Lieferantenanforderungen zur Informationssicherheit

Wolpert Holding GmbH
Schmalbachstraße 26
D-74626 Bretzfeld
Telefon: +49 79 46 / 91 15 - 0
Telefax: +49 79 46 / 91 15 990
E-Mail: info@wolpert-gruppe.de
Internet: www.wolpert-holding.de

Für die Wolpert Gruppe hat Informationssicherheit eine hohe Bedeutung.

Zur Einhaltung der notwendigen Informationssicherheitsstandards innerhalb der Wolpert Gruppe vereinbaren die Parteien in Ergänzung zu den allgemeinen Einkaufsbedingungen die hier folgenden Anforderungen an die Informationssicherheit für alle Leistungen im Bereich der Informations- und Telekommunikationstechnologie.

Diese Anforderungen zum Prototypenschutz gelten grundsätzlich für Unternehmen, die von der Wolpert Gruppe oder deren Kunden für einen Auftrag vorgesehen sind, für den der Austausch von Informationen notwendig ist. Grundsätzliche Voraussetzung dafür ist, dass ein Unternehmen der Wolpert Gruppe mit dem Auftragnehmer eine Geheimhaltungsvereinbarung schließt.

1. Allgemeines zur Leistungserbringung

Informationssicherheit bedeutet, dass in allen Prozessen in denen Informations- und Telekommunikationstechnik eingesetzt wird, ein angemessenes Maß an Integrität, Verfügbarkeit und Vertraulichkeit von Daten und Systemen nach aktuellem Stand der Technik gewährleistet wird. Dazu stellt der Auftragnehmer die nachfolgenden Punkte sicher.

1. Bei der Leistungserbringung ist sicherzustellen, dass der allgemeine Stand der Technik eingehalten wird. Dies umfasst die Einhaltung der einschlägigen DIN-Normen, Datenschutzvorschriften und entsprechender internationaler und europäischer Normen (z.B. DIN ISO, DIN EN) als Mindeststandard. Leistungen sind so zu erbringen, dass sie der Einhaltung der Informationssicherheitsstandards durch den Auftraggeber nicht entgegenstehen.
2. Bei Leistungen im Betrieb des Auftraggebers hat der Auftragnehmer dort geltende Sicherheitsvorschriften und Informationsrichtlinien einzuhalten, die ihm der Auftraggeber auf Anfrage zur Verfügung stellt. Bei Zugriff auf Informations- und Telekommunikationstechnologie des Auftraggebers hat der Auftragnehmer die dafür geltenden Informationssicherheitsrichtlinien und die nachfolgende Regelung strikt zu beachten, insbesondere auch bei Fernzugriffen (Remote-Zugriff).
   a. Eine Verarbeitung von Daten im Remotezugriff erfolgt nur, soweit dies im zugrundeliegenden Leistungsvertrag vereinbart oder geregelt ist. Hierunter fallen ebenfalls Tätigkeiten bei denen Daten von einem System in ein anderes migriert werden.
3. Bei einem Einsatz von IT-Systemen des Auftragnehmers müssen diese über die folgenden Basis-Sicherheitsmaßnahmen verfügen:
   - Die IT-Systeme müssen über die notwendigen Lizenzen verfügen.
   - Die IT-Systeme müssen ausreichend vor Schadsoftware geschützt sein. Es ist eine Endpoint-Protection zu verwenden, der eine tagesaktuelle Versorgung mit Updates gewährleistet.
   - Die Betriebssysteme auf den IT-Systemen müssen dem jeweils aktuellen Stand von Sicherheitsupdates des jeweiligen Betriebssystemanbieters entsprechen. Es sind nur Betriebssysteme zu verwenden, die vom Hersteller noch unterstützt und gepflegt werden.

