Datenschutzanforderungen von Microsoft an Lieferanten

Geltungsbereich

Die Datenschutzanforderungen von Microsoft an Lieferanten (Data Protection Requirements, „**DPR**“) gelten für alle Microsoft-Lieferanten, die personenbezogene oder vertrauliche Microsoft-Daten verarbeiten, während sie Leistungen erbringen (z. B. Dienstleistungen, Softwarelizenzen oder Cloud-Dienste bereitstellen), die in den Bestimmungen ihres Vertrags mit Microsoft (z. B. in Bestellbedingungen oder im Rahmenvertrag) angegeben sind („**Durchführen**“, „**Leistung erbringen/erfüllen**“ oder „**Leistung**“).

- Im Falle eines Konflikts zwischen den im vorliegenden Dokument enthaltenen Anforderungen und den in den vertraglichen Vereinbarungen zwischen dem Lieferanten und Microsoft festgelegten Anforderungen haben die DPR-Anforderungen Vorrang, es sei denn, der betreffende Lieferant gibt im DPR-Nachweis die korrekte Vertragsbestimmung an, die dem betreffenden DPR-Abschnitt widerspricht (in diesem Fall haben die Vertragsbedingungen Vorrang).
- Im Fall eines Konflikts zwischen den Anforderungen im vorliegenden Dokument und gesetzlichen oder rechtlichen Anforderungen haben letztere Vorrang.
- Falls der Microsoft-Lieferant als Controller agiert, gelten bezüglich der Verarbeitungsaktivitäten des betreffenden Lieferanten im Hinblick auf diese Datenschutzanforderungen nur die Anforderungen in Abschnitt J („Sicherheit“) und in Abschnitt A („Management“).
- Sollte der Microsoft-Lieferant keine personenbezogenen Microsoft-Daten, sondern nur vertrauliche Microsoft-Daten verarbeiten, gelten bezüglich der Verarbeitung der vertraulichen Microsoft-Daten durch den Lieferanten im Hinblick auf die vorliegenden Datenschutzanforderungen nur die Anforderungen in Abschnitt A („Management“), Abschnitt E („Speicherung“) und Abschnitt J („Sicherheit“).

Internationale Weitergabe von Daten

Dem Lieferanten ist die internationale Weitergabe von personenbezogenen Microsoft-Daten ohne vorherige schriftliche Genehmigung durch Microsoft untersagt, und er ist in jedem Fall ohne Einschränkung seiner sonstigen Verpflichtungen zur Einhaltung der Datenschutzanforderungen jeglicher Standardvertragsbedingungen, geltender Unternehmensrichtlinien oder sonstiger Bestimmungen verpflichtet, die von einer Datenschutzbehörde, dem Europäischen Datenschutzausschuss oder der Europäischen Kommission genehmigt und von Microsoft übernommen und vereinbart wurden (dies gilt unter anderem auch für EU-US Privacy Shield- und Swiss-US Privacy Shield-Abkommen zwischen der EU bzw. Schweiz und den USA sowie für allgemeine EU-Datenschutzbestimmungen). Der Lieferant erklärt sich damit einverstanden, Microsoft zu benachrichtigen, wenn er feststellt, dass er seine Verpflichtung zur Wahrung des von den Privacy Shield-Grundsätzen geforderten Datenschutzes nicht erfüllen kann. Zudem muss der Lieferant sicherstellen, dass alle Unterauftragsverarbeiter (wie im Anhang zum Beschluss der Europäischen Kommission K(2010) 593 in Klausel 1(d) der Standardvertragsklauseln von 2010 definiert) diese Regelungen ebenfalls einhalten.

Wichtige Definitionen

Die in den vorliegenden Datenschutzanforderungen (DPR) verwendeten Begriffe haben die unten genannten Bedeutungen. Wenn in diesen DPR eine Liste mit Beispielen enthalten ist, die auf Begriffe wie „unter anderem“, „wie etwa“, „z. B.“, „beispielsweise“ usw. folgen, müssen die Begriffe so interpretiert werden, als ob sie auch „ohne Einschränkung“ oder „jedoch nicht beschränkt auf“ enthalten würden, es sei denn, es werden ausdrücklich die Wörter „nur“ oder „ausschließlich“ genannt.

„**Controller**“ steht für die natürliche oder juristische Person, Behörde, Agentur oder jegliche andere Stelle, die alleinig oder gemeinsam mit anderen die Zwecke und Bedeutungen der Verarbeitung von personenbezogenen Daten bestimmt;

wenn die Zwecke und Bedeutungen der Verarbeitung durch die Europäische Union („**EU**“) oder die Gesetzgebung der Mitgliedsstaaten geregelt sind, wird der Controller (oder die Kriterien für die Ernennung des Controllers) möglicherweise durch diese Gesetze bestimmt.

„**Gesetz**“ steht für alle geltenden Gesetze, Regelungen, Statute, Verordnungen, Entscheidungen, Anweisungen, Gerichtsbeschlüsse, Gesetzbücher, Rechtssetzungen, Resolutionen und Anforderungen jeglicher staatlichen Behörde (Bund, Bundesland, Kommune oder international) mit Rechtsbefugnis. „**Unrechtmäßig**“ bedeutet, dass in irgendeiner Weise gegen das Gesetz verstoßen wird.

„**Personenbezogene Daten**“ sind Informationen in Bezug auf eine identifizierte oder identifizierbare natürliche Person („**Betroffene Person**“); als identifizierbare natürliche Person gilt jede Person, deren Identität direkt oder indirekt abgeleitet werden kann, insbesondere durch Verweise auf ein Identifikationsmerkmal wie einen Namen, eine Kennnummer, Standortdaten, eine Onlinekennung oder ein oder mehrere Faktoren, die sich auf den physischen, physiologischen, genetischen, mentalen, wirtschaftlichen, kulturellen oder sozialen Hintergrund dieser natürlichen Person beziehen.

„**Personenbezogene Microsoft-Daten**“ sind personenbezogene Daten, die von oder im Auftrag von Microsoft verarbeitet werden.

„**Rechte von betroffenen Personen**“ steht für das Recht einer betroffenen Person, auf personenbezogene Microsoft-Daten ihrer eigenen Person zuzugreifen, diese zu löschen, zu bearbeiten, zu exportieren, einzuschränken oder deren Verarbeitung zu widersprechen, sofern dies eine rechtliche Auflage ist.

„**Verarbeiten**“ bezieht sich auf jeden Vorgang oder auf eine Reihe von Vorgängen, die an personenbezogenen oder vertraulichen Microsoft-Daten durchgeführt werden, sei es automatisiert oder manuell. Beispiele für derartige Vorgänge sind Erfassung, Aufzeichnung, Anordnung, Strukturierung, Speicherung, Anpassung oder Änderung, Abruf, Konsultation, Nutzung, Offenlegung durch Übertragung, Verteilung oder anderweitige Zurverfügungstellung, Ausrichtung oder Zusammenlegung, Beschränkung, Löschung oder Vernichtung. Diese Bedeutungen gelten auch für die Begriffe „Verarbeitung“ und „Verarbeitet“.

