Auftragsverarbeitungs-vereinbarung

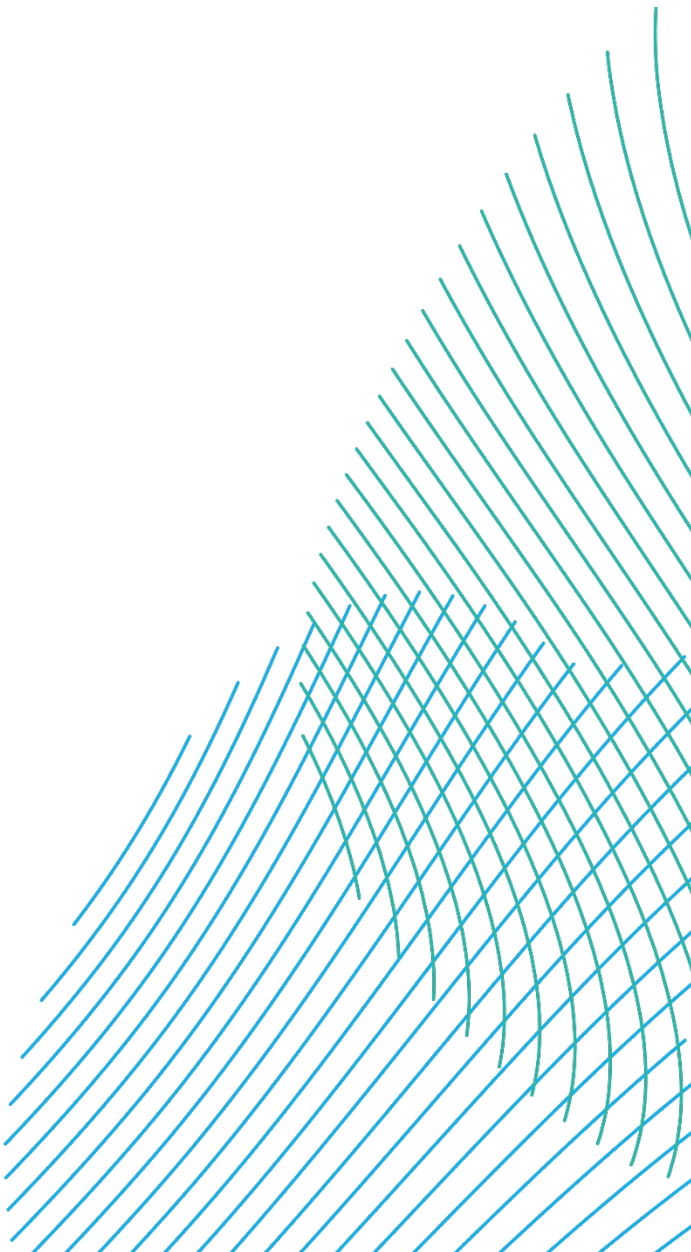
gemäß Artikel 28 Abs. 3 EU-Datenschutz-Grundverordnung („DSGVO“) zum Rahmen- oder Einzelvertrag Nr. oder Bestellung Nr.

zwischen der

(Auftraggeber)

und der

(Auftragnehmer)



Stand: 202311

Präambel
Der Auftraggeber möchte den Auftragnehmer mit den in Kapitel 2 Punkt 2.1 genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten im Auftrag. Insbesondere Art. 28 DSGVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist. Soweit die Leistungen zugleich für die RWE AG oder eines ihrer gem. § 15 ff. Aktiengesetz („AktG“) verbundenen Unternehmen erbracht werden, gilt diese Vereinbarung ebenfalls zugunsten dieser Unternehmen. Vor diesem Hintergrund wird Folgendes vereinbart:

Kapitel 1: Allgemeine Angaben zum Unternehmen

1.1 Angaben zum Unternehmen / Auftragnehmer

Name

Straße, Nr.

PLZ, Ort

Land

E-Mail

Telefon

1.2 Angaben zum Datenschutzbeauftragten des Auftragnehmers

Name

Unternehmen[1]

E-Mail

Telefon

1.3 Angaben zur Muttergesellschaft des Auftragnehmers[2]

Name

Land

☐ Es ist technisch und/oder organisatorisch ausgeschlossen, dass ein Datentransfer in ein Drittland erfolgt.

[1] Sofern abweichend vom unter 1.1 genannten Unternehmen (bspw. bei externem Datenschutzbeauftragten).
[2] Sofern abweichend von 1.1. geben Sie hier bitte die Kontaktdaten der Muttergesellschaft an, wenn der Auftragnehmer ein Unternehmen einer Unternehmensgruppe ist und die Muttergesellschaft außerhalb der EWR niedergelassen ist.

Kapitel 2: Angaben zur Verarbeitung personenbezogener Daten

2.1 Liefer- und Leistungsumfang

Benennen Sie den Liefer- und Leistungsumfang der als Auftragsverarbeitung gemäß Art. 28 DSGVO erbracht wird. Definieren Sie präzise den jeweils korrespondierenden Zweck sowie die Art der Verarbeitung von personenbezogenen Daten.

2.2 Ort der Leistungserbringung

Wichtig: Unter Berücksichtigung etwaig eingesetzter Unterauftragnehmer, vgl. Kapitel 3.6. und Anhang 2

☐ Die Erbringung der vertraglich vereinbarten Leistung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung von Teilleistungen oder der gesamten Dienstleistung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers in Schriftform oder dokumentiertem elektronischen Format und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

☐ Die Erbringung der vertraglich vereinbarten Leistung findet (ggf. teilweise) in einem Land außerhalb der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt („Drittland“). Das angemessene Schutzniveau wird unter den zusätzlich zu erfüllenden Anforderungen der Rechtsprechung des Europäischen Gerichtshofes („EuGH“), insb. der Rs. C-311/18 – "Schrems II", und den Empfehlungen des Europäischen Datenschutzausschusses (EDSA), gewährleistet.

