Datenschutzvereinbarung nach Artikel 28 DS-GVO

zwischen

Nutzer (Aufsichtsbehörden des Landes)

- (der “Verantwortlicher”) -

und

DVGW-Service & Consult GmbH
Josef-Wirmer-Str. 1-3, 53123 Bonn

- (“Auftragsverarbeiter ”) -

Einleitung

Der Auftragsverarbeiter wird personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten. Dieser Vertrag gilt im Zusammenhang mit der Nutzungsvereinbarung, sowie für alle zukünftigen Verträge, die sich auf diese Datenschutzvereinbarung beziehen.

Sofern der Gegenstand der künftigen Nutzung von DVGW-Metra eine Datenverarbeitung erfordert, die nicht in diesem Vertrag beschrieben ist, vereinbaren die Parteien, dass sie die, nach Art. 28 DS-GVO erforderlichen, zusätzlichen Informationen in die künftige Dienstleistungsvereinbarung aufnehmen werden. Dies gilt insbesondere, wenn es sich um zusätzliche oder abweichende Informationen zu folgenden Themen handelt:

- Gegenstand des Auftrags
- Zweck, Art und Umfang der vorgesehenen Datenverarbeitung
- Art der Daten
- Betroffene Personen
- Technische und organisatorische Maßnahmen

Die Vertragsparteien vereinbaren, dass für diese Vereinbarung alle Begriffs-Definitionen gemäß DS-GVO gelten.

1. Gegenstand und Dauer des Auftrags

1.1 Gegenstand des Auftrags

Der Auftragsverarbeiter stellt im Rahmen der Nutzung von DVGW-Metra dem Verantwortlichen auch die Möglichkeit zur Verfügung ein Rechte und Rollenkonzept abzubilden und verarbeitet in diesem Zusammenhang personenbezogene Daten.

1.2 Dauer der Verarbeitung

Die Dauer (Laufzeit) dieser Datenschutzvereinbarung entspricht der Laufzeit jeder Nutzungsvereinbarung, die auf diesen Vertrag verweist.

2. Details der Verarbeitung

2.1 Umfang und Art der Verarbeitung

Die Verarbeitung besteht in der Speicherung personenbezogener Daten für die Einhaltung von Rechte- und Rollenkonzepten im System, sowie in der Bereitstellung der IT-Dienstleitungen im Zusammenhang mit der Nutzung von DVGW-Metra.

2.2 Räumlicher Anwendungsbereich

Die Daten werden ausschließlich im Hoheitsgebiet eines Mitgliedstaates der Europäischen Union oder eines anderen Unterzeichners des Abkommens über den Europäischen Wirtschaftsraum verarbeitet und genutzt. Jede Übermittlung von Daten in ein Drittland außerhalb der EU oder des EWR bedarf der vorherigen schriftlichen Zustimmung des Verantwortlichen für die Verarbeitung und unterliegt den besonderen Anforderungen des Artikels 46 DS-GVO.

2.3 Art der Daten/ Datenkategorien

Der Gegenstand der Verarbeitung personenbezogener Daten umfasst die folgenden Datenarten/Kategorien (Liste/Beschreibung der Datenkategorien)

Kategorien personenbezogener Daten

- Anrede
- Vorname
- Nachname
- E-Mail-Adresse
- Angaben zu Organisationszugehörigkeit

Besondere Kategorien personenbezogener Daten

Besondere Kategorien personenbezogener Daten werden nicht verarbeitet.

2.4 Zwecke

Die Verarbeitung personenbezogener Daten dient dem Zweck im Rahmen des Rechte- und Rollenkonzepts die verschiedenen Berechtigungen im System zu steuern.

