Datenschutzanforderungen für Lieferanten von Microsoft

Geltungsbereich

Die Datenschutzanforderungen für Microsoft-Lieferanten („**DPR**“) gelten für jeden Microsoft-Lieferanten, der personenbezogene Daten von Microsoft oder vertrauliche Daten von Microsoft in Verbindung mit der Leistung dieses Lieferanten (z. B. die Bereitstellung von Diensten, Softwarelizenzen, Cloud-Diensten) gemäß den Bedingungen seines Vertrags mit Microsoft (z. B. Bestellbedingungen oder Rahmenvertrag) verarbeitet („**Durchführen**“ „**Durchführung**“ oder „**Leistung**“).

- Im Falle eines Konflikts zwischen den Datenschutzanforderungen und den in den vertraglichen Vereinbarungen zwischen dem Lieferanten und Microsoft festgelegten Anforderungen haben die Datenschutzanforderunagen Vorrang, es sei denn, der Lieferant weist auf die korrekte Bestimmung im Vertrag hin, die die anwendbare Datenschutzanforderung außer Kraft setzt (in diesem Fall haben die vertraglichen Bedingungen Vorrang).
- Im Falle eines Widerspruchs zwischen den hierin enthaltenen Anforderungen und gesetzlichen oder anderweitigen rechtlichen Anforderungen haben die gesetzlichen oder anderweitigen rechtlichen Anforderungen Vorrang.
- Falls der für Microsoft tätige Lieferant als für die Verarbeitung Verantwortlicher tätig ist, kann der Lieferant Gegenstand geringerer Anforderungen aus den DPR sein.
- Für den Fall, dass der Microsoft-Lieferant keine personenbezogenen Daten von Microsoft, sondern nur vertrauliche Daten von Microsoft verarbeitet, kann der Lieferant in Bezug auf diese DPR geringere Anforderungen haben.

Internationale Übermittlung von Daten

Ohne seine anderweitigen Verpflichtungen einzuschränken, wird der Lieferant keine internationale Übermittlung personenbezogener Daten von Microsoft vornehmen, es sei denn, Microsoft erteilt vorher eine schriftliche Genehmigung. In jedem Fall muss der Lieferant die Datenschutzanforderungen, einschließlich der Standardvertragsklauseln, oder, nach dem Ermessen von Microsoft, andere geeignete grenzüberschreitende Übermittlungsmechanismen einhalten, die von einer zuständigen Datenschutzbehörde oder der Europäischen Kommission genehmigt und von Microsoft angenommen oder gebilligt wurden. Nachfolgende Standardvertragsklauseln, die (i) von der Europäischen Kommission oder vom Europäischen Datenschutzbeauftragten angenommen und von der Europäischen Kommission genehmigt wurden, (ii) vom Vereinigten Königreich gemäß dem UK General Federal Data Protection Act, (iii) von der Schweiz gemäß dem Schweizerischen Bundesgesetz über den Datenschutz oder (iv) von einer Regierung in einer anderen Rechtsordnung als der Schweiz, dem Vereinigten Königreich und den Rechtsordnungen, die die Europäische Union/den Europäischen Wirtschaftsraum umfassen, offiziell angenommenen Klauseln zur Regelung der internationalen Übermittlung personenbezogener Daten, werden aufgenommen und haben für den Lieferanten ab dem Tag ihrer Annahme Bindungswirkung. Der Lieferant stellt außerdem sicher, dass alle Unterauftragsverarbeiter (wie in den Standardvertragsklauseln definiert) dies ebenfalls tun.

Wichtige Definitionen

Die folgenden in diesen DPR verwendeten Begriffe haben die folgende Bedeutung. Die Aufzählung von Beispielen nach „einschließlich“, „wie“, „z. B.“, „zum Beispiel“ oder ähnlichem, die in diesen DPR verwendet werden, sind so auszulegen, dass sie „ohne Einschränkung“ oder „aber nicht beschränkt auf“ beinhalten, es sei denn, sie werden durch Wörter wie „nur“ oder „ausschließlich“ eingeschränkt. Weitere Definitionen sind bitte dem Glossar am Ende dieses Dokuments zu entnehmen.

„**Verantwortlicher“** bezeichnet die Stelle, die die Zwecke und Mittel der Verarbeitung personenbezogener Daten bestimmt. Der Begriff „für die Verarbeitung Verantwortlicher“ umfasst ein Unternehmen, einen für die Verarbeitung Verantwortlichen (so, wie dieser Begriff in der DSGVO definiert ist) und gleichwertige Begriffe in den Datenschutzgesetzen, sofern der Kontext dies erfordert.

„**Cookies**“ sind kleine Textdateien, die von Websites und/oder Anwendungen auf Geräten gespeichert werden und Informationen enthalten, die dazu dienen, eine betroffene Person oder ein Gerät zu erkennen.

„**Datenvorfall**“ bezeichnet (1) eine Verletzung der Sicherheit, die zur versehentlichen oder unrechtmäßigen Zerstörung, zum Verlust, zur Änderung, zur unbefugten Offenlegung von oder zum Zugriff auf personenbezogene Daten von Microsoft oder

vertrauliche Daten von Microsoft führt, die vom Lieferanten oder seinen Unterauftragnehmern übertragen, gespeichert oder anderweitig verarbeitet werden, oder (2) eine Sicherheitslücke im Zusammenhang mit der Handhabung personenbezogener Daten von Microsoft oder vertraulicher Daten von Microsoft durch den Lieferanten.

„**Betroffene Person**“ bezeichnet als identifizierbare natürliche Person jemand, der direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

„**Recht der betroffenen Person“** bezeichnet das Recht einer betroffenen Person auf Zugang, Löschung, Bearbeitung, Export, Einschränkung oder Widerspruch gegen die Verarbeitung der personenbezogenen Daten dieser betroffenen Person, sofern dies gesetzlich vorgeschrieben ist.

„**Gesetz**“ bzw. „**gesetzlich**“ bezeichnet alle anwendbaren Gesetze, Regeln, Satzungen, Dekrete, Entscheidungen, Anordnungen, Verordnungen, Urteile, Kodizes, Erlasse, Beschlüsse und Anforderungen von Behörden (auf Bundes-, Landes-, kommunaler oder internationaler Ebene), die zuständig sind. „**Ungesetzlich**“ bedeutet jede Verletzung eines Gesetzes.

„**Vertrauliche Daten von Microsoft**“ sind alle Informationen, die bei einer Beeinträchtigung der Vertraulichkeit oder Integrität zu einem erheblichen Imageverlust oder finanziellen Schaden für Microsoft führen können. Dazu gehören Hardware- und Softwareprodukte von Microsoft, interne Geschäftsanwendungen, Marketingmaterialien vor der Veröffentlichung, Produktlizenzschlüssel und technische Dokumentationen zu Microsoft-Produkten und -Diensten.

„**Personenbezogene Daten von Microsoft**“ bezeichnet alle personenbezogenen Daten, die von oder im Namen von Microsoft verarbeitet werden.

„**Personenbezogene Daten**“ bezeichnet alle Informationen über eine betroffene Person und alle anderen Informationen, die nach dem Gesetz betrachtet „personenbezogene Daten“ oder „personenbezogene Informationen“ darstellen.