2.3 Art der Daten

Hinweis: An dieser Stelle sind die personenbezogenen Daten anzugeben, die im Auftrag verarbeitet werden. Dies umfasst explizit nicht die personenbezogenen Daten, die Sie im Zuge der Kommunikation mit den Beschäftigten von RWE oder Daten des RWE Unternehmens bei Anbahnung des Vertrages sowie intern zur Rechnungslegung oder anderweitigen internen organisatorischen Aufgaben verarbeiten.

RWE

2.3.1 Datenkategorien, für die die technischen und organisatorischen Maßnahmen "Standard" gelten

Datenkategorie		Datenobjekte der Datenkategorie
☐	Adressdaten	Straße, Hausnummer, Postleitzahl, Wohnort, Appartementnummer etc.
☐	Altersdaten	Alter, Geburtsdatum, Geburtsort
☐	Anwenderdaten	Login-Name, Passwörter, Token oder andere Credentials, Nachname und E-Mail-Adresse, optional Vorname, geschäftliche Kontaktdaten (Telefon, Mobil, Fax), Abteilungszugehörigkeit, Position im Unternehmen, Dauer der Betriebszugehörigkeit
☐	Berufliche Tätigkeiten	Arbeitgeber, Funktionstitel, Beschreibung der Funktion, gegenwärtige Verantwortungen und Projekte, Arbeitsort, Arbeitsmodalitäten und -bedingungen u. a.
☐	Bildaufzeichnungsdaten	Daten im Rahmen von Bildaufzeichnungen jedweder Art wie Filme, Fotografien, Videoaufzeichnungen, digitale Fotografien, Infrarotaufnahmen, Röntgenbilder, u. a.
☐	Elektronische Identifikationsdaten	IP-Adressen, Cookies, Verbindungszeiten und -daten, elektronische Unterschrift u. a.
☐	Finanzidentifikationsdaten	Bankidentifikation und Bankkontonummer, Kredit und Lastschriftkartennummern, Geheimcodes u. a.
☐	Geolokalisierungsdaten	Informationen über den Aufenthaltsort, zurückgelegte Wegstrecken und geografische Informationen, die durch Sensoren, Aktoren, Protokolle und/oder Funktionalitäten von Geräten erhoben und verarbeitet werden

Datenkategorie		Datenobjekte der Datenkategorie
☐	Mitarbeiterdaten	Personalnummer, Mitarbeiter-ID-Nummer
☐	Namensdaten	Vor- und Nachname, Titel, Geburtsname, weitere Namen
☐	Öffentliche Identifikationsdaten	Nationale (Steuer-)Identifikationsnummer, Personalausweisnummer, Reisepass-Registrierungsnummer, Sozialversicherungsausweisnummer, Kraftfahrzeugkennzeichen, u.a.
☐	Private Kontaktdaten	Telefonnummern, E-Mail-Adresse, Social Media-Accounts, Fax etc.
☐	Renten/Pensionen	Eintrittsdatum in den Ruhestand, Art des Systems, Austrittsdatum, Details über erhaltene und ausgeführte Zahlungen, Optionen, Begünstigte u. a.
☐	Tonaufzeichnungsdaten	Daten im Rahmen von Tonaufzeichnungen jedweder Art wie elektronische und magnetische Tonträgeraufzeichnungen, Aufzeichnungen von Telefongesprächen und Videokonferenzen u. a.
☐	Transaktionsdaten und Logfiles	Zutritt- und Zugangslogs, System bzw. Zugriffslogs, Kommunikationsverbindungen etc.
☐	Sonstige	

2.3.2 Datenkategorien, für die die technischen und organisatorischen Maßnahmen "Erweitert" gelten

Datenkategorie		Datenobjekte der Datenkategorie
☐	Biometrische Identifikationsdaten	Fingerabdrücke, Stimmenerkennung, Netzhautabbildung, Erkennung des Gesichtes, der Finger- oder Handform, Unterschriftsdynamik, u. a.
☐	Daten über strafrechtliche Verurteilungen und Straftaten	Führungszeugnis, Daten über Verfehlungen und Straftaten, Bußgeldbescheide u. a.
☐	Ethnische Daten	Angaben zur Herkunft, Abstammung, zu Landsmannschaften, u. a.
☐	Genetische Daten	Daten im Rahmen einer Erkennung, Untersuchung der Erblichkeit, DNS, u. a.
☐	Körperlicher Gesundheitszustand	Ärztliche Akte, oder Bericht, Diagnose, Behandlung, Untersuchungsergebnis, Behinderung oder Gebrechen, Diät; andere besondere gesundheitliche Anforderungen für die Behandlung, Reise oder Unterkunft etc.
☐	Sexualverhalten	Angaben zu Sexualverhalten, zum Geschlecht, zur Geschlechtsumwandlung u. a.
☐	Medizinische Daten	Daten über die Mittel und Verfahren, die für die medizinische oder paramedizinische Betreuung der Patienten benutzt werden u. a.
☐	Politische Zugehörigkeiten	Angaben zur Parteizugehörigkeit, zu politischen Meinungen und Präferenzen, zu ausgeübten politischen Positionen u. a.
☐	Weltanschauliche, militante oder religiöse Überzeugungen	Angaben zu weltanschaulichen, militanten oder religiösen Überzeugungen, zu Mitgliedschaften in solchen Vereinigungen,

Datenkategorie		Datenobjekte der Datenkategorie
		Positionen und Funktionen, Mitgliedsbeiträge und geleistete Zuwendungen u. a.
☐	Sonstige	

2.3.3 Aktivierung der technischen und organisatorischen Maßnahmen „Erweitert“

☐ Unabhängig von der oben getroffenen Auswahl der Datenkategorien sichert der Auftragnehmer zu, sämtliche in Anhang 1 Punkt 1 und 2 aufgeführten technischen und organisatorischen Maßnahmen einzuhalten.

2.3.4 Folgende technischen und organisatorischen Maßnahmen können nicht oder nur teilweise erfüllt werden

Bitte hier mit der zugehörigen Nummer aus Anhang 1 (z. B. „1.5.3“) und Begründung angeben.

