Auftragsverarbeitungsvereinbarung

gemäß Artikel 28 Abs. 3 EU-Datenschutz-Grundverordnung

zum Rahmen- oder Einzelvertrag vom

zwischen der

(Auftraggeber)

und der

(Auftragnehmer)

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. Insbesondere Art. 28 DS-GVO 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 einer ihrer gem. § 15 ff. AktG verbundenen Unternehmen erbracht wird, gilt diese Vereinbarung ebenfalls zugunsten dieser Unternehmen. Vor diesem Hintergrund wird Folgendes vereinbart:

Kapitel 1: Allgemeine Angaben zum Unternehmen

1.1. Angaben zum Unternehmen

Name _____

Straße _____ Nr. _____

Ort _____ PLZ _____

Land _____

E-Mail _____

Telefon _____

1.2. Angaben zum Datenschutzbeauftragten

Hinweis: Sofern keine rechtliche Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten einschlägig ist, ist ein Ansprechpartner für den Datenschutz zu benennen.

Name _____

E-Mail _____

Telefon _____

Kapitel 2: Angaben zur Verarbeitung personenbezogener Daten

2.1. Benennen Sie den Liefer- und Leistungsumfang, der als Auftragsverarbeitung gemäß Art. 28 DS-GVO 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 4, 4.6.

◉ 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. DS-GVO 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 (EDPB),

in folgenden Ländern durch Standarddatenschutzklauseln
(Art. 46 Abs. 2 lit. c und d DS-GVO) hergestellt: [1]

in folgenden Ländern durch einen Angemessenheitsbeschluss der Kommission
(Art. 45 Abs. 3 DS-GVO) gewährleistet:

in folgenden Ländern durch genehmigte Verhaltensregeln
(Art. 46 Abs. 2 lit. e i. V. m. 40 DS-GVO) hergestellt:

in folgenden Ländern durch einen genehmigten Zertifizierungsmechanismus
(Art. 46 Abs. 2 lit. f DS-GVO) hergestellt:

in folgenden Ländern durch folgende Maßnahmen
(Art. 46 Abs. 2 lit. a, Abs. 3 lit. a und b DS-GVO) hergestellt:

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.

	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, Kontaktdaten im Unternehmen (Telefon, Mobil, Fax), Abteilungszugehörigkeit, Position im Unternehmen, Dauer der Betriebszugehörigkeit.

[1] Sog. EU-Standardvertragsklauseln „Controller to Processor". Abschluss der EU-Standardvertragsklauseln im Falle der durch den Auftragnehmer beabsichtigten Leistungserbringung aus einem sog. Drittland, d. h. einem Land außerhalb der EU/EWR, ist die Grundsatzanforderung des Auftraggebers.

☐ 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.
☐ 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.
☐ Elektronische Identifikationsdaten	IP-Adressen, Cookies, Verbindungszeiten und -daten, elektronische Unterschrift u.a.
☐ Ethnische Daten	Angaben zur Herkunft, Abstammung, zu Landsmannschaften, u. a.
☐ Finanzidentifikationsdaten	Bankidentifikation und Bankkontonummer, Kredit und Lastschriftkartennummern, Geheimcodes u. a.
☐ Genetische Daten	Daten im Rahmen einer Erkennung, Untersuchung der Erblichkeit, DNS, 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.
☐ Körperlicher Gesundheitszustand	Ärztliche Akte, ärztlicher Bericht, Diagnose, Behandlung, Untersuchungsergebnis, Behinderung oder Gebrechen, Diät; andere besondere gesundheitliche Anforderungen für die Behandlung, Reise oder Unterkunft etc.
☐ Medikationsdaten	Daten über die Mittel und Verfahren, die für die medizinische oder paramedizinische Betreuung der Patienten benutzt werden u. a.
☐ 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.
☐ Philosophische, militante oder religiöse Überzeugungen	Angaben zu philosophischen, militanten oder zu nicht staatsreligiöser Überzeugung, zu Mitgliedschaften in solchen Vereinigungen, Positionen und Funktionen, Mitgliedsbeiträge und geleistete Zuwendungen u. a.
☐ Politische Zugehörigkeiten	Angaben zur Parteienzugehörigkeit, zu politischen Meinungen und Präferenzen, zu ausgeübten politischen Positionen 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