„**Verarbeiten**“ bezeichnet jeden Vorgang oder jede Reihe von Vorgängen, die mit personenbezogenen Daten oder vertraulichen Daten von Microsoft durchgeführt werden, unabhängig davon, ob sie automatisiert sind oder nicht, wie etwa z. B. das Erheben, das Aufzeichnen, die Organisation, die Strukturierung, die Speicherung, die Anpassung oder Veränderung, das Abrufen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder sonstige Bereitstellung, den Abgleich oder die Kombination, die Einschränkung, das Löschen oder die Vernichtung. Die Begriffe „Verarbeitung“ und „verarbeitet“ haben die gleiche Bedeutung.

„**Auftragsverarbeiter**“ bezeichnet eine Einrichtung, die personenbezogene Daten im Auftrag einer anderen Einrichtung verarbeitet, und schließt Dienstanbieter, Auftragsverarbeiter (so, wie dieser Begriff in der DSGVO definiert ist) und gleichwertige Begriffe in Datenschutzgesetzen ein, je nach Kontext.

„**Unterauftragnehmer**“ bezeichnet einen Dritten, an den der Lieferant seine Verpflichtungen im Zusammenhang mit dem Vertrag, der seine Leistung abdeckt, delegiert, einschließlich eines verbundenen Unternehmens des Lieferanten, das nicht direkt mit Microsoft zusammenarbeitet.

„**Unterauftragsverarbeiter**“ bezeichnet einen Dritten, den Microsoft mit einer Leistung beauftragt, wobei die Leistung die Verarbeitung personenbezogener Daten von Microsoft umfasst, für die Microsoft ein Auftragsverarbeiter ist.

Antwort des Lieferanten

Die Lieferanten bestätigen die Einhaltung dieser Anforderungen jährlich über einen von Microsoft verwalteten Online-Dienst. Im Leitfaden zum SSPA-Programm ist beschrieben, wie die Einhaltung der Vorschriften gehandhabt wird.

#	Datenschutzanforderungen für Lieferanten von Microsoft	Nachweis der Einhaltung
	Abschnitt A: Verwaltung	
1	Jeder anwendbare Vertrag zwischen Microsoft und dem Lieferanten (z. B. Rahmenvertrag, Leistungsbeschreibung, Bestellungen und andere Aufträge) enthält Datenschutz- und Sicherheitsbestimmungen in Bezug auf vertrauliche und personenbezogene Daten von Microsoft, einschließlich des Verbots des Verkaufs personenbezogener Daten von Microsoft und der Verarbeitung personenbezogener Daten von Microsoft außerhalb der direkten Geschäftsbeziehung zwischen Microsoft und dem Lieferanten. Für Unternehmen, die als Auftragsverarbeiter oder Unterauftragsverarbeiter in Verbindung mit der Leistung tätig sind, muss der Vertrag in Bezug auf die personenbezogenen Daten von Microsoft den Gegenstand und die Dauer der Verarbeitung, die Art und den Zweck der Verarbeitung, die Art der personenbezogenen Daten von Microsoft und die Kategorien der betroffenen Personen sowie die Pflichten und Rechte von Microsoft enthalten.	Der Lieferant muss den geltenden Vertrag zwischen Microsoft und dem Lieferanten vorlegen. Für Auftragsverarbeiter und Unterauftragsverarbeiter sind die Verarbeitungsbeschreibungen in der jeweiligen Vereinbarung (*z.B.*, Leistungsbeschreibung, Bestellungen) enthalten. Anmerkung: Unternehmen mit dringenden Direktbestellungen können die notwendige Beschreibung der Verarbeitungstätigkeiten zu einem späteren Zeitpunkt im Kaufvorgang hinzufügen lassen.
2	Wenn Microsoft bestätigt, dass Ihre Aufträge die Rolle eines Unterauftragsverarbeiters erfüllen, muss der Lieferant entsprechende Datenschutzvereinbarungen mit Microsoft abgeschlossen haben. Anmerkung: Microsoft wird diese Bezeichnung in Ihrem Profil veröffentlichen, wenn dies der Fall ist.	Standardvertragsklauseln, Zusatzvereinbarung über Online-Kundendaten und/oder Zusatzvereinbarung über die Datenverarbeitung durch Lieferanten und Partner für professionelle Dienstleistungen.
3	Der Lieferant weist Verantwortung und Rechenschaftspflicht für die Einhaltung der DPR an eine bestimmte Person oder Gruppe innerhalb des Unternehmens zu.	Der Lieferant benennt die Rolle der Person oder Gruppe, die für die Einhaltung der DPR für Lieferanten von Microsoft verantwortlich ist. Ein Dokument, in dem die Befugnisse und die Verantwortlichkeit dieser Person oder Gruppe beschrieben werden, die eine Rolle im Bereich Datenschutz und/oder Sicherheit spielt.

#	Datenschutzanforderungen für Lieferanten von Microsoft	Nachweis der Einhaltung
	Abschnitt A: Verwaltung (Forts.)	
4	Einrichtung, Aufrechterhaltung und jährliche Durchführung von Datenschutz- und Sicherheitsschulungen für Mitarbeiter, die Zugang zu personenbezogenen Daten haben, die vom Lieferanten in Verbindung mit der Leistung oder vertraulichen Daten von Microsoft verarbeitet werden. Wenn das Unternehmen des Lieferanten keine vorbereiteten Inhalte hat, kann er diesen Storyboard-Entwurf verwenden und ihn für sein Unternehmen anpassen. Anmerkung: Von den Mitarbeitern der Lieferanten kann verlangt werden, zusätzliche Schulungen zu absolvieren, die von Abteilungen Microsoft angeboten werden.	Jährliche Anwesenheitsnachweise sind verfügbar und können Microsoft auf Anfrage zur Verfügung gestellt werden. Zu den Schulungsinhalten gehören Datenschutz- und Sicherheitsgrundsätze. Die Dokumentation der Einhaltung der Schulungsanforderungen umfasst Nachweise über die Schulung in Bezug auf die gesetzlichen Datenschutzanforderungen, die Sicherheitsverpflichtungen und die Einhaltung der geltenden vertraglichen Anforderungen und Verpflichtungen.
5	Der Lieferant verarbeitet personenbezogene Daten von Microsoft nur in Übereinstimmung mit den dokumentierten Anweisungen von Microsoft, einschließlich Szenarien in Bezug auf die Übermittlung personenbezogener Daten von Microsoft an ein Drittland oder eine internationale Organisation, es sei denn, dies ist gesetzlich vorgeschrieben; in einem solchen Fall muss der Verarbeiter oder Unterverarbeiter (Lieferant) den für die Verarbeitung Verantwortlichen (Microsoft) vor der Verarbeitung über diese gesetzliche Anforderung informieren, es sei denn, das Gesetz verbietet eine solche Information aus wichtigen Gründen des öffentlichen Interesses.	Der Lieferant stellt alle von Microsoft dokumentierten Anweisungen (z. B. Vereinbarung, Leistungsbeschreibung oder Auftragsdokumentation) zusammen und bewahrt sie elektronisch an einem Ort auf, der für die an der Leistung beteiligten Mitarbeitenden und Auftragnehmer des Lieferanten leicht zugänglich ist.
	Abschnitt B: Hinweis	
6	Der Lieferant muss die Microsoft-Datenschutzerklärung verwenden, wenn er personenbezogene Daten im Namen von Microsoft erfasst. Der Datenschutzhinweis muss deutlich erkennbar sein und den betroffenen Personen zur Verfügung stehen, um ihnen die Entscheidung zu erleichtern, ob sie ihre personenbezogenen Daten an den Lieferanten übermitteln möchten. Anmerkung: Wenn Ihr Unternehmen selbst der für die Verarbeitung Verantwortliche ist, setzen Sie Ihren eigenen Datenschutzhinweis ein.	Der Lieferant verwendet einen Weiterleitungslink zur aktuellen, veröffentlichten Microsoft-Datenschutzerklärung. Die Datenschutzerklärung wird in jedem Zusammenhang veröffentlicht, in dem personenbezogene Daten eines Nutzers erfasst werden. Gegebenenfalls ist eine Offline-Version verfügbar, die vor der Datenerhebung bereitgestellt wird. Alle offline verwendeten Datenschutzerklärungen entsprechen der neuesten veröffentlichten Version und sind ordnungsgemäß datiert. Für die Dienstleistungen für Mitarbeitende von Microsoft wird der Microsoft-Datenschutzhinweis verwendet.

