SIEMENS

Anlage F: Vereinbarung zur Auftragsverarbeitung für Serviceleistungen

Stand: Juli 2021

1. Begriffsbestimmungen

1.1 „Anwendbares Datenschutzrecht" bezeichnet die gesetzlichen Vorschriften zum Schutz der Privatsphäre bei der Verarbeitung Personenbezogener Daten (z.B. die DS-GVO).

1.2 „Auftragsverarbeitungsereinbarung" oder „AV-Vereinbarung" bezeichnet die Vertragsklauseln zur Auftragsverarbeitung in dieser Anlage.

1.3 „Auftragsverarbeiter" bezeichnet jede natürliche oder juristische Person, die Personenbezogene Daten im Auftrag des Verantwortlichen Verarbeitet.

1.4 „Datenschutz-Kontakt" bezeichnet den in Ziffer 8 genannten Ansprechpartner für Datenschutzangelegenheiten.

1.5 „DS-GVO" bezeichnet die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016.

1.6 „Personenbezogene Daten" hat die in Art. 4 Nr. 1 DS-GVO beschriebene Bedeutung.

1.7 „Unterauftragsverarbeiter" bezeichnet jeden weiteren Auftragsverarbeiter, welcher durch Siemens zur Erbringung der Vertragsgegenständlichen Leistung im Rahmen dieser AV-Vereinbarung beauftragt wird. Unterauftragsverarbeiter sind nur solche Sub-unternehmer mit Zugang zu Personenbezogenen Daten.

1.8 „Verantwortlicher" bezeichnet den Kunden und / oder Weitere Leistungsempfänger als diejenige natürliche oder juristische Person(en), welche im Rahmen der Vertragsgegenständlichen Leistungen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden.

1.9 „Verarbeiten" oder „Verarbeitung" hat die in Art. 4 Nr. 2 DS-GVO beschriebene Bedeutung.

1.10 „Vertrag" bezeichnet den Vertrag zwischen dem Kunden und Siemens, dem diese AV-Vereinbarung als Anlage beigefügt ist.

1.11 „Verletzung des Schutzes Personenbezogener Daten" bezeichnet eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von, beziehungsweise zum, unbefugten Zugang zu Personenbezogenen Daten führt, die im Rahmen dieser AV-Vereinbarung Verarbeitet werden.

1.12 „Vertragsgegenständliche Leistung" bezeichnet solche Leistungen, die nach dem Vertrag erbracht werden und die die Verarbeitung von Personenbezogenen Daten durch Siemens als Auftragsverarbeiter für den Kunden als Verantwortlichen umfassen. Die Vertragsgegenständlichen Leistungen sind in Anlage F.1 zum Vertrag näher spezifiziert.

1.13 „Weitere Leistungsempfänger" bezeichnet sämtliche Dritte (z.B. Kunden oder verbundene Unternehmen des Kunden) welche nach der Vereinbarung zum Empfang von Vertragsgegenständlichen Leistungen berechtigt sind.

2. Zweck und Anwendungsbereich

2.1 Diese AV-Vereinbarung stellt den schriftlichen Auftragsdatenverarbeitungsvertrag zwischen Siemens und dem Kunden dar und findet Anwendung, soweit die Erbringung der Vertragsgegenständlichen Leistungen die Verarbeitung von Personenbezogenen Daten durch Siemens als Auftragsverarbeiter für den Kunden und/oder etwaige Weitere Leistungsempfänger als Verantwortliche umfasst.

2.2 Diese AV-Vereinbarung regelt die datenschutzrechtlichen Rechte und Pflichten zwischen dem Kunden und Siemens hinsichtlich der Vertragsgegenständlichen Leistungen, welche von dieser AV-Vereinbarung umfasst sind; sonstige Rechte und Pflichten richten sich ausschließlich nach den anderen Teilen des Vertrags.

2.3 Siemens verarbeitet Personenbezogene Daten nur in Übereinstimmung mit den Bestimmungen des Vertrags (einschließlich der Bestimmungen dieser AV-Vereinbarung).

2.4 Bei der Erbringung der Vertragsgegenständlichen Leistungen stellt Siemens sicher, dass alle Vorschriften zum Datenschutz, die für Auftragsverarbeiter unmittelbar anwendbar sind, eingehalten werden. Der Kunde stellt sicher, dass alle für den Kunden (und weitere Leistungsempfänger) geltenden rechtlichen Anforderungen eingehalten werden (insbesondere datenschutzrechtliche Vorschriften, die für Verantwortliche unmittelbar gelten).

