Vereinbarung zur Auftragsverarbeitung

Auftragsverarbeitungsvertrag (AVV / AV-Vertrag) gemäß Art. 28 DSGVO

AV-Vertrag zwischen

(Auftraggeber/Verantwortlicher)

und

DMRZ Deutsches Mittelstandsrechenzentrum Betreibergesellschaft mbH
Hans-Wunderlich-Straße 6
49078 Osnabrück
(Auftragnehmer/Auftragsverarbeiter)

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Gegenstand des Auftrags ergibt sich aus der Autorisierung als DMRZ-Partner und / oder aus DMRZ-Kunden/Endkunden Aufträgen/Verträgen. Es wird ausdrücklich auf die Leistungsvereinbarungen der Produkte sowie Dienste des DMRZ, welche in direktem Zusammenhang mit der lt. Autorisierung gewählten Partnerstufe stehen, verwiesen. Zentraler Gegenstand des Auftrages sind folgende Produkte/Leistungen: Housing, Hosting, IaaS/PaaS/SaaS (Infrastructure/Platform/Software as a Service), Backup, Consulting und die Erbringung von Carrier-Leistungen.

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Partnerschaft mit dem DMRZ und den Leistungsvereinbarungen der Produkte und Dienste des DMRZ.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber ergeben sich aus den Leistungsvereinbarungen der über das DMRZ bezogenen Produkte und Dienste.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind. Das angemessene Schutzniveau in Deutschland
– ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO);
– wird hergestellt durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO);
– wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DS-GVO);
– wird hergestellt durch genehmigte Verhaltensregeln (Art 46 Abs. 2 lit. e i.V.m. 40 DS-GVO);
– wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO).

(2) Art, Umfang und Zweck der Datenerhebung, -verarbeitung oder -nutzung

Der Auftraggeber hat den Auftragnehmer mit der Erbringung von Leistungen beauftragt.

Gegenstand der Datenerhebung, -verarbeitung oder -nutzung sind Daten, die nachfolgenden Datenarten/-kategorien angehören sowie Daten, die im Rahmen der Leistungserbringung und zum Zwecke der Vertragserfüllung genutzt werden müssen. Zusätzlich sind Daten eingeschlossen, die sich aus den Leistungsvereinbarungen der geschlossenen Aufträge und Verträge ergeben.

– Personenstammdaten (Name, Anschrift, Geburtsdatum etc.)
– Kommunikationsdaten (wie z. B. Telefon, E-Mail)
– Vertragsstammdaten (Vertragsverhältnis, Produktinteresse oder Vertragsinteresse)
– Kundenhistorie
– Vertragliche Abrechnungs- und Zahlungsdaten
– Planungs- und Steuerungsdaten
– Infrastrukturdaten (z.B. IP-Adressen)
– Gespeicherte Daten bei Wartungsarbeiten
– Im Gefahrenfall Zugriffe
– Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

Im Rahmen der nachfolgenden Produktkategorien werden Daten wie folgt genutzt:

Cloud Solutions (z.B. über das DMRZ verwaltete Dienste | Full-Managed):
– Sicherstellen der Funktion der Infrastruktur/Dienste/Leistungen
– Im Rahmen von Wartungsarbeiten
– Speichern der Benutzerdaten

Cloud Services (z.B. von Partnern verwaltete SaaS/PaaS Angebote | Self-Managed):
– Sicherstellen der Funktion der Infrastruktur/Dienste/Leistungen
– Im Rahmen von Wartungsarbeiten
– Speichern der Benutzerdaten

Infrastructure Services (z.B. Housing, Hosting, IaaS Angebote | Self-Managed):
– Sicherstellen der Funktion der Infrastruktur/Dienste/Leistungen
– Im Rahmen von Wartungsarbeiten
– Speichern der Benutzerdaten

Backup und Monitoring Angebote/Leistungen:
– Sicherstellen der Funktion der Infrastruktur/Dienste/Leistungen
– Im Rahmen von Wartungsarbeiten
– Speichern der Benutzerdaten