7	Bei der Erhebung personenbezogener Daten von Microsoft über ein Live- oder aufgezeichnetes Telefongespräch müssen die Lieferanten darauf vorbereitet sein, mit den betroffenen Personen die geltenden Praktiken der Datenerhebung, -verarbeitung, -nutzung und -aufbewahrung zu besprechen.	Ein Skript für Sprachaufzeichnungen beinhaltet, wie personenbezogene Daten von Microsoft verarbeitet werden, und beinhaltet: ▪ die Erhebung, ▪ die Verwendung und ▪ die Aufbewahrung
	Abschnitt C: Entscheidungsmöglichkeit und Einwilligung	
8	Gegebenenfalls muss der Lieferant die Einwilligung der betroffenen Person für alle seine Verarbeitungstätigkeiten (einschließlich aller neuen und aktualisierten Verarbeitungstätigkeiten) einholen und aufzeichnen, bevor er die personenbezogenen Daten der betroffenen Person erfasst. Der Lieferant überwacht die Effektivität der Einstellungsverwaltung, um sicherzustellen, dass der Zeitrahmen für die Berücksichtigung einer Einstellungsänderung die restriktivste lokale gesetzliche Vorschrift ist, die gilt.	Der Lieferant kann darstellen, wie eine betroffene Person ihre Einwilligung für eine Verarbeitungstätigkeit erteilt und dass der Umfang der Einwilligung alle Verarbeitungstätigkeiten des Lieferanten in Bezug auf die personenbezogenen Daten der betroffenen Person abdeckt. Der Lieferant kann darstellen, wie eine betroffene Person ihre Zustimmung zu einer Verarbeitungstätigkeit zurückzieht. Der Lieferant kann darstellen, wie die Einstellungen vor dem Start einer neuen Verarbeitungsaktivität geprüft werden. Anmerkung: Der Nachweis kann in Form von Screenshots der Benutzerinteraktion, des Ausprobierens des Dienstes oder der Einsicht in die technische Dokumentation erbracht werden.
9	Lieferanten, die Microsoft-Websites und/oder -Anwendungen oder Websites erstellen und verwalten, auf denen Markenzeichen von Microsoft zu sehen sind, müssen den betroffenen Personen einen transparenten Hinweis auf die Verwendung von Cookies geben und ihnen eine Wahlmöglichkeit bieten, die mit den Verpflichtungen in der Microsoft-Datenschutzerklärung und den lokalen gesetzlichen Anforderungen im Einklang steht. Sofern die auftraggebende Geschäftseinheit nicht ausdrücklich etwas anderes verlangt, sollten die Lieferanten das von 1ES erstellte Standardbanner zur Verwaltung der Auswahlsteuerung verwenden. Diese Anforderung gilt für Websites, die sich an Nutzer in der Europäischen Union/dem Europäischen Wirtschaftsraum und anderen Regionen mit geltenden Datenschutzgesetzen richten, und überall dort, wo die Microsoft-Datenschutzerklärung verwendet wird. Anmerkung: Microsoft-Unternehmenssponsoren müssen Microsoft-Websites im internen Web-Compliance-Portal (http://aka.ms/wcp) registrieren, damit der Bestand an Cookies katalogisiert und verwaltet werden kann.	Der Zweck jedes Cookies muss dokumentiert und es muss Auskunft über die Art des eingesetzten Cookies gegeben werden. ▪ Dauerhafte Cookies dürfen nicht verwendet werden, wenn Sitzungscookies ausreichen. ▪ Wenn dauerhafte Cookies verwendet werden, dürfen sie nicht später als 13 Monate nach dem Besuch eines Nutzers auf der Website ablaufen. Der Lieferant weist die Einhaltung der geltenden EU-Rechtsvorschriften nach, etwa: ▪ die Verwendung der Kennzeichnungskonvention „Datenschutz und Cookies“ für die Datenschutzerklärung, ▪ die Einholung der Zustimmung der Nutzer, bevor „nicht notwendige“ Cookies für Zwecke wie Werbung verwendet werden, und ▪ die Geltungsdauer der Zustimmung darf höchstens 6 Monate betragen und muss spätestens bei deren Ablauf neu eingeholt werden.

#	Datenschutzanforderungen für Lieferanten von Microsoft	Nachweis der Einhaltung
	Abschnitt D: Erhebung	
10	Der Lieferant muss die Erfassung der personenbezogenen Daten und/oder vertraulichen Daten von Microsoft überwachen, um sicherzustellen, dass nur die für die Durchführung erforderlichen Daten erfasst werden.	Der Lieferant kann Unterlagen vorlegen, aus denen hervorgeht, dass die gesammelten personenbezogenen Daten und/oder vertraulichen Daten von Microsoft für die Durchführung benötigt werden. Der Lieferant wird Microsoft auf Anfrage entsprechende Nachweise vorlegen.
11	Vor der Erhebung von Daten von Kindern (gemäß der Definition in der jeweiligen Rechtsordnung) muss der Lieferant die Zustimmung gemäß den örtlichen Datenschutzgesetzen einholen.	Der Lieferant kann Unterlagen vorlegen, die die Zustimmung der Eltern/Erziehungsberechtigten belegen. Der Lieferant wird Microsoft auf Anfrage entsprechende Nachweise vorlegen.
	Abschnitt E: Aufbewahrung	
12	Es ist sicherzustellen, dass personenbezogene Daten und vertrauliche Daten von Microsoft nicht länger aufbewahrt werden, als es für die Durchführung erforderlich ist, es sei denn, eine weitere Aufbewahrung der personenbezogenen Daten und/oder vertraulichen Daten von Microsoft ist gesetzlich vorgeschrieben.	Der Lieferant hält die dokumentierten Aufbewahrungsrichtlinien oder die von Microsoft im Vertrag (z. B. Leistungsbeschreibung, Bestellung) festgelegten Aufbewahrungsanforderungen ein. Der Lieferant wird Microsoft auf Anfrage entsprechende Nachweise vorlegen.
13	Es ist sicherzustellen, dass nach dem alleinigen Ermessen von Microsoft personenbezogene und vertrauliche Daten von Microsoft, die sich im Besitz oder unter der Kontrolle des Lieferanten befinden, an Microsoft zurückgegeben oder nach Abschluss der Leistung oder auf Aufforderung von Microsoft vernichtet werden. Innerhalb von Anwendungen müssen Abläufe bestehen sein, die sicherstellen, dass Daten sicher gelöscht werden, wenn sie entweder explizit von den Nutzern oder aufgrund anderer Auslöser, wie dem Alter der Daten, aus der Anwendung entfernt werden. Wenn die Vernichtung personenbezogener oder vertraulicher Daten von Microsoft erforderlich ist, muss der Lieferant physische Objekte, die personenbezogene Daen und/oder vertrauliche Daten von Microsoft enthalten, verbrennen, pulverisieren oder schreddern, so dass die Informationen nicht gelesen oder rekonstruiert werden können.	Der Lieferant führt Aufzeichnungen über die Entsorgung personenbezogener Daten und vertraulicher Daten von Microsoft (dies kann die Rückgabe an Microsoft zur Vernichtung beinhalten). Wenn die Vernichtung erforderlich ist oder von Microsoft verlangt wird, legt der Lieferant eine von einem leitenden Angestellten des Lieferanten unterzeichnete Bescheinigung über die Vernichtung vor.