2.5 Im Falle von Widersprüchen zwischen den Bestimmungen dieser AV-Vereinbarung und den Bestimmungen des Vertrags gehen die Bestimmungen dieser AV-Vereinbarung in Bezug auf die datenschutzrechtlichen Rechte und Pflichten der Parteien vor. Besteht Unklarheit darüber, ob sich eine Bestimmung auf datenschutzrechtliche Rechte und Pflichten der Parteien bezieht, gilt im Zweifel diese AV-Vereinbarung.

3. Beschreibung der von Siemens erbrachten Datenverarbeitungstätigkeiten

Die Datenverarbeitung erfolgt zum Zweck der Erbringung der Vertragsgegenständlichen Leistungen. Eine Beschreibung der von Siemens erbrachten Datenverarbeitungstätigkeiten, insbesondere eine Beschreibung der Kategorien von Personenbezogenen Daten und Kategorien von betroffenen Personen, ist in Anlage F1 enthalten

4. Weisungsbefugnis

4.1 Siemens wird als Auftragsverarbeiter nur im Rahmen der Weisungen des Kunden tätig. Die Parteien sind sich darüber einig, dass der Vertrag einschließlich dieser AV-Vereinbarung die abschließenden Weisungen des Kunden in Bezug auf die Verarbeitung von Personenbezogenen Daten durch Siemens als Auftragsverarbeiter darstellen.

4.2 Siemens ist im Rahmen des wirtschaftlich Zumutbaren verpflichtet, weitere vom Kunden erteilte Weisungen zu befolgen, sofern diese technisch durchführbar sind und keine wesentlichen Änderungen an der Erbringung der Vertragsgegenständlichen Leistungen (oder der zugrundeliegenden Software) erforderlich machen. Alle weiteren Weisungen müssen schriftlich zwischen dem Kunden und Siemens vereinbart werden und können zusätzliche Kosten für den Kunden verursachen. Sofern eine Weisung des Kunden nach Auffassung von Siemens gegen Anwendbares Datenschutzrecht verstößt, teilt Siemens dies dem Kunden unverzüglich mit. Siemens hat jedoch keine Verpflichtung, Weisungen des Kunden rechtlich zu prüfen.

4.3 Für den Fall, dass weitere Weisungen nach Anwendbarem Datenschutzrecht notwendig sind und sich Siemens und der Kunden nicht im Sinne von Art. 4.2 einigen können, hat der Kunde das Recht, die Vereinbarung außerordentlich zu kündigen.

5. Technische und organisatorische Maßnahmen

5.1 Siemens trifft die technischen und organisatorischen Maßnahmen in Anlage F3. Der Kunde bestätigt hiermit, dass das durch die technischen und organisatorischen Maßnahmen vermittelte Sicherheitsniveau im Verhältnis zum Risiko der Verarbeitung durch Siemens angemessen ist.

5.2 Der Kunde ist sich bewusst, dass die technischen und organisatorischen Maßnahmen der technischen Weiterentwicklung unterliegen. Siemens hat deshalb das Recht, angemessene Alternativmaßnahmen zu treffen, soweit dabei das vermittelte Schutzniveau nicht abgesenkt wird.

6. Vertraulichkeit der Verarbeitung

Siemens wird Mitarbeiter, die mit der Verarbeitung Personenbezogener Daten im Rahmen dieser AV-

Vereinbarung betraut sind, zum vertraulichen Behandlung der Personenbezogenen Daten verpflichten.

7. Unterauftragsverarbeiter

7.1 Siemens beauftragt einen Unterauftragsverarbeiter nur mit vorheriger Zustimmung des Kunden. Die Erteilung der Zustimmung darf nicht unangemessen verweigert werden. Hiermit stimmt der Kunde der Beauftragung der in Anlage F2 genannten Unterauftragsverarbeiter zu.

Bei der Beauftragung von Unterauftragsverarbeitern ist Siemens verpflichtet, mit jedem Unterauftragsverarbeiter eine Vereinbarung zu treffen, die den Unterauftragsverarbeiter im Wesentlichen die gleichen Verpflichtungen auferlegt, wie sie nach der AV-Vereinbarung für Siemens gelten. Auf dessen schriftliche Aufforderung hin, wird dem Kunden eine Abschrift der maßgeblichen Vertragsklauseln übersendet, sofern diese Vertragsklauseln keine kommerziellen oder aus anderen Gründen vertraulichen Informationen enthalten. In diesem Fall ist Siemens zur Schwärzung solcher Informationen berechtigt.

