SLASCONE

Auftragsverarbeitungsvertrag (AVV)

März 2026

PRÄAMBEL

Diese Vereinbarung zur Auftragsverarbeitung („AVV“) ist Bestandteil des Vertrags zwischen der SLASCONE GmbH („Anbieter“ oder „Auftragsverarbeiter“) und dem in dem jeweils anwendbaren Bestellformular, Angebot, Kostenvoranschlag, der Auftragsbestätigung, der Testbestätigung oder einer sonstigen schriftlichen Vereinbarung bezeichneten Kunden („Kunde“ oder „Verantwortlicher“) und wird in diesen einbezogen.

Diese AVV gilt, soweit der Anbieter im Zusammenhang mit den Leistungen personenbezogene Daten im Auftrag des Kunden verarbeitet.

1. DEFINITIONEN UND ANWENDUNGSBEREICH

1.1 Soweit in dieser AVV nicht anders definiert, haben großgeschriebene Begriffe die ihnen im Vertrag zugewiesene Bedeutung. Die Begriffe „personenbezogene Daten“, „Verarbeitung“, „Verantwortlicher“, „Auftragsverarbeiter“, „betroffene Person“, „Verletzung des Schutzes personenbezogener Daten“ und „Aufsichtsbehörde“ haben die ihnen in der DSGVO zugewiesene Bedeutung.

1.2 Diese AVV regelt die Verarbeitung personenbezogener Daten durch den Anbieter im Auftrag des Kunden im Zusammenhang mit den Leistungen nach dem Vertrag.

1.3 Im Verhältnis der Parteien zueinander handelt der Kunde hinsichtlich der im Rahmen dieser AVV im Auftrag des Kunden verarbeiteten personenbezogenen Daten als Verantwortlicher und der Anbieter als Auftragsverarbeiter, sofern das anwendbare Datenschutzrecht für eine bestimmte Verarbeitungstätigkeit nichts anderes verlangt.

1.4 Im Falle eines Widerspruchs zwischen dieser AVV und dem Vertrag geht diese AVV insoweit vor, als der Widerspruch die Verarbeitung personenbezogener Daten im Auftrag des Kunden betrifft.

2. GEGENSTAND, DAUER, ART UND ZWECK DER VERARBEITUNG

2.1 Gegenstand der Verarbeitung ist die Erbringung der Leistungen durch den Anbieter für den Kunden nach dem Vertrag.

2.2 Diese AVV bleibt so lange in Kraft, wie der Anbieter nach dem Vertrag personenbezogene Daten im Auftrag des Kunden verarbeitet.

2.3 Art und Zweck der Verarbeitung sowie die Kategorien betroffener Personen und die Kategorien personenbezogener Daten sind in ANLAGE A beschrieben.

3. WEISUNGEN DES KUNDEN

3.1 Der Anbieter verarbeitet personenbezogene Daten nur auf dokumentierte Weisungen des Kunden, sofern er nicht durch anwendbares Recht, dem er unterliegt, zu einer anderen Verarbeitung verpflichtet ist. Der Vertrag, diese AVV sowie die Nutzung und Konfiguration der Leistungen durch den Kunden stellen die vollständigen und dokumentierten Weisungen des Kunden zum Zeitpunkt des Inkrafttretens dieser AVV dar.

3.2 Der Kunde kann dem Anbieter zusätzliche angemessene dokumentierte Weisungen erteilen, sofern diese Weisungen:
a) mit dem Vertrag und dieser AVV im Einklang stehen;
b) für die Einhaltung des anwendbaren Datenschutzrechts durch den Kunden erforderlich sind; und
c) technisch umsetzbar sind.
Der Anbieter kann Weisungen ablehnen, die rechtswidrig, technisch nicht umsetzbar oder wesentlich außerhalb des vereinbarten Leistungsumfangs liegen. Für die Umsetzung zusätzlicher Weisungen, die außerhalb des üblichen Leistungsumfangs liegen, kann der Anbieter eine angemessene zusätzliche Vergütung verlangen.

3.3 Ist der Anbieter der Auffassung, dass eine Weisung des Kunden gegen das anwendbare Datenschutzrecht verstößt, wird er den Kunden unverzüglich hierüber informieren. Der Anbieter kann die Ausführung der betreffenden Weisung aussetzen, bis der Kunde diese bestätigt oder anpasst.

