

Anlage Datenverarbeitung und Sicherheit

In dieser Anlage werden die Rollen und Verantwortlichkeiten im Zusammenhang mit der Verarbeitung Personenbezogener Daten und den damit zusammenhängenden Sicherheitsverfahren festgelegt, soweit sie auf die erbrachten Services Anwendung finden.

1. Definitionen

Die in dieser Anlage verwendeten großgeschriebenen Begriffe, die noch nicht in dem Vertrag definiert wurden, werden nachstehend sowie in dieser Anlage definiert:

- 1.1. **Audit:** wie in Klausel 10 dieser Anlage definiert.
- 1.2. **Auftragsverarbeiter:** die Partei, die Personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.
- 1.3. **Befugtes Personal:** Mitarbeiter und/oder Auftragnehmer, die von Interxion für die Erfüllung seiner Verpflichtungen nach dem Vertrag eingesetzt werden.
- 1.4. **Betroffene Person:** sämtliche identifizierbare natürliche Personen, über die Interxion beziehungsweise der Kunde Personenbezogene Daten verarbeitet.
- 1.5. **Datenschutzrechtsvorschriften:** Die EU-Datenschutz-Grundverordnung (DSGVO) und alle anwendbaren Datenschutzrechtsvorschriften, die in dem Land gelten, in dem sich die Geschäftsräume befinden.
- 1.6. **Personenbezogene Daten:** alle Informationen, die sich auf eine Betroffene Person beziehen, die entweder Personenbezogenen Daten von Kunden oder Personenbezogene Daten von Besuchern sind.
- 1.7. **Personenbezogene Daten von Besuchern:** Personenbezogene Daten, die Interxion, wie in Klausel 12.2 dieser Anlage dargelegt, Verarbeitet.
- 1.8. **Personenbezogene Daten von Kunden:** Personenbezogene Daten, die auf dem Kundenequipment gespeichert sind oder das Kundenequipment durchlaufen.
- 1.9. **Verantwortlicher:** die Partei, die über die Zwecke und Mittel der Verarbeitung entscheidet.
- 1.10. **Verarbeitung:** jeder Vorgang oder jede Vorgangsreihe im Zusammenhang mit Personenbezogenen Daten, wie in den Datenschutzrechtsvorschriften definiert.
- 1.11. **Verletzung des Schutzes Personenbezogener Daten:** eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang oder zu einer sonstigen unbefugten Verarbeitung Personenbezogener Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.
- 1.12. **Unterauftragsverarbeiter:** die Einrichtung, die im Auftrag und unter den Weisungen des Verantwortlichen vom Auftragsverarbeiter für die Verarbeitung eingesetzt wird.

2. Einhaltung der Datenschutzrechtsvorschriften

- 2.1 Beide Parteien werden bei der im Zusammenhang mit dem Vertrag stattfindenden Verarbeitung Personenbezogener Daten in vollem Umfang Datenschutzrechtsvorschriften sowie die Bestimmungen dieser Anlage einhalten.

3. Aufgaben und Verantwortlichkeiten der Parteien

- 3.1 Interxion ist für die Sicherheit der Geschäftsräume verantwortlich. In dieser Eigenschaft agiert Interxion als Verantwortlicher für die Personenbezogenen Daten von Besuchern.
- 3.2 Interxion verarbeitet Personenbezogene Daten nur für bestimmte Zwecke, wie in dieser Anlage näher beschrieben wird. X wird Personenbezogene Daten weder verarbeiten, übermitteln, modifizieren, ergänzen oder ändern noch offenlegen oder die Offenlegung dieser Daten gegenüber Dritten gestatten, sofern dies nicht gesetzlich vorgeschrieben ist.
- 3.3 Neben der Rolle von Interxion als Verantwortlicher kann Interxion als Auftragsverarbeiter und der Kunde als Verantwortlicher angesehen werden, wenn und soweit die Services als Verarbeitung gelten.