2.4 Kategorien betroffener Personen

☐ Beschäftigte[3]
☐ Angehörige von Beschäftigten
☐ Bewerber/innen
☐ Kunden
☐ Beschäftigte von Geschäftspartnern der RWE Gruppe
☐ Externe Dritte[4]
☐ Sonstiges:

[3] Definition: Arbeitnehmerinnen und Arbeitnehmer der RWE Gruppe, einschließlich der Leiharbeitnehmerinnen und Leiharbeitnehmer im Verhältnis zum Entleiher; zu ihrer Berufsbildung Beschäftigte; Rehabilitandinnen und Rehabilitanden; Freiwillige, die einen Dienst nach dem Jugendfreiwilligendienstgesetz oder dem Bundesfreiwilligendienstgesetz leisten.
[4] Definition: Externe Dritte sind Personen mit denen Unternehmen der RWE Gruppe keine vertragliche Beziehung hat (bspw. Polizei, Ordnungsamt, Bergbehörde, Interessenten oder Besucher).

2.5 Vertreter des Auftragnehmers in der Europäischen Union gem. Art. 27 Abs. 1 DSGVO[5]

Name

Straße, Nr.

PLZ, Ort

Land

E-Mail

Telefon

Kapitel 3: Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 Abs. 3 DSGVO

Die Verarbeitung personenbezogener Daten erfolgt im Auftrag des Verantwortlichen (Auftraggeber) im Sinne der Art. 4 Nr. 8 i. V. m. Art. 28 DSGVO.

Die hier zugrundeliegende Vereinbarung zur Auftragsverarbeitung wird zwischen dem/den beauftragenden Unternehmen des genannten Rahmen- oder Einzelvertrages sowie in 1.1 genanntem Auftragsverarbeiter (Auftragnehmer) geschlossen. Sofern weitere verbundene Unternehmen gemäß §§ 15 ff. AktG der RWE AG dem Einzel- oder Rahmenvertrag beitreten, gilt diese Vereinbarung zur Auftragsverarbeitung auch für diese gleichermaßen.

3.1 Gegenstand und Dauer des Auftrags

3.1.1 Gegenstand des Auftrags

Der Gegenstand des Auftrags ergibt sich aus den jeweils abgeschlossenen Einzel- und/oder Rahmenverträgen.

3.1.2 Dauer des Auftrags/Kündigung

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung. Eine vorzeitige Beendigung der Laufzeit des Einzel- bzw. Rahmenvertrages durch fristlose Kündigung ist zulässig, sofern der Auftragnehmer seinen Pflichten aus dieser Vereinbarung nicht nachkommt oder sonstige anwendbare Datenschutzvorschriften vorsätzlich oder grob fahrlässig verletzt. Gleiches gilt, wenn der Auftragnehmer eine berechtigte Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer sich den Kontrollrechten des Auftraggebers auf vertragswidriger Weise

[5] Auszufüllen ausschließlich, sofern Ihr Geschäftssitz außerhalb der EU liegt.

widersetzt. Insbesondere die Nichteinhaltung der in dieser Vereinbarung festgelegten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

3.2 Konkretisierung des Auftragsinhalts

3.2.1 Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind in 2.1 aufgeführt.

3.2.2 Ort der Leistungserbringung

Die Orte für die Erbringung der vertraglich vereinbarten Leistung sowie die ggf. erforderlichen Garantien zur Gewährleistung eines angemessenen Datenschutzniveaus in Drittländern sind in 2.2 dargelegt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO sowie die Anforderungen der einschlägigen Rechtsprechung des EuGH (insb. der Rs. C-311/18 – „Schrems II“) und den Empfehlungen des Europäischen Datenschutzausschusses (EDSA) erfüllt sind. Der Auftragnehmer hat dem Auftraggeber die Erfüllung der besonderen Anforderungen an den Drittlandtransfer in geeigneter Weise nachzuweisen.

3.2.3 Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind die in 2.3 genannten Datenarten/-kategorien.

3.2.4. Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen die in 2.4 genannten Personengruppen.

3.3 Technische und organisatorische Maßnahmen

3.3.1 Der Auftragnehmer hat seine interne Unternehmensorganisation so zu gestalten, dass die Einhaltung der besonderen Anforderungen an den Schutz personenbezogener Daten gewährleistet ist. Er hat die technischen und organisatorischen Maßnahmen zu treffen, um die personenbezogenen Daten des Auftraggebers in angemessener Weise vor Missbrauch und Verlust gemäß den Anforderungen des geltenden Datenschutzrechts zu schützen. Eine Übersicht über die technischen und organisatorischen Maßnahmen ist diesem Vertrag als Anhang 1 (Technische & organisatorische Maßnahmen) beigefügt. Soweit der Auftragnehmer zusätzlich Datenkategorien gemäß Kapitel 2 Punkt 2.3.2 dieser Vereinbarung verarbeitet, sind sämtliche in Anhang 1 aufgeführten technischen und organisatorischen Maßnahmen einzuhalten. Andernfalls gelten die in Anhang 1 Nr. 1

aufgeführten technischen und organisatorischen Maßnahmen als Mindeststandard. Der Auftragnehmer überwacht regelmäßig die Einhaltung dieser Maßnahmen.

3.3.2 Eine Verarbeitung von Daten außerhalb der Betriebsräume des Auftragsverarbeiters (z. B. Telearbeit, Home-Office, mobiles Arbeiten) ist zulässig. Der Auftragnehmer stellt die Einhaltung der technischen und organisatorischen Maßnahmen für die Verarbeitungssituation sicher.

3.3.3 Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, Art. 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1 und 2 DSGVO 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, die Umstände 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 DSGVO zu berücksichtigen.

3.3.4 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist der Auftragnehmer verpflichtet, ein Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung sicherzustellen. Dem Auftragnehmer ist gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind schriftlich zu vereinbaren.

