

Nachfolgend finden Sie die technischen und organisatorischen Maßnahmen (TOM) i.S.d. Art. 32 DSGVO des Unterauftragnehmers

ANWR GROUP eG
Nord-West-Ring-Straße 11
63533 Mainhausen

Datenhaltung erfolgt in Azure (Microsoft Cloud Services).
Es wurde eine DSFA (Datenschutzfolgeabschätzung) durchgeführt.

Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO

der Organisation

ANWR GROUP eG

Nord-West-Ring-Straße 11 · 63533 Mainhausen

Tel: + 49 6182 928-0

info@anwr-group.com · www.anwr-group.com

Geltungsbereich: Zentrale Konzern-IT der ANWR-Gruppe ohne Banken

gültig ab: 01.12.2023

Version: 3.0

Änderungshistorie

| Version | Beschreibung | Bearbeiter | Datum |
|---------|----------------|---|------------|
| 1.0 | Ersterstellung | Fr. Siemes | 15.05.2018 |
| 2.0 | Überarbeitung | Hr. Ewers, Hr. Dulitz, Hr. Te Strote | 02.04.2020 |
| 3.0 | Überarbeitung | Hr. Ewers | 30.11.2023 |

| Version | Genehmigt durch | Datum |
|---------|----------------------------------|------------|
| 1.0 | Verena Siemes | 25.05.2018 |
| 2.0 | Andreas Ewers Sven Kulikowsky | 07.12.2020 |
| 3.0 | Andreas Ewers Sven Kulikowsky | 30.11.2023 |

Technische und organisatorische Maßnahmen

Zum Schutz der Verarbeitung personenbezogener, aber auch sonstiger betrieblicher Daten, wurden in allen Unternehmen der ANWR Gruppe ohne Banken, im Folgenden als „ANWR“ bezeichnet, folgende technische und organisatorische Maßnahmen (TOM) gemäß Art. 30 Abs. 1 lit. G) und Art. 32 DSGVO eingerichtet.

1 Maßnahmen zur Gewährleistung der Vertraulichkeit (Art. 32. Abs. 1 lit. b DSGVO)

1.1 Zutrittskontrolle

Schutzziel: Unbefugten soll der räumliche/körperliche Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten (pbD) verarbeitet oder genutzt werden, verwehrt werden.

| Technische Maßnahmen | Organisatorische Maßnahmen |
|--|--|
| <input checked="" type="checkbox"/> Alarmanlage | <input checked="" type="checkbox"/> Schlüsselregelung / Liste |
| <input checked="" type="checkbox"/> Automatisches Zutrittskontrollsystem | <input checked="" type="checkbox"/> Empfang / Rezeption / Pförtner |
| <input checked="" type="checkbox"/> Chipkarten / Transpondersysteme | <input checked="" type="checkbox"/> Besucher in Begleitung durch Mitarbeiter |
| <input checked="" type="checkbox"/> Sicherheitsschlösser | |
| <input checked="" type="checkbox"/> Absicherung der Gebäudeschächte | |
| <input checked="" type="checkbox"/> Türen mit Knauf Außenseite | |
| <input checked="" type="checkbox"/> Klingelanlage mit Kamera | |
| <input checked="" type="checkbox"/> Videoüberwachung der Eingänge | |

1.2 Zugangskontrolle

Schutzziel: Verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

| Technische Maßnahmen | Organisatorische Maßnahmen |
|--|--|
| <input checked="" type="checkbox"/> Login mit Benutzername + Passwort | <input checked="" type="checkbox"/> Verwalten von Benutzerberechtigungen |
| <input checked="" type="checkbox"/> Login mit biometrischen Daten | <input checked="" type="checkbox"/> Erstellen von Benutzerprofilen |
| <input checked="" type="checkbox"/> Anti-Viren-Software Server | <input checked="" type="checkbox"/> Zentrale Passwortvergabe |
| <input checked="" type="checkbox"/> Anti-Virus-Software Clients | <input checked="" type="checkbox"/> Richtlinie „Sicheres Passwort“ |
| <input checked="" type="checkbox"/> Firewall | <input checked="" type="checkbox"/> Allg. Richtlinie Datenschutz und / oder Sicherheit |
| <input checked="" type="checkbox"/> Mobile Device Management | <input checked="" type="checkbox"/> Mobile Device Policy |
| <input checked="" type="checkbox"/> Einsatz VPN bei Remote-Zugriffen | |
| <input checked="" type="checkbox"/> Verschlüsselung von Datenträgern | |
| <input checked="" type="checkbox"/> BIOS Schutz (separates Passwort) | |
| <input checked="" type="checkbox"/> Automatische Desktopsperrung | |
| <input checked="" type="checkbox"/> Verschlüsselung von Notebooks / Tablet | |