4. Verarbeitung Personenbezogener Daten (von Kunden)

- 4.1 Der Kunde erkennt hiermit an, dass Interxion keinen (logischen) Zugriff auf Personenbezogene Daten von Kunden hat und dass Interxion nicht in der Lage ist, die Verarbeitung Personenbezogener Daten von Kunden zu überwachen. Die Rolle und Verantwortung von Interxion beschränkt sich auf die Bereitstellung der Services. Wenn und soweit Interxion Personenbezogene Daten von Kunden als Auftragsverarbeiter verarbeitet, wird Interxion dies ausschließlich in Übereinstimmung mit dem Vertrag tun.
- 4.2 Interxion stellt sicher, dass sein Befugtes Personal:
 - über den vertraulichen Charakter Personenbezogener Daten informiert wird,
 - die entsprechenden Schulungen zu ihren Verantwortlichkeiten erhalten hat (einschließlich Sicherheits- und Datenschutzanforderungen, Verfahren zur Reaktion auf Zwischenfälle und Managementverfahren), und
 - den Benutzerauthentifizierungs- und Anmeldeverfahren beim Zugriff auf den Kundenraum und bei der Bereitstellung technischer Unterstützung an den Kunden unterliegt.

5. Sicherheit, Information, technische und organisatorische Maßnahmen

- 5.1 Interxion hat, wie im Folgenden dargelegt, wirtschaftlich angemessene und geeignete Maßnahmen und Garantien für die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit und den Schutz Personenbezogener Daten umgesetzt:
 - a) Informationssicherheit.

Interxion ist nach ISO 27001 zertifiziert und hält sich an die Best Practices für die Informationssicherheit, wie sie in diesem ISO-Standard definiert sind.
 - b) Physische Zutrittskontrolle.

Der Zutritt zu den Geschäftsräumen und Datenverarbeitungssystemen ist eingeschränkt.
 - c) Die Zugangskontrolle umfasst:
 - Eine Identitätszugangskarte; und/oder
 - biometrische Zugangsüberprüfung.
- Der physische Zutritt für Besucher wird überprüft und basiert ausschließlich auf der entsprechenden Authorisierung des Kunden.

d) Darüber hinaus werden folgende Kontrollsysteme eingesetzt:

- Videoüberwachung (digitale Videoaufnahme);
- Sicherheitspersonal 24/7;
- Unabhängige Gebäudesicherheit und Überwachungskontrollen; und
- Einbruchmeldung.

e) Logischer Zugang und Systemkontrolle.

- Richtlinie zur Zugangskontrolle.
- Der Zugang zu den der Kontrolle von Interxion unterliegenden Systemen ist auf das Personal mit den Zugangsrechten beschränkt.
- Die Zugangsrechte werden bei Beendigung des Vertrags widerrufen.
- Nutzer verwenden einmalige Passwörter (Passwortverwaltung stellt einmalige Passwörter sicher).
- Ereignisprotokolle, die auf Datenverarbeitungssystemen stattfindende Nutzeraktivitäten aufnehmen; Ereignisprotokolle werden regelmäßig überprüft.
- Zugriff auf Datenverarbeitungssysteme nur mit Transportsicherheit über VPN; sämtliche Zugriffe über VPN werden protokolliert und regelmäßig überprüft.

f) Netzwerksicherheitskontrolle umfasst:

- Firewalls
- System zur Vorbeugung von Angriffen

6 Unterauftragsverarbeiter

- 6.1 Die Parteien erklären sich damit einverstanden, dass der Einsatz eines Unterauftragsverarbeiters zulässig ist, sofern der Unterauftragsverarbeiter denselben Kontrollen unterliegt und dieselben Pflichten hat wie der Auftragsverarbeiter.
- 6.2 Vorbehaltlich der Klausel 6 der Allgemeinen Geschäftsbedingungen haften die Parteien für direkt aus einer Verletzung des Schutzes Personenbezogener Daten entstehende Schäden, die vom Unterauftragsverarbeiter aufgrund der Nichterfüllung seiner Verpflichtungen bei der Verarbeitung verursacht wurden.

7 Betroffenenrechte

- 7.1 Interxion wird den Kunden unverzüglich informieren, wenn er von einer Betroffenen Person ein Ersuchen in Bezug auf die Personenbezogenen Daten von Kunden erhält, die verarbeitet werden.
- 7.2 Der Kunde wird Interxion unverzüglich informieren, wenn er von einer Betroffenen Person ein Ersuchen über die Personenbezogenen Daten von Besuchern erhält, die verarbeitet werden.