2.5 Betroffene Personen (Betroffene)

Die von der Verarbeitung personenbezogener Daten betroffenen Personen sind die Nutzer innerhalb von DVGW-Metra

3. Technische und organisatorische Maßnahmen

(a) Der Auftragsverarbeiter verpflichtet sich alle in Anhang 3 aufgeführten technischen und organisatorischen Maßnahmen umzusetzen. Zu den technischen und organisatorischen Maßnahmen gehören insbesondere - aber nicht ausschließlich - die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit von Verarbeitungssystemen und -diensten. Der Auftragsverarbeiter verfügt über ein Verfahren zur regelmäßigen Prüfung, Bewertung und Begutachtung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(b) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Entwicklung, und der Auftragsverarbeiter kann geeignete Alternativmaßnahmen ergreifen. Diese dürfen jedoch das Sicherheitsniveau der genannten Maßnahmen nicht unterschreiten. Der Auftragsverarbeiter übermittelt dem Verantwortlichen für die Verarbeitung auf Verlangen die erforderlichen Angaben gemäß Artikel 30 Absatz 1 DS-GVO.

(c) Der Auftragsverarbeiter dokumentiert künftige Änderungen der technischen und organisatorischen Maßnahmen und meldet diese unverzüglich an den Verantwortlichen.

4. Berichtigung, Löschung und Sperrung von Daten

Der Auftragsverarbeiter darf die im Auftrag der verantwortlichen Stelle verarbeiteten Daten nur auf Anweisung der verantwortlichen Stelle berichtigen, löschen oder sperren. Wenn eine betroffene Person sich direkt an den Auftragsverarbeiter wendet und die Berichtigung, Sperrung oder Löschung ihrer personenbezogenen Daten verlangt, leitet der Auftragsverarbeiter dieses Ersuchen unverzüglich, spätestens jedoch innerhalb von 5 Werktagen nach Antragstellung, an den Verantwortlichen weiter.

5. Kontrollen und weitere Pflichten des Auftragsverarbeiters

Zusätzlich zur Einhaltung der Bestimmungen dieser Vereinbarung hat der Auftragsverarbeiter folgende Pflichten gemäß Artikel 28 DS-GVO:

- Schriftliche Bestellung - soweit gesetzlich vorgeschrieben - eines Datenschutzbeauftragten, der seine Aufgaben gemäß Artikel 37 bis 39 GDPR erfüllen kann. Die Kontaktdaten der Datenschutzbeauftragten lauten wie folgt:

  2B Advice GmbH
  Josef-Schumpeter-Allee 25
  53227 Bonn

Die Kontaktdaten des Ansprechpartners für den Datenschutz lauten wie folgt:

DVGW Service & Consult GmbH
Datenschutzbeauftragter 2B Advice GmbH
Tel: +49 (228) 926165 120
dvgw@2b-advice.com

- Der Auftragsverarbeiter ist verpflichtet sicherzustellen, dass sich alle Mitarbeiter zur Wahrung der Vertraulichkeit gemäß Artikel 28 Absatz 3 b DS-GVO verpflichtet haben. Der Auftragsverarbeiter garantiert, dass alle Personen, die im Rahmen dieser Vereinbarung Zugang zu personenbezogenen Daten des Verantwortlichen haben, zur Verschwiegenheit verpflichtet sind und über alle besonderen Datenschutzbestimmungen, die sich aus dieser Vereinbarung ergeben, einschließlich der Beschränkung der Verwendung auf bestimmte Zwecke gemäß den Anweisungen informiert sind.
- Der Auftragsverarbeiter muss alle erforderlichen technischen und organisatorischen Maßnahmen für diesen Auftrag gemäß Artikel 24 und 32 DS-GVO ergreifen und einhalten.
- Der Auftragsverarbeiter unterstützt den Verantwortlichen - unter Berücksichtigung der Art der Verarbeitung - durch geeignete technische und organisatorische Maßnahmen, soweit dies möglich ist, um der Verpflichtung des Verantwortlichen nachzukommen, auf Anträge auf Ausübung der Rechte der betroffenen Person gemäß Kapitel III der DS-GVO zu reagieren. Insbesondere indem er dem Verantwortlichen rechtzeitig alle erforderlichen Informationen zur Verfügung stellt, damit dieser dem Antrag der betroffenen Person auf Zugang, Datenübertragbarkeit, Berichtigung, Löschung, Einschränkung und Widerspruch nachkommen kann.
- Der Auftragsverarbeiter unterstützt auf Antrag des Verantwortlichen - unter Berücksichtigung der Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen - den Verantwortlichen bei der Einhaltung der Verpflichtungen gemäß den Artikeln 35 und 36 DS-GVO (Datenschutz-Folgeabschätzung und vorherige Konsultation) und stellt dem Verantwortlichen auf Antrag alle erforderlichen Informationen rechtzeitig zur Verfügung.
- Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über alle Überwachungstätigkeiten und Maßnahmen, die von der Aufsichtsbehörde gemäß dem anwendbaren nationalen Recht und den Artikeln 57 und 58 DS-GVO durchgeführt werden.
- Der Auftragsverarbeiter überwacht die Verarbeitung im Auftrag des Verantwortlichen durch regelmäßige Überprüfungen der Ausführung und Erfüllung des Auftrags, insbesondere die Einhaltung der erforderlichen Änderungen der Bestimmungen und Maßnahmen für die Durchführung des Auftrags.