☐ Sexualverhalten	Angaben zu Sexualverhalten, zum Geschlecht, zur Geschlechtsumwandlung 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.
☐ Sonstiges:	

2.4. Kategorien betroffener Personen

☐ Beschäftigte	*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.*
☐ Angehörige von Beschäftigten	
☐ Bewerber/innen	
☐ Kunden	
☐ Beschäftigte von Geschäftspartnern der RWE Gruppe	
☐ Externe Dritte	*Definition: Externe Dritte sind Personen mit denen Unternehmen der RWE Gruppe keine vertragliche Beziehung hat (bspw. Polizei, Ordnungsamt, Bergbehörde, Interessenten oder Besucher).*
☐ Sonstiges:	

2.5. Vertreter des Auftragnehmers in der Europäischen Union gem. Art. 27 Abs. 1 DS-GVO

Hinweis: Auszufüllen ausschließlich, sofern Ihr Geschäftssitz außerhalb der EU liegt.

Name _____

Straße _____ Nr. _____

Ort _____ PLZ _____

Land _____

E-Mail _____

Telefon _____

Kapitel 3: Technische und organisatorische Maßnahmen

Sie verpflichten sich zur Einhaltung der nachfolgend dargelegten technischen und organisatorischen Maßnahmen. Die dargelegten technischen und organisatorischen Maßnahmen sind für die in Auftrag gegebene Verarbeitung des Auftraggebers darzulegen. Sollten einzelne Maßnahmen nur teilweise oder nicht erfüllt werden bzw. nicht relevant sein, sind diese zwingend zu begründen.

3.1. Angaben zur Leistungserbringung (Mehrfachauswahl möglich)

3.1.1. Die Erbringung der vertraglichen Leistungen erfolgt …

☐ ausschließlich mit Hilfe von bereitgestellten Endgeräten der RWE Gruppe. Es werden keine Endgeräte Ihres Unternehmens verwendet.

☐ sowohl mit bereitgestellten Endgeräten der RWE Gruppen als auch mit Endgeräten Ihres Unternehmens.

☐ ausschließlich mit Endgeräten Ihres Unternehmens statt.

☐ ausschließlich an Standorten der RWE Gruppe statt. Ein Fernzugriff über nicht vertrauenswürdige Netzwerke findet nicht statt.

☐ sowohl an Standorten der RWE Gruppen als auch per Fernzugriff über nicht vertrauenswürdige Netzwerke.

☐ ausschließlich per Fernzugriff über nicht vertrauenswürdige Netzwerke.

3.1.2. Die Speicherung von Daten und das Hosting von Anwendungen jeglicher Art erfolgt …

☐ ausschließlich in einer Infrastruktur, die durch den Auftragnehmer oder einem beauftragten Unterauftragnehmer bereitgestellt wird (i. d. R. Software-as-a-Service).

☐ sowohl in einer Infrastruktur, die durch den Auftragnehmer oder einem beauftragten Unterauftragnehmer, als auch einer Infrastruktur, die durch den Auftraggeber bereitgestellt wird.

☐ ausschließlich in einer Infrastruktur, die durch den Auftraggeber bereitgestellt wird (i. d. R. On-Premise).

3.2. Angaben zu den umgesetzten Schutzmaßnahmen Ihres Unternehmens und beauftragten Unterauftragnehmern

3.2.1. Joiner-Mover-Leaver-Prozess (personelle Sicherheit)

Der Auftragsverarbeiter muss dafür sorgen, dass sämtliche mit der Auftragsverarbeitung betrauten Personen über bestehende Regelungen, Handlungsanweisungen und Verfahrensweisen zum Datenschutz informiert und zur Einhaltung verpflichtet sind.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.2. Rollen, Verantwortlichkeiten und Funktionstrennung

Der Auftragsverarbeiter muss dafür sorgen, dass die Aufgaben und Zuständigkeiten im Datenschutzprozess geregelt und zugänglich sind. Die Aufgaben und die hierfür erforderlichen Rollen und Funktionen müssen so strukturiert sein, dass unvereinbare Aufgaben wie operative und kontrollierende Funktionen auf verschiedene Personen verteilt werden. Für unvereinbare Funktionen muss eine Funktionstrennung festgelegt und dokumentiert sein. Auch Vertreter müssen der Funktionstrennung unterliegen.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.3. Zuweisung der Verantwortung