7.2 Siemens ist berechtigt, bestehende Unterauftragsverarbeiter auszutauschen oder neue zu beauftragen. Die Zustimmung des Kunden zur Beauftragung weiterer Unterauftragsverarbeiter erfolgt nach folgendem Verfahren:

(i) Siemens benachrichtigt den Kunden mindestens zehn (10) Tage vor dem Einsatz und Zugriff des neuen Unterauftragsverarbeiters auf Personenbezogene Daten des Kunden.

(ii) Wenn der Kunde in diesem Zeitraum nicht schriftlich, unter Angabe eines wichtigen Grundes, widerspricht, gilt die Zustimmung des Kunden als erteilt, sofern Siemens auf die Folge des widerspruchlosen Verstreichens der Frist hingewiesen hat.

(iii) Wenn der Kunde gegenüber Siemens widerspricht, so ist Siemens berechtigt, den Vertrag mit einer Frist von 10 Tagen zu kündigen. Anstelle der Kündigung hat Siemens das Recht, (a) den Vertrag ohne den beanstandeten Unterauftragsverarbeiter fortzuführen, (b) die notwendigen Maßnahmen zu ergreifen, um die Bedenken des Kunden aus dessen Widerspruch auszuräumen oder (c) mit Zustimmung des Kunden, denjenigen Teil der Vertragsgegenständliche Leistungen einzustellen, für den der entsprechende Unterauftragsverarbeiter eingesetzt worden wäre.

7.3 Siemens haftet für Pflichtverletzungen des Unterauftragsverarbeiters wie für eigene Pflichtverletzungen..

8. Datenschutz-Kontakt des Kunden

8.1 Der Kunde teilt Siemens den Namen und die Kontaktdaten seines Datenschutz-Kontakts mit, die in Anlage F4 anzugeben sind. Sofern der Kunde gemäß Anwendbarem Datenschutzrecht einen Datenschutzbeauftragten bestellt hat, ist dieser als Datenschutzkontakt zu benennen. Eventuelle Änderungen bezüglich des Datenschutz-Kontakts müssen Siemens unverzüglich schriftlich (einschließlich per E-Mail) mitgeteilt werden.

Soweit nicht ausdrücklich etwas anderes vereinbart ist, sind sämtliche Benachrichtigungen und Mitteilungen von Siemens im Rahmen dieses ADV-Vertrags gegenüber dem Datenschutz-Kontakt abzugeben. Die Benachrichtigung oder Mitteilung hat schriftlich (einschließlich per E-Mail) zu erfolgen.

8.2 Die namentliche Benennung des Datenschutzkontakts sowie die Mitteilung über eventuelle Änderungen können entfallen, wenn der Kunde die aktuellen Kontaktdaten seines Datenschutzkontakts auf einer öffentlich zugänglichen Webseite hinterlegt und pflegt und der Kunde die betreffende URL in Anlage F4 mitgeteilt hat.

9. Berichtigung, Löschung und Einschränkung der Verarbeitung

Siemens verpflichtet sich, die Berichtigung, Löschung oder Einschränkung der Verarbeitung entsprechend der Anweisungen des Kunden umzusetzen.

10. Meldepflichten und weitere Unterstützung durch Siemens

10.1 Wenn Siemens Kenntnis von einer Verletzung des Schutzes Personenbezogener Daten erlangt, wird Siemens den Kunden hiervon unverzüglich benachrichtigen. In diesem Fall wird Siemens (i) bei der Untersuchung eines derartigen Ereignisses in zumutbarem Umfang mit dem Kunden zusammenarbeiten, (ii) dem Kunden gegebenenfalls angemessene Unterstützung bei der Erfüllung dessen Verpflichtung zur Meldung von Sicherheitsverletzungen nach Anwendbarem Datenschutzrecht leisten und (iii) angemessene Abhilfemaßnahmen einleiten.

10.2 Siemens benachrichtigt den Kunden unverzüglich über (i) Beschwerden oder Anfragen von betroffenen Personen, deren Personenbezogene Daten im Rahmen dieser AV-Vereinbarung Verarbeitet werden (z.B. hinsichtlich der Berichtigung, Löschung und Einschränkung der Verarbeitung von Daten) oder (ii) Anordnungen und Anfragen von zuständigen Aufsichtsbehörden oder Gerichten.