3.4 Berichtigung, Einschränkung der Verarbeitung und Löschung von Daten sowie Unterstützung des Auftragsverarbeiters

3.4.1 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, mit Ausnahme der Regelungen unter 3.10 dieser Vereinbarung. Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 und 36 DSGVO. Wenn eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer die betroffene Person unverzüglich an den Auftraggeber verweisen und dessen Weisungen abwarten.

3.4.2 Soweit vom Leistungsumfang umfasst, sind Berechtigungs- und Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach

dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen. Die Regelungen in 3.10 bleiben hiervon unberührt.

3.5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

3.5.1 Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

3.5.1.1 Der Auftragnehmer wird dem Auftraggeber den zuständigen Datenschutzbeauftragten oder – sofern kein Datenschutzbeauftragter erforderlich ist – einen Ansprechpartner für den Datenschutz benennen (s. 1.2). Ein Wechsel des Datenschutzbeauftragten/Ansprechpartners ist dem Auftraggeber unverzüglich schriftlich mitzuteilen.

3.5.1.2 Sofern der Auftragnehmer seinen Sitz außerhalb der Union hat, benennt er einen Vertreter nach Art. 27 Abs. 1 DSGVO in der Union (s. 2.5).

3.5.1.3 Der Auftragnehmer stellt die Wahrung der Vertraulichkeit gem. Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO und/oder des etwaig gesetzlich bestehenden Fernmeldegeheimnisses sowie die Wahrung der Vertraulichkeit elektronischer Kommunikationsdaten sicher. 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 dieser Vereinbarung eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. Die sich daraus ergebende Geheimhaltungspflicht gilt über das Ende der Vereinbarung auf unbefristete Zeit hinaus, unabhängig von der Regelung über sonstige Geheimhaltungspflichten. Gleiches gilt für Daten, die dem Fernmeldegeheimnis unterliegen.

3.5.1.4 Der Auftragnehmer gewährleistet die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gem. Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO.

3.5.1.5 Auf Verlangen der Aufsichtsbehörde arbeiten der Auftraggeber und der Auftragnehmer bei der Erfüllung von deren Aufgaben zusammen.

3.5.1.6 Der Auftragnehmer informiert den Auftraggeber unverzüglich 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 im Auftrag beim Auftragnehmer ermittelt.

3.5.1.7 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.

3.5.1.8 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.

3.5.1.9 Der Auftragnehmer gewährleistet die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach 3.7 dieser Auftragsverarbeitungsvereinbarung.

3.6 Unterauftragsverhältnisse

3.6.1 Der Auftraggeber stimmt der Beauftragung der im Anhang 2 genannten Unterauftragnehmer des Auftragnehmers zu, sofern der Auftragnehmer diesen Unterauftragnehmern in Bezug auf die Verarbeitung personenbezogener Daten im Wesentlichen die gleichen Vertragspflichten auferlegt, an die auch der Auftragsverarbeiter im Rahmen dieser Auftragsverarbeitung gebunden ist. Die Maßgaben des Art. 28 Abs. 2-4 DSGVO sind im Verhältnis zu den Unterauftragnehmern einzuhalten. Bei Unterauftragnehmern mit Sitz in einem Drittland gilt diese Zustimmung, sofern die Grundsätze der Datenübermittlung gemäß Art. 44 ff. DSGVO sowie die Anforderungen der einschlägigen Rechtsprechung des EuGH (insb. der Rs. C- 311/18 – "Schrems II") und die Empfehlungen des Europäischen Datenschutzausschusses (EDSA) auch im Verhältnis zu den Unterauftragsnehmern eingehalten werden.

3.6.2 Der Auftragnehmer informiert den Auftraggeber über alle zukünftig beabsichtigten Änderungen bezüglich der Hinzufügung oder des Austauschs anderer Unterauftragnehmer und gibt dem Auftraggeber so die Möglichkeit, gegen solche Änderungen Einspruch zu erheben. Der Wechsel bestehender Unterauftragnehmer ist vor diesem Hintergrund zulässig, soweit:

3.6.2.1 der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und

3.6.2.2 der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und

3.6.2.3 im Übrigen die Vorgaben gem. 3.6.1 eingehalten werden.

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

3.6.4 Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform), für deren Erteilung Mindestvoraussetzung ist, dass sämtliche vertraglichen Regelungen in der Vertragskette auch dem weiteren Unterauftragnehmer auferlegt werden. Dies hat der Auftragnehmer dem Hauptauftraggeber in geeigneter Form nachzuweisen.

3.6.5 Auf Verlangen des Auftraggebers hat der Auftragnehmer eine Kopie der von ihm oder von Unterauftragnehmern im Rahmen dieser Vereinbarung abgeschlossenen Unterauftragsverarbeitungsverträge zu übermitteln.

3.7 Kontrollrechte des Auftraggebers

3.7.1 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.

3.7.2 Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO 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.

3.7.3 Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO, die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO, aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit erfolgen.

3.8 Mitteilung bei Verstößen des Auftragnehmers

3.8.1 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten,

Meldepflichten bei Datenschutzverletzungen, Datenschutz-Folgeabschätzungen und vorherigen Konsultationen. Hierzu gehören u. a.:

3.8.1.1 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;

3.8.1.2 die Verpflichtung, Verletzungen (einschließlich Fälle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung) personenbezogener Daten des Auftraggebers ohne Ansehen der Verursachung unverzüglich an den Auftraggeber zu melden;

3.8.1.3 die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber der betroffenen Person zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;

3.8.1.4 die Unterstützung des Auftraggebers bei dessen Datenschutz-Folgenabschätzung.

3.8.1.5 die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

3.9 Weisungsbefugnis des Auftraggebers

3.9.1 Der Auftragnehmer darf Daten nur im Rahmen des Einzel- bzw. Rahmenvertrages und gemäß den Weisungen des Auftraggebers erheben, nutzen oder auf sonstige Weise verarbeiten. Die Weisungen des Auftraggebers werden anfänglich durch diese Vereinbarung festgelegt und können vom Auftraggeber danach entsprechend 3.9.2 durch einzelne Weisungen geändert, ergänzt oder ersetzt werden. Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst ebenfalls Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten.