#	Datenschutzanforderungen für Lieferanten von Microsoft	Nachweis der Einhaltung
	Abschnitt F: Betroffene Personen	
	Betroffene Personen haben nach dem Gesetz bestimmte Rechte, darunter das Recht auf Zugang, Löschung, Bearbeitung, Export, Einschränkung und Widerspruch gegen die Verarbeitung ihrer personenbezogenen Daten („**Rechte der Betroffenen**“). Wenn eine betroffene Person ihre gesetzlichen Rechte in Bezug auf ihre personenbezogenen Daten von Microsoft ausüben möchte, muss der Lieferant Microsoft in die Lage versetzen, die folgenden Maßnahmen zu ergreifen oder diese Maßnahmen im Namen von Microsoft durchzuführen:	
14	Der Lieferant unterstützt Microsoft nach Möglichkeit durch geeignete technische und organisatorische Maßnahmen dabei, seinen Verpflichtungen nachzukommen, Anfragen von betroffenen Personen, die ihre Rechte ausüben möchten, ohne unangemessene Verzögerung zu beantworten. Sofern von Microsoft nicht anderweitig angewiesen, wird der Lieferant alle betroffenen Personen, die sich direkt an den Lieferanten wenden, an Microsoft verweisen, um ihre Rechte als betroffene Person auszuüben.	Der Lieferant führt einen Nachweis über dokumentierte Prozesse und Verfahren zur Unterstützung der Ausübung der Rechte der betroffenen Personen. Der Lieferant wird einen dokumentierten Nachweis über entsprechende Tests aufbewahren. Die Nachweise werden auf Anfrage von Microsoft durch den Lieferanten zur Verfügung gestellt.
15	Wenn der Lieferant sich direkt an die betroffene Person wendet oder einen Online-Selbstbedienungsmechanismus bereitstellt, verfügt er über Prozesse und Verfahren zur Identifizierung der betroffenen Person, die die Anfrage stellt.	Der Lieferant hat die Methode zur Identifizierung der von Microsoft betroffenen Personen dokumentiert. Der Lieferant wird Microsoft auf Anfrage entsprechende Nachweise vorlegen.
16	Wenn Microsoft darum bittet, personenbezogene Daten über eine betroffene Person zu finden, die nicht über einen Online-Selbstbedienungsmechanismus verfügbar sind, unternimmt der Lieferant angemessene Anstrengungen, um die angeforderten Daten zu finden, und bewahrt ausreichende Aufzeichnungen auf, um nachzuweisen, dass eine angemessene Suche durchgeführt wurde.	Der Lieferant führt einen dokumentierten Nachweis über die bestehenden Verfahren, um festzustellen, ob personenbezogene Daten von Microsoft gespeichert werden, und stellt Microsoft auf Anfrage die entsprechende Dokumentation zur Verfügung. Der Lieferant führt Aufzeichnungen, aus denen hervorgeht, welche Schritte er unternommen hat, um den Forderungen betroffener Personen nachzukommen. Diese Aufzeichnungen umfassen: ▪ Datum und Uhrzeit der Anfrage, ▪ Maßnahmen, die zur Beantwortung der Anfrage ergriffen wurden, und Aufzeichnungen darüber, wann Microsoft informiert wurde. Der Lieferant wird Microsoft auf Anfrage einen Nachweis über die Führung der Aufzeichnungen vorlegen.

#	Datenschutzanforderungen für Lieferanten von Microsoft	Nachweis der Einhaltung
	Abschnitt F: Betroffene Personen (Forts.)	
17	Der Lieferant teilt der betroffenen Person mit, welche Schritte sie unternehmen muss, um Zugang zu ihren personenbezogenen Daten von Microsoft zu erhalten oder ihre Rechte auf andere Weise auszuüben.	Der Lieferant bewahrt einen dokumentierten Nachweis über die Kommunikation und die Verfahren für den Zugang zu personenbezogenen Daten von Microsoft auf. Der Lieferant wird dokumentierte Nachweise aufbewahren und diese Microsoft auf Anfrage vorlegen.
18	Der Lieferant zeichnet Datum und der Uhrzeit von Anfragen zu den Rechten der betroffenen Personen und der Maßnahmen auf, die er als Reaktion auf diese Anfragen ergriffen hat. Wenn eine Anfrage abgelehnt wird, gibt der Lieferant der betroffenen Person auf Anweisung von Microsoft eine schriftliche Erklärung. Der Lieferant stellt Microsoft auf Anfrage Aufzeichnungen über Anfragen von Betroffenen zur Verfügung.	Der Lieferant bewahrt Aufzeichnungen über Anträge auf Zugang/Löschung auf und dokumentiert Änderungen, die an den personenbezogenen Daten von Microsoft vorgenommen wurden. Der Lieferant dokumentiert die Fälle, in denen Anträge abgelehnt werden, und bewahrt die Belege für die Prüfung und Genehmigung durch Microsoft auf. Der Lieferant weist nach, dass er Aufzeichnungen über Anfragen und Verweigerungen des Zugangs zu personenbezogenen Daten von Microsoft führt.
19	Der Lieferant muss Microsoft eine Kopie der angeforderten personenbezogenen Daten von Microsoft der authentifizierten betroffenen Person in einem geeigneten gedruckten, elektronischen oder mündlichen Format ermöglichen oder diese selbst erhalten.	Der Lieferant stellt der betroffenen Person die personenbezogenen Daten von Microsoft in einem verständlichen Format und in einer für die betroffene Person und den Lieferanten geeigneten Form zur Verfügung.
20	Der Lieferant muss angemessene Vorkehrungen treffen, um sicherzustellen, dass die an Microsoft oder eine authentifizierte betroffene Person freigegebenen personenbezogenen Daten von Microsoft nicht zur Identifizierung einer anderen Person verwendet werden können.	Der Lieferant führt einen dokumentierten Nachweis über die Verfahren im Zusammenhang mit den Vorkehrungen zur Vermeidung einer Identifizierung der betroffenen Person im Widerspruch zu den Vertragsbedingungen. Der Lieferant wird Microsoft auf Anfrage Nachweise vorlegen.
21	Wenn eine betroffene Person der Meinung ist, dass ihre personenbezogenen Daten von Microsoft nicht vollständig und richtig sind, muss der Lieferant das Problem an Microsoft weiterleiten und mit Microsoft zusammenarbeiten, um das Problem zu lösen.	Der Lieferant dokumentiert die Fälle von Unstimmigkeiten und leitet die Angelegenheit an Microsoft weiter. Der Lieferant wird Microsoft auf Anfrage entsprechende Nachweise vorlegen.