Carrier Leistungen (z.B. Telefonanschlüsse, Vernetzungen, Internetanschlüsse)
– Sicherstellen der Funktion der Infrastruktur/Dienste/Leistungen
– Im Rahmen von Wartungsarbeiten
– Speichern der Benutzerdaten

(3) Kategorien betroffener Personen:

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen jeweils den Auftraggeber sowie den Auftragnehmer:

– Kunden
– Interessenten
– Abonnenten
– Beschäftigte
– Lieferanten
– Handelsvertreter
– Ansprechpartner
– Freelancer

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hält zusätzlich zu der Einhaltung der Regelungen dieses Auftrags die gesetzlichen Pflichten gemäß Art. 28 bis 33 DS-GVO ein; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

(1) Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer werden Rüdiger Sievers und Björn Stange(DMRZ Deutsches Mittelstandsrechenzentrum Betreiberges. mbH, Hans-Wunderlich-Straße 6, 49078 Osnabrück, +49 (541) 2019-2600, service@dmrz.email) benannt.

(2) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO: Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

(3) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

(4) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

(5) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

(6) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

(7) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

(8) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Datengeheimnis

(1) Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers, das Datengeheimnis zu wahren.

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und sie auf das Datengeheimnis schriftlich verpflichtet. Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.

(3) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

7. Unterauftragsverhältnisse (Subunternehmer)

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

Neue Subunternehmer werden 14 Tage vor Beginn der Arbeitsaufnahme auf der Webseite veröffentlicht. Der Auftragnehmer führt vorher eine Auftragskontrolle nach Art. 28 Abs.2-4 DS-GVO durch.

Die Auslagerung auf Unterauftragnehmer oder der Wechsel der bestehenden Unterauftragnehmer sind zulässig, soweit:
– der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
– der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
– eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragsverarbeiter, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

8. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch
– die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
– die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
– aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision,

Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
– eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

9. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

10. Weisungsbefugnis und Pflichten des Auftraggebers

(1) Der Auftraggeber hat das Recht, Weisungen gegenüber dem Auftragnehmer zu erteilen. Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen.

Weisungsstellen bei Auftragnehmer sind:

E-Mail: service@dmrz.email
In Ausnahmefällen Telefon: +49 (541) 2019-2600

Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. der Vertreter mitzuteilen. Falls Weisungen, die unter Nr. 2 dieses Vertrages getroffenen Festlegungen ändern, aufheben oder ergänzen, sind diese nur zulässig, wenn eine entsprechende neue Festlegung erfolgt. Diese Weisung muss schriftlich erfolgen, bspw. über ein Ticket.

(2) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt oder er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

(3) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

11. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

12. Sonstiges

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter, etwa durch Pfändung oder Beschlagnahmung oder durch sonstige Ereignisse gefährdet sein, hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen. Der Auftragnehmer weist die Dritten darauf hin, dass die Verantwortlichkeit und das Eigentum an den Daten ausschließlich beim Auftraggeber liegen.

(2) Für Änderungen, Ergänzungen und Nebenabreden ist die Schriftform erforderlich.

(3) Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

13. Wirksamkeit der Vereinbarung

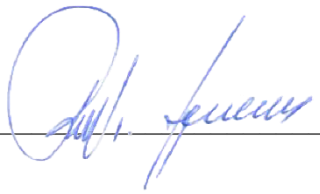
Sollte eine oder mehrere Klauseln aus diesem Vertrag unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Anlagen

Die folgenden Anlagen sind Bestandteile dieser Vereinbarung:

- Anlage 1: Technisch-organisatorische Maßnahmen zur Einhaltung des Datenschutzes
- Anlage 2: Liste der eingesetzten Subunternehmer/Unterauftragsnehmer

Stand: 01.11.2024

Verantwortlicher:	**Auftragsverarbeiter:**
	DMRZ Deutsches Mittelstandsrechenzentrum Betreiberges. mbH
Ort, Datum: _____	**Ort, Datum:** Osnabrück, 10.11.2024
Name: _____	**Name:** Rüdiger Sievers
Unterschrift: _____	**Unterschrift:** _____ 
Name: _____	**Name:** Björn Stange
Unterschrift: _____	**Unterschrift:** _____ 