3.9.2 Der Auftraggeber erteilt Weisungen grundsätzlich schriftlich, mindestens in Textform. Sofern eine Weisung des Auftraggebers nur mündlich erteilt wird, wird der Auftragnehmer die Bestätigung mindestens in Textform beim Auftraggeber anfordern. Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren und für die Dauer ihrer Geltung sowie anschließend für drei weitere volle Kalenderjahre aufzubewahren. Der Auftragnehmer informiert den Auftraggeber zudem, wenn er einer Weisung nicht nachkommen kann.

3.9.3 Weisungsberechtigte Personen auf Seiten des Auftraggebers, die auch als Ansprechpartner für im Rahmen der Vereinbarung anfallende Datenschutzfragen fungieren und bei Bedarf einen Kontakt zum Datenschutzbeauftragten des Auftraggebers herstellen,

sind die jeweils unterzeichnenden Personen der jeweiligen Einzel- und/oder Rahmenverträge. Sie sind einzeln weisungsberechtigt.

3.9.4 Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

3.10 Löschung von Daten und Rückgabe von Datenträgern

3.10.1 Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und 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.

3.10.2 Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens jedoch 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/Vernichtung ist dem Auftraggeber unaufgefordert vorzulegen.

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

3.11 Haftung

3.11.1 Macht eine betroffene Person gegenüber einem der Vertragspartner erfolgreich Schadensersatzansprüche aufgrund eines Verstoßes gegen die Regelungen der DSGVO geltend, findet Art. 82 DSGVO Anwendung.

3.11.2 Für alle sonstigen Schäden, die dem Auftraggeber durch die Nichteinhaltung einer erteilten Weisung entstehen, haftet der Auftragnehmer gemäß den gesetzlichen Regelungen.

3.12 Schlussbestimmungen

3.12.1 Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

3.12.2 Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schrift- oder Textform. Dies gilt auch für den Verzicht auf diese Formerfordernisse.

3.12.3 Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

Unterschriften

Ort und Datum	Ort und Datum
Unterschrift Auftraggeber	Unterschrift Auftragnehmer

Anhang 1

Technische und organisatorische Maßnahmen

1. Technische und organisatorische Maßnahmen „Standard“ (RWE AVV)

1.1 Zutrittskontrolle

1.1.1 Der Zutritt zu den zu schützenden Gebäudeteilen und Räumen ist angemessen geregelt und dokumentiert.

1.2 Zugriffskontrolle

1.2.1 Beim Einsatz von Mehrmandantensystemen ist eine ausreichende Mandantentrennung gegeben. Daten der verschiedenen Mandanten können untereinander nicht eingesehen oder verändert werden.

1.2.2 Alle Personen, die mit der Verarbeitung personenbezogener Daten betraut sind, werden über bestehende Vorschriften, Anweisungen und Verfahren zum Datenschutz informiert und zu deren Einhaltung verpflichtet. Alle an der Verarbeitung beteiligten Personen müssen vor Aufnahme der hier gegenständlichen Tätigkeit im Datenschutz geschult werden, auch im Hinblick auf die Anforderungen des EU-Rechts und sind auf das Datengeheimnis verpflichtet. Für die Behandlung von Mitarbeitern, die das Unternehmen verlassen, gibt es ausdrückliche Regelungen.

1.2.3 Es muss festgelegt werden, welche Zugriffsrechte an welche Personen im Rahmen ihrer Funktion ausgegeben und welche entzogen werden. Die Ausgabe/Entzug von Chipkarten, Token oder Zertifikaten muss dokumentiert werden. Zugriff auf Dateien durch Benutzer ist mit restriktiven Dateisystemrechten begrenzt. Jeder Benutzer darf nur auf die Dateien zugreifen können, die er zur Erfüllung der Aufgaben benötigt.

1.2.4 Zugang zu allen IT-Systemen und -Diensten ist durch eine angemessene Identifizierung und Authentifizierung der zugreifenden Nutzer, Dienste oder IT- Systeme gesichert. Es ist ein dem Schutzbedarf angemessener Identifizierungs- und Authentifizierungsmechanismus zu verwenden. Es werden starke Passwörter verwendet. Authentifizierungsdaten müssen während der Verarbeitung durch das IT- System oder die IT-Anwendungen jederzeit vor Ausspähung, Veränderung und Zerstörung geschützt werden. Geeignete Authentifizierungsverfahren wurden gewählt.

1.2.5 Regelungen über die Erteilung, Änderung und den Entzug von Berechtigungen sind vorhanden. Benutzerkennungen und Berechtigungen dürfen nur nach dem tatsächlichen Bedarf vergeben werden. Bei personellen Veränderungen werden die nicht mehr benötigten Benutzerkennungen und Berechtigungen entfernt.

1.2.6 Es muss dokumentiert werden, welche Benutzerkennungen, Benutzergruppen und Rechteprofile zugelassen und angelegt wurden. Die Dokumentation der zugelassenen Benutzer, angelegten Benutzergruppen und Rechteprofile muss regelmäßig auf ihre Aktualität überprüft werden.

1.2.7 Bei erhöhtem Schutzbedarf sind die Daten und Informationen nach dem Standard verschlüsselt, der dem „Stand der Technik" entspricht. Bei sehr hohen Anforderungen, z. B. an die Vertraulichkeit, ist eine Full-Volume- oder Full-Disk-Verschlüsselung und wenn zutreffend, eine angemessene Transportverschlüsselung einzusetzen.

1.3 Eingabekontrolle

Alle sicherheitsrelevanten Ereignisse von IT-Systemen und Anwendungen müssen protokolliert werden. Verfügen relevante IT-Systeme und Anwendungen über eine Logging-Funktion, so ist diese zu nutzen. Können betriebs- und sicherheitsrelevante Ereignisse nicht auf einem IT-System protokolliert werden, müssen andere IT- Systeme für die Protokollierung eingebunden werden (z. B. von Ereignissen auf Netzwerkebene).

