

Datenübermittlung-Folgenabschätzung

Microsoft 365

Rhein-Neckar-Verkehr GmbH

Möhlstraße 27

68165 Mannheim

Deutschland

Telefon: 0621 465-0

E-Mail: info@rnv-online.de

Inhaltsverzeichnis

1. Akteure	3
1.1 Datenexporteur	3
1.2 Datenimporteur	3
1.3 Zusätzliche Datenempfänger	3
2. Beschreibung der Übertragung	4
2.1 Startdatum	4
2.2 Umstände der Übermittlung	4
2.3 Übertragungskanäle	4
2.4 Externe Empfängergruppen außerhalb der EU	4
2.5 Wirtschaftszweig	4
2.6 Zweck der Datenverarbeitung	4
2.7 Datenkategorien	4
2.8 Format der Daten	5
2.9 Speicherort der übermittelten Daten	5
3. Rechtsvorschriften und Gepflogenheiten (im Bestimmungsdrittland)	6
3.1 Beurteilungszeitraum (Beginn)	6
3.2 Beurteilungszeitraum (Ende)	6
3.3 Rechtsvorschriften	6
3.4 Geltende Beschränkungen und Garantien	6
3.5 Frühere Ersuchen um Offenlegung seitens Behörden	6
4. Garantien	7
4.1 Technische und organisatorische Maßnahmen	7
4.2 Rechtsgrundlage	7
4.3 Weitere Maßnahmen	7
5. Bewertung	9
5.1 Risiken	9
5.2 Risikokartierung	9
6. Maßnahmen	11
7. Bericht	12

1. Akteure

1.1 Datenexporteur

Rhein-Neckar-Verkehr GmbH

Möhlstraße 27

68165 Mannheim

Telefon: 06214650

E-Mail: info@rnv-online.de

1.2 Datenimporteur

Microsoft Corporation

One Microsoft Way, Redmond WA 98052, USA

98052-6399 Redmond, Washington

1.3 Zusätzliche Datenempfänger

Keine Angaben

2. Beschreibung der Übertragung

2.1 Startdatum

Keine Angaben

2.2 Umstände der Übermittlung

- Keine Angaben

2.3 Übertragungskanäle

- Der Inhalt wird verschlüsselt

2.4 Externe Empfängergruppen außerhalb der EU

- Auftragsverarbeiter
- Unterauftragsverarbeiter

2.5 Wirtschaftszweig

- Information und Kommunikation

2.6 Zweck der Datenverarbeitung

- Bereitstellung von Microsoft 365 für die RNV GmbH
- Konfiguration, Betrieb, Überwachung und Pflege von Anwendungssoftware
- Unterstützung der Geschäftsprozesse mittels Dokumentenverarbeitung und Kommunikation (E-Mail und Messenger)

2.7 Datenkategorien

- Allgemeine Adressdaten: - Name - Vorname - Straße mit Hausnummer - PLZ - Ort
- Allgemeine Kontaktdaten (kurz): - Telefonnummer - Mobilfunknummer - E-Mail-Adresse
- Besondere Kategorien von Daten
- Inhalte von Dokumenten, Inhalte von E-Mails, Worddokumenten, PDF`s usw. können je nach Prozess

personenbezogene Daten enthalten.

- IP-Adresse

2.8 Format der Daten

- Text (XML, JSON, TXT, DOCX)
- Datenbank

2.9 Speicherort der übermittelten Daten

Sicherstellung der Datenresidenz innerhalb der EU: Dublin

3. Rechtsvorschriften und Gepflogenheiten (im Bestimmungsdrittland)

3.1 Beurteilungszeitraum (Beginn)

Keine Angaben

3.2 Beurteilungszeitraum (Ende)

Keine Angaben

3.3 Rechtsvorschriften

- US - Executive Order 12333 (EO 12333)
- US - FISA Section 702
- US - US Clarifying Lawful Overseas Use of Data Act ("CLOUD Act")

3.4 Geltende Beschränkungen und Garantien

- Der Zugriff durch staatliche Stellen ist auf das Notwendigste beschränkt und verhältnismäßig. Microsoft 365 benachrichtigt seine Kunden über Anfragen von US-Behörden. Aus diesen Gründen fechtet Microsoft 365 die Geheimhaltungsverfügungen der US-Regierung an, wenn diese glauben, dass sie einer zweiten juristischen Prüfung bedürfen. Bei allen Fällen, bei denen Microsoft 365 gerichtlich gegen eine Geheimhaltungsverfügung im vergangenen Jahr vorgegangen ist, wurden diese zurückgezogen. [vgl. <https://news.microsoft.com/de-de/im-daten-dschungel-wie-microsoft-mit-dem-cloud-act-umgeht/> abgerufen am 04.07.2023]