„**Verarbeiter**“ steht für eine natürliche oder juristische Person, Behörde, Agentur oder sonstige Stelle, die personenbezogene Daten im Auftrag des Controllers verarbeitet.

„**Verletzung des Schutzes von Daten**“ bezieht sich auf einen Sicherheitsverstoß, der dazu führt, dass übertragene, gespeicherte oder anderweitig verarbeitete personenbezogene Daten oder vertrauliche Microsoft-Daten versehentlich oder unrechtmäßig vernichtet, verändert, unbefugten Personen mitgeteilt/zugänglich gemacht werden oder verloren gehen.

„**Vertrauliche Microsoft-Daten**“ sind Informationen, deren Offenlegung durch Verstöße gegen Vertraulichkeit oder Integrität den Ruf von Microsoft erheblich schädigen oder zu großen finanziellen Verlusten für das Unternehmen führen kann. Dies umfasst Hardware und Software, interne Branchenanwendungen, Vorabversionen von Marketingmaterial, Lizenzschlüssel für Produkte von Microsoft sowie technische Dokumentationen zu Microsoft-Produkten und -Diensten.

Nr.	Datenschutzanforderungen von Microsoft an Lieferanten	Compliance-Nachweis	Antwort
	Abschnitt A: Management		
1	Jede geltende Vereinbarung zwischen Microsoft und dem Lieferanten (z. B. Rahmenvertrag, Arbeitsaufstellung, Bestellungen und andere Aufträge) enthält Bestimmungen zum Datenschutz und zur Datensicherheit, die sich auf vertrauliche und personenbezogene Microsoft-Daten beziehen, sofern anwendbar. Für Unternehmen, die als Verarbeiter agieren, müssen in der Vereinbarung der Gegenstand und die Dauer der Verarbeitung, die Art und der Zweck der Verarbeitung, die Art der personenbezogenen Microsoft-Daten und die Kategorien der betroffenen Personen sowie die Rechte und Pflichten von Microsoft dargelegt sein.	Der Lieferant muss den geltenden Vertrag zwischen Microsoft und dem Lieferanten vorlegen. Für Verarbeiter sind die Verarbeitungsbeschreibungen in der geltenden Vereinbarung (*z. B.* in der Arbeitsaufstellung oder in den Bestellungen) enthalten. Hinweis: Bei Unternehmen mit Direktbestellungen kann es vorkommen, dass die erforderliche Beschreibung der Verarbeitungsaktivitäten erst später im Einkaufsprozess hinzugefügt wird.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*
2	Er muss einer designierten Person oder Gruppe innerhalb des Unternehmens die Zuständigkeit und Verantwortung für die Einhaltung der Datenschutzanforderungen zuweisen.	Benennung der Person oder Gruppe, die damit beauftragt wurde, die Einhaltung der Compliance mit den DPR von Microsoft an Lieferanten sicherzustellen. Ein Dokument mit einer Beschreibung der Zuständigkeit und Verantwortung dieser Person oder Gruppe, der eine Datenschutz- und/oder Sicherheitsrolle übertragen wurde.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*
3	Er muss eine jährliche Mitarbeiterschulung zum Datenschutz und zur Sicherheit einführen, auf dem neuesten Stand halten und für alle Mitarbeiter, die Zugang zu personenbezogenen oder vertraulichen Microsoft-Daten haben, durchführen. Wenn in Ihrem Unternehmen noch keine derartigen Inhalte ausgearbeitet wurden, können Sie diesen Storyboard-Entwurf verwenden, den Sie an Ihr Unternehmen anpassen können.	Jährliche Unterlagen zum Nachweis der Teilnahme sind verfügbar. Der Schulungsinhalt umfasst die Datenschutz- und Sicherheitsprinzipien.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*

Nr.	Datenschutzanforderungen von Microsoft an Lieferanten	Compliance-Nachweis	Antwort
	Abschnitt A: Management (Fortsetzung)		
4	Er darf personenbezogene Microsoft-Daten ausschließlich in Übereinstimmung mit den dokumentierten Vorgaben von Microsoft verarbeiten. Dies gilt auch für die Weitergabe von personenbezogenen Microsoft-Daten an ein Drittland oder an eine internationale Organisation. Ausgenommen hiervon sind Situationen, in denen das geltende Recht andere Regelungen trifft. In diesem Fall muss der Verarbeiter (Lieferant) den Controller (Microsoft) vor der Verarbeitung über die betreffende gesetzliche Vorgabe informieren, sofern die Offenlegung dieser Information nicht aus zwingenden Gründen des öffentlichen Interesses durch dieses Gesetz untersagt ist.	Dokumentierter Nachweis der Vorgaben, die in einem Vertrag (z. B. in einer Arbeitsaufstellung oder in einer Bestellung) festgehalten sind oder als Teil eines elektronischen Systems erfasst werden, das bei der Erbringung der Leistung genutzt wird.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*

Nr.	Datenschutzanforderungen von Microsoft an Lieferanten	Compliance-Nachweis	Antwort
	Abschnitt B: Hinweis		
5	Der Lieferant muss sich an die Microsoft-Datenschutzbestimmungen halten, wenn er personenbezogene Daten im Auftrag von Microsoft erfasst. Der Lieferant muss für betroffene Personen klare Datenschutzhinweise zur Verfügung stellen, damit sie entscheiden können, ob sie dem Lieferanten ihre personenbezogenen Daten mitteilen möchten. Hinweis: Wenn Ihr Unternehmen der Controller der Verarbeitungsaktivität ist, müssen Sie Ihren eigenen Datenschutzhinweis veröffentlichen. *Wenden Sie sich an SSPAHelp@microsoft.com, um Zugriff auf die richtigen Microsoft-Hinweise zu erhalten.*	Der Lieferant verwendet einen Weiterleitungslink, der zu den aktuellen veröffentlichten Microsoft-Datenschutzbestimmungen führt. Die Datenschutzbestimmungen werden in jedem Kontext veröffentlicht, in dem die personenbezogenen Daten eines Benutzers erfasst werden. Falls anwendbar, ist eine Offlineversion verfügbar, die vor der Datenerfassung bereitgestellt wird. Alle offline verwendeten Datenschutzbestimmungen entsprechen der neuesten veröffentlichten Version und haben das richtige Datum. Für Microsoft-Mitarbeiterdienste wird der Datenschutzhinweis von Microsoft (Microsoft Data Protection Notice) verwendet.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*
6	Lieferanten, die personenbezogene Microsoft-Daten über Live-Telefonanrufe oder Anrufaufzeichnungen erfassen, müssen in der Lage sein, die anwendbaren Praktiken bezüglich Datenerfassung, -handhabung, -nutzung und -speicherung mit den betroffenen Personen zu diskutieren.	Ein Skript für Sprachaufzeichnungen befasst sich auch damit, wie die personenbezogenen Microsoft-Daten verarbeitet werden, sowie mit der ▪ Erfassung, ▪ Verwendung und ▪ Speicherung.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*