1.3 Zugriffskontrolle

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

| Technische Maßnahmen | Organisatorische Maßnahmen |
|--|--|
| <input checked="" type="checkbox"/> Externer Aktenvernichter (DIN 66399) | <input checked="" type="checkbox"/> Einsatz Berechtigungskonzepte |
| <input checked="" type="checkbox"/> Physische Löschung von Datenträgern → Datenträger werden zerstört, nicht gelöscht. | <input checked="" type="checkbox"/> Minimale Anzahl an Administratoren |
| | <input checked="" type="checkbox"/> Datenschutztresor |
| | <input checked="" type="checkbox"/> Verwaltung Benutzerrechte durch Administratoren und Service-Desk |

1.4 Trennungskontrolle

Schutzziel: Gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

| Technische Maßnahmen | Organisatorische Maßnahmen |
|--|---|
| <input checked="" type="checkbox"/> Trennung von Produktiv- und Testumgebung logisch | <input checked="" type="checkbox"/> Steuerung über Berechtigungskonzept |
| <input checked="" type="checkbox"/> Physikalische Trennung (Systeme / Datenbanken / Datenträger) | <input checked="" type="checkbox"/> Festlegung von Datenbankrechten |
| <input checked="" type="checkbox"/> Mandantenfähigkeit relevanter Anwendungen | |

2 Maßnahmen zur Gewährleistung der Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Weitergabekontrolle

Schutzziel: Gewährleisten, dass pbD 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 pbD durch Einrichtungen zur Datenübertragung vorgesehen ist.

| Technische Maßnahmen | Organisatorische Maßnahmen |
|--|--|
| <input checked="" type="checkbox"/> Email-Verschlüsselung Nur falls Gegenseite keine Verschlüsselung unterstützt, wird unverschlüsselt gesendet | <input checked="" type="checkbox"/> Persönliche Übergabe mit Protokoll |
| <input checked="" type="checkbox"/> Einsatz von VPN | <input checked="" type="checkbox"/> Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts |

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| <input checked="" type="checkbox"/> Bereitstellung über verschlüsselte Verbindungen wie sftp, https | <input checked="" type="checkbox"/> Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden |

2.2 Eingabekontrolle

Schutzziel: Gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem pbD in Datenverarbeitungssysteme eingegeben, in diesen Systemen verändert oder entfernt worden sind.

| Technische Maßnahmen | Organisatorische Maßnahmen |
|--|---|
| <input checked="" type="checkbox"/> Technische Protokollierung der Eingabe, Änderung und Löschung von Daten in den wesentlichen Systemen für Kundendaten und Personaldaten | <input checked="" type="checkbox"/> Vier-Augenprinzip bei Personaldaten |

3 Maßnahmen zur Gewährleistung der Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

3.1 Verfügbarkeitskontrolle

Schutzziel: Gewährleisten, dass pbD gegen zufällige Zerstörung oder Verlust geschützt sind.

