Anlage zum Vertrag
„Entwicklung einer Webanwendung in agiler Arbeitsweise (Scrum) für Förderprüfungen EEW“

Vereinbarung über die Auftragsverarbeitung (AVV) gemäß Art. 28 Abs. 3 DSGVO

zwischen der

Deutsche Energie-Agentur GmbH (dena)

vertreten durch die Geschäftsführung Corinna Enders und Kristina Haverkamp,

Chausseestraße 128a,

10115 Berlin,

nachfolgend „dena“ oder „Auftraggeber“ genannt

und

[Name des Vertragspartners]

- vertreten durch …….. –

[Anschrift des Vertragspartners]

nachfolgend „Auftragnehmer“ genannt

Präambel

Die dena möchte den Auftragnehmer mit den im Vertrag zur Entwicklung einer Webanwendung in agiler Arbeitsweise (Scrum) für Förderprüfungen EEW („Hauptvertrag“) genannten Leistungen beauftragen.

Im Rahmen der Leistungserbringung wird der Auftragnehmer für die dena ausschließlich im Auftrag und nach dessen Weisung personenbezogene Daten nach Art. 28 DSGVO im Sinne von Art. 4 Nr. 2 DSGVO verarbeiten. Zur Wahrung dieser Anforderungen schließen die Parteien die vorliegende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

1 Begriffsbestimmungen

1.1 Verantwortlicher ist gem. Art. 4 Abs. 7 DSGVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

1.2 Auftragsverarbeiter ist gem. Art. 4 Abs. 8 DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

1.3 Personenbezogene Daten sind gem. Art. 4 Abs. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

1.4 Besonders schutzbedürftige personenbezogene Daten sind personenbezogenen Daten gem. Art. 9 DSGVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, personenbezogene Daten gem. Art. 10 DSGVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln sowie genetische Daten gem. Art. 4 Abs. 13 DSGVO, biometrischen Daten gem. Art. 4 Abs. 14 DSGVO, Gesundheitsdaten gem. Art. 4 Abs. 15 DSGVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

1.5 Verarbeitung ist gem. Art. 4 Abs. 2 DSGVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

1.6 Aufsichtsbehörde ist gem. Art. 4 Abs. 21 DSGVO eine von einem Mitgliedstaat gem. Art. 51 DSGVO eingerichtete unabhängige staatliche Stelle.

2 Gegenstand der Auftragsverarbeitungsvereinbarung (AVV)

Der Auftragnehmer erbringt für die Auftraggeberin Leistungen zur Entwicklung einer Webanwendung in agiler Arbeitsweise (Scrum) für Förderprüfungen EEW auf Grundlage des o. g. Hauptvertrages. Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung der Auftraggeberin. Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende AVV.

Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein die Auftraggeberin verantwortlich. Jedoch ist der Auftragnehmer insbesondere zu entsprechenden Schutzmaßnahmen und Informationen verpflichtet.

Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch der Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die von der Auftraggeberin stammen oder für die Auftraggeberin erhoben wurden.

2.1 Gegenstand des Auftrags

Der Gegenstand des Auftrags ergibt sich aus der Leistungsbeschreibung zum Vertrag „Entwicklung einer Webanwendung in agiler Arbeitsweise (Scrum) für Förderprüfungen EEW vom xx.09.2024“, auf die hier verwiesen wird (im Folgenden Leistungsbeschreibung).

2.2 Dauer

Die Laufzeit dieser Auftragsverarbeitungsvereinbarung (AVV) richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

2.3 Konkretisierung des Auftragsinhalts

Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung.

2.3.1 Art und Zweck der vorgesehenen Verarbeitung

Der Zweck der vorgesehenen Verarbeitung ist die Entwicklung einer Webanwendung (“Steuerungstool”) als Management- und Controlling-Tool der Prozesse zur Abwicklung der Förderprüfungen und zur Verwaltung der Prüffälle und den dazugehörigen Dokumenten.

Der Auftragnehmer wird für der Auftraggeberin personenbezogene Daten nach Maßgabe der nachfolgend beschriebenen Prozesse verarbeiten, welche konkreter in Kapitel 2 der Leistungsbeschreibung beschrieben sind:

- Entwicklung einer Webanwendung als Managementtool mit umfangreichem Funktionsspektrum

- Weiterentwicklung und Anpassung von Features
- Testing der IT-Infrastruktur und Software
- Support- und Wartungsarbeiten (Aktualisierung / Pflege) für:
    - Software der Webanwendung (Steuerungstool)
    - Datenbank
    - Schnittstellen
- Löschen, Anonymisieren und Archivieren von Daten

Zutreffendes bitte ankreuzen und ggf. sonstige Art der Verarbeitung ergänzen

☒ erheben und erfassen ☒ organisieren und ordnen ☒ speichern

☒ anpassen oder verändern ☒ auslesen ☒ abfragen

☒ verwenden ☒ offenlegen durch Übermittlung

☒ verbreiten oder eine andere Form der Bereitstellung ☒ abgleichen oder verknüpfen

☒ einschränken ☒ löschen oder vernichten ☒

……..