3.4 Soweit der Anbieter nach anwendbarem Recht verpflichtet ist, personenbezogene Daten anders als nach Weisung des Kunden zu verarbeiten, wird er den Kunden vor der Verarbeitung über diese rechtliche Verpflichtung informieren, sofern das betreffende Recht eine solche Information nicht aus wichtigen Gründen des öffentlichen Interesses untersagt.

4. PFLICHTEN DES AUFTRAGSVERARBEITERS

4.1 Der Anbieter stellt sicher, dass die von ihm zur Verarbeitung personenbezogener Daten befugten Personen:

a) Vertraulichkeitsverpflichtungen unterliegen oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterstehen; und

b) nur insoweit auf personenbezogene Daten zugreifen, als dies für die Durchführung des Vertrags erforderlich ist und den dokumentierten Weisungen des Kunden entspricht.

4.2 Der Anbieter setzt geeignete technische und organisatorische Maßnahmen um und hält diese aufrecht, um personenbezogene Daten gegen zufällige oder unrechtmäßige Zerstörung, Verlust, Veränderung, unbefugte Offenlegung oder unbefugten Zugang zu schützen, wobei der Stand der Technik, die Implementierungskosten, die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die Risiken für die Rechte und Freiheiten natürlicher Personen berücksichtigt werden.

Die zum Zeitpunkt des Inkrafttretens dieser AVV geltenden technischen und organisatorischen Maßnahmen sind in ANLAGE C beschrieben.

4.3 Der Anbieter kann die technischen und organisatorischen Maßnahmen von Zeit zu Zeit aktualisieren oder ändern, sofern solche Änderungen das allgemeine Sicherheitsniveau für die von dieser AVV erfasste Verarbeitung nicht wesentlich verringern.

4.4 Unter Berücksichtigung der Art der Verarbeitung wird der Anbieter den Kunden in angemessenem Umfang durch geeignete technische und organisatorische Maßnahmen, soweit möglich, dabei unterstützen, Anfragen zur Ausübung der Rechte betroffener Personen nach dem anwendbaren Datenschutzrecht zu beantworten.

Erhält der Anbieter unmittelbar von einer betroffenen Person einen Antrag in Bezug auf personenbezogene Daten, die im Auftrag des Kunden verarbeitet werden, wird der Anbieter diesen Antrag, sofern dies nicht rechtlich untersagt ist, unverzüglich an den Kunden weiterleiten. Der Anbieter wird auf einen solchen Antrag nur auf dokumentierte Weisung des Kunden oder soweit gesetzlich erforderlich antworten.

4.5 Unter Berücksichtigung der Art der Verarbeitung und der dem Anbieter zur Verfügung stehenden Informationen wird der Anbieter den Kunden in angemessenem Umfang bei der Erfüllung der Pflichten des Kunden nach den Artikeln 32 bis 36 DSGVO unterstützen, insbesondere in Bezug auf:

a) die Sicherheit der Verarbeitung;

b) die Meldung und Behandlung von Verletzungen des Schutzes personenbezogener Daten;

c) Datenschutz-Folgenabschätzungen; und

d) vorherige Konsultationen mit Aufsichtsbehörden.

4.6 Der Anbieter wird den Kunden unverzüglich informieren, nachdem er Kenntnis von einer Verletzung des Schutzes personenbezogener Daten erlangt hat, die personenbezogene Daten betrifft, die im Auftrag des Kunden verarbeitet werden.
Soweit dem Anbieter verfügbar, umfasst eine solche Mitteilung:
a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, einschließlich, soweit möglich, der Kategorien und der ungefähren Anzahl betroffener Personen und betroffener Datensätze;
b) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
c) die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und zur Abmilderung ihrer möglichen nachteiligen Auswirkungen; und
d) die Kontaktdaten einer Ansprechperson, bei der weitere Informationen eingeholt werden können.
Der Anbieter kann die Informationen schrittweise bereitstellen, wenn es nicht möglich ist, alle Informationen gleichzeitig zur Verfügung zu stellen.