Technisch-organisatorische Maßnahmen

Technisch-organisatorische Maßnahmen zur Einhaltung des Datenschutzes (Anlage 1)

Einleitung

Technisch-organisatorische Maßnahmen beschreiben die technischen und organisatorischen Sicherheitskontrollen, die im Zusammenhang mit den Dienstleistungen des DMRZ, dem technischen Support und anderen Dienstleistungen im Rahmen von indirekten (Kunden/Partner) und direkten (Endkunden) Verträgen/Aufträgen durchgeführt werden. Diese Technisch-organisatorischen Maßnahmen werden als Anhang zum Auftragsverarbeitungsvertrag (AVV) aufgenommen.

DMRZ führt Datenverarbeitung an unterschiedlichen Standorten durch. Dies betrifft den Sitz des DMRZ in Osnabrück und Hennef sowie den Betrieb von Serversystemen in Deutschland. Detaillierte Standortangaben können auf Wunsch über die Leistungsbeschreibungen der jeweiligen Rechenzentrumsbetreiber eingesehen werden. Angaben zu den Betreibern sind im Bereich Subunternehmer/Unterauftragsnehmer ausgewiesen. Bei Fragen wenden Sie sich bitte an das DMRZ.

Die Kunden des DMRZ haben sich laut Art. 28 DS-GVO von der Einhaltung der technischen und organisatorischen Maßnahmen zur Einhaltung des Datenschutzes zu überzeugen, welche in Art. 32 Abs. 1 DS-GVO konkretisiert werden. Grundlage hierfür bildet diese Dokumentation. Die Gliederung dieser Dokumentation richtet sich nach dem Aufbau des Art. 32 Abs. 1 DS-GVO.

1. Vertraulichkeit (Art. 32 Abs. 1 Ziff. b DS-GVO)

1.1 Zutrittskontrolle

1.1.1 Zutrittskontrolle (Osnabrück)

In den einzelnen Bereichen des Firmengebäudes wird die Zutrittskontrolle durch ein elektronisches Zutrittskontrollsystem geregelt. Im Innenbereich des Firmengebäudes sind unterschiedliche Sicherheitszonen eingerichtet, für die, zeitlich begrenzt, unterschiedliche Berechtigungen eingerichtet werden. Jeder Mitarbeiter erhält einen Zugangscode, der einer Gruppe zugeordnet ist, die den Zugangsbereich regelt.

Es ist ein Empfang eingerichtet, der den Zutritt von betriebsfremden Personen kontrolliert. Besucher müssen klingeln und sich nach Zutritt zum Gebäude beim Empfang anmelden. Besucher werden nicht registriert. Innerhalb des Firmenbereichs werden die Besucher geführt. Dabei liegt es in der Verantwortung des Empfangs, die Besucher zu den jeweiligen Mitarbeitern zu führen. Jeder Mitarbeiter ist dann für seine Besucher verantwortlich.

Nebenausgänge, Fluchttüren und sonstige Notausgänge können von außen nicht geöffnet werden.

1.1.2 Zutrittskontrolle (Rechenzentrum Medialine Eurotrade AG, Frankfurt)

Es existieren folgende Maßnahmen zur Zutrittskontrolle:

- Überwachung des Geländes/dem Gebäude des Rechenzentrums außerhalb der
- Betriebsstunden durch Wachpersonal.
- Alarmanlage gegen Einbruch existiert.
- Schließsystem mit Sicherheitsschlössern.
  Nutzung von Token, Programmierung auf jeden einzelnen Mitarbeiter.
- Besucher werden durch interne Mitarbeiter begleitet.
- Zutritt zum Serverraum nur durch autorisierte Mitarbeiter.
- Sorgfältige Auswahl von Reinigungspersonal.
- Schlüssel- bzw. Tokenregelung (Schlüssel-/Tokenverwaltung, Schlüssel-/Tokenausgabe)