#	Datenschutzanforderungen für Lieferanten von Microsoft	Nachweis der Einhaltung
	Abschnitt G: Unterauftragnehmer	
	Beabsichtigt der Lieferant, einen Unterauftragnehmer mit der Verarbeitung personenbezogener Daten oder vertraulicher Daten von Microsoft zu beauftragen, muss der Lieferant:	
22	Der Lieferant informiert Microsoft vor der Vergabe von Unteraufträgen oder vor Änderungen bezüglich der Hinzufügung oder des Austauschs von Unterauftragnehmern. Anmerkung: Der Lieferant muss angeben, dass er diese Verpflichtung auch dann akzeptiert, wenn er derzeit keine Unterauftragnehmer einsetzt, dies aber in Zukunft tun könnte.	Lieferanten müssen sicherstellen, dass die personenbezogenen Daten von Microsoft nur von Unternehmen bearbeitet werden, die Microsoft bekannt sind, wie es im jeweiligen Vertrag (z. B. Leistungsbeschreibung, Nachtrag, Bestellung) verlangt wird oder in der SSPA-Datenbank erfasst ist. Der Lieferant kann seine Unterlieferantenliste online stellen und einen Link zu der Seite in der SSPA-Datenbank einfügen.
23	Lieferanten müssen Art und Umfang der personenbezogenen und vertraulichen Daten von Microsoft, die von Unterauftragnehmern weiterverarbeitet werden, dokumentieren, und sicherstellen, dass die erhobenen Informationen für die Durchführung erforderlich sind.	Der Lieferant führt eine Dokumentation über die personenbezogenen und vertraulichen Daten von Microsoft, die an Unterauftragnehmer weitergegeben oder übertragen werden. Der Lieferant wird Microsoft auf Anfrage entsprechende Nachweise vorlegen.
24	Wenn Microsoft für die Verarbeitung personenbezogener Daten von Microsoft verantwortlich ist, müssen Lieferanten sicherstellen, dass der Unterauftragnehmer personenbezogene Daten von Microsoft in Übereinstimmung mit den von der betroffenen Person angegebenen Kontakteinstellungen verwendet.	Der Lieferant muss zeigen, wie eine Microsoft-Datenschutzeinstellung von Unterauftragnehmern genutzt wird. Er muss Belege (z. B. Screenshots, SLA, Leistungsbeschreibung usw.) vorlegen, aus denen der Zeitrahmen hervorgeht, innerhalb dessen ein Unterauftragnehmer eine Änderung der Einstellungen anerkennen muss.
25	Der Lieferant muss die Verarbeitung personenbezogener Daten oder vertraulicher Daten von Microsoft durch den Unterauftragnehmer auf die Zwecke beschränken, die zur Erfüllung des Vertrags des Lieferanten mit Microsoft erforderlich sind.	Der Lieferant kann Unterlagen vorlegen, aus denen hervorgeht, dass die personenbezogenen Daten von Microsoft, die einem Unterauftragnehmer zur Verfügung gestellt werden, für die Durchführung erforderlich sind. Der Lieferant wird Microsoft auf Anfrage entsprechende Nachweise vorlegen.

#	Datenschutzanforderungen für Lieferanten von Microsoft	Nachweis der Einhaltung
	Abschnitt G: Unterauftragnehmer (Forts.)	
26	Der Lieferant muss Beschwerden auf Hinweise auf eine unbefugte oder unrechtmäßige Verarbeitung von personenbezogenen Daten von Microsoft überprüfen.	Der Lieferant kann nachweisen, dass er über Systeme und Verfahren verfügt, um Beschwerden über die unbefugte Nutzung oder Weitergabe von personenbezogenen Daten von Microsoft durch einen Unterauftragnehmer zu bearbeiten. Der Lieferant wird Microsoft auf Anfrage entsprechende Nachweise vorlegen.
27	Microsoft ist unverzüglich zu benachrichtigen, wenn der Lieferant erfährt, dass ein Unterauftragnehmer personenbezogene Daten oder vertrauliche Daten von Microsoft zu einem anderen als dem mit der Leistung verbundenen Zweck verarbeitet hat.	Der Lieferant hat den Unterauftragnehmern Anweisungen und Mittel zur Verfügung gestellt, um den Missbrauch von Daten von Microsoft zu melden. Der Lieferant wird Microsoft auf Anfrage entsprechende Nachweise vorlegen.
28	Wenn der Lieferant im Auftrag von Microsoft personenbezogene Daten von Dritten erhebt, muss der Lieferant sicherstellen, dass die Datenschutzrichtlinien und -praktiken der Dritten mit dem Vertrag des Lieferanten mit Microsoft und den DPR übereinstimmen.	Der Lieferant kann Unterlagen über die durchgeführte Due-Diligence-Prüfung der Datenschutzpolitik und -praktiken des Dritten vorlegen. Der Lieferant wird Microsoft auf Anfrage entsprechende Nachweise vorlegen.

29	Es müssen unverzügliche Maßnahmen zur Minderung eines tatsächlichen oder potenziellen Schadens ergriffen werden, der durch die unbefugte oder unrechtmäßige Verarbeitung personenbezogener und vertraulicher Daten von Microsoft durch einen Unterauftragnehmer verursacht wurde.	Der Lieferant ist verpflichtet, Nachweise über den Plan und das Verfahren aufzubewahren und Microsoft auf Anfrage einen Nachweis über die Dokumentation vorzulegen.
Abschnitt H: Qualität		
30	Der Lieferant muss die Integrität aller personenbezogenen Daten von Microsoft wahren und sicherstellen, dass sie für die angegebenen Zwecke, für die sie verarbeitet wurden, richtig, vollständig und relevant bleiben.	Der Lieferant kann nachweisen, dass es Verfahren zur Validierung der personenbezogenen Daten von Microsoft gibt, wenn diese erhoben, erstellt und aktualisiert werden. Der Lieferant kann nachweisen, dass Überwachungs- und Stichprobenverfahren vorhanden sind, um die Genauigkeit laufend zu überprüfen und bei Bedarf zu korrigieren. Der Lieferant wird Microsoft auf Anfrage entsprechende Nachweise vorlegen.

#	Datenschutzanforderungen für Lieferanten von Microsoft	Nachweis der Einhaltung
	Abschnitt I: Überwachung und Durchsetzung	
31	Der Lieferant verfügt über einen Notfallplan, der den Lieferanten verpflichtet, Microsoft gemäß den vertraglichen Anforderungen oder unverzüglich, je nachdem, was früher eintritt, zu benachrichtigen, sobald er von einem Datenvorfall Kenntnis erhält. Der Lieferant muss auf Aufforderung oder Anweisung von Microsoft mit Microsoft bei der Untersuchung, Abschwächung oder Behebung des Vorfalls zusammenarbeiten, einschließlich der Bereitstellung von Daten, Informationen, Zugang zu Personal des Lieferanten oder Hardware, die für die Durchführung einer forensischen Untersuchung erforderlich sind. Anmerkung: Wie Lieferanten Microsoft über einen Vorfall informieren müssen, ist im Leitfaden zum SSPA-Programm beschrieben.	Der Lieferant verfügt über einen Plan zur Reaktion auf Vorfälle, der einen Schritt zur Benachrichtigung der Kunden (Microsoft) enthält, wie in diesem Abschnitt beschrieben. Der Lieferant wird Microsoft auf Anfrage entsprechende Nachweise vorlegen.
32	Der Lieferant setzt einen Plan zur Abhilfe und Überwachung der Lösung jedes Datenvorfalls durch, um sicherzustellen, dass rechtzeitig geeignete Abhilfemaßnahmen ergriffen werden.	Der Lieferant verfügt über dokumentierte Verfahren, mit denen er auf einen Datenvorfall bis zur Schließung reagiert. Der Lieferant wird Microsoft auf Anfrage entsprechende Nachweise vorlegen.
33	Wenn Microsoft für die Verarbeitung personenbezogener Daten von Microsoft verantwortlich ist, richtet der Lieferant ein formelles Beschwerdeverfahren ein, um auf alle Datenschutzbeschwerden zu reagieren, die personenbezogene Daten von Microsoft betreffen.	Der Lieferant verfügt über Mittel zur Entgegennahme von Beschwerden, die personenbezogene Daten von Microsoft betreffen, und hat ein dokumentiertes Beschwerdeverfahren zur Behandlung von Beschwerden. Der Lieferant wird Microsoft auf Anfrage entsprechende Nachweise vorlegen.