4.7 Der Anbieter wird dem Kunden alle Informationen zur Verfügung stellen, die vernünftigerweise erforderlich sind, um die Einhaltung der Verpflichtungen des Anbieters aus dieser AVV und dem anwendbaren Datenschutzrecht nachzuweisen.

4.8 Der Anbieter wird personenbezogene Daten nicht verkaufen und sie nicht zu eigenen Zwecken verarbeiten, außer:
a) soweit dies zur Erbringung der Leistungen nach dem Vertrag und den Weisungen des Kunden erforderlich ist;
b) soweit dies nach anwendbarem Recht erforderlich ist; oder
c) soweit dies nach dem anwendbaren Datenschutzrecht anderweitig zulässig ist, wenn der Anbieter für eine solche spezifische Verarbeitungstätigkeit als eigenständiger Verantwortlicher handelt.

5. PFLICHTEN DES KUNDEN

5.1 Der Kunde ist für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten nach dem Vertrag verantwortlich, insbesondere für:
a) das Vorliegen einer geeigneten Rechtsgrundlage;
b) die Rechtmäßigkeit der Offenlegung personenbezogener Daten an den Anbieter;
c) die Rechtmäßigkeit der Weisungen des Kunden an den Anbieter; und
d) die Einhaltung der Transparenz- und Informationspflichten des Kunden gegenüber betroffenen Personen.

5.2 Der Kunde ist für die Richtigkeit, Qualität und Rechtmäßigkeit der dem Anbieter bereitgestellten personenbezogenen Daten verantwortlich und dafür, dass er den Anbieter nicht anweist, personenbezogene Daten über das für die Zwecke des Vertrags Erforderliche hinaus zu verarbeiten.

5.3 Der Kunde ist dafür verantwortlich, die Leistungen in einer Weise zu konfigurieren und zu nutzen, die mit dem anwendbaren Datenschutzrecht im Einklang steht, insbesondere im Hinblick auf Benutzerzugriffe, Aufbewahrungseinstellungen und Löschanfragen.

5.4 Der Kunde wird dem Anbieter die angemessene Mitwirkung und die Informationen zur Verfügung stellen, die erforderlich sind, damit der Anbieter rechtmäßige Weisungen nach dieser AVV befolgen kann.

6. UNTERAUFTRAGSVERARBEITER

6.1 Der Kunde erteilt dem Anbieter eine allgemeine Genehmigung, Unterauftragsverarbeiter für die Verarbeitung personenbezogener Daten im Auftrag des Kunden im Zusammenhang mit den Leistungen einzusetzen.

6.2 Die zum Zeitpunkt des Inkrafttretens dieser AVV genehmigten Unterauftragsverarbeiter sind in ANLAGE B aufgeführt.

6.3 Der Anbieter kann von Zeit zu Zeit Unterauftragsverarbeiter hinzufügen oder ersetzen. Der Anbieter wird den Kunden im Voraus über jede beabsichtigte Hinzufügung oder Ersetzung eines Unterauftragsverarbeiters informieren, indem er ANLAGE B aktualisiert oder einen anderen angemessenen Benachrichtigungsmechanismus verwendet.

6.4 Der Kunde kann einem neuen Unterauftragsverarbeiter aus angemessenen datenschutzbezogenen Gründen innerhalb von dreißig (30) Tagen nach Erhalt der Mitteilung widersprechen. Widerspricht der Kunde, werden die Parteien nach Treu und Glauben erörtern, ob eine wirtschaftlich angemessene Lösung erzielt werden kann.
Steht eine solche Lösung vernünftigerweise nicht zur Verfügung, kann der Anbieter entweder:
a) den betreffenden Unterauftragsverarbeiter für den Kunden nicht einsetzen;
b) dem Kunden gestatten, den betroffenen Teil der Leistungen auszusetzen oder zu kündigen; oder
c) wenn der neue Unterauftragsverarbeiter für die weitere Erbringung der Leistungen wesentlich ist, die betroffenen Leistungen nach Maßgabe des Vertrags beenden.

6.5 Der Anbieter wird jedem Unterauftragsverarbeiter Datenschutzpflichten auferlegen, die, soweit sie für die von diesem Unterauftragsverarbeiter erbrachten Leistungen anwendbar sind, keinen geringeren Schutz bieten als die in dieser AVV festgelegten Pflichten.