3.5 Frühere Ersuchen um Offenlegung seitens Behörden

Laut des Transparentberichts vom Januar bis Juni 2022 gab es die meisten Anfragen seitens den US-Behörden. Insgesamt waren es insgesamt 480 Anfragen, von denen 383 durch Anträge mit angegeben Konten durch die US-Behörden erfolgt sind. Davon wurden 19 Abonnenten oder Transaktionsdaten offengelegt. Bei den Restlichen Anfragen wurden 19% der Daten ohne Inhalt vorgelegt und 75% dieser Anfragen diesbezüglich abgelegt. Dieser Transparenzbericht sollte halbjährlich aktualisiert werden. Der letzte stammt aber von Januar bis Juni 2022. [vgl. [Angang](#)]

4. Garantien

4.1 Technische und organisatorische Maßnahmen

- Technisch organisatorische Maßnahmen Standort Mannheim

4.2 Rechtsgrundlage

- Art. 46 Abs. 2 lit. c DS-GVO (Standardvertragsklauseln)
- der DPA von Microsoft 365 bezieht nicht nur die SCCs ein, sondern legt auch die Verpflichtungen von Microsoft 365 in Bezug auf Vertraulichkeit und Sicherheit der Verarbeitung fest. Des Weiteren führt Microsoft für Mitarbeiter mit Zugriff auf Kundendaten, Professional Service-Daten und personenbezogenen Daten Daten entsprechend den geltenden Datenschutzvorschriften und Branchenstandards regelmäßige und verpflichtende Datenschutz-, Datensicherheits- und Sensibilisierungsschulungen durch. [vgl DPA <https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=14>]

4.3 Weitere Maßnahmen

Unter diesem Link befinden sich Informationen u.a. was die Verschlüsselung angeht:

"Microsoft Products and Services Data Protection Addendum (DPA)", abrufbar unter:

[<https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=14>]

Verschlüsselung:

Für ruhende Kundendaten verwendet Microsoft 365 BitLocker, Azure Storage Service Encryption, Distributed Key Manager (DKM) und Microsoft 365 Dienstverschlüsselung.

Für Kundendaten während der Übertragung verwendet Office 365 branchenübliche sichere Transportprotokolle wie Internet Protocol Security (IPsec) und Transport Layer Security (TLS) zwischen Microsoft-Rechenzentren und zwischen Benutzergeräten und Microsoft-Rechenzentren. [vgl. <https://learn.microsoft.com/de-de/microsoft-365/compliance/office-365-encryption-in-the-microsoft-cloud-overview?view=o365-worldwide> abgerufen am 05.07.2023]

ISO/IEC 27001

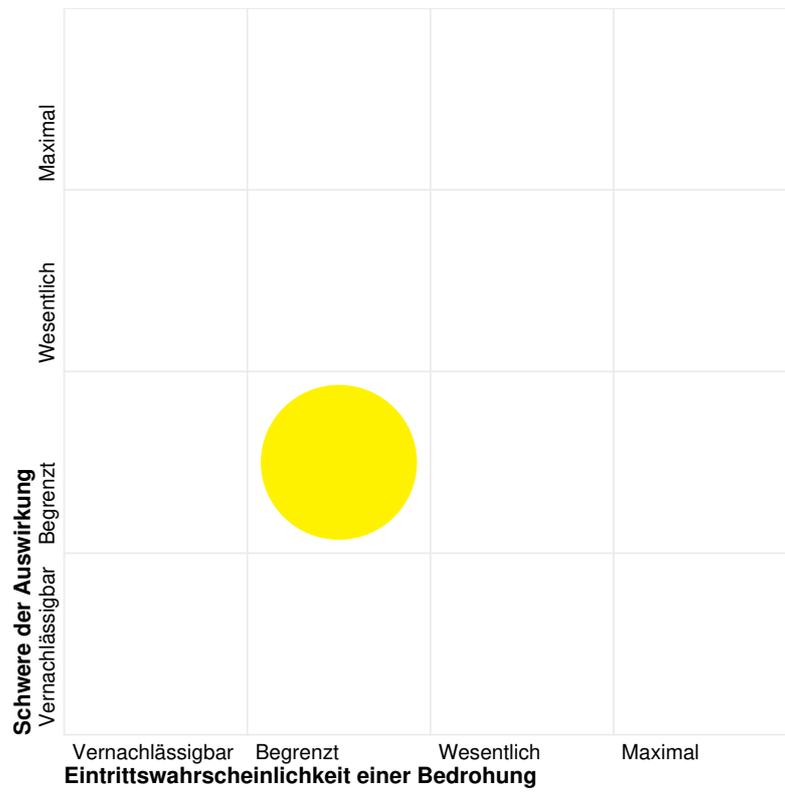
Berichte Dritter in Bezug auf die Cloud-Produkte: SOC1-Typ- II, SOC2-Typ-II und SOC3 [vgl
<https://learn.microsoft.com/de-de/compliance/regulatory/offering-soc-2> abgerufen am 05.07.2023]