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

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.4. Schutz von sensiblen Informationen am Arbeitsplatz

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

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.5. Vergabe von Zutrittsberechtigungen

Es muss festgelegt werden, welche Zutrittsberechtigungen an welche Personen im Rahmen ihrer Funktion vergeben bzw. ihnen entzogen werden. Die Ausgabe bzw. der Entzug von verwendeten Zutrittsmitteln wie Chipkarten muss dokumentiert werden. Wenn Zutrittsmittel kompromittiert wurden, müssen sie ausgewechselt werden. Bei längeren Abwesenheiten müssen berechtigte Personen vorübergehend gesperrt werden.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.6. Vergabe von Zugangsberechtigungen

Es muss festgelegt werden, welche Zugangsberechtigungen an welche Personen im Rahmen ihrer Funktion vergeben bzw. ihnen entzogen werden. Werden Zugangsmittel wie Chipkarten verwendet, so muss die Ausgabe bzw. der Entzug dokumentiert werden. Bei längeren Abwesenheiten muss berechtigte Personen vorübergehend gesperrt werden.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.7. Vergabe von Zugriffsrechten

Es muss festgelegt werden, welche Zugriffsrechte an welche Personen im Rahmen ihrer Funktion vergeben bzw. ihnen entzogen werden. Werden im Rahmen der Zugriffskontrolle Chipkarten oder Token verwendet, so muss die Ausgabe bzw. der Entzug dokumentiert werden. Bei längeren Abwesenheiten müssen berechtigte Personen vorübergehend gesperrt werden. Es muss mittels einer Autorisierungskomponente sichergestellt werden, dass Benutzer nur Aktionen durchführen können, zu denen sie berechtigt sind. Jeder Zugriff auf geschützte Inhalte und Funktionen muss kontrolliert werden, bevor er ausgeführt wird. Sollte es nicht möglich sein, Zugriffsrechte zuzuweisen, muss dafür ein zusätzliches Sicherheitsprodukt eingesetzt werden. Ist die Zugriffskontrolle fehlerhaft, müssen Zugriffe abgelehnt werden. Ebenso muss der Zugriff auf Dateien durch die Benutzer mit restriktiven Dateisystemberechtigungen beschränkt werden. Zugriffsrechte müssen restriktiv vergeben werden. Jeder Benutzer darf nur auf die Dateien zugreifen können, die er für seine Aufgabenerfüllung benötigt. Das Zugriffsrecht selbst wiederum muss auf die notwendige Zugriffsart beschränkt sein.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.8. Identifikation und Authentisierung

Der Zugriff auf alle IT-Systeme und Dienste muss durch eine angemessene Identifikation und Authentisierung der zugreifenden Benutzer, Dienste oder IT-Systeme abgesichert sein. Vorkonfigurierte Authentisierungsmittel müssen vor dem produktiven Einsatz geändert werden. Es muss dem Schutzbedarf angemessene Identifikations- und Authentisierungsmechanismen verwendet werden. Verwendete Passwörter müssen sicher sein. Für sichere Passwörter muss es eine Passwort-Richtlinie geben. Authentisierungsdaten müssen durch das IT-System bzw. die IT-Anwendungen bei der Verarbeitung jederzeit gegen Ausspähung, Veränderung und Zerstörung geschützt werden. Es muss sichergestellt sein, dass sich Benutzer geeignet authentisieren, wenn diese auf geschützte Ressourcen zugreifen wollen. Dafür muss eine geeignete Authentisierungsmethode ausgewählt und der Auswahlprozess dokumentiert 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.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.9. Aufgabenverteilung und Funktionstrennung

Die definierten unvereinbaren Aufgaben und Funktionen müssen durch das Identitäts- und Berechtigungsmanagement getrennt werden.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.10. Regelung für Einrichtung, Änderung und Entzug von Berechtigungen

Benutzerkennungen und Berechtigungen dürfen nur aufgrund des tatsächlichen Bedarfs vergeben werden. Bei personellen Veränderungen müssen die nicht mehr benötigten Benutzerkennungen und Berechtigungen entfernt werden. Beantragen Mitarbeiter Berechtigungen, die über den Standard hinausgehen, dürfen diese nur nach zusätzlicher Begründung vergeben werden.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.11. Dokumentation der Benutzerkennungen und Rechteprofile