6. Unterauftragsverarbeiter

(a) Der Auftragsverarbeiter kann auch Unterauftragsverarbeiter mit der Durchführung der Dienstleistungen beauftragen. Wenn der Auftragsverarbeiter Unterauftragsverarbeiter beauftragt, führt der Auftragsverarbeiter eine Liste der Unterauftragsverarbeiter, die die

personenbezogenen Daten des Verantwortlichen verarbeiten dürfen, und stellt dem Verantwortlichen auf Anfrage eine Kopie dieser Liste zur Verfügung.

(b) Alle Unterauftragsverarbeiter sind verpflichtet, die gleichen Verpflichtungen einzuhalten wie der Auftragsverarbeiter im Rahmen dieser Vereinbarung, die für die Durchführung der Unterauftragsverarbeitung gelten. Der Verantwortliche kann verlangen, dass der Auftragsverarbeiter den Unterauftragsverarbeiter überprüft oder bestätigt, dass eine solche Prüfung stattgefunden hat (oder, sofern verfügbar, den Verantwortlichen bei der Einholung eines externen Prüfberichts über die Tätigkeiten des Unterauftragsverarbeiters unterstützt), um die Einhaltung dieser Verpflichtungen sicherzustellen. Der Verantwortlicher ist auch berechtigt, auf schriftliche Anfrage Kopien der entsprechenden Bedingungen der Vereinbarung des Auftragsverarbeiters mit Unterauftragsverarbeitern, die personenbezogene Daten verarbeiten dürfen, zu bekommen, es sei denn, die Vereinbarung enthält vertrauliche Informationen; in diesem Fall kann der Bearbeiter eine redigierte Version der Vereinbarung zur Verfügung stellen.

(c) Der Auftragsverarbeiter haftet für die Handlungen und Unterlassungen seiner Unterauftragsverarbeiter in dem gleichen Umfang, in dem der Auftragsverarbeiter haftbar wäre, wenn er die Leistungen jedes Unterauftragsverarbeiters direkt im Rahmen dieser Vereinbarung erbringen würde.

(d) Der Verantwortliche stimmt der Verwendung der folgenden Unterauftragsverarbeiter bei der Erbringung der Dienstleistungen gemäß den Bedingungen dieser Vereinbarung zu:

Microsoft Ireland

One Microsoft Place, South County Business Park, Carmanhall And Leopardstown, Dublin

D18 P521, Irland

Explicatis GmbH

Max-Planck-Straße 6-8

50858 Köln

(e) Der Auftragsverarbeiter teilt dem Verantwortlichen jeden neuen Unterauftragsverarbeiter mit, bevor er den Unterauftragsverarbeiter beauftragt, personenbezogene Daten im Zusammenhang mit der Erbringung der betreffenden Dienstleistungen zu verarbeiten. Der Verantwortliche kann der Verwendung eines neuen Unterauftragsverarbeiters widersprechen, indem er den Verantwortlichen unverzüglich innerhalb von zehn (10) Werktagen nach Erhalt der Mitteilung des Verantwortlichen schriftlich benachrichtigt. Für den Fall, dass der Verantwortlicher einem neuen Unterauftragsverarbeiter widerspricht, wird der Auftragsverarbeiter angemessene Anstrengungen unternehmen, um dem Verantwortlichen eine Änderung der Dienste zur Verfügung zu stellen oder eine wirtschaftlich sinnvolle Änderung der Konfiguration des Verantwortlichen oder der Nutzung der Dienste zu empfehlen, um die Verarbeitung personenbezogener Daten durch den betreffenden