Nr.	Datenschutzanforderungen von Microsoft an Lieferanten	Compliance-Nachweis	Antwort
	Abschnitt C: Entscheidungsmöglichkeit und Einverständnis		
7	Wenn sich der Lieferant als Rechtsgrundlage für die Datenverarbeitung auf eine Einverständniserklärung stützt, muss er vor der Erfassung der personenbezogenen Daten einer betroffenen Person vor all seinen Verarbeitungsaktivitäten (dies schließt auch neue und aktualisierte Verarbeitungsaktivitäten ein) das Einverständnis der betroffenen Person einholen und dokumentieren.	Der Lieferant kann erläutern, wie eine betroffene Person einer Verarbeitungsaktivität zustimmt, und nachweisen, dass der Umfang der Einverständniserklärung alle Verarbeitungsaktivitäten des Lieferanten abdeckt, die mit den personenbezogenen Daten der betroffenen Person in Zusammenhang stehen. Der Lieferant kann erläutern, wie eine betroffene Person ihre Zustimmung zu einer Verarbeitungsaktivität widerruft. Der Lieferant kann erläutern, wie die Einstellungen vor dem Start einer neuen Verarbeitungsaktivität geprüft werden. Der Lieferant überwacht die Effektivität der Einstellungsverwaltung, um sicherzustellen, dass der Zeitrahmen für die Berücksichtigung einer Einstellungsänderung der strengsten lokalen gesetzlichen Auflage entspricht, die anwendbar ist. Hinweis: Als Nachweis können Screenshots der Benutzerinteraktion vorgelegt werden. Auch eine experimentelle Vorführung des Dienstes oder eine Gelegenheit zur Einsicht in die technische Dokumentation sind zulässig.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*

Nr.	Datenschutzanforderungen von Microsoft an Lieferanten	Compliance-Nachweis	Antwort
	Abschnitt C: Entscheidungsmöglichkeit und Einverständnis (Fortsetzung)		
8	Cookies sind kleine Textdateien, die von Websites und/oder Anwendungen auf Geräten gespeichert werden. Sie enthalten Informationen, die zur Erkennung einer betroffenen Person oder eines Geräts verwendet werden. Lieferanten, die Microsoft-Websites und/oder -Anwendungen erstellen und verwalten, müssen die betroffenen Personen deutlich auf den Einsatz von Cookies hinweisen und ihnen die Entscheidung über die Verwendung von Cookies ermöglichen. Lieferanten, die Microsoft-Websites und/oder -Anwendungen erstellen und verwalten, müssen sicherstellen, dass der Einsatz von Cookies den Verpflichtungen der Microsoft-Datenschutzbestimmungen und den Auflagen regionaler Gesetze, z. B. den Bestimmungen der EU, entspricht.	Der Zweck jedes Cookies muss dokumentiert werden, und die Art des implementierten Cookies muss klar ersichtlich sein. ▪ Wenn Sitzungscookies ausreichen, dürfen keine beständigen Cookies verwendet werden. ▪ Wenn beständige Cookies verwendet werden, müssen diese spätestens 2 Jahre nach dem Website-Besuch des Benutzers ablaufen. Bei EU-Benutzern darf das Ablaufdatum eines beständigen Cookies 13 Monate nicht überschreiten. Die Einhaltung von EU-Gesetzen muss geprüft werden. Beispiele: ▪ Verwendung der Bezeichnungskonvention „Datenschutz und Cookies“ bei den Datenschutzbestimmungen und ▪ unbedingte Einholung einer bestätigenden Einverständniserklärung des Benutzers, bevor Cookies für „nebensächliche“ Zwecke wie Werbung verwendet werden.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*

Nr.	Datenschutzanforderungen von Microsoft an Lieferanten	Compliance-Nachweis	Antwort
	Abschnitt D: Erfassung		
9	Der Lieferant muss die Erfassung der personenbezogenen und/oder vertraulichen Microsoft-Daten überwachen, um sicherzustellen, dass nur Daten erfasst werden, die zur Erbringung der Leistung nötig sind.	Der Lieferant kann eine Dokumentation vorlegen, aus der hervorgeht, dass die erfassten personenbezogenen und/oder vertraulichen Microsoft-Daten für die Erbringung der Leistung erforderlich sind.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*
10	Wenn der Lieferant personenbezogene Daten von dritten Parteien für Microsoft erfasst, muss der Lieferant sicherstellen, dass die Datenschutzrichtlinien und -praktiken der dritten Partei im Einklang mit dem Vertrag des Lieferanten mit Microsoft sowie mit den DPR-Anforderungen stehen.	Der Lieferant kann die erfolgte Erfüllung seiner Sorgfaltspflicht hinsichtlich der Datenschutzrichtlinien und -praktiken der dritten Partei in einer Dokumentation nachweisen.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*
11	Bevor der Lieferant personenbezogene Microsoft-Daten durch die Installation oder Nutzung von ausführbarer Software auf dem Gerät einer betroffenen Person erfasst, muss die Notwendigkeit der Erfassung dieser Informationen in einem gültigen Lieferantenvertrag mit Microsoft dokumentiert sein.	Die Zustimmung von Microsoft zur Verwendung von ausführbarer Software auf dem Gerät einer betroffenen Person ist in dem gültigen Vertrag festgehalten.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*
12	Vor der Erfassung sensibler personenbezogener Microsoft-Daten (Daten, die Aufschluss über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten, Daten zum Gesundheitszustand oder Daten zum Sexualleben bzw. zu der sexuellen Ausrichtung einer natürlichen Person geben) muss die Notwendigkeit der Erfassung dieser personenbezogenen Microsoft-Daten in einem gültigen Lieferantenvertrag mit Microsoft dokumentiert sein.	Die Notwendigkeit der Erfassung sensibler personenbezogener Microsoft-Daten wird in dem gültigen Vertrag mit Microsoft festgehalten.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*

Nr.	Datenschutzanforderungen von Microsoft an Lieferanten	Compliance-Nachweis	Antwort
	Abschnitt E: Speicherung		
13	Er muss sicherstellen, dass personenbezogene und vertrauliche Microsoft-Daten nicht länger gespeichert werden, als nötig ist, um die Leistungen zu erbringen, es sei denn, die weitere Speicherung der personenbezogenen und/oder vertraulichen Microsoft-Daten ist eine rechtliche Auflage.	Der Lieferant hält dokumentierte Speicherungsrichtlinien oder Speicherungsanforderungen ein, die von Microsoft im Vertrag (z. B. in der Arbeitsaufstellung oder der Bestellung) angegeben wurden.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*
14	Er muss sicherstellen, dass nach eigenem Ermessen von Microsoft die personenbezogenen und vertraulichen Microsoft-Daten im Besitz oder unter Kontrolle des Lieferanten an Microsoft zurückgegeben oder vernichtet werden, sobald die Dienstleistungen fertiggestellt wurden oder wenn Microsoft dies verlangt. In Anwendungen müssen Prozesse implementiert sein, die für eine sichere Datenlöschung sorgen, wenn Daten explizit durch Benutzer oder aufgrund von Auslösern wie dem Alter der Daten aus der Anwendung entfernt werden. Wenn die Vernichtung von personenbezogenen oder vertraulichen Microsoft-Daten erforderlich ist, muss der Lieferant die physischen Gegenstände, auf denen sich die personenbezogenen und/oder vertraulichen Microsoft-Daten befinden, so verbrennen, pulverisieren oder zerstückeln, dass die Daten nicht gelesen oder rekonstruiert werden können.	Der Lieferant bewahrt Aufzeichnungen zur Entsorgung von personenbezogenen und vertraulichen Microsoft-Daten auf (z. B. Rückgabe an Microsoft zur Vernichtung). Wenn eine Vernichtung erforderlich ist oder von Microsoft verlangt wird, muss der Lieferant ein Vernichtungszertifikat vorlegen, das von einem leitenden Angestellten des Lieferanten unterzeichnet wurde.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*