10.3 Auf Anfrage des Kunden unterstützt Siemens den Kunden im Rahmen des Zumutbaren bei:

(i) der Beantwortung von Beschwerden, Anfragen oder Anordnungen nach Ziffer 10.2

(ii) der Erfüllung sonstiger datenschutzrechtlichen Verpflichtungen nach dem Anwendbaren Datenschutzrecht.

Siemens hat das Recht, dem Kunden die Kosten für solche Unterstützungsleistungen nach Aufwand in Rechnung zu stellen, insbesondere bei häufig wiederkehrenden oder umfangreichen Unterstützungsleistungen. In einem solchen Fall informiert Siemens den Kunden vorab über den voraussichtlichen Aufwand und die sich daraus ergebenden Kosten. Das vorgenannte Recht besteht nicht, wenn die Unterstützungsleistung durch eine schuldhafte Verletzung der Vereinbarung oder des Anwendbaren Datenschutzrechts durch Siemens veranlasst wurde..

11. Kontrollrechte

11.1 Der Kunde ist nach Maßgabe der Ziffern 11.2 und 11.3 berechtigt, die Einhaltung der in dieser AV-Vereinbarung festgelegten Pflichten zum Schutz Personenbezogener Daten (insbesondere im Hinblick auf die technischen und organisatorischen Maßnahmen) durch Siemens oder Unterauftragsverarbeiter in jährlichen Abständen und anlassbezogen zu überprüfen, wobei diese Prüfungen auf die Informationen und Datenverarbeitungssysteme beschränkt sind, die für die Erbringung der Vertragsgegenständlichen Leistungen von Bedeutung sind.

11.2. Soweit Siemens und Unterauftragsverarbeiter für die Vertragsgegenständlichen Leistungen Zertifizierungen durchführen und regelmäßige Prüfberichte erstellen, sind zur Ausübung der Kontrollrechte nach dieser AV-Vereinbarung zunächst diese Zertifizierungen und Prüfberichte zu verwenden. Auf Verlangen des Kunden stellt Siemens (i) die entsprechenden Auszüge aus den Prüfberichten und (ii) Informationen und Unterlagen zu den, für die Vertragsgegenständlichen Leistungen vorhandenen Zertifizierungen und Prüfberichte zur Verfügung. Die zur Verfügung gestellten Prüfberichte, Informationen und Unterlagen sind vertrauliche Informationen von Siemens.

11.3. Nur wenn die Zertifikate und Prüfberichte für den Kunden nicht ausreichen, um die Anforderungen an Audits und Kontrollen nach Anwendbarem Datenschutzrecht einzuhalten, hat der Kunde das Recht auf eigene Kosten (i) zusätzliche Informationen und Unterlagen anzufordern, sowie (ii) nach vorheriger Mitteilung mit einer angemessenen Frist eine weitergehende Prüfung der für die Verarbeiteten Personenbezogenen Daten relevanten Kontrollumgebung und der Sicherheitspraktiken vorzunehmen, wobei die Siemens-Betriebsabläufe hierdurch nicht gestört werden dürfen und die Prüfung im Einklang mit Siemens-Sicherheitsrichtlinien und dem anwendbaren Datenschutzrecht zu erfolgen hat.

12. Vertragsende

Vorbehaltlich abweichender Vereinbarungen zwischen den Parteien wird Siemens mit Beendigung der AV-Vereinbarung alle Personenbezogenen Daten, welche Siemens von dem Kunden zur Verfügung gestellt wurden, oder welche im Zusammenhang mit der Erbringung der Vertragsgegenständliche Leistung erhoben wurden, löschen. Die Löschung wird durch Siemens auf Anfrage schriftlich bestätigt.

Anlage F1: Beschreibung der Datenverarbeitungstätigkeiten

In diesem Anhang werden die grundlegenden Datenverarbeitungstätigkeiten im Rahmen der von Siemens SI angebotenen Service-Leistungen sowie die hiervon betroffenen Personen und die Kategorien der verarbeiteten personenbezogenen Daten beschrieben.

Sofern eine Service-Leistung die Verarbeitung zusätzlicher oder anderer Kategorien von Betroffenen oder von verarbeiteten personenbezogenen Daten zum Inhalt hat, finden sich die diesbezüglichen Informationen in den dazugehörigen Leistungsbeschreibungen.

