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: 3.1 - Entwurf

Änderungshistorie

Version	Beschreibung	Bearbeiter	Datum
1.0	Ersterstellung	Fr. Siemes	15.05.2018
2.0	Uberarbeitung	Hr. Ewers, Hr. Dulitz, Hr. Te Strote	02.04.2020
3.			

Version	Genehmigt durch	Datum
1.0	Verena Siemes	25.05.2018
2.0	Andreas Ewers Sven Kulikowsky	07.12.2020

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
☒ Alarmanlage	☒ Schlüsselregelung / Liste
☒ Automatisches Zugangskontrollsystem	☒ Empfang / Rezeption / Pförtner
☒ Chipkarten / Transpondersysteme	☒ Besucher in Begleitung durch Mitarbeiter
☒ Sicherheitsschlösser	
☒ Absicherung der Gebäudeschächte	
☒ Türen mit Knauf Außenseite	
☒ Klingelanlage mit Kamera	
☒ Videoüberwachung der Eingänge	

1.2 Zugangskontrolle

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

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Login mit Benutzername + Passwort	☒ Verwalten von Benutzerberechtigungen
☒ Login mit biometrischen Daten	☒ Erstellen von Benutzerprofilen
☒ Anti-Viren-Software Server	☒ Zentrale Passwortvergabe
☒ Anti-Virus-Software Clients	☒ Richtlinie „Sicheres Passwort"
☒ Firewall	☒ Allg. Richtlinie Datenschutz und / oder Sicherheit
☒ Mobile Device Management	☒ Mobile Device Policy
☒ Einsatz VPN bei Remote-Zugriffen	
☒ Verschlüsselung von Datenträgern	
☒ BIOS Schutz (separates Passwort)	
☒ Automatische Desktopsperre	
☒ 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
☒ Aktenschredder (mind. Stufe 3, cross cut)	☒ Einsatz Berechtigungskonzepte
☒ Externer Aktenvernichter (DIN 32757)	☒ Minimale Anzahl an Administratoren
☒ Physische Löschung von Datenträgern → Datenträger werden zerstört, nicht gelöscht.	☒ Datenschutztresor
	☒ 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
☒ Trennung von Produktiv- und Testumgebung logisch	☒ Steuerung über Berechtigungskonzept
☒ Physikalische Trennung (Systeme / Datenbanken / Datenträger)	☒ Festlegung von Datenbankrechten
☒ 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
☒ Email-Verschlüsselung Nur falls Gegenseite keine Verschlüsselung unterstützt, wird unverschlüsselt gesendet	☒ Persönliche Übergabe mit Protokoll
☒ Einsatz von VPN	☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Bereitstellung über verschlüsselte Verbindungen wie sftp, https	☒ 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
☒ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten in den wesentlichen Systemen für Kundendaten und Personaldaten	☒ 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
☒ Feuer- und Rauchmeldeanlagen	☒ Backup & Recovery-Konzept (ausformuliert)
☒ Feuerlöscher Serverraum	☒ Kontrolle des Sicherungsvorgangs
☒ Serverraumüberwachung Temperatur und Feuchtigkeit	☒ Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4) für zentrale IT in Mainhausen
☒ Serverraum klimatisiert	☒ Getrennte Partitionen für Betriebssysteme und Daten
☒ USV	
☒ Schutzsteckdosenleisten Serverraum	
☒ RAID System / Festplattenspiegelung	
☒ Alarmmeldung bei unberechtigtem Zutritt zum Serverraum	
☒ 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
☒ PbD Endkunden-Daten von Marktplätzen werden anonymisiert.	☒ 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
☒ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung	☒ Externer Datenschutzbeauftragter
☒ Anderweitiges dokumentiertes Sicherheits-Konzept	☒ Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet
	☒ Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich
	☒ Interner Informationssicherheits-Beauftragter (Chief Data Officer)
	☒ Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
	☒ Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
	☒ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
	☒ 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
☒ Einsatz von Firewall und regelmäßige Aktualisierung	☒ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Daten-Pannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
☒ Einsatz von Spamfilter und regelmäßige Aktualisierung	☒ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
☒ Einsatz von Virenscanner und regelmäßige Aktualisierung	☒ Einbindung von DSB und ISB in Sicherheitsvorfälle und Datenpannen
☒ Intrusion Prevention System (IPS)	☒ Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem

5.3 Datenschutzfreundliche Voreinstellungen

Schutzziel: Privacy by design / Privacy by default

Technische Maßnahmen	Organisatorische Maßnahmen
☒ 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
	☒ Abschluss einer Vereinbarung zur Auftragsverarbeitung