Nr.	Datenschutzanforderungen von Microsoft an Lieferanten	Compliance-Nachweis	Antwort
	Abschnitt F: Betroffene Personen		
	Betroffene Personen haben ein Zugangsrecht zu ihren personenbezogenen Daten sowie das Recht, diese zu löschen, zu bearbeiten, zu exportieren, zu beschränken und gegen deren Verarbeitung Einspruch zu erheben („**Rechte der betroffenen Personen**“). Wenn eine betroffene Person ihre Rechte im Rahmen der Rechtssprechung hinsichtlich ihrer personenbezogenen Microsoft-Daten wahrnehmen möchte, hat der Lieferant folgende Verpflichtungen:		
15	Er muss Microsoft soweit möglich durch entsprechende technische und organisatorische Maßnahmen bei der Erfüllung der Pflichten hinsichtlich der Beantwortung von Anfragen von betroffenen Personen unterstützen, die ihre Rechte wahrnehmen möchten.	Es müssen Prozesse und Verfahren implementiert sein, die die Wahrnehmung der Rechte von betroffenen Personen ermöglichen.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*
16	Er muss unverzüglich auf alle Anfragen im Zusammenhang mit den Rechten von betroffenen Personen reagieren.	Der Lieferant prüft in regelmäßig durchgeführten Tests, ob er die Rechte von betroffenen Personen im Ernstfall unterstützen kann.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*
17	Sofern nicht anderweitig von Microsoft instruiert, verweist der Lieferant alle betroffenen Personen, die ihn im Zusammenhang mit ihren Rechten kontaktieren, direkt an Microsoft. Der Lieferant muss der betroffenen Person mitteilen, welche Schritte sie unternehmen muss, um Zugang zu ihren personenbezogenen Microsoft-Daten zu erlangen oder um ihre sonstigen Rechte wahrzunehmen. *Wenden Sie sich an SSPAHelp@microsoft.com, wenn Sie Unterstützung bei dieser Anforderung benötigen.*	Der Lieferant teilt die Schritte mit, die für den Zugriff auf die personenbezogenen Daten erforderlich sind, sowie die verfügbaren Methoden für das Aktualisieren der Daten.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*
18	Wenn der Lieferant der betroffenen Person direkt antwortet, muss er die Identität der betroffenen Person, die die Anfrage stellt, überprüfen.	Der Lieferant hat die Methode zur Identifizierung von betroffenen Personen im Zusammenhang mit Microsoft dokumentiert.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*

Nr.	Datenschutzanforderungen von Microsoft an Lieferanten	Compliance-Nachweis	Antwort
	Abschnitt F: Betroffene Personen (Fortsetzung)		
	Wenn eine betroffene Person authentifiziert wurde, hat der Lieferant folgende Pflichten:		
19	Er muss feststellen, ob er im Besitz der personenbezogenen Microsoft-Daten zu der betroffenen Person ist oder sie kontrolliert.	Der Lieferant verfügt über Verfahren, mit denen er ermitteln kann, ob sich personenbezogene Daten in seinem Besitz befinden.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*
20	Er muss angemessene Bemühungen unternehmen, um die angeforderten personenbezogenen Microsoft-Daten zu finden und ausreichende Unterlagen aufbewahren, um zu demonstrieren, dass eine angemessene Suche durchgeführt wurde.	Der Lieferant pflegt eine Aufzeichnung, in der die Schritte genannt werden, die zur Erfüllung von Anfragen im Zusammenhang mit den Rechten von betroffenen Personen ergriffen werden. Die Dokumentation umfasst ▪ Datum und Uhrzeit der Anfrage, ▪ ergriffene Maßnahmen zur Erfüllung der Anfrage und ▪ den Zeitpunkt, zu dem Microsoft informiert wurde.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*
21	Er muss Datum und Uhrzeit der Anfragen im Zusammenhang mit den Rechten von betroffenen Personen und der vom Lieferanten bezüglich dieser Anfragen unternommenen Handlungen aufzeichnen. Er muss Microsoft auf Anfrage Unterlagen zu Anfragen von betroffenen Personen zur Verfügung stellen.	Der Lieferant verwaltet Aufzeichnungen von Zugangsanfragen und Dokumentänderungen, die an personenbezogenen Daten vorgenommen wurden.	
	Nachdem eine betroffene Person authentifiziert wurde und der Lieferant festgestellt hat, dass er im Besitz der personenbezogenen Microsoft-Daten ist, hat der Lieferant folgende Pflichten:		
22	Bei Bitten um eine Kopie der personenbezogenen Daten muss er der betroffenen Person die personenbezogenen Microsoft-Daten in geeigneter gedruckter oder elektronischer Form bereitstellen oder mündlich mitteilen.	Der Lieferant stellt der betroffenen Person die personenbezogenen Daten in einem Format bereit, das verständlich und sowohl für die betroffene Person als auch für den Lieferanten praktisch ist.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*

Nr.	Datenschutzanforderungen von Microsoft an Lieferanten	Compliance-Nachweis	Antwort
	Abschnitt F: Betroffene Personen (Fortsetzung)		
23	Wenn die Anfrage abgelehnt wird, muss die betroffene Person auf Anweisung von Microsoft eine schriftliche Erklärung erhalten, die den zuvor von Microsoft gegebenen relevanten Anweisungen entspricht. *Wenden Sie sich an SSPAHelp@microsoft.com, wenn Sie Unterstützung bei dieser Anforderung benötigen.*	Er muss Fälle dokumentieren, in denen Anfragen abgelehnt werden, und einen Nachweis über die Prüfung und Genehmigung durch Microsoft speichern.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*
24	Der Lieferant muss angemessene Maßnahmen ergreifen, um sicherzustellen, dass die an die betroffene Person ausgegebenen personenbezogenen Microsoft-Daten nicht zur Identifizierung einer anderen Person genutzt werden können.	Der Lieferant muss nachweisen, dass angemessene Maßnahmen ergriffen werden, damit die ausgegebenen Daten nicht zur Identifizierung einer anderen Person genutzt werden können (beispielsweise darf er nicht die gesamte Datenseite fotokopieren, wenn personenbezogene Daten für eine betroffene Person nur eine Zeile ausmachen).	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*
25	Wenn eine betroffene Person und ein Lieferant unterschiedlicher Meinung sind, ob die personenbezogenen Microsoft-Daten vollständig und korrekt sind, muss der Lieferant das Problem an Microsoft eskalieren und Microsoft nach Bedarf bei der Lösung des Problems unterstützen. *Wenden Sie sich an SSPAHelp@microsoft.com, wenn Sie Unterstützung bei dieser Anforderung benötigen.*	Der Lieferant dokumentiert Fälle unterschiedlicher Meinung und eskaliert das Problem an Microsoft.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*