#	Datenschutzanforderungen für Lieferanten von Microsoft	Nachweis der Einhaltung
	Abschnitt J: Sicherheit	
	Der Lieferant muss ein Informationssicherheitsprogramm einrichten, umsetzen und aufrechterhalten, das Richtlinien und Verfahren zum Schutz und zur sicheren Aufbewahrung der personenbezogenen Daten und vertraulichen Daten von Microsoft in Übereinstimmung mit der guten Branchenpraxis und gemäß den gesetzlichen Bestimmungen umfasst. Das Sicherheitsprogramm des Lieferanten muss die unten aufgeführten Standards, die Anforderungen 34–50, erfüllen.	Eine gültige ISO 27001-Zertifizierung ist ein akzeptabler Ersatz für Abschnitt J. Lieferanten können sich an das SSPA wenden, um diesen Ersatz zu beantragen. Anmerkung: Lieferanten müssen die Bescheinigung vorlegen.
34	Lieferanten müssen jährliche Netzsicherheitsbewertungen durchführen, die Folgendes umfassen: ▪ Überprüfung größerer Änderungen an der Umgebung, wie z. B. eine neue Systemkomponente, Netztopologie, Firewall-Regeln, ▪ Durchführung von Schwachstellen-Scans und ▪ Führung von Änderungsprotokollen.	Der Lieferant verfügt über dokumentierte Netzwerkbewertungen, Änderungsprotokolle und Scan-Ergebnisse. Die geforderten Änderungsprotokolle müssen Änderungen nachverfolgen, Informationen über den Grund für die Änderung liefern und den Namen und Titel des designierten Genehmigers enthalten.
35	Der Lieferant muss eine Richtlinie für mobile Geräte definieren, kommunizieren und implementieren, die die Nutzung von personenbezogenen Daten oder vertraulichen Daten von Microsoft, auf die über ein mobiles Gerät zugegriffen wird, sichert und einschränkt.	Der Lieferant weist nach, dass er eine konforme Richtlinie für mobile Geräte verwendet, wenn die Verarbeitung personenbezogener oder vertraulicher Daten von Microsoft die Verwendung eines mobilen Geräts erfordert.
36	Alle Geräte, die zur Unterstützung der Leistung eingesetzt werden, müssen verbucht werden und einen konkreten Verantwortlichen haben. Der Lieferant ist dafür verantwortlich, ein Inventar dieser Informationsbestände zu führen, die zulässige und genehmigte Nutzung der Bestände festzulegen und das angemessene Schutzniveau für die Bestände während ihres gesamten Lebenszyklus zu gewährleisten.	Inventar der zur Unterstützung der Leistung verwendeten Geräte. Das Inventar dieser Geräte muss Folgendes umfassen: ▪ Standort des Geräts, ▪ Datenklassifizierung der Daten auf dem Gerät, ▪ Aufzeichnungen über die Rückgabe von Geräten bei Beendigung des Arbeitsverhältnisses oder der Geschäftsvereinbarung und ▪ Aufzeichnungen über die Entsorgung von Datenträgern, wenn diese nicht mehr benötigt werden.

#	Datenschutzanforderungen für Lieferanten von Microsoft	Nachweis der Einhaltung
	Abschnitt J: Sicherheit (Forts.)	
37	Einführung und Aufrechterhaltung von Verfahren zur Verwaltung von Zugriffsrechten, um unbefugten Zugriff auf personenbezogene Daten oder vertrauliche Daten von Microsoft unter der Kontrolle des Lieferanten zu verhindern.	Der Lieferant weist nach, dass er einen Plan zur Verwaltung der Zugriffsrechte eingeführt hat, der Folgendes umfasst: ▪ Verfahren zur Zugangskontrolle, ▪ Identifizierungsverfahren, ▪ Sperrverfahren nach erfolglosen Versuchen, ▪ robuste Parameter für die Auswahl von Authentifizierungsnachweisen, ▪ Deaktivierung von Nutzerkonten bei Beendigung des Arbeitsverhältnisses innerhalb von 48 Stunden und ▪ strenge Passwortkontrollen, die die Länge und Komplexität von Passwörtern erzwingen und deren Wiederverwendung verhindern, Der Lieferant weist nach, dass er über ein etabliertes Verfahren zur Überprüfung des Benutzerzugriffs auf personenbezogene Daten und vertrauliche Daten von Microsoft verfügt, das den Grundsatz des geringsten Privilegs durchsetzt. Der Prozess umfasst: ▪ klar definierte Benutzerrollen, ▪ Verfahren zur Überprüfung und Rechtfertigung der Genehmigung des Zugriffs auf Rollen, und ▪ Tests, dass Benutzer in Rollen mit Zugriff auf Microsoft-Daten eine dokumentierte Begründung für ihre Zugehörigkeit zu der Gruppe/Rolle haben.
38	Der Lieferant definiert und implementiert Verfahren zur Patch-Verwaltung, die Sicherheitspatches für Systeme, die zur Verarbeitung personenbezogenen Daten oder vertraulicher Daten von Microsoft verwendet werden, Priorität einräumen. Diese Verfahren umfassen: ▪ einen definierter Risikoansatz zur Priorisierung von Sicherheitspatches, ▪ die Fähigkeit zur Handhabung und Umsetzung von Notfallpatches, ▪ die Anwendbarkeit auf Betriebssysteme und Serversoftware wie Anwendungsserver und Datenbanksoftware, ▪ die Dokumentation aller Risiken, die durch den Patch gemindert werden, und alle Ausnahmen zu verfolgen, und die Anforderungen für die Ausmusterung von Software, die von der Herstellerfirma nicht mehr unterstützt wird.	Der Lieferant kann ein implementiertes Patch-Management-Verfahren nachweisen, das diese Anforderung erfüllt und mindestens die folgenden Punkte abdeckt: ▪ Zuweisung des Schweregrads als Grundlage für die Prioritätensetzung. (Schweregraddefinitionen sind dokumentiert.) ▪ Dokumentiertes Verfahren zur Implementierung von Notfall-Patches. ▪ Der Lieferant stellt sicher, dass keine Betriebssysteme verwendet werden, die von der Herstellerfirma nicht mehr unterstützt werden. ▪ Patch-Management-Aufzeichnungen, die Genehmigungen und Ausnahmen verfolgen.
39	Der Lieferant installiert Anti-Virus- und Anti-Malware-Software auf Geräten, die mit dem Netzwerk verbunden	Es gibt Aufzeichnungen, die belegen, dass Antiviren- und Anti-Malware-Software aktiv eingesetzt wird.