Unterauftragsverarbeiter zu vermeiden, ohne den Verantwortlichen unangemessen zu belasten. Wenn der Auftragsverarbeiter nicht in der Lage ist, diese Änderung innerhalb einer angemessenen Frist, die dreißig (30) Tage nicht überschreiten darf, zur Verfügung zu stellen, kann der Verantwortlicher die anwendbaren Verträge nur in Bezug auf die Dienstleistungen kündigen, die vom Auftragsverarbeiter nicht ohne die Verwendung des Gegenstands an den neuen Unterauftragsverarbeiter erbracht werden können, indem er den Auftragsverarbeiter schriftlich benachrichtigt. Der Auftragsverarbeiter erstattet dem Verantwortlichen alle vorausbezahlten Gebühren für den Rest der Laufzeit solcher Verträge nach dem Wirksamwerden der Kündigung in Bezug auf diese gekündigten Dienste, ohne dem Verantwortlichen eine Strafe für diese Kündigung aufzuerlegen.

(f) Leistungen, die der Auftragsverarbeiter von Dritten als reine Nebenleistungen zur Durchführung der Geschäftstätigkeit in Anspruch nimmt, gelten nicht als Unterauftragsverhältnisse im Rahmen dieser Vereinbarung. Dazu gehören z.B. Reinigungsdienste, reine Telekommunikationsdienste ohne besondere Bezugnahme auf Dienstleistungen des Auftragsverarbeiters für den Verantwortlichen, Post- und Kurierdienste, Transportdienste oder Sicherheitsdienstleistungen.

7. Überwachungsrechte des Verantwortlichen

(a) Der Verantwortliche kann in Absprache mit dem Auftragsverarbeiter Audits hinsichtlich der technischen und organisatorischen Maßnahmen sowie eine Kontrolle der Anforderungen durchführen, die zur Erfüllung der übrigen Anforderungen dieser Vereinbarung erforderlich sind. Der Verantwortliche kann auch Prüfer damit beauftragen. Die verantwortliche Stelle kann in den Geschäftsräumen des Auftragsverarbeiters Inspektionen durchführen, die in der Regel zwei (2) Wochen im Voraus angekündigt werden, um die Einhaltung dieser Vereinbarung durch den Auftragsverarbeiter zu überprüfen. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen die zur Erfüllung seiner Verpflichtungen erforderlichen Informationen und die erforderlichen Unterlagen zur Verfügung zu stellen.

(b) Im Hinblick auf die Überwachungspflichten des Verantwortlichen gemäß DS-GVO vor dem Beginn der Datenverarbeitung und während der Laufzeit des Auftrags hat der Verantwortliche sicherzustellen, dass der Verantwortliche die Einhaltung der getroffenen technischen und organisatorischen Maßnahmen bestätigen kann. Zu diesem Zweck hat der Auftragsverarbeiter dem Verantwortlichen auf Verlangen den Nachweis über die Durchführung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 DS-GVO zu erbringen. Der Nachweis der Umsetzung von Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann auch in Form von aktuellen Bescheinigungen, Berichten oder Auszügen von unabhängigen Stellen (z.B. externe Prüfer, interne Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung oder Qualitätsprüfer) oder durch eine entsprechende Zertifizierung im Rahmen eines IT-Sicherheits- oder Datenschutzaudits erbracht werden.

8. Mitteilung von Verstößen durch den Auftragsverarbeiter

(a) Der Auftragsverarbeiter benachrichtigt den Verantwortlichen unverzüglich in allen Fällen, in denen der Auftragsverarbeiter oder dessen Beschäftigte gegen die Bestimmungen über den Schutz personenbezogener Daten des Verantwortlichen oder andere in dieser Vereinbarung festgelegte Bestimmungen verstoßen.