Nr.	Datenschutzanforderungen von Microsoft an Lieferanten	Compliance-Nachweis	Antwort
	Abschnitt G: Offenlegung gegenüber dritten Parteien		
	Wenn der Lieferant beabsichtigt, bei der Verarbeitung von personenbezogenen oder vertraulichen Microsoft-Daten auf einen Zulieferer zurückzugreifen, hat er folgende Pflichten:		
26	Er muss vor der Weiterbeauftragung der Dienstleistungen oder Durchführung von Änderungen hinsichtlich zusätzlicher oder anderer Zulieferer eine ausdrückliche schriftliche Genehmigung von Microsoft einholen. *Wenden Sie sich an SSPAHelp@microsoft.com, wenn Sie Unterstützung bei dieser Anforderung benötigen.*	Er muss sicherstellen, dass die personenbezogenen Microsoft-Daten nur von Unternehmen verarbeitet werden, die Microsoft bekannt sind. Außerdem muss die Verarbeitung den Anforderungen im geltenden Vertrag (z. B. in der Arbeitsaufstellung, in einem Zusatz oder in der Bestellung) entsprechen oder in der SSPA-Datenbank erfasst sein.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*
27	Er muss die Art und den Umfang der personenbezogenen und vertraulichen Microsoft-Daten, die durch Zulieferer verarbeitet werden, dokumentieren. Außerdem muss er sicherstellen, dass die erfassten Daten tatsächlich für die Erbringung der Leistung erforderlich sind.	Der Lieferant pflegt eine Dokumentation zu den personenbezogenen und vertraulichen Microsoft-Daten, die an Zulieferer weitergegeben oder übertragen werden.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*
28	Er muss sicherstellen, dass der Zulieferer die personenbezogenen Microsoft-Daten im Einklang mit der angegebenen bevorzugten Kommunikationsmethode der betroffenen Person nutzt.	Er muss erläutern, wie die Einstellung einer betroffenen Person im Zusammenhang mit Microsoft von Zulieferern verwendet wird. Er muss eine entsprechende Dokumentation vorlegen, die den Zeitrahmen festlegt, in dem ein Zulieferer eine Einstellungsänderung berücksichtigen muss.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*
29	Er muss die Verarbeitung der personenbezogenen Microsoft-Daten durch den Zulieferer auf die Zwecke beschränken, die zur Erfüllung des Vertrags des Lieferanten mit Microsoft nötig sind.	Der Lieferant kann eine Dokumentation vorlegen, aus der hervorgeht, dass die einem Zulieferer zur Verfügung gestellten personenbezogenen Microsoft-Daten für die	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*

		Erbringung der Leistung erforderlich sind.	
Nr.	Datenschutzanforderungen von Microsoft an Lieferanten	Compliance-Nachweis	Antwort
Abschnitt G: Offenlegung gegenüber dritten Parteien (Fortsetzung)			
30	Er muss auf Beschwerden hin überprüfen, ob eine unberechtigte Nutzung oder unrechtmäßige Verarbeitung personenbezogener Microsoft-Daten vorliegt.	Der Lieferant kann nachweisen, dass Systeme und Verfahren implementiert sind, um auf Beschwerden hinsichtlich unberechtigter Nutzung oder Offenlegung von personenbezogenen Microsoft-Daten durch einen Zulieferer zu reagieren.	*<Konform> <Nicht konform> <Trifft nicht zu> <Rechtlicher Konflikt> <Vertraglicher Konflikt>*
31	Er muss Microsoft sofort informieren, wenn er erfährt, dass ein Zulieferer personenbezogene oder vertrauliche Microsoft-Daten für andere Zwecke als die Erbringung seiner Leistung verarbeitet hat.	Der Lieferant hat die Anweisung und Mittel für einen Zulieferer bereitgestellt, damit der Missbrauch von Microsoft-Daten gemeldet werden kann.	*<Konform> <Nicht konform> <Trifft nicht zu> <Rechtlicher Konflikt> <Vertraglicher Konflikt>*
32	Er muss sofort Maßnahmen ergreifen, um tatsächliche oder potenzielle Schäden zu mindern, die durch die unberechtigte Nutzung oder unrechtmäßige Verarbeitung personenbezogener und vertraulicher Microsoft-Daten entstehen können.	Der Lieferant kann nachweisen, dass er über einen Plan und Verfahren verfügt, die Anwendung finden, sollten personenbezogene und vertrauliche Microsoft-Daten von einem Zulieferer missbräuchlich verwendet werden.	*<Konform> <Nicht konform> <Trifft nicht zu> <Rechtlicher Konflikt> <Vertraglicher Konflikt>*
Abschnitt H: Qualität			
33	Der Lieferant muss die Integrität von allen personenbezogenen Microsoft-Daten wahren und sicherstellen, dass sie korrekt, vollständig und für die angegebenen Zwecke, für die sie verarbeitet wurden, relevant sind.	Der Lieferant kann nachweisen, dass er Verfahren zur Prüfung von personenbezogenen Microsoft-Daten bei ihrer Erfassung, Erstellung und Aktualisierung implementiert hat. Der Lieferant kann nachweisen, dass Überwachungs- und Stichprobenverfahren implementiert sind, um die Korrektheit fortlaufend zu	*<Konform> <Nicht konform> <Trifft nicht zu> <Rechtlicher Konflikt> <Vertraglicher Konflikt>*

		überprüfen und bei Bedarf wiederherzustellen.	

Nr.	Datenschutzanforderungen von Microsoft an Lieferanten	Compliance-Nachweis	Antwort
	Abschnitt I: Überwachung und Durchsetzung		
34	Der Lieferant muss über einen Plan für die Reaktion auf Vorfälle verfügen, in dessen Rahmen er Microsoft unverzüglich benachrichtigt, wenn er eine Verletzung des Schutzes der Daten oder eine Sicherheitslücke im Zusammenhang mit seiner Bearbeitung von personenbezogenen oder vertraulichen Microsoft-Daten bemerkt. *Wenden Sie sich an SSPAHelp@microsoft.com, um einen Vorfall zu melden.*	Der Lieferant verfügt über einen Plan für die Reaktion auf Vorfälle, der einen Schritt zur Benachrichtigung von Kunden (Microsoft) gemäß der Beschreibung in diesem Abschnitt enthält.	*<Konform> <Nicht konform> <Trifft nicht zu> <Rechtlicher Konflikt> <Vertraglicher Konflikt>*
35	Er darf jegliche Pressemitteilung oder andere öffentliche Aussage in Bezug auf eine Verletzung des Schutzes von Daten im Zusammenhang mit personenbezogenen oder vertraulichen Microsoft-Daten nur nach Genehmigung von Microsoft veröffentlichen, außer wenn eine gesetzliche Auflage es anders vorsieht.	Der Lieferant verpflichtet sich, diese Anforderung im Ernstfall zu erfüllen.	*<Konform> <Nicht konform> <Trifft nicht zu> <Rechtlicher Konflikt> <Vertraglicher Konflikt>*
36	Er muss einen Korrekturplan implementieren und die Behebung der Verletzungen des Schutzes von Daten und der Schwachstellen bezüglich personenbezogener oder vertraulicher Microsoft-Daten überwachen, um sicherzustellen, dass zeitnah geeignete Korrekturmaßnahmen ergriffen werden.	Der Lieferant hat die Maßnahmen dokumentiert, die er als Reaktion auf eine Verletzung des Schutzes von Daten ergreift, um diese zu beheben.	*<Konform> <Nicht konform> <Trifft nicht zu> <Rechtlicher Konflikt> <Vertraglicher Konflikt>*
37	Er muss ein formelles Beschwerdeverfahren für alle Datenschutzbeschwerden im Zusammenhang mit personenbezogenen Microsoft-Daten einführen.	Der Lieferant verfügt über die Mittel zum Erhalt von Beschwerden hinsichtlich personenbezogener Microsoft-Daten und über ein dokumentiertes Beschwerdeverfahren für die Reaktion auf Beschwerden.	*<Konform> <Nicht konform> <Trifft nicht zu> <Rechtlicher Konflikt> <Vertraglicher Konflikt>*