8 Verletzung des Schutzes Personenbezogener Daten

- 8.1 Interxion wird den Kunden unverzüglich und in jedem Fall innerhalb von vierundzwanzig (24) Stunden benachrichtigen, nachdem Interxion von dem begründeten Verdacht einer Verletzung des Schutzes Personenbezogener Daten Kenntnis erlangt hat und wird dem Kunden ausreichende Informationen zur Verfügung stellen, die es dem Kunden ermöglichen, seinen Pflichten zur Meldung einer Verletzung des Schutzes Personenbezogener Daten nachzukommen. Eine solche Benachrichtigung muss mindestens: (i) die Art der Verletzung des Schutzes Personenbezogener Daten beschreiben; (ii) die Kontaktdaten des Datenschutzbeauftragten von Interxion oder einer sonstigen Anlaufstelle für weitere Informationen mitteilen; (iii) die wahrscheinlichen Folgen der Verletzung des Schutzes Personenbezogener Daten beschreiben; und (iv) die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes Personenbezogener Daten darlegen.
- 8.2 Interxion arbeitet mit dem Kunden zusammen und ergreift alle wirtschaftlich vertretbaren Schritte, die vom Kunden zur Unterstützung bei der Untersuchung, Minderung und Behebung solcher Verletzungen des Schutzes Personenbezogener Daten unternommen werden.
- 8.3 Im Falle einer Verletzung des Schutzes Personenbezogener Daten wird Interxion keinen Dritten ohne vorherige schriftliche Einwilligung des Kunden informieren, es sei denn und soweit, eine Meldung durch Interxion ist aufgrund der Datenschutzrechtsvorschriften erforderlich.
- 8.4 Vorbehaltlich der Klausel 6 der Allgemeinen Geschäftsbedingungen haften die Parteien für jegliche Schäden, die direkt aus einer Verletzung des Schutzes Personenbezogener Daten entstehen.

9 Datenschutz-Folgenabschätzung

- 9.1 Interxion wird auf Verlangen des Kunden dem Kunden angemessene Unterstützung bei der etwaigen Datenschutz-Folgenabschätzung, die gemäß Artikel 35 DSGVO oder Artikel 36 DSGVO erforderlich sein kann, gewähren; dies erfolgt in jedem Fall ausschließlich in Bezug auf die physische Sicherheit der Geschäftsräume und der Services, die von Interxion im Zusammenhang mit dem Vertrag erbracht werden.

10 Auditrechte

- 10.1 Um die Einhaltung dieser Anlage durch Interxion zu überprüfen, kann der Kunde ein Audit in den Geschäftsräumen in Übereinstimmung mit dem Auditverfahren durchführen, das unten in der Klausel dieser Anlage beschrieben wird ("Audit").
- 10.2 Auditfragen werden vom Kunden mindestens 15 (fünfzehn) Geschäftstage vor dem beabsichtigten Audittermin durch Mitteilung an Interxion gemacht. In dem Antrag ist anzugeben:
1. wann das Audit vorzugsweise stattfindet;
 2. wie lange das Audit dauert; und
 3. der (die) Name(n) des Auditors (der Auditoren), der (die) das Audit durchführt (durchführen) ("Zugelassener Auditor").
- 10.3 Jeder Auditor muss eine separate Geheimhaltungsvereinbarung unterzeichnen, die nicht weniger strenge Geheimhaltungsbestimmungen als die in dem Vertrag enthaltenen enthält.
- 10.4 Das Audit findet während der Geschäftszeiten und nur in Anwesenheit eines ernannten Mitarbeiters von Interxion statt. Dieser Mitarbeiter beaufsichtigt die Durchführung des Audits und ist der einzige Ansprechpartner, der dem Zugelassenen Auditor Informationen zur Verfügung stellt.
- 10.5 Interxion gestattet den Auditoren Zugang zu den Geschäftsräumen, Aufzeichnungen, weiteren Unterlagen und Systemen (einschließlich Betriebsaufzeichnungen und Handbücher), soweit sie für die Erfüllung des Vertrags verwendet werden,

und soweit der Mitarbeiter von Interxion vernünftigerweise davon überzeugt ist, dass sie für die Durchführung des Audits relevant sind.