| Technische Maßnahmen | Organisatorische Maßnahmen |
|--|--|
| <input checked="" type="checkbox"/> Feuer- und Rauchmeldeanlagen | <input checked="" type="checkbox"/> Backup & Recovery-Konzept (ausformuliert) |
| <input checked="" type="checkbox"/> Feuerlöscher Serverraum | <input checked="" type="checkbox"/> Kontrolle des Sicherungsvorgangs |
| <input checked="" type="checkbox"/> Serverraumüberwachung Temperatur und Feuchtigkeit | <input checked="" type="checkbox"/> Existenz eines Notfallplans (z.B. BSI IT-Grundschrift 100-4) für zentrale IT in Mainhausen |
| <input checked="" type="checkbox"/> Serverraum klimatisiert | <input checked="" type="checkbox"/> Getrennte Partitionen für Betriebssysteme und Daten |
| <input checked="" type="checkbox"/> USV | |
| <input checked="" type="checkbox"/> Schutzsteckdosenleisten Serverraum | |
| <input checked="" type="checkbox"/> RAID System / Festplattenspiegelung | |
| <input checked="" type="checkbox"/> Alarmmeldung bei unberechtigtem Zutritt zum Serverraum | |
| <input checked="" type="checkbox"/> Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums. | |

4 Maßnahmen zur Gewährleistung der Nichtverkettbarkeit durch Zweckbestimmung (Art. 32 Abs. 1 lit. a DSGVO)

4.1 Pseudonymisierung und Verschlüsselung

Schutzziel: Sicherstellung der Nichtdecodierbarkeit (d.h. pbD können keiner spezifischen betroffenen Person zugeordnet werden) verarbeiteter pbD durch Pseudonymisierung und Verwendung allgemeiner Verschlüsselungsverfahren

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| <input checked="" type="checkbox"/> PbD Endkunden-Daten von Marktplätzen werden anonymisiert. | <input checked="" type="checkbox"/> Interne Anweisung, personenbezogene Endkunden-Daten von Marktplätzen im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren |

5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

5.1 Datenschutzkonzept und Datenschutzmanagement-System

Schutzziel: regelmäßiges Monitoring und Kontrollschritte zur Überwachung ordnungsgemäßer Verarbeitung

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|--|
| <input checked="" type="checkbox"/> Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung | <input checked="" type="checkbox"/> Externer Datenschutzbeauftragter |
| <input checked="" type="checkbox"/> Anderweitiges dokumentiertes Sicherheits-Konzept | <input checked="" type="checkbox"/> Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet |
| | <input checked="" type="checkbox"/> Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich |
| | <input checked="" type="checkbox"/> Interner Informationssicherheits-Beauftragter (Chief Data Officer) |
| | <input checked="" type="checkbox"/> Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt |
| | <input checked="" type="checkbox"/> Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach |
| | <input checked="" type="checkbox"/> Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden |

| Technische Maßnahmen | Organisatorische Maßnahmen |
|----------------------|---|
| | <input checked="" type="checkbox"/> Regelmäßige Kontrollhandlungen durch externen DSB inkl. Berichterstattung an den Vorstand |

5.2 Incident-Response-Management

Schutzziel: Unterstützung bei der Reaktion auf Sicherheitsverletzungen

| Technische Maßnahmen | Organisatorische Maßnahmen |
|---|---|
| <input checked="" type="checkbox"/> Einsatz von Firewall und regelmäßige Aktualisierung | <input checked="" type="checkbox"/> Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Daten-Pannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde) |
| <input checked="" type="checkbox"/> Einsatz von Spamfilter und regelmäßige Aktualisierung | <input checked="" type="checkbox"/> Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen |
| <input checked="" type="checkbox"/> Einsatz von Virens Scanner und regelmäßige Aktualisierung | <input checked="" type="checkbox"/> Einbindung von DSB und ISB in Sicherheitsvorfälle und Datenpannen |
| <input checked="" type="checkbox"/> Intrusion Prevention System (IPS) | <input checked="" type="checkbox"/> Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem |

5.3 Datenschutzfreundliche Voreinstellungen

Schutzziel: Privacy by design / Privacy by default

| Technische Maßnahmen | Organisatorische Maßnahmen |
|--|----------------------------|
| <input checked="" type="checkbox"/> Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind. | |

5.4 Auftragskontrolle

Schutzziel: Gewährleisten, dass pbD, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können

| Technische Maßnahmen | Organisatorische Maßnahmen |
|----------------------|---|
| | <input checked="" type="checkbox"/> Abschluss einer Vereinbarung zur Auftragsverarbeitung |