Produkt	Serviceleistung	Erläuterung
Gebäudesicherheitsanlagen **Gebäudeautomationssysteme, auf die Sicherheitsanlagen aufgeschaltet sind**	**Wartungs-, Inspektions- und Instandsetzungsleistungen** (vor Ort oder im Wege des Fernzugriffs)	In dem im Servicevertrag genannten System abgelegte Daten (z.B. Namen von Mitarbeitern, in Log-files protokollierte Nutzeraktionen) können eingesehen werden
	Back-up-Services	Dateien mit personenbezogenen Daten des Kunden (z.B. Benutzernamen im Anlagen-Log und deren Aktivitäten, Namen von Mitarbeitern und deren Zutritte zu bestimmten Sicherheits-bereichen oder Aufzeichnungen von Videoüberwachungssystemen) werden ausgelesen und auf Sicherungsmedien (z.B. Portable Drive, lokale Server) gespeichert und ggf. zurückgespielt
Betroffene Personen • Mitarbeiter des Kunden und ggf. seiner Dienstleister, die das jeweilige Produkt betreiben und/oder konfigurieren • Besucher / unternehmensfremde Dritte, die den überwachten Bereich betreten		
Kategorien von Daten • Personenstammdaten (Name, Benutzername, Personalnummer, Büroadresse, Gültigkeit der Zutrittsberechtigung etc.) • Geschäftliche Kontaktdaten (E-Mail-Adresse, Telefonnummer) • Zutrittsdaten (Ort und Zeitpunkt von Zutritten) • IP-Adressen von Endgeräten mit denen auf das System zugegriffen wurde • geloggte Aktivität (z.B. Änderungen an der Konfiguration des Systems) • nur bei Videoüberwachungsprodukten : Videoaufzeichnungen		

Produkt	Serviceleistung	Erläuterung
Gebäudeautomationssysteme	**Back-up-Services**	Dateien mit personenbezogenen Daten des Kunden (z.B. Benutzernamen im Anlagen-Log und deren Aktivitäten) werden ausgelesen und auf Sicherungsmedien (z.B. Portable Drive, lokale Server) gespeichert und ggf. zurückgespielt
Betroffene Personen • Mitarbeiter des Kunden und ggfl. seiner Dienstleisterr, die das jeweilige Gebäudeautomations-Produkt betreiben und/oder konfigurieren		
Kategorien von Daten • Benutzername • IP-Adressen von Endgeräten mit denen auf das System zugegriffen wurde • geloggte Aktivität (z.B. Änderungen an der Konfiguration des Systems)		

Anlage F2: Eingesetzte Unterauftragsverarbeiter

Gebäudesicherheitsanlagen

Im Rahmen von Services für Gebäudesicherheitsanlagen ggf. eingesetzte Unterauftragsverarbeiter:

Betroffene Produkte	**Name und Geschäftssitz des Unterauftragsverarbeiters**	**vom Unterauftragsverarbeiter durchgeführte Tätigkeit** (mit Möglichkeit zum Zugriff auf personenbezogene Daten des Kunden)
SiNVR	Schille Informationssysteme GmbH Goseriede 4 D-30159 Hannover	Analyse von Videosequenzen zur Fehlerbehebung (3rd Level-Support) Analyse der Konfiguration und der Systemdatenbank zur Fehlerbehebung (3rd Level-Support) Analyse der Logfiles zur Fehlerbehebung (3rd Level-Support)
SISTORE / Vectis	Vanderbilt International GmbH Borsigstraße 34 D-65205 Wiesbaden	Analyse von Videosequenzen zur Fehlerbehebung (3rd Level-Support) Analyse der Konfiguration und der Systemdatenbank zur Fehlerbehebung (3rd Level-Support) Analyse der Logfiles zur Fehlerbehebung (3rd Level-Support)
SDC	PELWECKYJ Videotechnik GmbH Güterstraße 2 64807 Dieburg	Analyse von Videosequenzen zur Fehlerbehebung (3rd Level-Support) Analyse der Konfiguration und der Systemdatenbank zur Fehlerbehebung (3rd Level-Support) Analyse der Logfiles zur Fehlerbehebung (3rd Level-Support)
SIPORT	AUTEC Gesellschaft für Automationstechnik mbH Bahnhofstraße 57-61B 55234 Framersheim	Analyse der Konfiguration und der Systemdatenbank zur Fehlerbehebung (3rd Level-Support) Analyse der Logfiles zur Fehlerbehebung (3rd Level-Support)
MyTMA	LÜTH & DÜMCHEN Automatisierungsprojekt GmbH Borkumstr. 2 13189 Berlin	Analyse der Konfiguration und der Systemdatenbank zur Fehlerbehebung (3rd Level-Support) Analyse der Logfiles zur Fehlerbehebung (3rd Level-Support)