Nr.	Datenschutzanforderungen von Microsoft an Lieferanten	Compliance-Nachweis	Antwort
	Abschnitt J: Sicherheit		
	Der Lieferant muss ein Datensicherheitsprogramm einführen, implementieren und pflegen, das Richtlinien und Verfahren zum kontinuierlichen Schutz von personenbezogenen und vertraulichen Microsoft-Daten umfasst. Dieses Programm muss an die in der Branche üblichen Praktiken und an die gesetzlichen Anforderungen angeglichen werden. Das vom Lieferanten eingesetzte Sicherheitsprogramm muss die unten genannten Standards (Anforderungen 38 bis 56) erfüllen.	Die Schutzmechanismen können über die aufgeführten hinausgehen, wie für die Einhaltung von Regelwerken (z. B. HIPPA, GLBA) oder vertraglichen Bestimmungen erforderlich. Ein gültiger ISO 27001- oder SOC 2-Bericht mit Informationen zur Sicherheit wird als Ersatz für Abschnitt J akzeptiert. Wenden Sie sich an SSPAHelp@microsoft.com, wenn Sie diesen Ersatz anwenden möchten. Hinweis: Sie müssen eine Dokumentation zur Verfügung stellen, in der der Umfang dieser Zertifizierungen/Berichte beschrieben wird.	
38	Er muss jährliche Analysen der Netzwerksicherheit durchführen, die Folgendes umfassen: ▪ Prüfung wichtiger Änderungen an der Umgebung, wenn beispielsweise eine neue Systemkomponente, Netzwerktopologie oder Firewallregeln eingeführt wurden, ▪ Durchführung von Scans zur Überprüfung auf Schwachstellen und ▪ Pflege von Änderungsprotokollen.	Der Lieferant hat Netzwerkanalysen, Änderungsprotokolle und Scanergebnisse dokumentiert. In den erforderlichen Änderungsprotokollen müssen Änderungen nachvollzogen werden, und es müssen Informationen zum Grund der Änderung sowie Name und Titel der festgelegten genehmigenden Stelle enthalten sein.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*
39	Der Lieferant muss eine Mobilgeräterichtlinie festlegen, bekannt geben und implementieren. Diese muss den Schutz von personenbezogenen oder vertraulichen Microsoft-Daten, die auf einem Mobilgerät zugänglich sind oder genutzt werden, gewährleisten und die Nutzung derartiger Daten beschränken.	Der Lieferant weist die Verwendung einer kompatiblen Mobilgeräterichtlinie nach, wenn für die Verarbeitung von personenbezogenen oder vertraulichen Microsoft-Daten ein	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*

		Mobilgerät verwendet werden muss.	

Nr.	Datenschutzanforderungen von Microsoft an Lieferanten	Compliance-Nachweis	Antwort
	Abschnitt J: Sicherheit (Fortsetzung)		
40	Alle Ressourcen, die zur Erbringung seiner Leistung genutzt werden, müssen berücksichtigt werden und einen identifizierten Eigentümer haben. Der Lieferant ist für die Pflege einer Bestandsliste dieser Informationsressourcen verantwortlich. Er muss für eine akzeptable und autorisierte Nutzung der Ressourcen sorgen und diese während des gesamten Lebenszyklus angemessen schützen.	Bestandsliste der Geräteressourcen, die zur Erfüllung der Leistung verwendet werden. Die Bestandsliste dieser Ressourcen muss Folgendes umfassen: ▪ Standort des Geräts, ▪ Datenklassifizierung der Daten auf der Ressource, ▪ Aufzeichnung über die Ressourcenwiederherstellung bei Beendigung eines Angestelltenverhältnisses oder einer Unternehmensvereinbarung und ▪ Aufzeichnung über die Entsorgung von Datenspeichermedien, wenn sie nicht mehr benötigt werden.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*

Nr.	Datenschutzanforderungen von Microsoft an Lieferanten	Compliance-Nachweis	Antwort
	Abschnitt J: Sicherheit (Fortsetzung)		
41	Er muss Verwaltungsverfahren für Zugriffsrechte einrichten und pflegen, um den unbefugten Zugriff auf personenbezogene oder vertrauliche Microsoft-Daten unter der Kontrolle des Lieferanten zu verhindern.	Der Lieferant weist nach, dass er einen Plan zur Verwaltung von Zugriffsrechten implementiert hat, der Folgendes umfasst: ▪ Verfahren für die Zugriffssteuerung, ▪ Identifikationsverfahren, ▪ Sperrungsverfahren nach fehlgeschlagenen Versuchen, ▪ Kennwortzurücksetzung so oft wie erforderlich, aber spätestens nach 90 Tagen, ▪ zuverlässige Parameter für die Auswahl der Anmeldeinformationen zur Authentifizierung und ▪ Deaktivierung von Benutzerkonten innerhalb von 48 Stunden nach Ausscheiden eines Mitarbeiters. Der Lieferant weist nach, dass er ein Verfahren für die Prüfung des Benutzerzugriffs auf personenbezogene und vertrauliche Microsoft-Daten eingerichtet hat, wobei die Regel der geringsten Rechte Anwendung findet. Dieses Verfahren muss Folgendes umfassen: ▪ klar definierte Benutzerrollen, ▪ Verfahren für die Prüfung und Rechtfertigung einer Zugriffsgenehmigung für Rollen und ▪ Tests, ob Benutzer in Rollen, die Zugriff auf Microsoft-Daten besitzen, eine dokumentierte Rechtfertigung haben, Mitglied der Gruppe/Rolle zu sein.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*