1. Bei Vertragsbeendigung enden gleichzeitig Zugangsberechtigungen für Personal des Auftragnehmers zu Systemen und zum Betriebsgelände des Auftraggebers. Dafür bereitgestellte Ausweise und sonstige zur Authentifizierung zur Verfügung gestellten Gegenstände werden dem Auftraggeber unaufgefordert zurückgegeben.
2. Durch den Auftragnehmer sind Lieferungen und Leistungen, insbesondere elektronisch (z.B. via Email oder Datentransfer) übertragene Lieferungen und Leistungen, sowie sämtliche im Rahmen der Leistung eingesetzten Datenträger auf Schadsoftware (z.B. Trojaner, Viren, Spyware usw.), unter Verwendung aktuellster Prüf- und Analyseverfahren zu prüfen und hierdurch die Freiheit von Schadsoftware sicherzustellen. Wird Schadsoftware erkannt, darf der Datenträger nicht eingesetzt werden. Erkennt der Auftragnehmer beim Auftraggeber Schadsoftware, wird er den Auftraggeber unverzüglich darüber informieren. Die gleichen Verpflichtungen gelten für jede Form der elektronischen Kommunikation.
3. Der Auftragnehmer verpflichtet sich, alle Informationen und Daten des Auftraggebers nach dem Stand der Technik sofort wirksam gegen unberechtigten Zugriff, Veränderung, Zerstörung oder Verlust, unerlaubter Verarbeitung und sonstigen Missbrauch zu sichern. Bei der Sicherung von Auftraggeber-Daten sind sämtliche Vorkehrungen und Maßnahmen nach dem aktuellen Stand der Technik zu beachten, um jederzeit Datenbestände verlust- und rechtssicher zu archivieren und wiederherzustellen.
4. Die Informationen und Daten des Auftraggebers dürfen vom Auftragnehmer nur für die vertraglich vereinbarten Zwecke und soweit dies zur Vertragserfüllung erforderlich ist genutzt werden. Bei Verarbeitung von Daten verschiedener Auftraggeber ist deren Trennung nachprüfbar zu gewährleisten (Mandantentrennung).

2. Kontrollrechte

1. Der Auftraggeber ist dazu berechtigt, die Einhaltung der Vorschriften aus dieser Vereinbarung im erforderlichen Umfang in Form von Audits zu kontrollieren. Der Auftragnehmer gewährt dazu dem Auftraggeber nach Absprache, ungehinderten Zutritt, Zugang und Zugriff zu informationsverarbeitenden Systemen, Programmen, Dateien und Informationen, die mit der Durchführung der Tätigkeiten in Verbindung stehen. Dem Auftraggeber sind durch den Auftragnehmer alle Auskünfte zu erteilen, die zur Erfüllung der Kontrollfunktion benötigt werden.
2. Ist der Auftragnehmer ISO 27001 bzw. BSI Grundschutz zertifiziert, oder verfügt er über ein gültiges TISAX Label, dient dies als Nachweis für die Einhaltung der hier beschriebenen Vorschriften. Dazu müssen alle für die Leistungserbringung relevanten Standorte, Prozesse, Organisationseinheiten und IT-Systeme im Anwendungsbereich der Zertifizierung enthalten sein. Ein Nachweis ist dem Auftraggeber auf Anfrage unverzüglich zu übergeben.
3. Sämtliche erbrachten Leistungen und damit zusammenhängende Tätigkeiten sind vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zur Verfügung zu stellen.

4. Verhalten bei Vorfällen

1. Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, falls durch Pfändung, Beschlagnahme oder sonstigen behördlichen Zugriff, in einem Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter die Gefahr besteht, dass nicht berechtigte Personen auf Daten von Unternehmen der Wolpert Gruppe zugreifen. Der Auftragnehmer wird die Dritten darüber informieren, dass es sich um Daten von Unternehmen der Wolpert Gruppe handelt.
2. Der Auftragnehmer hat den Auftraggeber bei Kenntniserlangen oder begründetem Verdacht auf Datenschutzverletzungen, Sicherheitsverletzungen und anderen Manipulationen des Verarbeitungsablaufs, die Wolpert-Daten betreffen, unverzüglich zu informieren und sofort – in Abstimmung mit dem Auftraggeber – alle erforderlichen Schritte zur Aufklärung des Sachverhalts und zur Schadensbegrenzung einzuleiten. Die Meldung hat per E-Mail oder per Telefon (sofern E-Mail nicht möglich ist) zu erfolgen. Auch bei Verdacht ist umgehend eine Meldung durchzuführen.

Kontaktdaten:

Position	**E-Mail**
Informationssicherheitsbeauftragter	ISB@wolpert-holding.de

Beispiele für einen Datenschutz und Informationssicherheitsvorfall können sein:

- Verlust von Datenträgern, Dokumenten oder Geräten mit Wolpert-Informationen
- Verletzung (oder Verdacht auf Verletzung) der Vertraulichkeit durch Ausspähen (z.B. im Zug)
- Schadsoftware-Befall
- Verletzung der in diesem Dokument niedergeschriebenen Regelungen
- Feststellung von unbefugtem Zutritt zu Wolpert-Räumlichkeiten oder eigenen Räumlichkeiten
- Fehlgeleitetete E-Mails
- etc.