6.6 Der Anbieter bleibt im nach dem anwendbaren Datenschutzrecht erforderlichen Umfang für die Erfüllung der Verpflichtungen seiner Unterauftragsverarbeiter verantwortlich.

7. INTERNATIONALE DATENÜBERMITTLUNGEN

7.1 Der Anbieter wird personenbezogene Daten nicht in ein Land außerhalb des Europäischen Wirtschaftsraums übermitteln, sofern eine solche Übermittlung nicht im Einklang mit dem anwendbaren Datenschutzrecht erfolgt.

7.2 Soweit der Anbieter oder ein Unterauftragsverarbeiter personenbezogene Daten in ein Land außerhalb des Europäischen Wirtschaftsraums übermittelt, stellt der Anbieter sicher, dass ein geeigneter Übermittlungsmechanismus nach dem anwendbaren Datenschutzrecht besteht, wie zum Beispiel:
a) ein Angemessenheitsbeschluss;
b) die EU-Standardvertragsklauseln; oder
c) ein anderer gesetzlich anerkannter Übermittlungsmechanismus.

7.3 Soweit dies nach dem anwendbaren Datenschutzrecht erforderlich ist, wird der Anbieter im Zusammenhang mit internationalen Datenübermittlungen geeignete ergänzende Maßnahmen umsetzen.

7.4 Auf angemessene Anfrage des Kunden wird der Anbieter Informationen zu dem Übermittlungsmechanismus bereitstellen, auf den sich relevante internationale Datenübermittlungen stützen, soweit dies rechtlich und vertraglich zulässig ist.

8. PRÜFUNG UND NACHWEIS DER COMPLIANCE

8.1 Der Anbieter kann seine Prüfungs- und Informationspflichten nach dieser AVV erfüllen, indem er Folgendes bereitstellt:
a) aktuelle Zertifizierungen, Bescheinigungen, Berichte oder Auszüge aus Berichten unabhängiger Prüfer;
b) Zusammenfassungen relevanter Sicherheits- und Compliance-Dokumentationen;
c) Antworten auf angemessene Due-Diligence-Fragebögen; und
d) sonstige Informationen, die vernünftigerweise erforderlich sind, um die Einhaltung dieser AVV nachzuweisen.

Der Anbieter kann darüber hinaus, soweit angemessen, Informationen zu einschlägigen Zertifizierungen und unabhängigen Bewertungen, einschließlich Informationen zu einer ISO/IEC-27001-Zertifizierung, zur Verfügung stellen, um die Beurteilung der Compliance des Anbieters sowie seiner technischen und organisatorischen Maßnahmen durch den Kunden zu unterstützen.

8.2 Reichen die nach Ziffer 8.1 bereitgestellten Informationen nicht aus, um die Einhaltung dieser AVV nachzuweisen, kann der Kunde selbst oder durch einen zur Vertraulichkeit verpflichteten unabhängigen Dritten eine Prüfung verlangen, vorbehaltlich der folgenden Bedingungen:
a) mindestens dreißig (30) Tage vorherige schriftliche Ankündigung, sofern nicht eine kürzere Frist von einer Aufsichtsbehörde verlangt wird;

b) höchstens einmal pro Kalenderjahr, sofern nicht eine Verletzung des Schutzes personenbezogener Daten, ein wesentlicher Compliance-Verstoß oder eine Anfrage einer Aufsichtsbehörde eine zusätzliche Prüfung rechtfertigt;
c) der Umfang der Prüfung muss auf Informationen beschränkt sein, die für die Verarbeitung des Kunden nach dieser AVV relevant sind;
d) die Prüfung muss während der üblichen Geschäftszeiten und in einer Weise durchgeführt werden, die eine unangemessene Beeinträchtigung des Geschäftsbetriebs des Anbieters vermeidet;
e) der Kunde darf keinen Zugang zu Informationen erhalten, die andere Kunden des Anbieters betreffen; und
f) der Kunde trägt seine eigenen Kosten und erstattet dem Anbieter die angemessenen internen und externen Kosten, die im Zusammenhang mit der Prüfung entstehen, es sei denn, die Prüfung weist einen wesentlichen Verstoß des Anbieters gegen diese AVV nach.