- 10.6 Der Kunde stellt sicher, dass der Zugelassene Auditor während der Durchführung eines Audits Folgendes vermeidet: (i) die Verursachung jeglicher Beschädigung oder Verletzung von Interxion Personal, der Geschäftsräume und der dort befindlichen Systeme und (ii) jegliche Störung der Services von Interxion, die für die anderen Kunden von den Geschäftsräumen aus gesteuert und verwaltet werden.
- 10.7 Wenn ein Audit durchgeführt wird, muss der Kunde sicherstellen, dass die internen Sicherheitsregeln von Interxion bezüglich des Zugangs zu seinen Geschäftsräumen vom Zugelassenen Auditor eingehalten werden. Dies umfasst verschiedene physische, logische Sicherheitsmaßnahmen, einschließlich, aber nicht beschränkt auf die Hausordnung von Interxion, die auf Anfrage von Interxion bezogen werden können. Der Zugelassene Auditor darf kein anderes Equipment außer des Kundenequipments berühren oder schalten.
- 10.8 Der Kunde trägt stets die Kosten im Zusammenhang mit dem Audit (z.B. Reisekosten und Stundensätze der Auditoren). Die auf Seiten von Interxion für Audits (z.B. die Mitarbeiter von Interxion) anfallenden Kosten werden vom Kunden zu dem von den Parteien vereinbarten Satz für Hands & Eyes-Services getragen.
- 10.9 Der Austausch von Informationen bezüglich der Erbringung der Services im Rahmen des Vertrags ist nur erlaubt, sofern dadurch die Vertraulichkeitsverpflichtungen nicht verletzt werden.

11 Datenübermittlungen

- 11.1 Interxion verarbeitet keine Personenbezogenen Daten von Kunden, sodass Personenbezogene Daten von Kunden nicht außerhalb Europas übermittelt werden.
- 11.2 Soweit grenzüberschreitende Datenübermittlungen außerhalb Europas in Bezug auf Personenbezogene Daten von Besuchern stattfinden, vereinbaren die Parteien, die anwendbaren Europäischen Standarddatenschutzklauseln unter Bezugnahme auf diesen Vertrag aufzunehmen und einzuhalten.

12 Informationen über die Verarbeitung Personenbezogener Daten durch Interxion als Verantwortlicher

- 12.1 Die Art und Zweck der Verarbeitung durch Interxion als Verantwortlicher:
 1. Zur Wahrung der berechtigten Interessen von Interxion an der physischen Sicherheit seiner Geschäftsräume wird Interxion Personenbezogene Daten von Betroffenen Personen, die die Geschäftsräume betreten, erheben und/oder abrufen.
 2. Für die Erfüllung des Vertrags wird Interxion :
 - a. Personenbezogene Daten von Kundenkontakten zur Authentifizierung und Gestattung des Zugriffs auf das Kundenportal benötigen.
 - b. Personenbezogene Daten von Kundenkontakten für die Erbringung von Services und die damit verbundenen Geschäftszwecke benötigen.
 - c. Kartenleserinformationen über Betroffene Personen aufzeichnen, die den Kundenraum betreten (falls zutreffend).
- 12.2 Die Arten von Personenbezogenen Daten von Besuchern:
 1. Zutrittsdaten beim Betreten der Geschäftsräume: vollständige Namen, Überprüfung der ID-Nummern.
 2. Zugriffsprotokollinformationen vom Kartenleser mit Namen, Zugangsausweisnummern und Datum/Zeit, wann der Kundenraum betreten wurde.
 3. Videoüberwachungsbilder, die in und um die Geschäftsräume aufgenommen und erfasst wurden.
 4. Zugang zum Fingerabdruck: biometrische Informationen.
 5. Die Namen, geschäftliche E-Mail-Adressen, Telefonnummern der Beschäftigten und Auftragnehmer von Kunden.
 6. Die Namen der befugten Personen des Kunden, die auf das Kundenportal zugreifen.
- 12.3 Die Kategorien Betroffener Personen, auf die sich die Personenbezogenen Daten von Besuchern beziehen, sind:
 1. Beschäftigte und Auftragnehmer des Kunden;
 2. Beschäftigte und Auftragnehmer von Interxion; und
 3. Sonstige Betroffene Personen, die Geschäftsräume aufsuchen.