Es muss dokumentiert werden, welche Benutzerkennungen, angelegte Benutzergruppen und Rechteprofile zugelassen und angelegt wurden. Die Dokumentation der zugelassenen Benutzer, angelegten Benutzergruppen und Rechteprofile muss regelmäßig auf Aktualität hin überprüft werden. Die Dokumentation muss vor unberechtigtem Zugriff geschützt werden.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.12. Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme

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. Reine zeitgesteuerte Wechsel müssen vermieden werden. 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.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.13. Geeignetes Schlüsselmanagement für kryptografische Verfahren

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.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.14. Verschlüsselung der Kommunikationsverbindungen

Kommunikationsverbindungen müssen geeignet verschlüsselt werden. Es müssen sicherheitstechnische Anforderungen an die Kommunikationsverbindung zwischen Geräten und Systemen im vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken definiert werden. Dabei muss sichergestellt sein, dass die Vertraulichkeit, Integrität und Authentizität der übertragenen Daten gewährleistet sind. Zusätzlich muss die Authentizität der Kommunikationspartner gewährleistet sein.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.15. Verschlüsselung von Daten und Informationen

Bei erhöhtem Schutzbedarf sollte die Daten und Informationen des Verantwortlichen mit einem als sicher geltenden Produkt bzw. Verfahren verschlüsselt werden. Dies sollte auch für virtuelle Maschinen mit produktiven Daten gelten. Es sollte nicht nur ein TPM allein als Schlüsselschutz dienen. Das Wiederherstellungspasswort sollte an einem geeigneten sicheren Ort gespeichert werden. Bei sehr hohen Anforderungen z. B. an die Vertraulichkeit sollte eine Full Volume oder Full Disk Encryption erfolgen.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.16. Sicheres Löschen und Vernichten von kryptografischen Schlüsseln

Nicht mehr benötigte Schlüssel und Zertifikate muss sicher gelöscht bzw. vernichtet werden.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.17. Datensicherung gemäß dem Minimalsicherungskonzept

Der Auftragsverarbeiter muss ein Minimaldatensicherungskonzept für die Datensicherung erstellen. Dieses muss festlegen, welche Anforderungen für die Datensicherung mindestens einzuhalten sind und wer dafür verantwortlich ist. Das Minimaldatensicherungskonzept muss mindestens eine kurze Beschreibung dazu enthalten, welche IT-Systeme und welche darauf befindlichen Daten durch welche Datensicherung gesichert werden, wie die Datensicherungen erstellt und wiederhergestellt werden können, welche Parameter zu wählen sind sowie welche Hard- und Software eingesetzt wird. Der Auftragsverarbeiter muss regelmäßige Datensicherungen gemäß dem (Minimal-) Datensicherungskonzept erstellen. Die erstellten Datensicherungen müssen in geeigneter Weise vor dem Zugriff Dritter geschützt werden. Es muss regelmäßig getestet werden, ob die Datensicherung wie gewünscht funktioniert, vor allem, ob gesicherte Daten problemlos und in angemessener Zeit zurückgespielt werden können.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.18. Virenschutzprogramme für Endgeräte, Gateways und IT-Systeme

Abhängig vom verwendeten Betriebssystem, anderen vorhandenen Schutzmechanismen, sowie der Verfügbarkeit geeigneter Virenschutzprogramme, muss für den konkreten Einsatzzweck ein entsprechendes Schutzprogramm ausgewählt und installiert werden. Es dürfen nur Produkte für den Enterprise-Bereich eingesetzt werden. Produkte für reine Heimanwender oder Produkte ohne Herstellersupport dürfen nicht im professionellen Wirkbetrieb eingesetzt werden. Es dürfen nur Cloud-Funktionen solcher Produkte verwendet werden, bei denen keine gravierenden, nachweisbaren Daten- oder Geheimschutzaspekte dagegen sprechen.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.19. Restriktive Konfiguration der Firewall