Nr.	Datenschutzanforderungen von Microsoft an Lieferanten	Compliance-Nachweis	Antwort
	Abschnitt J: Sicherheit (Fortsetzung)		
42	Er muss Verfahren für die Patchverwaltung definieren und implementieren, die Sicherheitspatches für Systeme priorisieren, welche für die Verarbeitung von personenbezogenen oder vertraulichen Microsoft-Daten verwendet werden. Diese Verfahren müssen Folgendes umfassen: ▪ eine definierte Risikostrategie für die Priorisierung von Sicherheitspatches ▪ die Möglichkeit zur Verarbeitung und Implementierung von Notfallpatches ▪ die Anwendbarkeit auf Betriebssystem- und Serversoftware wie Anwendungsserver- und Datenbanksoftware ▪ die Dokumentierung des Risikos, das durch den Patch eingedämmt wird, und Verfolgung eventueller Ausnahmen und ▪ Voraussetzungen für die Ausmusterung von Software, die nicht mehr vom entwickelnden Unternehmen unterstützt wird.	Der Lieferant kann ein implementiertes Verfahren für die Patchverwaltung nachweisen, das diese Anforderung erfüllt und mindestens folgende Punkte abdeckt: ▪ Es muss ein Schweregrad für die Priorisierung zugewiesen sein. (Es sind Definitionen der Schweregrade dokumentiert.) ▪ Es muss ein Verfahren für die Implementierung von Notfallpatches implementiert sein. ▪ Es muss sichergestellt werden, dass keine Betriebssysteme verwendet werden, die vom Entwicklerunternehmen nicht mehr unterstützt werden. ▪ Es müssen Unterlagen zur Patchverwaltung vorhanden sein, in denen Genehmigungen und Ausnahmen verfolgt werden.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*
43	Er muss Antivirus- und Antischadsoftware auf allen Geräten installieren, die mit dem Netzwerk verbunden sind, das für die Verarbeitung der personenbezogenen und vertraulichen Microsoft-Daten verwendet wird. Dies umfasst unter anderem auch Server sowie Desktop-PCs in Produktions- und Schulungsumgebungen. So soll ein Schutz vor möglicherweise schädlichen Viren und Anwendungen mit Schadsoftware gewährleistet werden. Er muss Malwareschutz-Definitionen täglich oder je nach Anweisung des Anbieters der Antivirus- und Antischadsoftware aktualisieren. Hinweis: Dies gilt für alle Betriebssysteme inklusive Linux.	Es müssen Aufzeichnungen vorhanden sein, die eine aktive Nutzung von Antivirus- und Antischadsoftware belegen. Hinweis: Diese Anforderung gilt für alle Betriebssysteme.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*
44	Lieferanten, die Software für Microsoft entwickeln, müssen im Buildprozess das Prinzip der konzeptionsintegrierten Sicherheit („Security by Design“) anwenden.	Die Lieferantendokumente mit technischen Spezifikationen enthalten Prüfpunkte für eine Sicherheitsprüfung in ihren Entwicklungszyklen.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>*

			<Vertraglicher Konflikt>

Nr.	Datenschutzanforderungen von Microsoft an Lieferanten	Compliance-Nachweis	Antwort
	Abschnitt J: Sicherheit (Fortsetzung)		
45	Er muss ein Programm zur Verhinderung von Datenverlust (Data Loss Prevention, „**DLP**“) implementieren. Die Daten müssen ordnungsgemäß klassifiziert, bezeichnet und geschützt werden, und der Lieferant muss die bei der Verarbeitung von personenbezogenen oder vertraulichen Microsoft-Daten verwendeten Informationssysteme im Hinblick auf Eindringversuche, Verlust und sonstige unbefugte Aktivitäten überwachen. Das DLP-Programm muss mindestens ▪ die Nutzung von dem Branchenstandard entsprechenden host-, netzwerk- und cloudbasierten Angriffserkennungssystemen (Intrusion Detection Systems, „**IDS**“) verlangen, wenn Sie personenbezogene oder vertrauliche Microsoft-Daten aufbewahren, ▪ die Implementierung von modernen Intrusionsschutzsystemen (Intrusion Protection Systems, „**IPS**“) verlangen, die für die Überwachung und aktive Beendigung von Datenverlust konfiguriert sind, ▪ im Fall eines Sicherheitsverstoßes auf einem System die Analyse des Systems verlangen, um sicherzustellen, dass sonstige Sicherheitslücken ebenfalls geschlossen werden, ▪ erforderliche Verfahren für die Überwachung des Systems mit Tools zur Angriffserkennung beschreiben und ▪ einen Prozess für die Reaktion auf Vorfälle und deren Bewältigung festlegen, der durchgeführt werden muss, wenn Ereignisse in Bezug auf eine Verletzung des Schutzes von Daten festgestellt werden.	Dokumentierter Einsatz eines Angriffserkennungssystems/Intrusionsschutzsystems mit implementierten Verfahren für die sofortige Reaktion, wenn eine Schwachstelle oder eine Verletzung des Schutzes von Daten festgestellt wird.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*

Nr.	Datenschutzanforderungen von Microsoft an Lieferanten	Compliance-Nachweis	Antwort
	Abschnitt J: Sicherheit (Fortsetzung)		
46	Er muss die Untersuchungsergebnisse der Reaktion auf Vorfälle sofort an das leitende Management und an Microsoft melden. *Wenden Sie sich an SSPAHelp@microsoft.com, um Microsoft zu informieren.*	Es müssen Systeme und Verfahren implementiert sein, um Untersuchungsergebnisse bezüglich der Reaktion auf Vorfälle an Microsoft zu melden.	*<Konform> <Nicht konform> <Trifft nicht zu> <Rechtlicher Konflikt> <Vertraglicher Konflikt>*
47	Systemadministratoren, das Betriebspersonal, das Management und Drittparteien müssen an einer jährlichen Sicherheitsschulung teilnehmen.	Einrichtung eines Schulungsprogramms zum Thema Sicherheit, das Folgendes umfasst: ▪ jährliche Schulung zur Reaktion auf Vorfälle und ▪ simulierte Ereignisse und automatisierte Mechanismen zur Erleichterung einer effektiven Reaktion auf Krisensituationen. Bewusstsein über die Notwendigkeit einer Verhinderung von Vorfällen und Kenntnis der Risiken, die mit dem Download von Schadsoftware verbunden sind.	*<Konform> <Nicht konform> <Trifft nicht zu> <Rechtlicher Konflikt> <Vertraglicher Konflikt>*
48	Der Lieferant muss sicherstellen, dass personenbezogene und vertrauliche Microsoft-Daten durch Planverfahren zur Sicherung vor unbefugtem Zugriff, unberechtigter Nutzung, Offenlegung, Manipulation und Vernichtung geschützt werden.	Der Lieferant kann eine Dokumentation der Reaktions- und Wiederherstellungsverfahren nachweisen. Dort muss detailliert angegeben sein, wie die Organisation ein Störereignis bewältigt und ihre Datensicherheit auf einem zuvor festgelegten Niveau hält, das auf vom Management genehmigten Zielen im Hinblick auf die kontinuierliche Datensicherheit basiert. Der Lieferant kann nachweisen, dass er Verfahren definiert und implementiert hat, mit denen kritische Daten in regelmäßigen Abständen gesichert, auf sichere Weise gespeichert und effektiv wiederhergestellt werden können.	*<Konform> <Nicht konform> <Trifft nicht zu> <Rechtlicher Konflikt> <Vertraglicher Konflikt>*