1.4 Verfügbarkeitskontrolle

1.4.1 Es muss ein Mindestsicherungskonzept für die Datensicherung geben. Dieses muss die Mindestanforderungen an die Datensicherung definieren und festlegen, wer dafür verantwortlich ist. Es ist eine kurze Beschreibung vorhanden, welche IT- Systeme und welche Daten darauf, durch welche Datensicherung gesichert werden und wie die Datensicherungen erstellt und wiederhergestellt werden können. Die erstellten Datensicherungen müssen in geeigneter Weise vor dem Zugriff Dritter geschützt werden.

1.4.2 Bei der Archivierung muss festgelegt werden, welche Mitarbeiter zuständig sind und welcher Funktions- und Leistungsumfang angestrebt wird. Die Ergebnisse müssen in einem Archivierungskonzept festgehalten werden. Das Archivierungskonzept muss regelmäßig an aktuelle Gegebenheiten angepasst werden. Zugriffe auf elektronische Archive sind zu protokollieren und der Zugriff auf diese streng zu begrenzen.

1.4.3 Es gibt Regelungen wie sicherheitsrelevante Ereignisse behandelt und dokumentiert werden, wie erforderliche Maßnahmen zur Behebung des Problems ausgewählt werden, wie Ursachen zu beseitigen sind und ein sicherer Zustand wiederherzustellen ist.

1.5 Zugangskontrolle

1.5.1 Hard- und Softwareprodukte stammen nur aus bekannten und seriösen Quellen. Zuverlässiger technischer Support ist sichergestellt. Die Lieferkette ist nachvollziehbar.

1.5.2 Für alle Geschäftsprozesse, Anwendungen, IT-Systeme, Räume und Gebäude sowie Kommunikationsverbindungen muss festgelegt werden, wer für sie und ihren Schutz verantwortlich ist.

1.5.3 Alle Mitarbeiter müssen darauf aufmerksam gemacht werden, dass weder sensible Informationen noch IT-Systeme an unbeaufsichtigten Arbeitsplätzen frei zugänglich sein dürfen.

1.5.4 Auf den Systemen, auf denen RWE Informationen verarbeitet werden, einschließlich auf den verbundenen Systemen (z. B. Servern, Gateways, Clients sowie Computergeräten, mobilen Geräten, etc.), ist eine Malware-Schutzlösung installiert. Malware-Schutzsoftware wird automatisch und innerhalb definierter Zeiträume verteilt. Regelmäßige Überprüfungen finden statt zur Feststellung, dass Malware- und Virenschutzsoftware nicht deaktiviert oder in der Funktion eingeschränkt wurde, die Konfiguration korrekt ist und Updates und Patterns innerhalb definierter Zeiträume korrekt angewendet werden.

1.5.5 Es dürfen nur Cloud-Funktionen solcher Produkte genutzt werden, wenn keine gravierenden, nachweisbaren Datenschutz- oder Vertraulichkeitsaspekte dagegen sprechen.

1.5.6 Die gesamte Kommunikation zwischen den beteiligten Netzen muss durch die Firewall geleitet werden. Es muss sichergestellt sein, dass von außen keine unberechtigten Verbindungen zum geschützten Netz aufgebaut werden können. Ebenso dürfen keine unautorisierten Verbindungen aus dem geschützten Netz heraus aufgebaut werden. Regeln wurden definiert, die festlegen, welche Kommunikationsverbindungen und Datenströme erlaubt sind.

1.5.7 Verschiedene Netze müssen angemessen physisch getrennt sein (mindestens z. B. in ein internes Netz, eine demilitarisierte Zone (DMZ) und z. B. das Internet). Die Übergänge zwischen verschiedenen Netzen müssen durch Firewalls gesichert werden. Nicht vertrauenswürdige Netze (z. B. Internet) und vertrauenswürdige Netze müssen durch eine zweistufige entsprechende Firewall-Struktur getrennt werden. Für Anwendungen, die über das Internet zugänglich sind, existiert eine mehrstufige IT-Architektur. Netzsegmente werden je nach Schutzbedarf voneinander getrennt, um den Datenverkehr zwischen Segmenten mit unterschiedlichem Schutzbedarf zu verhindern.

1.5.8 Die Verbindung zwischen der App und den Backend-Systemen muss durch kryptographische Maßnahmen gesichert sein. Wenn eine App über ein Benutzerkonto auf Backend-Systeme zugreift, muss dafür ein dediziertes Dienste-Konto verwendet werden.

1.5.9 Es wird sichergestellt, dass technische Schwachstellen behoben werden. Sollten IT- Komponenten, Software oder Konfigurationsdaten geändert werden, so werden Patches nur aus autorisierten Quellen bezogen und Sicherheitsaspekte werden berücksichtigt. Insgesamt muss sichergestellt werden, dass das angestrebte Sicherheitsniveau während und nach den Änderungen erhalten bleibt.

1.5.10 Die möglichen Zugänge und Kommunikationsschnittstellen für den Verbindungsaufbau zur Fernwartung sind auf das Notwendige zu beschränken. Alle Fernwartungsverbindungen müssen nach dem Fernzugriff wieder getrennt werden. Fernwartungssoftware sollte nur auf Systemen installiert werden, auf denen sie benötigt wird.

1.5.11 Für alle VPN-Komponenten muss eine sichere Konfiguration definiert werden. Es müssen Authentifizierungs- und Verschlüsselungsmethoden verwendet werden, die als sicher gelten und eine ausreichende Schlüssellänge aufweisen.

1.5.12 Bevor ein IT-System, eine Anwendung oder eine App eingeführt wird, muss sichergestellt werden, dass es nur die für seine Funktion erforderlichen Mindestberechtigungen erhält. Nicht unbedingt notwendige Berechtigungen sind zu hinterfragen und gegebenenfalls zu unterbinden.