Die gesamte Kommunikation zwischen den beteiligten Netzen muss über die Firewall geleitet werden. Es muss sichergestellt sein, dass von außen keine unerlaubten Verbindungen in das geschützte Netz aufgebaut werden können. Ebenso dürfen keine unerlaubten Verbindungen aus dem geschützten Netz heraus aufgebaut werden. Für die Firewall müssen eindeutige Regeln definiert werden, die festlegen, welche Kommunikationsverbindungen und Datenströme zugelassen werden. Alle anderen Verbindungen müssen durch die Firewall unterbunden werden (Whitelist-Ansatz). Die Kommunikationsbeziehungen mit angeschlossenen Dienst-Servern (z. B. E-Mail-Servern, Web-Servern), die über die Firewall geführt werden, müssen in den Regeln berücksichtigt sein. Es dürfen keine IT-Systeme von außen über die Firewall auf das interne Netz zugreifen. Es müssen Verantwortliche benannt werden, die Filterregeln entwerfen, umsetzen und testen. Zudem muss geklärt werden, wer Filterregeln verändern darf. Die getroffenen Entscheidungen sowie die relevanten Informationen und Entscheidungsgründe müssen dokumentiert werden.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.20. Netztrennung

Das Netzwerk muss mindestens in drei Sicherheitszonen physisch separiert sein: internes Netz, demilitarisierte Zone (DMZ) und Außenanbindungen (inklusive Internetanbindung sowie Anbindung an andere nicht vertrauenswürdige Netze). Zonenübergänge muss durch eine Firewall abgesichert werden. Diese Kontrolle muss dem Prinzip der lokalen Kommunikation folgen, sodass von Firewalls ausschließlich erlaubte Kommunikation weitergeleitet wird (Whitelisting). Nicht vertrauenswürdige Netze (z. B. Internet) und vertrauenswürdige Netze müssen durch eine zweistufige Firewall-Struktur getrennt werden. Um Internet und externe DMZ netztechnisch zu trennen, muss mindestens ein zustandsbehafteter Paketfilter eingesetzt werden. Jeder ein- und ausgehender Datenverkehr muss durch den äußeren Paketfilter bzw. den internen Paketfilter kontrolliert und gefiltert werden.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.21. Verbindung von Apps mit Backend Systemen

Die Verbindung zwischen App und Backend-Systemen muss durch kryptografische Maßnahmen abgesichert werden. Hierbei muss überprüft werden, ob die vom Betriebssystem angebotenen Verfahren für die App ausreichend sicher sind oder ob eventuell eigene Methoden auf Applikationsebene implementiert werden müssen. Wenn eine App über ein Benutzerkonto auf Backend-Systeme zugreift, muss dafür ein dediziertes Dienstekonto verwendet werden.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.22. Patch-, Änderungs- und Update Management

Wenn IT-Komponenten, Software oder Konfigurationsdaten geändert werden sollen, muss es dafür Vorgaben geben, die auch Sicherheitsaspekte berücksichtigen. Alle Patches und Änderungen müssen geeignet geplant, genehmigt und dokumentiert werden. Wenn Patches installiert und Änderungen durchgeführt werden, müssen Rückfall-Lösungen vorhanden sein. An größeren Änderungen muss der Datenschutzbeauftragte beteiligt sein. Insgesamt muss sichergestellt werden, dass das angestrebte Sicherheitsniveau während und nach den Änderungen erhalten bleibt.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.23. Fernwartung

Wird per Fernwartung auf Clients zugegriffen, muss dieser Zugriff vom Benutzer des IT-Systems initiiert werden. Der Benutzer des fernadministrierten Clients muss dem Fernzugriff explizit zustimmen. Die möglichen Zugänge und Kommunikationsschnittstellen für einen Verbindungsaufbau müssen auf das notwendige Maß beschränkt werden. Ebenso müssen alle Fernwartungsverbindungen nach dem Fernzugriff getrennt werden. Es muss sichergestellt werden, dass Fernwartungssoftware nur auf Systemen installiert ist, auf denen sie benötigt wird. Fernwartungsverbindungen über nicht vertrauenswürdige Netze müssen verschlüsselt werden. Die Auswahl der Authentisierungsmethode und die Gründe, die zu der Auswahl geführt haben, müssen dokumentiert werden. Fernwartungszugänge muss im Identitäts- und Berechtigungsmanagement berücksichtigt werden.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.24. Sichere Konfiguration eines VPN

Für alle VPN-Komponenten muss eine sichere Konfiguration festgelegt werden. Dabei **müssen** als sicher geltende Authentisierungs- und Verschlüsselungsverfahren mit ausreichender Schlüssellänge verwendet werden. Auch muss der zuständige Administrator regelmäßig kontrollieren, ob die Konfiguration noch sicher ist und sie eventuell für alle IT-Systeme anpassen.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.25. Kontrolliertes Einbinden von Daten und Inhalten bei Webanwendungen und Apps