Gebäudeautomationssysteme

Im Rahmen von Services für Gebäudeautomationssysteme ggf. eingesetzte Unterauftragsverarbeiter

Betroffene Produkte	**Name und Geschäftssitz des Unterauftragsverarbeiters**	**vom Unterauftragsverarbeiter durchgeführte Tätigkeit** (mit Möglichkeit zum Zugriff auf personenbezogene Daten des Kunden)

Service Portal

Im Rahmen der Bereitstellung des Service Portals ggf. eingesetzte Unterauftragsverarbeiter

Betroffene Produkte	**Name und Geschäftssitz des Unterauftragsverarbeiters**	**vom Unterauftragsverarbeiter durchgeführte Tätigkeit** (mit Möglichkeit zum Zugriff auf personenbezogene Daten des Kunden)
Service Portal	Amazon Web Services EMEA SARL 38 avenue John F. Kennedy 1855 Luxemburg	Bereitstellung der Cloud Plattform
Service Portal	SAP SE Dietmar-Hopp-Allee 16 69190 Walldorf	Bereitstellung von Schnittstellen

Anlage F3: Technische und organisatorische Maßnahmen gem. Art. 32 DS-GVO

I. Einleitung

In diesem Dokument werden die technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten („Maßnahmen“) beschrieben, die der Auftragnehmer im Zusammenhang mit der von ihm durchgeführten Verarbeitung unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen mindestens trifft.

Sofern in dem zugrunde liegenden Vertrag hiervon abweichende, besondere Maßnahmen vereinbart werden, gelten solche besonderen Maßnahmen anstelle der oder zusätzlich zu den in diesem Dokument beschriebenen Maßnahmen.

II. Grundlegende Maßnahmen

Die grundlegenden Maßnahmen gewährleisten den Schutz der Vertraulichkeit und der Integrität der Systeme, mit denen Siemens personenbezogene Daten verarbeitet, insbesondere im Wege des Fernzugriffs. Diese Maßnahmen gelten für alle von Siemens durchgeführten Verarbeitungen, sofern nicht im zugrundeliegenden Vertrag abweichend vereinbart.

1. Innerbetriebliche Organisation

Der Auftragnehmer hat einen betrieblichen Datenschutzbeauftragten bestellt. Alle Mitarbeiter und Dienstleister des Auftragnehmers mit Zugriff auf personenbezogene Daten werden verpflichtet, diese nur auf Anweisung und ausschließlich zur Erbringung der vertraglich vereinbarten Leistungen zu verarbeiten.

2. Schutz vor unbefugtem Zugang

Unbefugten ist der Zutritt zu Geschäftsräumen oder Rechenzentren, in denen Datenverarbeitungstätigkeiten stattfinden, zu verwehren.

Maßnahmen:

Der Auftragnehmer schützt die Gebäude oder Geschäftsräume durch angemessene Zutrittskontrollsysteme basierend auf einer Sicherheitseinstufung der Gebäude oder Geschäftsräume und entsprechend definiertem Zutrittsberechtigungskonzept. Alle Gebäude oder Geschäftsräume sind durch technische Zutrittskontrollmaßnahmen z.B. unter Verwendung eines Kartenleser-Systems gesichert. Abhängig von der Sicherheitseinstufung werden Grundstücke, Gebäude oder einzelne Bereiche durch zusätzliche Maßnahmen gesichert. Dazu können spezielle Zutrittsprofile, Biometrie, Pin-Pads, Vereinzelungsschleusen, Video-Überwachung und Wachpersonal gehören.

Zutrittsrechte für autorisierte Personen werden gemäß den festgelegten Kriterien individuell erteilt. Dies gilt auch hinsichtlich externer Personen.

3. Schutz von Rechnern

Die für die Verarbeitung verwendeten Rechner sind gegen unbefugte Nutzung abzusichern und zu schützen.

