsfreie Stromversorgung (USV)
- Getrennte Aufbewahrung von Datenbeständen
- Mehrschichtige Virenschutz-/ Firewallarchitektur
- Notfallplanung
- Feuer-/Wasser- und Temperaturfrühwarnsystem in den Serverräumen
- Betreuung der IT durch qualifizierte und ständig weitergebildete Mitarbeiter

Trennungskontrolle
Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Logische bzw. technische Trennung von Daten
- Benutzerprofile
- Zugriffsberechtigungen
- Speicherung in spezifischen Speicherbereichen

B) Zusätzliche spezifische technische und organisatorische Maßnahmen im Hinblick auf die Verarbeitung und Nutzung personenbezogener Daten bei Service- und Wartungsarbeiten an Anlagen des Auftraggebers in dessen Betriebsstätte

- Verwendung von benutzerbezogenen und individualisierten Anmeldeinformationen
- Beim Transport von Daten: Verschlüsselung von Daten und Datenträgern in Abhängigkeit von deren Schutzbedürftigkeit insbesondere mittels Datei- und Festplattenverschlüsselung auf Hard- oder Softwarebasis
- Datenschutzkonforme Löschung von Daten

C) Zusätzliche spezifische technische und organisatorische Maßnahmen im Hinblick auf die Verarbeitung und Nutzung personenbezogener Daten bei Service- und Wartungsarbeiten an Anlagen des Auftraggebers unter Einsatz von Fernwartungssoftware

Soweit Fernwartung Bestandteil der zu erbringenden Dienstleistung ist (z.B. Teleservice):

- Einsatz von anerkannten Softwarelösungen zur Fernwartung
- Durchführung einer Fernwartungssitzung nur nach Autorisierung durch den Auftraggeber (Eingabe Passwort-Code durch Kunden an dessen Computer)
- Verschlüsselte Datenübertragung nach Einwilligung des Auftraggebers
- Darstellung der während der Fernwartungssitzung durchgeführten Aktionen am Bildschirm des Auftraggebers
- Herrschaft des Kunden über die Fernwartungssitzung mit jederzeitiger Möglichkeit zum Abbruch der Wartungssitzung

Grasbrunn, 23.07.2024

D) Zusätzliche spezifische technische und organisatorische Maßnahmen im Hinblick auf die Verarbeitung und Nutzung personenbezogener Daten in Cloud-Dienstleistungen

Soweit Cloud-Dienstleistungen Bestandteil der zu erbringenden Dienstleistung ist

- Datenspeicherung innerhalb EU oder sicherem Drittland
- Einholung von Selbstauskünften bei Dienstleistern bezüglich deren Maßnahmen zur Umsetzung datenschutzrechtlicher Anforderungen
- Prozessvorgaben und Prüfschemata zur Cloud-Implementierung inkl. Lösch- und Berechtigungskonzepten
- Verwendung von benutzerbezogenen und individualisierten Anmeldeinformationen
- Vorgaben zur Festlegung von Passwörtern (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
- Berechtigungskonzepte auf Applikations- und Datenebene mit differenzierten Berechtigungsstufen (Profile, Rollen, Transaktionen und Objekte)
- Protokollierung der vergebenen Zugriffsberechtigungen
- Verschlüsselung von Daten und Datenträgern in Abhängigkeit von deren Schutzbedürftigkeit