Der Auftragsverarbeiter muss sicherstellen, dass Webanwendungen und Apps ausschließlich vorgesehene Daten und Inhalte einbindet und an den Benutzer ausliefert. Falls Webanwendungen und Apps eine Upload-Funktion für Dateien anbieten, muss diese Funktion durch den Auftragsverarbeiter so weit wie möglich eingeschränkt werden. Auch Zugriffs- und Ausführungsrechte müssen in diesem Fall restriktiv gesetzt werden. Zudem muss sichergestellt werden, dass ein Benutzer Dateien nur im vorgegebenen Pfad speichern kann. Die Entwickler müssen sicherstellen, dass der Benutzer den Ablageort der Uploads nicht beeinflussen kann. Die Ziele der Weiterleitungsfunktion einer Webanwendung müssen ausreichend eingeschränkt werden, sodass Benutzer ausschließlich auf vertrauenswürdige Webseiten weitergeleitet werden.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.26. Konfiguration der Protokollierung auf System- und Netzebene

Alle sicherheitsrelevanten Ereignisse von IT-Systemen und Anwendungen müssen protokolliert werden. Sofern die in der Protokollierungsrichtlinie als relevant definierten IT-Systeme und Anwendungen über eine Protokollierungsfunktion verfügen, muss diese benutzt werden. Wenn die Protokollierung eingerichtet wird, müssen dabei die Herstellervorgaben für die jeweiligen IT-Systeme oder Anwendungen beachtet werden. Es muss in angemessenen Intervallen stichpunktartig überprüft werden, ob die Protokollierung noch korrekt funktioniert. Die Intervalle müssen in der Protokollierungsrichtlinie definiert werden. Sofern betriebs- und sicherheitsrelevante Ereignisse nicht auf einem IT-System protokolliert werden können, müssen weitere IT-Systeme zur Protokollierung (z. B. von Ereignissen auf Netzebene) integriert werden.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.27. Minimierung und Kontrolle von Berechtigungen

Bevor ein IT-System, Anwendung oder App eingeführt wird, muss sichergestellt werden, dass sie nur die minimal benötigten Berechtigungen für ihre Funktion erhält. Nicht unbedingt notwendige Berechtigungen müssen hinterfragt und gegebenenfalls unterbunden werden. Sicherheitsrelevante Berechtigungseinstellungen müssen so fixiert werden, dass sie nicht durch Benutzer oder IT-System, Anwendung oder App geändert werden können. Wo dies technisch nicht möglich ist, müssen die Berechtigungseinstellungen regelmäßig geprüft und erneut gesetzt werden.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.28. Löschung und Vernichtung von Informationen

Es muss geregelt werden, wie die Löschung und Vernichtung von Informationen erfolgt. Dabei muss geregelt werden, welche Informationen und Betriebsmittel unter welchen Voraussetzungen gelöscht und entsorgt werden dürfen. Ebenso muss festgelegt werden, in welchen räumlichen Bereichen Entsorgungs- und Vernichtungseinrichtungen aufgebaut werden sollen. Bevor bereits benutzte Datenträger weitergegeben oder noch einmal eingesetzt werden, müssen alle Daten darauf sicher gelöscht werden. Dazu müssen den Mitarbeitern geeignete Verfahren zur Verfügung stehen.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.29. Archivierung von Informationen

Es muss definiert werden, welche Ziele mit der Archivierung erreicht werden sollen. Hierbei muss insbesondere berücksichtigt werden, welche Regularien einzuhalten sind, welche Mitarbeiter verantwortlich sind und welcher Funktions- und Leistungsumfang angestrebt wird. Die Ergebnisse müssen in einem Archivierungskonzept erfasst werden. Das Archivierungskonzept muss regelmäßig an die aktuellen Gegebenheiten angepasst werden. Alle Zugriffe auf elektronische Archive muss protokolliert werden. Dafür müssen Datum, Uhrzeit, Benutzer, Client-System und die ausgeführten Aktionen sowie Fehlermeldungen aufgezeichnet werden.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.30. Geregelte Außerbetriebnahme von IT-Systemen und Datenträgern