(b) Den Vertragsparteien ist bekannt, dass Artikel 33 und Artikel 34 DS-GVO eine Pflicht zur Unterrichtung der Datenschutzbehörden sowie der betroffenen Personen im Falle einer Verletzung des Schutzes personenbezogener Daten vorschreiben können. Solche Vorfälle sind daher dem Verantwortlichen unverzüglich, spätestens jedoch innerhalb von 48 Stunden nach Bekanntwerden des Verstoßes, mitzuteilen. Dies gilt auch bei schwerwiegenden Betriebsstörungen oder bei Verdacht auf einen Verstoß gegen die Bestimmungen über den Schutz personenbezogener Daten oder sonstige Unregelmäßigkeiten im Umgang mit personenbezogenen Daten des Verantwortlichen. In Absprache mit dem Verantwortlichen ergreift der Auftragsverarbeiter geeignete Maßnahmen, um die Daten zu sichern und mögliche nachteilige Auswirkungen auf die betroffenen Personen zu begrenzen. Werden dem Verantwortlichen Verpflichtungen gemäß Artikel 33 und 34 DS-GVO auferlegt, so muss der Auftragsverarbeiter ihn bei der Erfüllung dieser Verpflichtungen unterstützen.

9. Weisungsbefugnis des Verantwortlichen

(a) Die Daten dürfen nur im Rahmen der abgeschlossenen Verträge und der erteilten Weisungen von der verantwortlichen Stelle verarbeitet werden. Im Rahmen der beschriebenen Auftragsbedingungen in diesem Vertrag behält sich die verantwortliche Stelle ein allgemeines Weisungsrecht über Art, Umfang und Methode der Datenverarbeitung vor, das durch individuelle Weisungen ergänzt werden kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind zu vereinbaren und zu dokumentieren. Der Auftragsverarbeiter darf Informationen nur dann an Dritte oder an die betroffene Person gemäß dieser Vereinbarung weitergeben, wenn dies zur Erfüllung der Verpflichtung aus dem Hauptvertrag unbedingt erforderlich ist oder wenn er zuvor die schriftliche Zustimmung des Verantwortlichen eingeholt hat.

(b) Der Auftragsverarbeiter dokumentiert alle vom Verantwortlichen erteilten Weisungen, einschließlich des Namens der Person, die die Weisung erteilt hat, sowie Datum und Inhalt der Weisung.

(c) Die verantwortliche Stelle hat mündliche Anweisungen unverzüglich schriftlich oder per E-Mail (in Textform) zu bestätigen. Der Auftragsverarbeiter darf die Daten nicht für andere Zwecke verwenden und darf sie insbesondere nicht an Dritte weitergeben, es sei denn, er ist gesetzlich dazu verpflichtet. Es dürfen keine Kopien oder Duplikate ohne Wissen des Verantwortlichen angefertigt werden. Dies gilt nicht für Sicherungskopien, soweit diese zur Sicherstellung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie für Daten, die zur Einhaltung gesetzlicher Aufbewahrungsfristen erforderlich sind.

(d) Der Auftragsverarbeiter hat den Verantwortlichen gemäß Artikel 28 Absatz 3 letzter Satz DS-GVO unverzüglich zu informieren, wenn er der Ansicht ist, dass ein Verstoß gegen die gesetzlichen Datenschutzbestimmungen vorliegt und er eine Anweisung für rechtswidrig hält. Er kann in solchen Fällen die Ausführung der betreffenden Weisung aufschieben, bis diese vom Verantwortlichen bestätigt oder geändert wird.

10. Löschung der Daten und Rückgabe der Datenträger

(a) Nach Abschluss der vertraglichen Arbeiten oder auf Verlangen des Verantwortlichen - spätestens bei Ende des Dienstleistungsvertrages - hat der Auftragsverarbeiter alle in seinem Besitz befindlichen Unterlagen und alle im Zusammenhang mit dem Auftrag anfallenden Arbeitsprodukte und Daten an den Verantwortlichen zurückzugeben oder nach vorheriger Zustimmung des Verantwortlichen in geeigneter Weise zu löschen. Gleiches gilt für Testdaten und Ausschussmaterial. Das Löschprotokoll ist auf Verlangen vorzulegen.

(b) Unterlagen, die zum Nachweis einer ordnungsgemäßen Datenverarbeitung bestimmt sind, sind vom Auftragsverarbeiter über das Vertragsende hinaus entsprechend den jeweiligen Aufbewahrungsfristen aufzubewahren. Der Auftragsverarbeiter kann diese Unterlagen nach Ablauf eines jeden Dienstleistungsvertrages an den Verantwortlichen übergeben.