8.3 Der Anbieter kann einem Prüfer widersprechen, der nach vernünftiger Auffassung des Anbieters nicht ausreichend qualifiziert oder unabhängig ist oder ein unmittelbarer Wettbewerber des Anbieters ist.

9. RÜCKGABE UND LÖSCHUNG PERSONENBEZOGENER DATEN

9.1 Nach Beendigung oder Ablauf des Vertrags wird der Anbieter nach Wahl des Kunden personenbezogene Daten, die im Auftrag des Kunden verarbeitet wurden, löschen oder zurückgeben, sofern nicht anwendbares Recht die Aufbewahrung der personenbezogenen Daten verlangt.

9.2 Der praktische Ablauf, Zeitpunkt und das Format für den Datenexport, die Rückgabe, die Löschung sowie etwaige damit zusammenhängende Aufbewahrungsfristen können im Vertrag, in der anwendbaren Dokumentation oder in den Standard-Offboarding-Verfahren des Anbieters näher beschrieben sein, sofern diese Verfahren mit dem anwendbaren Datenschutzrecht, dieser AVV und dem Vertrag im Einklang stehen.

9.3 Der Anbieter kann personenbezogene Daten, die in Backup-Systemen enthalten sind, für einen begrenzten Zeitraum entsprechend den üblichen Backup-Aufbewahrungspraktiken des Anbieters aufbewahren, sofern diese aufbewahrten personenbezogenen Daten weiterhin im Einklang mit dieser AVV geschützt bleiben und im ordnungsgemäßen Verlauf gelöscht werden.

9.4 Soweit der Anbieter nach anwendbarem Recht zur Aufbewahrung personenbezogener Daten verpflichtet ist, wird er diese personenbezogenen Daten weiterhin im Einklang mit dieser AVV schützen und sie nicht weiter verarbeiten, außer soweit dies nach anwendbarem Recht erforderlich ist.

10. ZUSAMMENARBEIT MIT AUFSICHTSBEHÖRDEN

10.1 Der Anbieter wird, soweit dies nach dem anwendbaren Datenschutzrecht erforderlich ist, mit Aufsichtsbehörden in Bezug auf die von dieser AVV erfasste Verarbeitung personenbezogener Daten zusammenarbeiten und den Kunden unverzüglich über jede Anfrage, Prüfung oder sonstige verbindliche Maßnahme einer Aufsichtsbehörde informieren, die sich speziell auf die personenbezogenen Daten des Kunden bezieht, sofern ihm dies nicht rechtlich untersagt ist.

11. KONTAKTSTELLE

11.1 Die Kontaktstelle des Anbieters für Datenschutzangelegenheiten im Rahmen dieser AVV lautet:
SLASCONE GmbH
E-Mail: support@slascone.com
Der Anbieter kann die Kontaktdaten von Zeit zu Zeit durch Mitteilung an den Kunden aktualisieren.

12. HAFTUNG

12.1 Die Haftung jeder Partei nach dieser AVV unterliegt den im Vertrag geregelten Haftungsausschlüssen und Haftungsbeschränkungen, soweit solche Ausschlüsse oder Beschränkungen nicht nach dem anwendbaren Datenschutzrecht unzulässig sind.

12.2 Nichts in dieser AVV ist so auszulegen, dass die Rechte betroffener Personen nach dem anwendbaren Datenschutzrecht eingeschränkt werden.

13. SCHLUSSBESTIMMUNGEN

13.1 Diese AVV unterliegt dem Recht, das den Vertrag regelt, sofern das anwendbare Datenschutzrecht nichts anderes verlangt.

13.2 Der Anbieter kann diese AVV von Zeit zu Zeit aktualisieren, um Änderungen im anwendbaren Datenschutzrecht, in behördlichen Leitlinien, bei Unterauftragsverarbeitern oder nicht wesentliche administrative Änderungen der Verarbeitungspraxis des Anbieters abzubilden, sofern solche Aktualisierungen das den personenbezogenen Daten unter dieser AVV gewährte Schutzniveau nicht wesentlich verringern und keine Zustimmung des Kunden nach anwendbarem Recht erforderlich ist.

13.3 Sollte eine Bestimmung dieser AVV unwirksam oder nicht durchsetzbar sein, bleiben die übrigen Bestimmungen hiervon unberührt und in vollem Umfang wirksam.