1.5.13 Die Löschung und Vernichtung von Informationen erfolgt nach Vorgaben der Auftragsverarbeitung.

1.5.14 Es gibt klare Anweisungen für den Umgang mit nicht mehr benötigten Datenträgern. Dazu gehört auch der Umgang mit geschriebenem oder gedrucktem Papier. Auch muss geregelt und dokumentiert sein, wie IT-Systeme und Datenträger datenschutzkonform außer Betrieb genommen und entsorgt werden.

1.5.15 Informationen auf mobilen Datenträgern und Geräten sind ausreichend gegen unbefugtes Auslesen geschützt.

1.5.16 Wenn Daten an ein Datenbanksystem weitergeleitet werden, muss ein sicherer Schutz gegen SQL-Injections eingerichtet werden.

1.5.17 Systeme, Anwendungen und Geräte müssen angemessen gehärtet werden, bevor sie eingesetzt werden. Dazu gehört mindestens die Evaluierung der notwendigen Ports, Kommunikationsprotokolle und Funktionen. Bei der Härtung von Systemen, Anwendungen und Geräten ist die Forderung nach "Datenschutz durch datenschutzfreundliche Voreinstellungen" zu berücksichtigen. Es dürfen nur notwendige personenbezogene Daten verarbeitet und die erforderlichen Funktionalitäten freigeschaltet werden. Alle nicht benötigten Dienste und Anwendungen sind zu deaktivieren oder zu deinstallieren, insbesondere Netzwerkdienste. Alle nicht benötigten Funktionen in der Firmware sind zu deaktivieren. Nicht benötigte Benutzerkennungen sind zu löschen oder zumindest so zu deaktivieren, dass unter diesen Kennungen keine Anmeldungen am System möglich sind.

1.5.18 Vorhandene Standard-Identifikatoren sind soweit möglich zu ändern oder zu deaktivieren. Voreingestellte Passwörter von Standard-Identifikatoren müssen geändert werden.

1.5.19 Es wurden Änderungskontrollprozesse definiert, dokumentiert, spezifiziert und durchgesetzt, die den gesamten Lebenszyklus von Informationssystemen regeln.

1.5.20 Für die Software-Entwicklung gelten die Grundsätze der sicheren Kodierung.

1.6 Weitergabekontrolle

1.6.1 Die Übermittlung von Daten an Dritte (z. B. bei Datenbanken oder Datensätzen mit beschränktem Zugang), wird nur mit geeigneten Maßnahmen zur Datenminimierung umgesetzt.

1.6.2 Die Kommunikationsverbindungen müssen angemessen verschlüsselt sein. Es muss sichergestellt sein, dass die Vertraulichkeit, Integrität und Authentizität der übertragenen Daten gewährleistet ist. Die Authentizität der Kommunikationspartner muss gewährleistet sein.

1.6.3 Bei der Weitergabe von Daten macht das Unternehmen von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch.

1.7 Auftragskontrolle

1.7.1 Speicherung personenbezogener Daten erfolgt ausschließlich in einer Infrastruktur des RWE-Konzerns (i. d. R. on-premise) oder auf eigenen Systemen des Lieferanten und im Falle einer vom Unterauftragnehmer bereitgestellten Infrastruktur (i. d. R. Software-as-a-Service) nur mit entsprechenden Datenschutzvereinbarungen.

1.7.2 Vor Einführung neuer oder Änderungen an bestehenden IT-Umgebungen, in denen im Rahmen der Auftragsverarbeitung personenbezogene Daten der RWE verarbeitet werden, sind einhergehende relevante Informationssicherheitsrisiken identifiziert, bewertet, behandelt, werden überwacht und in akzeptablen Grenzen gehalten.

1.7.3 Es gibt Regelungen zum Umgang auch mit externen Dienstleistern (z. B. bei Werkverträgen, Handwerkern, Wartung von Systemen) sowie entsprechende Verschwiegenheitserklärung, persönliche Begleitung in Sicherheitszonen oder die Protokollierung deren Aufenthalts und Aktivitäten.

1.7.4 Der Auftragsverarbeiter muss sicherstellen, dass Webanwendungen und Apps nur die vorgesehenen Daten und Inhalte integrieren und an den Nutzer liefern. Bieten Webanwendungen und Apps eine Upload-Funktion für Dateien an, muss diese Funktion vom verantwortlichen Unternehmen so weit wie möglich eingeschränkt werden. Auch die Zugriffs- und Ausführungsrechte müssen in diesem Fall restriktiv gesetzt werden.

1.7.5 Für die Auslagerung der Datenverarbeitung werden nur Rechenzentren genutzt, für die qualifizierte und dem Risiko der Verarbeitung angemessene Zertifikate vorliegen.

1.7.6 Ein Datenschutzmanagementsystem ist etabliert, welches die Anforderungen der DSGVO/des geltenden Datenschutzrechts erfüllt.

1.8 Trennbarkeit

1.8.1 Entwicklungs-, Test- und Produktionssysteme werden in (zumindest logisch) klar getrennten Netzsegmenten betrieben. Für Test- und Entwicklungszwecke werden nur Testdaten verwendet. Testdaten, basierend auf Echtdaten, werden anonymisiert.

1.8.2 Aufgaben und Verantwortlichkeiten im Datenschutzprozess sind geregelt und zugänglich.

1.8.3 Aufgaben und dafür erforderliche Rollen und Funktionen sind so strukturiert, dass unvereinbare Aufgaben wie Betriebs- und Kontrollfunktionen auf verschiedene Personen verteilt sind. Für unvereinbare Funktionen muss eine Funktionstrennung definiert und dokumentiert werden. Auch Vertreter müssen der Funktionstrennung unterworfen werden.

2. Technische und organisatorische Maßnahmen „Erweitert“ (RWE AVV)

2.1 Zutrittskontrolle

Code- oder ID-Karten, die an betriebsfremde Personen ausgegeben werden, haben eine eng begrenzte Gültigkeit, die anhand des Aufenthaltszwecks festgelegt wird. Die Vergabe bzw. der Entzug von Besucher- und Firmenausweisen geschieht in revisionsfähiger Weise. Besucherausweise werden täglich eingezogen. Persönliche Daten von Firmenbesuchern werden in ein Besucherbuch / eine Besucherliste aufgenommen. Es erfolgt eine konkrete Festlegung und Dokumentation von zutrittsberechtigten und qualifizierten Personen zu den Serverräumen.