Es muss geregelt und dokumentiert werden, wie IT-Systeme und Datenträger außer Betrieb zu nehmen sind. Dabei muss sichergestellt sein, dass vor der Aussonderung alle auf einem IT-System oder Datenträger gespeicherten Informationen sicher gelöscht sind.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.31. Mandantentrennung im Falle von Outsourcing

Durch ein geeignetes Mandantentrennungskonzept muss sichergestellt werden, dass Anwendungs- und Datenkontexte verschiedener Kunden sauber getrennt sind.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.32. Sicherheitsrelevante Ereignisse

Es müssen geeignete Melde- und Alarmierungswege festgelegt und dokumentiert werden. Es muss klar definiert sein, was ein Datenschutzvorfall ist. Ein Datenschutzvorfall muss so weit wie möglich von Störungen im Tagesbetrieb abgegrenzt sein. Kontaktinformationen müssen immer aktuell und leicht zugänglich sein. Damit ein Sicherheitsvorfall erfolgreich behoben werden kann, muss der Auftragsverarbeiter zunächst das Problem eingrenzen und die Ursache finden. Danach muss er die erforderlichen Maßnahmen auswählen, um das Problem zu beheben. Es muss eine Freigabe erteilt werden, bevor die Maßnahmen umgesetzt werden. Anschließend muss die Ursache beseitigt und ein sicherer Zustand hergestellt werden.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.33. Schutz vor SQL-Injection

Werden Daten an ein Datenbank-System weitergeleitet, müssen die Entwickler Stored Procedures bzw. Prepared SQL Statements einsetzen, wenn dies von der Einsatzumgebung unterstützt wird. Wenn weder Stored Procedures noch Prepared SQL Statements eingesetzt werden können, müssen die SQL-Queries separat abgesichert werden.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.34. Härtung von System, Applikationen und Geräten

Es muss eine Strategie entwickelt werden, wie Systeme, Applikationen und Geräte vor Einsatz in der Infrastruktur gehärtet werden. Die Strategie muss mindestens die Bewertung notwendiger Ports, Kommunikationsprotokolle und Funktionen beinhalten. Die Härtung von Systemen, Applikationen und Geräte muss die Anforderung "Datenschutz durch datenschutzfreundliche Voreinstellungen" berücksichtigen. Es dürfen nur erforderliche personenbezogene Daten verarbeitet werden und die notwendigen Funktionalitäten freigegeben. Alle nicht benötigten Dienste und Anwendungen müssen deaktiviert oder deinstalliert werden, vor allem Netzdienste. Auch alle nicht benötigten Funktionen in der Firmware müssen deaktiviert werden. Nicht benötigte Benutzerkennungen müssen entweder gelöscht oder zumindest so deaktiviert werden, dass unter diesen Kennungen keine Anmeldungen am System möglich sind. Vorhandene Standard-Kennungen müssen soweit wie möglich geändert oder deaktiviert werden. Voreingestellte Passwörter von Standard-Kennungen müssen geändert werden.

☐ Die Anforderung ist erfüllt. ☐ Nicht relevant.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

3.2.35. Betrieb und Aufrechterhaltung eines Datenschutz Managementsystems

Der Auftragsverarbeiter muss einen Beauftragten für den Schutz personenbezogener Daten benennen, sofern hierzu eine rechtliche Verpflichtung besteht. In jedem Fall muss der Auftragsverarbeiter einen kompetenten Ansprechpartner für den Datenschutz benennen. Sowohl der Datenschutzbeauftragte als auch der Ansprechpartner müssen über die für das Unternehmen notwendige Fachkunde verfügen, der höchsten Managementebene direkt unterstellt sein und direkt an diese berichten. Bei der Ausübung ihrer Tätigkeit dürfen keine Interessenkonflikte bestehen. Der Auftragsverarbeiter muss ein Datenschutz- und Risikomanagementsystem etablieren, welches den Anforderungen der DSGVO entspricht. Es muss eine angemessene, aussagekräftige Dokumentation für Verarbeitungen vorliegen. Die Dokumentation muss auch die konkrete Umsetzung und Implementierung technischer und organisatorischer Maßnahmen vorsehen. Zur Gewährleistung einer dauerhaften Aktualität von Unterlagen sowie einer kontinuierlichen Verbesserung der Prozesse muss der Plan-Do-Check-Act-Zyklus herangezogen werden. Ein Datenschutzbericht über die Funktionsweise und Wirksamkeit des Datenschutzmanagementsystems sowie etwaige Störungen und datenschutzrelevante Ereignisse muss mindestens einmal jährlich erstellt und auf Anfrage zur Verfügung gestellt werden.