1.2 Zugangskontrolle

Die Zugangskontrolle verhindert, dass Datenverarbeitungsanlagen von Unbefugten genutzt werden können. Die Server im Rechenzentrum werden ausschließlich von namentlich benannten Mitarbeitern der DMRZ administriert und diese verfügen hierzu über entsprechende Benutzerkonten. Die Administration erfolgt über das Internet mittels verschlüsselter Verbindungen. Mitarbeiter des Rechenzentrumbetreibers haben keinen Zugang zu Kundendaten oder der Datenverarbeitungssoftware.

Um nicht autorisierten Zugang über das Internet zu verhindern sind Serversysteme grundsätzlich durch Firewalls geschützt. Zum weiteren Schutz sind Kunden-/Gast-Netzwerke durch eigenständige Firewalls gesichert und abhängig von der Leistungsbeschreibung durch ein dediziertes virtuelles Netzwerk von den anderen Betriebsbereichen abgetrennt. Zugriffe auf das Management Netzwerk werden über eine eigene hardwarebasierte Firewall geschützt.

Der Zugang zu Rechnern in den Büroräumen der DMRZ wird über Benutzerkonten kontrolliert. Hierzu hat jeder Mitarbeiter auf seinem Rechner ein eigenes Benutzerkonto. Der Zugriff auf das bürointerne Netzwerk von außerhalb der Büroräume ist ausschließlich über eine VPN-Verbindung (Virtual Private Network) möglich. Das bürointerne Netzwerk wird ebenfalls von einer hardwarebasierten Firewall geschützt.

Der Zugang zu den Datenverarbeitungssystemen ist mit Benutzerkennung und einem sicheren Authentifizierungsverfahren geschützt. Zusätzlich werden Zugriffe auf Core-Systeme durch entsprechende ACLs (Access Control Lists) geschützt.

Es sind Regeln zur Bildung eines sicheren Passworts festgelegt.

1.3 Zugriffskontrolle

Die Zugriffskontrolle gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

In den vom Auftragnehmer genutzten Datenverarbeitungssystemen sind Berechtigungsprofile hinterlegt, in denen die zugriffsberechtigten Personen festgelegt sind. Die Rechte werden in einem geregelten Verfahren vergeben, und die Notwendigkeit der bestehenden Rechte wird regelmäßig kontrolliert. Die Einrichtung und Freigabe werden dokumentiert.

Der Auftragnehmer hat die technischen und organisatorischen Maßnahmen getroffen, die sicherstellen, dass ausscheidenden Mitarbeitern sämtliche Unterlagen, Zugangsberechtigungen und Zugriffsrechte entzogen bzw. gelöscht werden, um einen unberechtigten Zugriff auf die Daten des Auftraggebers zu verhindern.

Der Zugang zu Daten über Kunden für den DMRZ-Support ist auf ein Mindestmaß beschränkt. Dieser Zugang erfolgt über eine eigene Installation. Damit ist es möglich, Informationen zu den Kunden einzusehen, die für die Aufgaben des Supports notwendig sind. Diese Rolle muss jedem Supportmitarbeiter individuell zugewiesen werden.

Der Zugriff auf technischer Ebene auf Kundendaten, z.B. über Serverinstanzen / Cloud Account des Kunden, ist ausschließlich eigens dafür benannten Mitarbeitern aus dem Team „Service & Support“ der DMRZ möglich. In diesem Fall verwenden besagte Mitarbeiter jeweils eigene Benutzerkonten. Der Zugriff ist nur gestattet, wenn eine Supportaufgabe vorliegt, die nicht durch den Kunden oder den Support allein gelöst werden kann und der Auftraggeber seine Einwilligung zum Zugriff schriftlich erteilt hat. Diese wird im Ticketsystem protokolliert. Sollte die Aufgabe auch durch direkten Zugriff auf die Daten nicht lösbar sein, kann eine lokale Kopie der Daten z.B. für Debuggingzwecke erstellt und dem verantwortlichen Softwareentwickler / Vorlieferant zugänglich gemacht werden.