2.2 Zugriffskontrolle

2.2.1 Zugriffsrechte werden auf die genehmigte Systemfunktionalität beschränkt und eine angemessene Funktionstrennung besteht. Benutzer-IDs und Passwörter dürfen nicht geteilt werden. Administrative Zugriffe auf Systeme, die RWE Informationen speichern oder verarbeiten, sind auf eine minimale Anzahl von Administratoren beschränkt und durch ein Multi-Faktor-Authentifizierungsverfahren (oder, wenn eine Multi-Faktor-Authentifizierung technisch nicht möglich ist, durch gleichwertige Sicherheitsmaßnahmen, wie z. B. temporär generierte Passwörter) geschützt.

2.2.2 Administrative Zugriffe werden immer protokolliert, um unberechtigten Zugriff auf und/oder unberechtigte Manipulation von RWE-Informationen erkennen und untersuchen zu können.

2.3 Eingabekontrolle

Die Integrität von personenbezogenen Daten ist durch digitale Signaturen sicherzustellen.

2.4 Verfügbarkeitskontrolle

2.4.1 Der Auftragsverarbeiter stellt sicher, dass die Hardware- und Softwareprodukte (Assets) in Inventarlisten erfasst sind, gegen unbefugte Änderungen geschützt sind, aktuell gehalten werden, regelmäßig gesichert werden und die erforderlichen Angaben über die Assets enthalten und – falls zutreffend – Compliance-Anforderungen in Bezug auf die Betriebsmittel enthalten. Die Assets sind einem Verantwortlichen zuzuordnen, der für den Betrieb der Assets verantwortlich ist.

2.4.2 Eine Zertifizierung, wie z. B. IEC/ISO 27001 oder gleichwertig, ist vorhanden und wird vom Anbieter auf Nachfrage nachgewiesen. Der Anbieter sichert zu, dass die im Auftragsverarbeitungsvertrag beschriebenen Verarbeitungen in der Anwendbarkeitserklärung der Zertifizierungen („Statement of Applicability“) enthalten sind.

2.5 Zugangskontrolle

2.5.1 Authentifizierungsdaten müssen während der Verarbeitung durch das IT-System oder die IT-Anwendungen jederzeit vor Ausspähung, Veränderung und Zerstörung geschützt werden. Es müssen geeignete Authentifizierungsverfahren gewählt werden. Die Komponente muss die Benutzer dazu zwingen, sichere Passwörter gemäß einer Passwort-Richtlinie zu benutzen. Es müssen Grenzwerte für fehlgeschlagene Anmeldeversuche definiert sein. Alle angebotenen Authentisierungsverfahren müssen das gleiche Sicherheitsniveau aufweisen.

2.5.2 Die Grundsätze “Least Privilege”, “Need-to-know” und “Segregation of Duties” sind einzuhalten. Rollenbasierte Berechtigungskonzepte sind anzuwenden.

2.5.3 Es muss eine Passwortrichtlinie erstellt werden. Änderungen hinsichtlich der Passwortrichtlinie müssen einheitlich für alle Geräte, IT-Systeme und Anwendungen möglichst zeitgleich umgesetzt werden. Die Passwortrichtlinie muss sichere und komplexe Passwörter fordern. Es müssen Maßnahmen ergriffen werden, um die Kompromittierung von Passwörtern zu erkennen. Standardpasswörter müssen durch ausreichend starke Passwörter ersetzt und vordefinierte Kennungen müssen geändert werden. Nach einem Passwortwechsel dürfen mindestens die letzten fünf Passwörter nicht mehr genutzt werden. Passwörter müssen so sicher wie

möglich gespeichert werden. Bei der Authentisierung in vernetzten Systemen dürfen Passwörter nicht unverschlüsselt über unsichere Netze übertragen werden.

2.5.4 Für die Verschlüsselung und Signaturbildung müssen unterschiedliche Schlüssel benutzt werden. Wenn Schlüssel verwendet werden, müssen die authentische Herkunft und die Integrität der Schlüsseldaten überprüft werden.

2.5.5 Es wird sichergestellt, dass alle Systeme, Netzwerke und Endgeräte, die personenbezogene Daten verarbeiten, durch Maßnahmen gesichert werden, die Datenlecks vermeiden.

2.5.6 Es gibt ein formelles Genehmigungsverfahren, das Systeme und Anwendungen, die personenbezogene Daten enthalten, durchlaufen müssen, bevor sie Zugang zum Netz erhalten.

Anhang 2

Unterauftragnehmer

Unterauftrag-nehmer (Name des Unterneh-mens)	Anschrift/ Land	Beschreibung der Teil-leistungen / Datenverar-beitung[6]	Ort der Daten-verarbeitung (z. B. Server-standort, Ort des Zugriffs, etc.)	Beschreibung der Sicherheitsmaß-nahmen betreffend die Übermittlung an Drittländer (Art. 44 ff DSGVO)[7]

[6] Bitte achten Sie bei der Beschreibung von Gegenstand und Art auch auf die klare Abgrenzung von Verantwortlichkeiten, falls mehrere Unterauftragnehmer eingesetzt werden.

[7] Soweit personenbezogene Daten in ein Drittland übermittelt werden, tragen Sie bitte hier die Drittlandgarantien ein, die der Auftragnehmer mit dem jeweiligen Unterauftragnehmer vereinbart hat, sowie die zusätzlichen Sicherheitsmaßnahmen, um ein angemessenes Datenschutzniveau zu gewährleisten. Geben Sie – sofern erforderlich - bitte auch an, dass ein Data Transfer Impact Assessment durchgeführt wurde. Verweise auf ein separat abrufbares oder zur Verfügung gestelltes Dokument sind ebenfalls möglich.

RWE