☐ Die Anforderung ist erfüllt.

☐ Die Anforderung ist teilweise erfüllt.

☐ Die Anforderung ist nicht erfüllt.

Kapitel 4: Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag gemäß Artikel 28 Abs. 3 DS-GVO

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

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.

4.1. Gegenstand und Dauer des Auftrags

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

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

4.2. Konkretisierung des Auftragsinhalts

4.2.1. 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.

4.2.2. 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. DS-GVO sowie die Anforderungen der einschlägigen Rechtsprechung des EuGH (insb. der Rs. C-311/18 – „Schrems II“) und den Empfehlungen des Europäischen Datenschutzausschusses (EDPB) erfüllt sind. Der Auftragnehmer hat das Vorliegen der Erfüllung der besonderen Voraussetzungen der Art. 44 ff. DS-GVO dem Auftraggeber in geeigneter Weise nachzuweisen.

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

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

4.3. Technische und organisatorische Maßnahmen

4.3.1. Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor der Auftragserteilung und vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung, zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Sofern der Auftraggeber nicht widerspricht, werden die dokumentierten Maßnahmen Grundlage

des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

4.3.2. Der Auftragnehmer hat die Sicherheit gem. Art. 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.

4.3.3. 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 schriftlich zu vereinbaren.

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

4.4.1. 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 4.10 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.

4.4.2. Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen. Die Regelungen in 4.10 bleiben hiervon unberührt.

4.5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

4.5.1.1. 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.

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

4.5.1.3. Wahrung der Vertraulichkeit gem. Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO und/oder des etwaig gesetzlich bestehenden Fernmeldegeheimnisses sowie Wahrung der Vertraulichkeit elektronischer Kommunikationsdaten. 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.

4.5.1.4. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gem. Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO.

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

4.5.1.6. 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.

4.5.1.7. 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.

4.5.1.8. 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.

4.5.1.9. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach 4.7 dieser Auftragsverarbeitungsvereinbarung.

4.6. Unterauftragsverhältnisse

4.6.1. Der Auftraggeber stimmt der Beauftragung von Unterauftragnehmern durch den Auftragnehmer 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 Maßgabe des Art. 28 Abs. 2-4 DS-GVO ist 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. DS-GVO sowie die Anforderungen der einschlägigen Rechtsprechung des EuGH (insb. der Rs. C-311/18 – "Schrems II") und den Empfehlungen des Europäischen Datenschutzausschusses (EDPB) auch im Verhältnis zu den Unterauftragsnehmern eingehalten werden.

4.6.2. 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:

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

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

4.6.2.3. im Übrigen die Vorgaben gem. 4.6.1 eingehalten werden.

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

4.6.4. 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.

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

4.7. Kontrollrechte des Auftraggebers

4.7.1. 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.

4.7.2. 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.

4.7.3. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann 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) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit erfolgen.

4.8. Mitteilung bei Verstößen des Auftragnehmers

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

4.8.1.1. 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;

4.8.1.2. 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;

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

4.8.1.4. die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung.

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

4.9. Weisungsbefugnis des Auftraggebers

4.9.1. 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 Vereinbarungfestgelegt und können vom Auftraggeber danach entsprechend 4.9.2 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.

4.9.2. 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.

4.9.3. 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. Einen Wechsel einer/der weisungsberechtigten Person(en) wird der Auftraggeber dem Auftragnehmer unverzüglich mitteilen (mind. Textform).

4.9.4. 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.

4.10. Löschung von Daten und Rückgabe von Datenträgern

4.10.1. 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.

4.10.2. 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 gelangte 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.

4.10.3. 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.

4.11. Haftung

4.11.1. Macht eine betroffene Person gegenüber einem der Vertragspartner erfolgreich einen Schaden aufgrund eines Verstoßes gegen die Regelungen der DS-GVO geltend, findet Art. 82 DS-GVO Anwendung.

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

4.12. Schlussbestimmungen

4.12.1. 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.

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

4.12.3. 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, Datum	Unterschrift/en Auftragnehmer