Anhang 1
Datenübermittlung in Drittländer

Eine Datenübermittlung in Drittländer ist nicht vorgesehen.

Anhang 2
Technische und organisatorische Maßnahmen

1. Zutrittskontrolle zu Räumen und Anlagen

Technische und organisatorische Maßnahmen zur Zutrittskontrolle zu Räumen und Anlagen, insbesondere zur Berechtigungsprüfung:

Unbefugter Zutritt (im physikalischen Sinne) wird verhindert. Dazu gibt es ein Raumkonzept, das Zutrittszonen nach grün (öffentlicher Raum), gelb (interne Räume) und rot (Räume mit hohem Schutzbedarf festlegt.

Technische und organisatorische Maßnahmen zur Zutrittskontrolle zu Räumen und Anlagen, insbesondere zur Berechtigungsprüfung sind eingesetzt. Dazu zählen Zutrittskontrollsysteme (Schlüssel, Ausweisleser, Chipkarte), eine nachgehaltene Ausgabe von Zutrittsmedien inkl. der Kontrolle des Entzuges bei Funktionswechsel oder Kündigung, Trennung der Bereiche durch verschlossene Türen, Sicherheitspersonal inkl. Wachpersonal außerhalb der Betriebszeiten und, wo sinnvoll, Überwachungseinrichtungen (Alarmanlage, Video/CCTV-Monitor).

2. Zugangskontrolle auf Systeme

Technische und organisatorische Maßnahmen zur Benutzeridentifikation und -authentifizierung:

Unbefugter Zugang auf IT-Systeme wird verhindert.

Technische (ID-/Passwortsicherheit) und organisatorische (Benutzerstammdaten) Maßnahmen zur Benutzeridentifikation und -authentifizierung werden eingesetzt. Dies sind unter anderem Passwortverfahren (inkl. Sonderzeichen, Mindestlänge), grundsätzlicher Einsatz der 2-Faktor Authentisierung für alle Authentisierungsvorgänge, Least Privilege Mechanismus, automatische Sperrung (z.B. Passwort oder Timeout) – auch der Geräte nach längerer Abwesenheit bis zum Update auf aktuellen Stand, Anlegen nur eines Stammdatensatzes pro Benutzer, erzwungen durch den übergreifenden Verzeichnisdienst und die grundsätzliche Verschlüsselung von Data at Rest und Data in Transit.

3. Zugriffskontrolle

Anforderungsgerechte Definition des Berechtigungsschemas und der Zugriffsrechte sowie Überwachung und Protokollierung der Zugriffe:

Aktivitäten in IT-Systemen, die nicht unter die zugewiesenen Zugriffsrechte fallen, werden verhindert.

Die Zugriffskontrolle auf Daten stellt sicher, dass nur Aktivitäten ausgeführt werden können, die den jeweils zugewiesenen Zugriffsrechten entsprechen. Dazu gehört ein angemessen definiertes Berechtigungsschema, das Rollen, Profile und spezifische Rechte für Transaktionen und Objekte umfasst. Zugriffe werden überwacht und protokolliert, während technische Maßnahmen wie Zugriffsbeschränkungen sowie Rechte zur Veränderung oder Löschung von Daten sicherstellen, dass nur autorisierte Personen entsprechende Aktionen durchführen können.

Dritte nur mit Registrierung zulässig

4. Weitergabekontrolle

Maßnahmen zum Transport, zur Übertragung und Kommunikation oder zur Speicherung von Daten auf Datenträgern (manuell oder elektronisch) und zur nachträglichen Prüfung:

Die Weitergabe personenbezogener Daten wird kontrolliert.

Die Weitergabekontrolle umfasst alle Maßnahmen, die sicherstellen, dass personenbezogene Daten bei elektronischer Übermittlung, Datentransport, Kommunikation oder Speicherung auf Datenträgern nur autorisiert weitergegeben werden. Dazu gehören der Einsatz von Verschlüsselung oder Tunnelverfahren wie VPN, elektronische Signaturen zur Absicherung der Identität und Integrität, die Protokollierung sämtlicher Übertragungen sowie technische und organisatorische Maßnahmen zur Transportsicherheit, um eine nachträgliche Prüfung und vollständige Nachvollziehbarkeit der Datenweitergabe zu gewährleisten.