Nr.	Datenschutzanforderungen von Microsoft an Lieferanten	Compliance-Nachweis	Antwort
	Abschnitt J: Sicherheit (Fortsetzung)		
49	Er muss Pläne für Geschäftskontinuität und Notfallwiederherstellung einrichten und testen.	Ein Notfallwiederherstellungsplan muss alle der folgenden Punkte umfassen: ▪ Festgelegte Kriterien zur Ermittlung, ob ein System für den Geschäftsbetrieb des Lieferanten kritisch ist. ▪ Eine Auflistung der auf den festgelegten Kriterien basierenden kritischen Systeme, die bei einem Notfall wiederhergestellt werden müssen. ▪ Für jedes kritische System ein festgelegtes Verfahren zur Notfallwiederherstellung, mit dem sichergestellt ist, dass auch ein Techniker, der das System nicht kennt, die Anwendung in weniger als 72 Stunden wiederherstellen kann ▪ Jährlich (oder häufiger) durchgeführter Test und eine Prüfung der Notfallwiederherstellungspläne, um sicherzustellen, dass die Wiederherstellungsziele erfüllt werden können.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*

Nr.	Datenschutzanforderungen von Microsoft an Lieferanten	Compliance-Nachweis	Antwort
	Abschnitt J: Sicherheit (Fortsetzung)		
50	Der Lieferant muss die Identität einer Person authentifizieren, bevor er dieser Person Zugang zu personenbezogenen oder vertraulichen Microsoft-Daten gewährt.	Es muss sichergestellt sein, dass alle Benutzer-IDs eindeutig sind und jeder eine auf dem Branchenstandard basierende Authentifizierungsmethode wie Azure Active Directory zugewiesen ist. Bei höheren Zugriffsberechtigungen (Administrator oder sonstige Arten erweiterter Berechtigungen) muss der Einsatz eines zweiten Faktors erforderlich sein (z. B. eine Smartcard oder ein telefonischer Authentifikator).	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*
51	Der Lieferant muss personenbezogene und vertrauliche Microsoft-Daten, die in Netzwerken übertragen werden, durch eine Verschlüsselung mit Transport Layer Security („**TLS**“) oder Internet Protocol Security („**IPsec**“) schützen. Diese Verfahren sind in NIST 800-52 und NIST 800-57 beschrieben, es kann jedoch auch ein gleichwertiger anderer Branchenstandard verwendet werden. Der Lieferant muss die Bereitstellung jeglicher personenbezogener oder vertraulicher Microsoft-Daten per unverschlüsselter Übertragung ablehnen.	Der Prozess der Erstellung, Bereitstellung und Ersetzung von TLS oder anderen Zertifikaten muss festgelegt sein und umgesetzt werden.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*
52	Auf allen Geräten des Lieferanten (Laptops, Workstations usw.), die Zugang zu personenbezogenen oder vertraulichen Microsoft-Daten haben oder diese verarbeiten, muss eine Datenträgerverschlüsselung erfolgen.	Er muss alle Geräte verschlüsseln, um Bitlocker oder einer gleichwertigen, in der Branche anerkannten Lösung für Datenträgerverschlüsselung auf allen Client-Geräten zu genügen, die für die Verarbeitung von personenbezogenen oder	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*

		vertraulichen Microsoft-Daten genutzt werden.	

Nr.	Datenschutzanforderungen von Microsoft an Lieferanten	Compliance-Nachweis	Antwort
	Abschnitt J: Sicherheit (Fortsetzung)		
53	Es müssen Systeme und Verfahren (unter Verwendung aktueller Branchenstandards wie in der Beschreibung in der Norm NIST 800-111 enthalten) für die Verschlüsselung ruhender (aufbewahrter) Daten sowie aller personenbezogenen und/oder vertraulichen Microsoft-Daten implementiert sein. Dies schließt alle der folgenden Informationen ein: ▪ Anmeldedaten (z. B. Benutzernamen/Kennwörter) ▪ als Zahlungsinstrument genutzte Daten (z. B. Kreditkartennummern und Bankkontonummern) ▪ immigrationsbezogene persönliche Daten ▪ Daten medizinischer Profile (z. B. Nummern medizinischer Berichte/biometrische Marker oder Identifikationsmerkmale wie etwa DNA, Fingerabdrücke, Retina und Iris des Auges, Sprachmuster, Gesichtszüge sowie zu Authentifizierungszwecken verwendete Handvermessungen) ▪ von Behörden ausgestellte Identifizierungsdaten (z. B. Sozialversicherungsnummern oder Führerscheinnummern) ▪ Daten von Microsoft-Kunden (z. B. Sharepoint, O365-Dokumente, OneDrive-Kunden) ▪ Material in Bezug auf nicht bekannt gegebene Microsoft-Produkte ▪ Geburtsdatum ▪ Profilinformationen von Kindern ▪ geografische Echtzeitdaten ▪ privater (nicht geschäftlicher) Wohnsitz ▪ private (nicht geschäftliche) Telefonnummern ▪ Religion ▪ politische Überzeugungen ▪ sexuelle Ausrichtung/Vorlieben ▪ Antwort auf Sicherheitsfragen (z. B. Zwei-Faktor-Authentifizierung, Kennwortzurücksetzung) o Geburtsname der Mutter	Sicherstellung, dass die in dieser Zeile aufgelisteten ruhenden personenbezogenen und vertraulichen Microsoft-Daten verschlüsselt aufbewahrt werden.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*

Nr.	Datenschutzanforderungen von Microsoft an Lieferanten	Compliance-Nachweis	Antwort
	Abschnitt J: Sicherheit (Fortsetzung)		
54	Bei der Verarbeitung von Kreditkarten im Auftrag von Microsoft muss er für jeden Kartenaussteller die anwendbaren Standards zur Handhabung von Kreditkarten befolgen.	Nachweis der Compliance durch jährliche Vorlegung einer Zertifizierung des Payment Card Industry Data Services Standard („**PCI-DSS**“). *Einreichung von PCI-DSS-Zertifizierungen bei SSPA. Wenden Sie sich an SSPAHelp@microsoft.com*, falls Sie Fragen haben.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*
55	Der Lieferant muss physische Microsoft-Gegenstände in einer Umgebung mit kontrolliertem Zugang aufbewahren.	Es müssen Systeme und Verfahren eingerichtet sein, um den physischen Zugang zu digitalen, ausgedruckten, archivierten und als Sicherung dienenden Kopien von Microsoft-Daten zu verwalten. Der Weg und die Vernichtung von physischen Medien mit Microsoft-Daten müssen in einer Kontrollkette verfolgt werden.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*
56	Alle personenbezogenen Microsoft-Daten in einer Entwicklungs- oder Testumgebung müssen anonymisiert werden.	Personenbezogene Microsoft-Daten dürfen nicht in Entwicklungs- oder Testumgebungen verwendet werden; wenn es keine Alternative gibt, müssen sie anonymisiert werden, um die Identifizierung von betroffenen Personen oder den Missbrauch personenbezogener Daten zu verhindern. Hinweis: Anonymisierte Daten sind nicht mit pseudonymisierten Daten zu verwechseln. Anonymisierte Daten sind Daten, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, sodass die betroffene Person der personenbezogenen Daten nicht oder nicht mehr identifizierbar ist.	*<Konform>* *<Nicht konform>* *<Trifft nicht zu>* *<Rechtlicher Konflikt>* *<Vertraglicher Konflikt>*