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

DMRZ verarbeitet die Daten mehrerer Kunden auf den gleichen Servern. Die strikte Trennung der Daten einzelner Kunden voneinander wird durch eine Reihe von Maßnahmen sichergestellt: Jeder Kunde hat eine eigene virtuelle Cloud Umgebung mit eigenen Benutzerkonten innerhalb einer mehrstufig automatisierten Cloud Betriebsplattform, die wiederum Multi-Tenant fähig ist. Bei Cloud Umgebungen, die ausschließlich über das DMRZ verwaltet werden oder eine Integration zwischen der automatisierten Cloud Betriebsplattform und der über das DMRZ gemanagten Cloud Umgebung notwendig ist, übernehmen DMRZ-Mitarbeiter die Trennung und oder Integration der Systeme und Netzwerke.

2. Integrität (Art. 32 Abs. 1 Ziff. b DS-GVO)

2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

Wie unter 1.4 beschrieben unterscheidet das DMRZ zwischen dem Betrieb von Systemen innerhalb einer durch das DMRZ verwalteten Umgebung (Full-Managed) und einer automatisierten Cloud Betriebsplattform (Self-Managed) bei der die Pflege dieser Systeme liegen jedoch vollkommen in den Händen des Kunden. Damit liegen auch alle Sicherungsmaßnahmen in den Händen des Kunden. Das Management Netz der DMRZ ist von Kunden- / Gastnetzwerken abgekapselt.

Bezugnehmend auf die Cloud Betriebsplattform sind Kunden-Netze im Standard durch VLAN voneinander getrennt. Diese VLANs werden automatisch verwaltet. Eine Doppelvergabe ist nicht möglich. Ebenfalls werden öffentliche IP-Adressen automatisiert vergeben. Es existiert eine virtuelle Firewall vor jedem durch den Kunden oder das DMRZ angelegtes Netzwerk. Abhängig von der Partnerstufe und durch das DMRZ vergeben Rechte innerhalb der Cloud Betriebsplattform kann diese durch den Kunden vollständig eigenständig verwaltet werden.

Der Kunde kann kostenpflichtig die Erstellung von regelmäßigen Backups hinzubuchen und ebenfalls eigenständig verwalten. Die Verschlüsselung der Backup Datensätze ist obligatorisch und erfolgt kundenseitig. Diese Passwörter sind der DMRZ nicht bekannt und können auch nicht ausgelesen oder zurückgesetzt werden.

Bei der durch das DMRZ verwalteten Umgebung werden Netzwerke sowie VLANs und Firewalls nur von speziell geschulten Mitarbeitern gepflegt. Gleiches gilt für die Verwaltung von öffentlichen IP-Adressen.

2.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind. Zugriffe auf Management Systeme werden protokolliert. Konfigurationsänderungen werden protokolliert und gespeichert. Zur Gewährleistung der Eingabekontrolle sind die von Softwareherstellern mitgebrachen Log Mechanismen
und Transaktionsprotokolle, zur Protokollierung von Eingaben für Anwendungen, vorhanden. Zusätzlich werden Änderungen mittels eines ticketbasierenden Change Management Software System durchgeführt, protokoliert und archiviert.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 Ziff. b DS-GVO)

Ein mehrstufiges Sicherheitskonzept stellt die Verfügbarkeit der Daten sicher. Alle physikalischen Datenträger (Festplatten) sind als RAID-Verbund ausfallsicher angelegt und jede Komponente des verwendeten Storage Area Network (SAN) ist

redundant vorhanden. Der Status der Datenträger wird laufend automatisch überwacht und defekte Festplatten werden unverzüglich ausgetauscht.

Für das interne Management und das interne Office werden Backups nach einem Backup-Plan durchgeführt.