5. Datenspeicherung und Vertraulichkeit – Schadsoftware und Angriffsschutz

Maßnahmen zur Gewährleistung der Verfügbarkeit und Vertraulichkeit:

Im Rahmen der Datenspeicherung sind technische und organisatorische Maßnahmen umgesetzt, um die Vertraulichkeit personenbezogener Daten sicherzustellen und diese wirksam vor Schadsoftware, Angriffen und sonstigen Sicherheitsbedrohungen zu schützen. Alle gespeicherten Daten sind gegen unbefugte Kenntnisnahme und unzulässige Veränderungen abgesichert. Hierzu werden aktuelle Virenschutzlösungen sowie weitere Schutzmechanismen gegen schädliche Programme eingesetzt. Zusätzlich bestehen Maßnahmen zum Schutz vor unbefugten Zugriffen und technischen Angriffen, einschließlich abgestufter Zugriffsberechtigungen, systemseitiger Zugriffsbeschränkungen und kontinuierlicher Überwachung sicherheitsrelevanter Ereignisse.

6. Verfügbarkeitsmanagement

Weitere Maßnahmen zur Gewährleistung der Verfügbarkeit:

Die Daten werden vor unbeabsichtigter Zerstörung oder Verlust geschützt.

Die Verfügbarkeitskontrolle umfasst alle Maßnahmen, die die physische und logische Sicherheit von Daten sicherstellen und einen kontinuierlichen Betrieb ermöglichen. Dazu gehören regelmäßige Backup-Verfahren mit nicht durch Microsoft kontrollierter Software, die Spiegelung von Daten in unterschiedlicher Azure-Datacenter innerhalb der EU sowie die Verfügbarkeitszusage für die MS-Dienste. Zum Schutz der Daten sind durch Antiviren- und Firewall-Systeme, ein SIEM und ein SOC im Einsatz. Ergänzend stellt ein Notfallwiederherstellungsplan nach ISO 27001 sicher, dass Daten und Systeme auch im Schadensfall schnell wiederhergestellt und betriebsbereit gemacht werden können.

7. Widerherstellbarkeit

Die Wiederherstellbarkeit von Daten ist gewährleistet.

Zur Sicherstellung der Verfügbarkeit und Integrität personenbezogener Daten werden alle relevanten Systeme regelmäßig und automatisiert gesichert (On-Premise, Microsoft Azure, Microsoft 365 und Dynamics CRM). Die Backups erfolgen nach definierten Intervallen und Aufbewahrungsfristen, werden getrennt vom Produktivsystem gespeichert und gegen unbefugten Zugriff geschützt. Sicherungs- und Wiederherstellungsprozesse werden überwacht, protokolliert und regelmäßig durch Wiederherstellungstests überprüft; Zugriffe auf Backup-Systeme sind rollenbasiert und auf autorisierte IT-Administratoren beschränkt.

8. Trennungskontrolle

Maßnahmen zur getrennten Verarbeitung (Speicherung, Änderung, Löschung, Übermittlung) von Daten für verschiedene Zwecke:

Zur Sicherstellung der Trennkontrolle ist gewährleistet, dass die Verarbeitung personenbezogener Daten ausschließlich zu den vorgesehenen Zwecken der Methan-VO erfolgt. Statistische Auswertungen werden ausschließlich in anonymisierter Form durchgeführt, sodass kein Rückschluss auf einzelne betroffene Personen möglich ist; sofern personenbezogene Daten verarbeitet werden, erfolgt dies ausschließlich im Rahmen des definierten Rollen- und Rechtekonzepts. Darüber hinaus besteht eine strikte Trennung zwischen Produktiv- und Testumgebungen, um eine Vermischung von Echt- und Testdaten zu verhindern. Zusätzlich ist eine Mandanten- und Nutzertrennung umgesetzt, durch die sichergestellt wird, dass Daten und Zugriffsrechte klar abgegrenzt

sind und ausschließlich autorisierte Nutzer Zugriff auf die jeweils zugewiesenen Daten erhalten.