ANLAGE A EINZELHEITEN DER VERARBEITUNG

1. Gegenstand

Erbringung der SLASCONE Licensing & Analytics Leistungen sowie damit zusammenhängendes Hosting, Support, Wartung, Backup, Monitoring und technische Administration.

2. Art der Verarbeitung

Die Verarbeitung kann je nach Anwendungsfall Folgendes umfassen:

- Erhebung
- Erfassung
- Organisation
- Strukturierung
- Speicherung
- Anpassung oder Veränderung
- Auslesen
- Abfrage
- Verwendung
- Offenlegung durch Übermittlung, soweit dies für die Erbringung der Leistungen erforderlich ist
- Einschränkung
- Löschung
- Vernichtung

3. Zweck der Verarbeitung

Verarbeitung, die für die Bereitstellung, den Betrieb, den Support, die Sicherheit, die Wartung und die Verbesserung der vertraglichen Leistungen nach dem Vertrag erforderlich ist.

4. Kategorien betroffener Personen

Je nach Nutzung der Leistungen durch den Kunden können zu den betroffenen Personen gehören:

- Mitarbeiter und Nutzer des Kunden
- Interessenten, Wiederverkäufer, Partner des Kunden sowie deren Mitarbeiter
- Endkunden des Kunden sowie deren Mitarbeiter
- sonstige Personen, deren personenbezogene Daten der Kunde in die Leistungen hochlädt oder über die Leistungen verarbeitet

5. Kategorien personenbezogener Daten

Je nach Nutzung der Leistungen durch den Kunden können zu den personenbezogenen Daten gehören:

- Identifikationsdaten, wie Vor- und Nachname

- Kontaktdaten, wie geschäftliche E-Mail-Adresse, Postanschrift, Telefonnummer, Unternehmen, Land und Titel
- Konto- und Nutzerdaten
- Lizenz- und Berechtigungsdaten
- Nutzungs-, Kommunikations-, Geräte- und netzwerkbezogene Daten, die im Zusammenhang mit der Nutzung der Leistungen erzeugt werden
- vom Kunden übermittelte supportbezogene Informationen
- sonstige personenbezogene Daten, die der Kunde in die Leistungen hochlädt oder über die Leistungen verarbeitet

6. Besondere Kategorien personenbezogener Daten

Der Anbieter verlangt für die gewöhnliche Nutzung der Leistungen nicht, dass der Kunde besondere Kategorien personenbezogener Daten übermittelt. Der Kunde darf besondere Kategorien personenbezogener Daten nur hochladen, wenn dies ausdrücklich schriftlich vereinbart wurde und geeignete Schutzmaßnahmen umgesetzt wurden.

7. Häufigkeit der Verarbeitung

Fortlaufend oder ad hoc, abhängig von der Nutzung der Leistungen durch den Kunden während der Laufzeit des Vertrags.

ANLAGE B GENEHMIGTE UNTERAUFTRAGSVERARBEITER

Zum Zeitpunkt des Inkrafttretens dieser AVV setzt der Anbieter für die Leistungen die folgenden Unterauftragsverarbeiter ein:

Name und Anschrift des Unterauftragsverarbeiters	Zweck	Standort / Region
Microsoft Ireland Operations Limited, One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521 Ireland	Cloud-Hosting, Infrastruktur, Speicher und damit zusammenhängende Plattformleistungen für SLASCONE Licensing & Analytics	Hosting-Region EU / EWR, vorbehaltlich der für die jeweilige Kundenumgebung verwendeten Konfiguration

Der Anbieter kann diese Anlage gemäß Ziffer 6 dieser AVV aktualisieren.

ANLAGE C TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Der Anbieter setzt technische und organisatorische Maßnahmen um und hält diese aufrecht, die darauf ausgelegt sind, personenbezogene Daten gegen zufällige oder unrechtmäßige Zerstörung, Verlust, Veränderung, unbefugte Offenlegung oder unbefugten Zugang zu schützen. Solche Maßnahmen werden unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen ausgestaltet.