Maßnahmen:

Zugang zu Rechnern (z.B. Notebooks, Workstations) erhalten nur authentifizierte Benutzer unter Verwendung von bspw. folgenden Maßnahmen: Datenverschlüsselung, individualisierte Passwortvergabe (mind. 8 Zeichen, regelmäßig automatisch verfallend), Mitarbeiterausweise mit PKI-basierter Verschlüsselung, automatische Systemsperrung bei Inaktivität. Der Schutz der verwendeten Rechner gegen Angriffe sowie gegen zufällige oder mutwillige Zerstörung oder Änderung erfolgt u.a. durch Intrusion Detection-Systeme, Firewalls und regelmäßig aktualisierte Malware-Filter.

4. Schutz von Daten bei der Weitergabe, beim Transport und beim Fernzugriff

Es ist dafür Sorge zu tragen, 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.

Maßnahmen:

Absicherung der elektronischen Kommunikationswege durch Einrichtung geschlossener Netzwerke und Verfahren zur Datenverschlüsselung. Sofern ein physischer Datenträger-Transport erfolgt, werden die Daten nur verschlüsselt transportiert. Fernwartungsverbindungen werden mittels Verschlüsselung geschützt. Datum, Art und Umfang der Fernwartung werden protokolliert.

III. Spezifische Maßnahme für Leistungen, bei denen Siemens Daten des Kunden in IT-Systemen speichert

Diese spezifischen Maßnahmen gewährleisten den Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der IT-Systeme, in denen Siemens Daten des Kunden speichert. Sie finden Anwendung, wenn die Speicherung von Daten maßgeblicher Bestandteil der vertragsgegenständlichen Leistungen von Siemens darstellt und nicht bloß vorübergehend erfolgt.

1. Schutz vor unbefugter Verarbeitung

Es ist zu gewährleisten, dass die zur Benutzung eines IT-Systems 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.

Maßnahmen:

Zugriff auf personenbezogene Daten in IT-Systemen wird auf der Grundlage eines rollenbezogenen Berechtigungskonzepts gewährt. Ferner werden bei Bedarf unberechtigte Zugriffe auf personenbezogene Daten durch Datenverschlüsselung verhindert.

2. Gewährleistung der Nachvollziehbarkeit

Es ist zu gewährleisten, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Maßnahmen:

Der Auftragnehmer erlaubt nur authentifizierten Benutzern auf der Grundlage eines rollenbezogenen Berechtigungskonzepts den Zugriff auf personenbezogene Daten. Zugriffe auf personenbezogene Daten werden in Log-Dateien erfasst, die deren Erstellung, Veränderung und Entfernung detailliert protokollieren.

3. Gewährleistung von Integrität, Verfügbarkeit und Belastbarkeit

Es ist zu gewährleisten, dass die für die Verarbeitung verwendeten Systeme gegen Ausfälle abgesichert und personenbezogene Daten somit jederzeit uneingeschränkt verfügbar und gegen Verlust geschützt sind.

Maßnahmen:

Personenbezogene Daten speichert der Auftragnehmer unter Verwendung redundanter Systeme in Abhängigkeit der Sicherheitseinstufung. Zusätzlich verwendet der Auftragnehmer unterbrechungsfreie Stromversorgungen (z.B. UPS, Batterien, Generatoren) zur Sicherstellung der Stromversorgung in seinen Rechenzentren. Es ist ein umfassendes schriftliches Notfall-Konzept erstellt. Notfallprozesse und -Systeme werden regelmäßig getestet

Anlage F4: Angabe der Kontaktdaten des Datenschutzbeauftragten des Kunden

Der Kunde erklärt folgendes:

1. Nach den bestehenden gesetzlichen Regelungen sind wir zur Benennung eines Datenschutzbeauftragten verpflichtet (Zutreffendes bitte ankreuzen): ☐ Ja ☐ Nein
2. Die Kontaktdaten unseres Datenschutzbeauftragten lauten wie folgt (Angaben nur erforderlich, wenn zuvor unter Ziffer 1 „Ja“ angekreuzt):

Firma: _____

Name des Datenschutzbeauftragten: _____

Ggf. Abteilungsbezeichnung: _____

Straße: _____

PLZ und Ort: _____

Telefon: _____

E-Mail: _____

Sofern unter obiger Ziffer 1 „Ja“ angekreuzt: Änderungen der Person oder der Kontaktdaten des Datenschutzbeauftragten werden wir Siemens in Textform mitteilen.