Standardmäßig werden keine eigenständigen / zusätzlichen Backups von Kundensystemen vorgenommen. Wie erwähnt, bietet die DMRZ jedoch entsprechende Backuplösungen kostenpflichtig an. Bei ausgewählten Produkten/Diensten (meist aus dem Bereich Full-Managed / Cloud Solutions) übernimmt das DMRZ sogenannte Managed Service Leistungen. Bei diesen Leistungen kann ein Backup enthalten sein, Details können den entsprechenden Leistungsbeschreibungen entnommen werden.

Die Rechenzentren der DMRZ bietet durch vollklimatisierte Sicherheitsräume zusammen mit einer Löschanlage weitgehenden Schutz vor Schäden durch äußere Einflüsse wie Feuer, Gas und Wasser. Die Rechenzentrumsbetreiber der DMRZ garantieren zusätzlich eine unterbrechungsfreie Stromversorgung. Die Rechenzentrumsbetreiber sind in Anlage 2 – Subunternehmer/Unterauftraggeber aufgeführt. Weitere Details gehen aus den entsprechenden Leistungsbeschreibungen der Betreiber detailliert hervor.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 Ziff. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

4.1 Datenschutzmanagement

DMRZ ist sich seiner Verantwortung in Bezug auf Datenschutz sehr bewusst. Deshalb wird dem Datenschutzmanagement eine besondere Stellung in unserem Haus zuteil.

Unsere Mitarbeiter sind umfassend mit dem Thema durch Schulungen und andere Sensibilisierungsmaßnahmen vertraut gemacht worden.

Wir sind uns aber auch der Tatsache bewusst, dass Datenschutz und IT-Sicherheit zwei Seiten einer Medaille darstellen und damit untrennbar miteinander verbunden sind. Dem tragen wir in einer Richtlinie zur Informationssicherheit und einer IT-Sicherheitsrichtlinie Rechnung. Deren Umsetzung wird durch sämtliche Mitarbeiter unseres Unternehmens sichergestellt.

Das Datenschutzmanagement wurde in die bestehenden Qualitätsicherungssysteme, sowie in das Changemanagement und Ticketing System integriert und orientiert sich an den in den Systemen bereits etablierten Berechtigungsstrukturen.

Der Aufbau unseres Datenschutz- und IT-Sicherheitsmanagements orientiert sich am BSI-Grundschutz.

4.2 Incident-Reponse-Management

Innerhalb der DMRZ wurde ein sehr umfangreiches Incident und Ticket Systeme eingeführt. Anfragen sind ausschließlich über diese Plattform zu stellen und werden innerhalb des Systems entsprechend verwaltet und archiviert. Telefonische Anfragen werden von den Mitarbeitern in eine schriftliche Anfrage verwandelt.

Für die internen Prozesse zur Qualitätssicherung, Installationsüberwachung und zum Zwecke des Change-Managements wird eine weitere, unabhängige „interne“ Plattform betrieben. Zu diesem System haben nur autorisierte Mitarbeiter Zugriff.

Alle Mitarbeiter, die mit der Entwicklung, der Bereitstellung und der Unterstützung der über die DMRZ angebotenen Dienste und Produkte in Kontakt kommen, wurden geschult und haben sich mit ihren Aufgaben in diesem Zusammenhang vertraut gemacht.

4.3 Datenschutzfreundliche Voreinstellungen

Die zur Eingabe von Daten bestehenden Portale sind so konzipiert, dass ausschließlich Daten erhoben werden, die zur Ausführung der bestellten Leistung entweder für den Bestellprozess selbst, zur Installation oder zur Durchführung von Wartungsarbeiten benötigt werden.

Die Art der Daten, die vom Auftraggeber erfasst und verarbeitet werden, liegen rein in der Verantwortung des Auftraggebers. So hat der Auftraggeber das dem Verarbeitungsrisiko angemessene Schutzniveau zu ermitteln und die diesbezügliche Schutzbedarfsklassifizierung zu dokumentieren.

4.4 Auftragskontrolle

Ziel der Auftragskontrolle ist es, zu gewährleisten, dass die Verarbeitung personenbezogener Daten durch einen Dritten im Auftrag Ihres Unternehmens (Auftragsdatenverarbeitung) nur entsprechend den Weisungen des Auftraggebers erfolgt.