#	Datenschutzanforderungen für Lieferanten von Microsoft	Nachweis der Einhaltung
	Abschnitt J: Sicherheit (Forts.)	
	sind, das zur Verarbeitung personenbezogener Daten und vertraulicher Daten von Microsoft verwendet wird, einschließlich Servern, Produktions- und Schulungsdesktops, um sich vor potenziell schädlichen Viren und bösartigen Softwareanwendungen zu schützen. Der Lieferant aktualisiert die Anti-Malware-Definitionen täglich oder gemäß den Anweisungen des Anti-Viren-/Anti-Malware-Anbieters. Anmerkung: Dies gilt für alle Betriebssysteme einschließlich Linux.	Anmerkung: Diese Anforderung gilt für alle Betriebssysteme.
40	Lieferanten, die Software für Microsoft entwickeln, müssen die Grundsätze des „Security-by-Design“ in den Erstellungsprozess einbeziehen.	Die technischen Spezifikationen der Lieferanten enthalten Kontrollpunkte für die Sicherheitsvalidierung in ihren Entwicklungszyklen.
41	Lieferanten setzen ein Programm zur Verhinderung von Datenverlusten („**DLP**“) ein, um Eindringlinge, Verluste und andere nicht autorisierte Aktivitäten zu verhindern. Daten müssen ordnungsgemäß klassifiziert, gekennzeichnet und geschützt werden, und der Lieferant muss die verwendeten Informationssysteme, in denen personenbezogene Daten oder vertrauliche Daten von Microsoft verarbeitet werden, auf Eindringen, Verlust und andere unbefugte Aktivitäten überwachen. Das DLP-Programm verlangt mindestens: ▪ die Verwendung von branchenüblichen Host-, Netzwerk- und Cloud-basierten Intrusion Detection Systemen („**IDS“**), wenn der Lieferant personenbezogene Daten oder vertrauliche Daten von Microsoft speichert, ▪ erfordert die Implementierung fortgeschrittener Schutzsysteme vor Eindringlingen („**IPS**“), die so konfiguriert sind, dass sie Datenverluste überwachen und aktiv verhindern, ▪ für den Fall, dass in ein System eingebrochen wird, eine Analyse des Systems, um sicherzustellen, dass alle verbleibenden Schwachstellen ebenfalls beseitigt werden, ▪ die Beschreibung der erforderlichen Verfahren zur Überwachung von Werkzeugen zur Erkennung von Systemkompromittierungen, ▪ die Einrichtung eines Verfahrens für die Reaktion auf Vorfälle und das Management von Vorfällen, das bei Feststellung eines Datenvorfalls durchgeführt werden muss, und	Ein dokumentiertes DLP-Programm mit Verfahren zur Verhinderung von Eindringlingen, Verlusten und anderen unbefugten Aktivitäten (und mindestens allen in diesem Abschnitt genannten Punkten).

#	Datenschutzanforderungen für Lieferanten von Microsoft	Nachweis der Einhaltung
	Abschnitt J: Sicherheit (Forts.)	
	▪ verlangt Mitteilungen (an alle Mitarbeiter des Lieferanten und Unterauftragnehmer, die von der Leistung des Lieferanten abgezogen werden) über das unbefugte Herunterladen und die Verwendung von personenbezogenen Daten oder vertraulichen Daten von Microsoft.	
42	Der Lieferant muss Untersuchungsergebnisse aus der Reaktion auf Vorfälle unverzüglich an die Geschäftsleitung und an Microsoft weiterleiten.	Es müssen Systeme und Prozesse vorhanden sein, um Microsoft die Ergebnisse der Untersuchung von Zwischenfällen mitzuteilen.
43	Systemadministratoren, Betriebspersonal, Management und Dritte müssen jährlich eine Sicherheitsschulung absolvieren.	Der Lieferant etabliert ein Sicherheitstrainingsprogramm, das Folgendes umfasst: ▪ jährliche Schulungen zur Reaktion auf Zwischenfälle und ▪ simulierte Ereignisse und automatisierte Mechanismen, die eine wirksame Reaktion auf Krisensituationen erleichtern. ▪ Der Lieferant sensibilisiert für die Vorbeugung von Vorfällen, z. B. für die mit dem Herunterladen von Schadsoftware verbundenen Risiken.
44	Der Lieferant muss sicherstellen, dass die Backup-Planungsprozesse die personenbezogenen Daten und vertraulichen Daten von Microsoft vor unbefugter Nutzung, Zugriff, Offenlegung, Änderung und Zerstörung schützen.	Der Lieferant kann dokumentierte Reaktions- und Wiederherstellungsprozeduren vorweisen, aus denen hervorgeht, wie die Organisation mit einer Störung umgeht und ihre Informationssicherheit auf der Grundlage der vom Management genehmigten Ziele für die Kontinuität der Informationssicherheit auf einem vorher festgelegten Niveau aufrechterhält. Der Lieferant kann nachweisen, dass er Verfahren zur regelmäßigen Sicherung, sicheren Aufbewahrung und effektiven Wiederherstellung kritischer Daten definiert und umgesetzt hat.
45	Erstellung und Prüfung von Plänen zur Geschäftskontinuität und zur Notfallwiederherstellung.	Ein Notfallwiederherstellungsplan muss Folgendes enthalten: ▪ definierte Kriterien, um festzustellen, ob ein System für den Geschäftsbetrieb des Lieferanten kritisch ist. ▪ die Auflistung kritischer Systeme auf der Grundlage der festgelegten Kriterien, die im Katastrophenfall wiederhergestellt werden müssen. ▪ ein definiertes Notfallwiederherstellungsverfahren für jedes kritische System, das sicherstellt, dass ein Ingenieur, der das System nicht kennt, die Anwendung in weniger als 72 Stunden wiederherstellen kann.

#	Datenschutzanforderungen für Lieferanten von Microsoft	Nachweis der Einhaltung
	Abschnitt J: Sicherheit (Forts.)	
		▪ jährliche (oder häufigere) Tests und Überprüfungen von Notfallplänen, um sicherzustellen, dass die Wiederherstellungsziele erreicht werden können.
46	Der Lieferant authentifiziert die Identität einer Person, bevor er dieser Person Zugang zu personenbezogenen Daten oder vertraulichen Daten von Microsoft gewährt und stellt sicher, dass der Zugang auf den Tätigkeitsbereich der jeweiligen Person beschränkt ist, der zur Unterstützung der Leistung zulässig ist.	Der Lieferant vergewissert sich, dass alle Benutzer-IDs eindeutig sind und dass für jede eine Standard-Authentifizierungsmethode wie Azure Active Directory verwendet wird. Für den erweiterten Zugang (administrative oder andere Arten von erweiterten Rechten) muss ein zweiter Faktor verwendet werden, z. B. eine Smartcard oder ein telefonbasierter Authentifikator. Dokumentiertes Informationssicherheitsprogramm, das Verfahren umfasst, mit denen sichergestellt wird, dass alle Mitarbeiter von Zulieferern und Unterauftragnehmern nicht mehr oder länger Zugang zu personenbezogenen Daten oder vertraulichen Daten von Microsoft haben, als zur Unterstützung der Leistung erforderlich ist.
47	Der Lieferant muss alle im Zusammenhang mit seiner Leistung verarbeiteten Daten bei der Übertragung über Netze durch Verschlüsselung mit Transport Layer Security („**TLS**“) oder Internet Protocol Security („**IPsec**“) schützen. Diese Methoden sind in den NIST 800-52 und NIST 800-57 beschrieben; es kann auch ein entsprechender Industriestandard verwendet werden. Der Lieferant muss die Übermittlung personenbezogener Daten oder vertraulicher Daten von Microsoft auf unverschlüsseltem Wege ablehnen.	Das Verfahren zum Erstellen, Bereitstellen und Ersetzen von TLS- oder anderen Zertifikaten muss definiert und durchgesetzt werden.
48	Alle Geräte des Lieferanten (Laptops, Workstations usw.), von denen auf personenbezogene Daten oder vertrauliche Daten von Microsoft zugegriffen oder die von dort aus verarbeitet werden, müssen eine festplattenbasierte Verschlüsselung verwenden.	Der Lieferant verschlüsselt alle Geräte gemäß BitLocker oder einer anderen branchenüblichen Festplattenverschlüsselungslösung für alle Client-Geräte, die zur Verarbeitung personenbezogener Daten oder vertraulicher Daten von Microsoft verwendet werden.
49	Es müssen Systeme und Verfahren (unter Verwendung aktueller Industriestandards wie dem im Standard **NIST 800-111** beschriebenen) vorhanden sein, um alle ruhenden personenbezogenen Daten und/oder vertraulichen Daten von Microsoft (wenn sie gespeichert werden) zu verschlüsseln; Beispiele hierfür sind unter anderem:	Der Lieferant überprüft, ob die ruhenden personenbezogenen Daten und vertraulichen Daten von Microsoft verschlüsselt sind.