5. Bewertung

5.1 Risiken

Bezeichnung	Zugriff auf personenbezogene Daten durch US-Behörden
Beschreibung	<p>Aufgrund der Verwendung von Microsoft 365 und damit der Datenübermittlung in die USA, besteht hierbei die Gefahr, dass US-Behörden Zugriff auf personenbezogene Daten erhalten. Allerdings wurden in wenigen Fällen personenbezogene Daten herausgegeben.</p> <p>Quelle: https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report, abgerufen am 03.07.2023</p>
Risikokategorie	Offenlegung der übertragenen Daten
Eintrittswahrscheinlichkeit	Begrenzt
Schwere der Auswirkung (Schadenspotenzial für die betroffene Person)	Begrenzt

5.2 Risikokartierung



6. Maßnahmen

Bezeichnung	Abschluss eines Vertrags zur Auftragsverarbeitung inkl. EU-Standardvertragsklauseln
Beschreibung	Einhaltung der datenschutzrechtlichen Vorgaben gem. Art. 28 sowie 44, 46 (2) lit. c DSGVO
Planung der Umsetzung bis	
Status der Umsetzung	

Bezeichnung	Durchführung einer Datenübermittlung-Folgenabschätzung ("Transfer Impact Assessment")
Beschreibung	Beschreibung Einhaltung der vertraglichen Vorgaben aus Klausel 14 der EU-Standardvertragsklauseln.
Planung der Umsetzung bis	
Status der Umsetzung	

7. Bericht

Autor	Hinweise
Kristina Rados, 06.07.2023	ALLGEMEIN: Der Rhein-Neckar-Verkehr GmbH erkennt an, dass grundsätzlich Risiken für die Gewährleistung des Schutzes personenbezogener Daten bei der Übermittlung in Drittländer wie beispielsweise USA bestehen.
Kristina Rados, 06.07.2023	<p>BEWERTUNG OFFENLEGUNG:</p> <p>Wie zuvor dargestellt, fanden mehrere Behördenanfragen statt, von denen Microsoft im Zeitraum von Januar bis Juli 2022 nur wenige Daten an Behörden weitergegeben wurden. Es ist nicht davon auszugehen, dass die Anzahl der Behördenanfragen und die Herausgabe durch Microsoft an die Behörden ansteigen wird.</p>
Kristina Rados, 06.07.2023	<p>BEWERTUNG VERTRAGLICHE MAßNAHMEN:</p> <p>Des Weiteren wurden i. S. d Art. 46 Abs. 2 lit. c DSGVO die in Abs. 1 genannten geeigneten Garantien durch den Abschluss von Standardvertragsklauseln sichergestellt und in einem DPA (AVV) festgehalten.</p>
Kristina Rados, 06.07.2023	<p>ERGEBNIS:</p> <p>Es besteht insgesamt kein bzw. geringer Grund zur Annahme, dass die für die Verarbeitung personenbezogener Daten durch den Datenimporteur geltenden Rechtsvorschriften und Gepflogenheiten im Bestimmungsdrittland (hier: USA), einschließlich Anforderungen zur Offenlegung personenbezogener Daten oder Maßnahmen, die öffentlichen Behörden den Zugang zu diesen Daten gestatten, den Datenimporteur an der Erfüllung seiner Pflichten gemäß den EU-Standardvertragsklauseln hindern.</p> <p>Die Datenübermittlung kann demnach im Rahmen von "Microsoft 365" durch den Rhein Neckar Verkehr GmbH stattfinden, da die Risiken hier als akzeptabel zu bewerten sind.</p>

Anhänge zu Rechtsvorschriften und Gepflogenheiten:

- [Transparenzbericht Microsoft 365 \(Transparenzbericht Microsoft LERR_2022_H1\(2\).xlsx\)](#)