Der Anbieter unterhält und entwickelt seine Informationssicherheits- und Datenschutzmaßnahmen im Rahmen seiner allgemeinen Sicherheitsgovernance und seiner betrieblichen Prozesse fort. Der Anbieter kann darüber hinaus, soweit angemessen, Informationen zu einschlägigen Zertifizierungen und unabhängigen Bewertungen, einschließlich Informationen zu einer ISO/IEC-27001-Zertifizierung, zur Verfügung stellen, um die Beurteilung der technischen und organisatorischen Maßnahmen des Anbieters durch den Kunden zu unterstützen. Zur Klarstellung: Solche Zertifizierungsinformationen ergänzen die in dieser Anlage beschriebenen Maßnahmen, ersetzen diese jedoch nicht.

1. Zutritts- und Zugangskontrolle

Der Anbieter setzt Maßnahmen um, die darauf ausgelegt sind, unbefugten Personen den Zugang zu Systemen zu verwehren, in denen personenbezogene Daten verarbeitet werden. Solche Maßnahmen können je nach Anwendungsfall Folgendes umfassen:

- rollenbasierte Zugriffskontrollen
- Least-Privilege-Prinzipien für interne Zugriffe
- Authentifizierungskontrollen für administrative Zugriffe
- Mehrfaktor-Authentifizierung für privilegierte Zugriffe, soweit anwendbar
- Verfahren zur Vergabe, Überprüfung, Änderung und Entziehung von Zugriffsrechten
- logische Zugriffsbeschränkungen auf Produktionssysteme und Administrationswerkzeuge

2. Systemsicherheit

Der Anbieter setzt Maßnahmen um, die darauf ausgelegt sind, Systeme und Leistungen gegen unbefugten Zugriff, böswillige Aktivitäten und technische Schwachstellen zu schützen. Solche Maßnahmen können je nach Anwendungsfall Folgendes umfassen:

- Netzwerksicherheitskontrollen wie Firewalls, Verkehrsfilterung und Segmentierung, soweit angemessen
- sichere Konfigurations- und Härtungsmaßnahmen
- Endpoint-Schutz und Malware-Schutz für verwaltete Geräte, soweit anwendbar
- Schwachstellenmanagement-Prozesse
- Sicherheits-Patching- und Update-Verfahren
- kontrollierter administrativer Zugriff auf Infrastruktur- und Leistungskomponenten

3. Verschlüsselung und Übertragungssicherheit

Der Anbieter setzt Maßnahmen um, die darauf ausgelegt sind, personenbezogene Daten während der Übertragung und Speicherung zu schützen. Solche Maßnahmen können je nach Anwendungsfall Folgendes umfassen:

- Verschlüsselung bei der Übertragung unter Verwendung branchenüblicher Protokolle, soweit unterstützt
- Verschlüsselung ruhender Daten, soweit dies durch die zugrunde liegende Infrastruktur und die Leistungskonfiguration unterstützt wird
- sichere Remote-Zugriffsmethoden, soweit eine Fernadministration erforderlich ist
- Verfahren zur Handhabung von Schlüsseln und Geheimnissen, die den verwendeten Leistungen und der eingesetzten Infrastruktur angemessen sind

4. Berechtigung und Trennung

Der Anbieter setzt Maßnahmen um, die darauf ausgelegt sind sicherzustellen, dass personenbezogene Daten nur durch befugtes Personal und innerhalb des vorgesehenen Rahmens verarbeitet werden. Solche Maßnahmen können je nach Anwendungsfall Folgendes umfassen:

- Trennung von Produktions- und Nicht-Produktionsumgebungen, soweit angemessen
- Mandantentrennung und logische Trennungsmechanismen innerhalb der Servicearchitektur
- administrative Kontrollen für Datenbank-, Anwendungs- und Infrastrukturberechtigungen
- Funktionstrennung, soweit dies für kritische Funktionen angemessen ist

5. Protokollierung und Überwachung

Der Anbieter setzt Maßnahmen um, die darauf ausgelegt sind, betriebliche und sicherheitsbezogene Ereignisse zu erkennen, zu untersuchen und darauf zu reagieren. Solche Maßnahmen können je nach Anwendungsfall Folgendes umfassen:

- Protokollierung relevanter administrativer, betrieblicher und sicherheitsbezogener Ereignisse, soweit angemessen
- Überwachungsmechanismen zur Erkennung betrieblicher oder sicherheitsbezogener Anomalien
- Alarmierungs- und Eskalationsprozesse für relevante Vorfälle
- Prüfung und Aufbewahrung von Protokollen entsprechend den betrieblichen und sicherheitsbezogenen Anforderungen