#	Datenschutzanforderungen für Lieferanten von Microsoft	Nachweis der Einhaltung
	Abschnitt J: Sicherheit (Forts.)	
	▪ Anmeldedaten (z. B. Benutzername/Passwörter) ▪ Daten zu Zahlungsmitteln (z. B. Kreditkarten- und Kontonummern) ▪ einwanderungsrechtliche personenbezogene Daten ▪ medizinische Profildaten (z. B. Krankenaktennummern oder biometrische Marker oder Identifikatoren wie DNA, Fingerabdrücke, Netzhaut- und Irisabdrücke, Stimmmuster, Gesichtsmuster und Handmaße, die zu Authentifizierungszwecken verwendet werden) ▪ behördlich vergebene Identifizierungsdaten (z. B. Sozialversicherungs- oder Führerscheinnummern) ▪ Daten von Microsoft-Kunden (z. B. SharePoint, O365-Dokumente, OneDrive-Kunden) ▪ Material im Zusammenhang mit unangekündigten Microsoft-Produkten ▪ Geburtsdatum ▪ Profilinformationen für Kinder ▪ geografische Daten in Echtzeit ▪ persönliche (nicht geschäftliche) Postanschrift ▪ persönliche (nicht geschäftliche) Telefonnummern ▪ Religion ▪ politische Meinungen ▪ sexuelle Orientierung/Präferenz ▪ Antworten auf Sicherheitsfragen (z. B. Zwei-Faktor-Authentifizierung, Passwort-Reset) ▪ Mädchenname der Mutter	
50	Der Lieferant anonymisiert alle personenbezogenen Daten von Microsoft, die in einer Entwicklungs- oder Testumgebung verwendet werden.	Personenbezogene Daten von Microsoft dürfen nicht in Entwicklungs- oder Testumgebungen verwendet werden; wenn es keine Alternative gibt, müssen sie anonymisiert werden, um die Identifizierung der betroffenen Personen oder den Missbrauch personenbezogener Daten zu verhindern. Anmerkung: Anonymisierte Daten unterscheiden sich von pseudonymisierten Daten. Anonymisierte Daten sind Daten, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, wenn die betroffene Person der personenbezogenen Daten nicht oder nicht mehr identifizierbar ist.

Glossar

„Bevollmächtigter“ ist eine Person, die die entsprechende Befugnis hat, im Namen des Unternehmens zu unterschreiben. Diese Person verfügt über die erforderlichen Kenntnisse im Bereich des Datenschutzes und der Sicherheit oder hat vor der Einreichung ihrer Antwort auf eine Aktion des SSPA-Programms einen Fachexperten konsultiert. Mit der Unterzeichnung eines SSPA-Formulars bestätigen sie zudem, dass sie die Datenschutzbestimmungen gelesen und verstanden haben.

„EUDPR“ bezeichnet die Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union und zum freien Datenverkehr sowie zur Aufhebung der Verordnung (EG) Nr. 45/2001 und der Entscheidung Nr. 1247/2002/EG.

„Freelancer“ bezeichnet Personen, die Aufgaben oder Dienstleistungen auf Abruf ausführen, die über digitale Plattformen oder andere Mittel vermittelt werden.

„**DSGVO**“ bezeichnet die Vorschrift (EU) 2016/679 des Europäischen Parlaments und des Rats vom 27. April 2016 über den Schutz natürlicher Personen bezüglich der Verarbeitung personenbezogener Daten und der freien Bewegung solcher Daten, die die Direktive 95/46/EC aufhebt (Datenschutz-Grundanforderungen);

„Datenschutzanforderungen“ bedeutet die DSGVO, die EUDPR, lokale EU/EWR-Datenschutzgesetze, das kalifornische Verbraucherschutzgesetz, Cal. Civ. Code § 1798.100 et seq. (*„CCPA“*), den UK Data Protection Act 2018 und alle damit zusammenhängenden oder nachfolgenden Gesetze, Verordnungen und sonstigen rechtlichen Anforderungen, die im Vereinigten Königreich gelten, sowie alle anwendbaren Gesetze, Verordnungen und sonstigen rechtlichen Anforderungen in Bezug auf (a) Datenschutz und Datensicherheit; oder (b) die Verwendung, Erhebung, Aufbewahrung, Speicherung, Sicherheit, Offenlegung, Übertragung, Entsorgung und sonstige Verarbeitung personenbezogener Daten.

„EU-Modellklauseln“ und „Standardvertragsklauseln“ bezeichnet (i) die Standarddatenschutzklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern, die kein angemessenes Datenschutzniveau gewährleisten, wie in Artikel 46 DSGVO beschrieben und durch den Beschluss (EU) 2021/914 der Europäischen Kommission vom 4. Juni 2021 genehmigt; (ii) alle Nachfolge-Standardvertragsklauseln, die (a) von der Europäischen Kommission, (b) vom Europäischen Datenschutzbeauftragten und von der Europäischen Kommission genehmigt, (c) vom Vereinigten Königreich gemäß dem UK General Federal Data Protection Act, (d) von der Schweiz gemäß dem Schweizerischen Bundesgesetz über den Datenschutz oder (e) von einer Regierung in einer anderen Rechtsordnung als der Schweiz, dem Vereinigten Königreich und den Rechtsordnungen der Europäischen Union/des Europäischen Wirtschaftsraums, in denen die Klauseln die internationale Übermittlung personenbezogener Daten regeln, angenommen wurden. Sie werden aufgenommen und haben für den Lieferanten ab dem Tag ihrer Annahme Bindungswirkung.

„Website-Hosting“ Ein Website-Hosting-Dienst ist ein Online-Dienst, der im Auftrag von Microsoft Websites unter der Microsoft-Domäne erstellt und/oder pflegt, d. h. der Lieferant stellt alle Materialien und Dienste zur Verfügung, die zur Erstellung und Pflege einer Website erforderlich sind, und macht sie im Internet zugänglich. Der „Web-Hosting-Dienstleister“ oder „Web-Host“ ist der Lieferant, der die Instrumente und Dienste bereitstellt, die für die Anzeige der Website oder Webseite im Internet erforderlich sind, wie z. B. Cookies oder Web-Beacons für Werbung.