Zur Auftragskontrolle wird ein definierter Prozess verwendet, der insbesondere folgende Inhalte betrachtet: Aufträge werden nur nach einer vorherigen Überprüfung der Zulässigkeit bei Auftragsdatenverarbeitungen schriftlich getroffen. Zusätzliche Vereinbarungen bedürfen ebenfalls der Schriftform. Der Auftrag enthält eine klare Abgrenzung der Kompetenzen und Pflichten zwischen Auftragnehmer und Auftraggeber. Unterauftragsverhältnisse sind offen zu legen und entsprechend zu überprüfen.

Vor der Vergabe erfolgt eine Überprüfung der technisch- organisatorischen Maßnahmen des Auftragnehmers. Wenn erforderlich, werden zusätzliche Sicherheitsmaßnahmen definiert und umgesetzt. Zur Überwachung der ordnungsgemäßen Vertragsausführung erfolgt mindestens einmal im Jahr eine Kontrolle des Auftragnehmers. Diese kann auch durch einen entsprechenden Nachweis erbracht werden (z.B. TÜV Audit).

Sonstige Angaben

Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Wesentliche Änderungen sind schriftlich festzuhalten und dem Auftraggeber bekannt zu geben.

Weiterführende Informationen sind den Leistungsbeschreibungen der Produkte/Dienste/Verträge zu entnehmen. Zusätzlich wird auf die Leistungsbeschreibungen der Vorlieferanten sowie Subunternehmer/Unterauftragsnehmer verwiesen. Dieser Verweis ist gerade in Bezug auf den Betrieb von IT- und Kommunikationssystemen zu beachten.

Stand: 01.11.2024

Subunternehmer/Unterauftragnehmer

Liste der eingesetzten Subunternehmer/Unterauftragsnehmer (Anlage 2)

UNTERAUFTRAGNEHMER	LEISTUNG/BEREICH	SITZ/ANSCHRIFT
Autotask GmbH	CRM / ERP Lösung | Ticket-System | Kundenportal	Germany: 80336, München
Amazon Web Services, Inc.	Rechenzentrumsbetrieb	USA: WA 98109, Seattle
Microsoft Corporation	Rechenzentrumsbetrieb	USA: WA 98052-6399, Redmond
Medialine Eutrotrade AG	Rechenzentrumsbetrieb	Germany: 55566, Bad Sobernheim
AGILESTORAGE Europe GmbH	Support Infrastruktur	Germany: 85375, Neufahrn BY Switzerland: 6331, Hünenberg ZG
Juniper Networks GmbH	Support Infrastruktur	Germany: 80807, München
Mikrotīkls SIA	Support Infrastruktur	Latvia: LV-1039, Riga
Babylon Software Solution	Software- und Portalentwicklung	Macedonia: 1000, Skopje
1&1 Versatel GmbH	Carrier-Leistungen	Germany: 13407 Berlin
Telekom Deutschland GmbH	Carrier-Leistungen	Germany: 53227 Bonn
Plusnet Infrastruktur GmbH & Co. KG	Carrier-Leistungen	Germany: 50829, Köln
Cloudflare, Inc.	Domain- und DNS-Leistungen	USA: CA 94107, San Francisco
EPAG Domainservices GmbH	Domain- und DNS-Leistungen	Germany: 53113, Bonn
united-domains AG	Domain- und DNS-Leistungen	Germany: 82319, Starnberg
Kaseya Inc.	Endpoint Management & Monitoring	USA: FL 33131, Miami
Open Text Software GmbH	Support Back- und Migrationslösung	Germany: 85630, Grasbrunn
3iMedia GmbH	Support Telekommunikationslösung	Germany: 76149, Karlsruhe
Enreach Group	Support Telekommunikationslösung	Netzerlands: Flevoland 1321
Swyx Solutions GmbH	Support Telekommunikationslösung	Germany: 44227, Dortmund

Stand: 01.11.2024