6. Verfügbarkeit und Belastbarkeit

Der Anbieter setzt Maßnahmen um, die darauf ausgelegt sind, die Verfügbarkeit und Belastbarkeit der Leistungen sowie der darüber verarbeiteten personenbezogenen Daten aufrechtzuerhalten. Solche Maßnahmen können je nach Anwendungsfall Folgendes umfassen:

- für die Leistung geeignete Backup- und Wiederherstellungsprozesse
- Belastbarkeits- und Kontinuitätsmaßnahmen auf Grundlage der zugrunde liegenden Cloud-Infrastruktur und der betrieblichen Verfahren des Anbieters
- Verfahren zur Wiederherstellung der Verfügbarkeit und des Zugangs zu personenbezogenen Daten nach einem Vorfall

- Tests oder Validierungen relevanter Wiederherstellungs- und Rücksicherungsprozesse, soweit angemessen

7. Vertraulichkeits- und Personalmaßnahmen

Der Anbieter setzt Maßnahmen um, die darauf ausgelegt sind sicherzustellen, dass mit personenbezogenen Daten befasste Personen angemessen befugt und informiert sind. Solche Maßnahmen können je nach Anwendungsfall Folgendes umfassen:

- Vertraulichkeitsverpflichtungen oder gesetzliche Verschwiegenheitspflichten für Personal mit Zugang zu personenbezogenen Daten
- Schulungs- und Sensibilisierungsmaßnahmen zu Datenschutz und Sicherheit
- Onboarding- und Offboarding-Verfahren für Personalzugriffe
- Überprüfung von Zugriffsrechten des Personals, soweit angemessen

8. Entwicklungs- und Änderungsmanagement

Der Anbieter setzt Maßnahmen um, die darauf ausgelegt sind sicherzustellen, dass Änderungen an Systemen und Software kontrolliert und angemessen überprüft werden. Solche Maßnahmen können je nach Anwendungsfall Folgendes umfassen:

- kontrollierte Deployment- und Change-Management-Verfahren
- Test- und Validierungsprozesse für relevante Änderungen
- Trennung von Entwicklungs-, Test- und Produktionsaktivitäten, soweit angemessen
- Verfahren zur Steuerung und Freigabe von Änderungen, die Sicherheit oder Verarbeitungsvorgänge betreffen

9. Lieferanten- und Unterauftragsverarbeiter-Management

Der Anbieter setzt Maßnahmen um, die darauf ausgelegt sind sicherzustellen, dass relevante Unterauftragsverarbeiter und Lieferanten einer angemessenen Kontrolle unterliegen. Solche Maßnahmen können je nach Anwendungsfall Folgendes umfassen:

- Due-Diligence- und Auswahlverfahren für relevante Unterauftragsverarbeiter und Dienstleister
- vertragliche Datenschutz- und Sicherheitsverpflichtungen, die Unterauftragsverarbeitern nach Maßgabe des Rechts auferlegt werden
- Prüfung relevanter Sicherheitsinformationen von Unterauftragsverarbeitern oder Lieferanten, soweit angemessen

10. Überprüfung und Verbesserung

Der Anbieter setzt Maßnahmen um, die darauf ausgelegt sind sicherzustellen, dass technische und organisatorische Maßnahmen auch im Zeitverlauf angemessen bleiben. Solche Maßnahmen können je nach Anwendungsfall Folgendes umfassen:

- regelmäßige Überprüfung und Aktualisierung der Sicherheitsmaßnahmen
- Anpassung der Maßnahmen im Lichte technischer Entwicklungen, von Risikobewertungen, betrieblicher Erfahrungen und rechtlicher Anforderungen
- Überprüfung relevanter Vorfälle und daraus abgeleiteter Verbesserungen, soweit angemessen

Zur Klarstellung: Bestimmte technische und organisatorische Maßnahmen werden über die Cloud-Infrastruktur-Anbieter des Anbieters und damit verbundene Managed Services umgesetzt, die für den Betrieb der Leistungen verwendet werden, einschließlich Microsoft Azure, soweit anwendbar.