2.4 Art der personenbezogenen Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien):

☒ Personen- und Unternehmensstammdaten (inkl. Kontaktdaten wie Telefonnummer, Mobilfunknummer, E-Mail-Adresse)

☒ Kontakt- und Kommunikationsdaten (Korrespondenz z. B. Telefonnotizen, E-Mail-Verkehr, Vermerke)

☒ Urlaubsdaten: urlaubsbedingte Abwesenheiten (z. B. aus Abwesenheitsnotizen in E-Mails bzw. Hinweise zur Verfügbarkeit von Ansprechpartnern)

☒Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse, Zuordnungsmerkmale, Vertragsumfang, Vertragskonditionen)

☒ KfW und BAFA bezogene Kundenhistorie und Kundenbeziehung (z.B. Geschäftsverbindung, Kundentyp, Branchenzuordnung)

☒ Vertragsabrechnungs- und Zahlungsdaten (z.B. Kontonummer, Bankleitzahl, Name des Kreditinstituts, Name des Kontoinhabers, Kreditkartennummer, Überweisungsbetrag, Verwendungszweck)

☒ Zuordnungsmerkmale (z.B. GP-Nummer, Darlehenskontonummer, Nummer der Förderprüfung)

☒ Planungs- und Steuerungsdaten

☒ Score-Werte: Prüfungsdaten: Prüfberichte zur Förderprüfung, Unterlagen zur Prüfungsplanung, Schriftverkehr

☒ Qualifikationen (ohne polizeiliches Führungszeugnis) (z.B. Zeugnisse, Beurteilungen, Abmahnungen, Aus- und Weiterbildungsdaten, Lebenslauf, Fortbildungsnachweis, Nachweis der Zuverlässigkeit (ohne polizeiliches Führungszeugnis), Studienbescheinigungen insbesondere für eingesetzte Fachprüfer für die Förderprüfungen vor Ort)

☒ Bilddaten (z.B. Bilder, Videobilder, Videoaufzeichnungen)

☒ Mit Antrag bzw. Verwendungsnachweis eingereichte Daten (z. B. Kommunikationsdaten in Form von E-Mailverläufen zur Klärung technischer Sachverhalte, Namen von Projektverantwortlichen und Contractinggebern und zugehörige Liefer- und Leistungsverträge, Rechnungen und Ausgabenbelege (Kontoauszüge), Angaben zu Lieferanten/Vertragspartnern des antragstellenden Unternehmens sowie ggf. Protokolle/Erklärungen zur Installation und Inbetriebnahme der geförderten Anlagen (wenn nicht unternehmensbezogen)

☒ Verträge: Produkt-/Programmbezeichnung + jeweilige Produktnummer sowie Modulnummer/ Verwendungszweck), Vertragsreferenzen, Vertragsdatum, Datum Antragseingang, Datum Einreichung Verwendungsnachweis Saldo zum Stichtag, Fördersumme, Kreditbetrag und Tilgungszuschuss, Angebote bzw. Kostenaufstellungen für Energie- und Ressourceneffizienzmaßnahmen bzw. Vergleichsanlagen (Referenzanlagen), Rechnungen für die geförderten Maßnahmen Angebote bzw. Kostenaufstellungen für Energie- und Ressourceneffizienzmaßnahmen bzw. Vergleichsanlagen (Referenzanlagen)

☒ Produkt-/Programmbezeichnung + jeweilige Produktnummer sowie Modulnummer/ Verwendungszweck)

☒ Rechnungen für die geförderten Maßnahmen

☒ Daten zum Unternehmen und dessen technischen Anlagen: Betriebsstandort, Betriebszeiten, Nutzung, technische Anlagen, Produkte, Produktionsmengen, Energie- und Ressourceneffizienzmaßnahmen, Art der Strom- und Wärmeversorgung, Energieträger, Energiebedarf, Energetische Kennwerte und Messdaten, Berechnungen bzw. Simulationen, hierfür eingesetzte Software, Energiekosten, Wirtschaftlichkeit von Energie- und Ressourceneffizienzmaßnahmen, Energie-, Ressourcen- und CO2-Einsparung, Unternehmenszertifikate z. B. für die Zertifizierung mit einem Energie- bzw. Umweltmanagementsystem

☒ Nachweise im Zusammenhang mit den Energie- und Ressourceneffizienzmaßnahmen, z. B. Nachhaltigkeitsnachweis für Biomasse-Brennstoffe; In Einzelfällen

☒ Fallbezogener Schriftverkehr: Beratungsberichte und Daten zu Entwicklungen im Unternehmen (z. B. zum Erreichen der Treibhausgasneutralität)

☒ Kundenbeziehung und Kundenhistorie (z. B. Geschäftsbeziehungen zu KfW / BAFA, Kundentyp, Branchenzuordnung)

☒ Daten zum Fördervorhaben (z. B. Vorhaben-/Antragsdaten, detaillierte Unternehmensdaten, Produktdaten, Planungs- und Berechnungsunterlagen, betriebswirtschaftliche Kennzahlen, Berichtsdaten)

☒ Daten zur Förderprüfung (z. B. Art der Prüfung, ggf. Nennung der Verdachtsmomente)

☒ Zuordnungsmerkmale (z. B. Geschäftspartner-ID, Darlehenskontonummer, Nummer der Förderprüfung)

☒ Daten des Antragsstellenden/Fördernehmenden: Name der Geschäftsführung, bzw. der verantwortlichen sachverständigen Person (Vorname, Nachname, Titel, etc.), ggf. Straße und Hausnummer, Postleitzahl, Stadt, Telefonnummer, Faxnummer, E-Mail-Adresse (wenn nicht unternehmensbezogen)

☒ Daten des Energieberatenden des Antragsstellenden/Fördernehmenden: Name des Unternehmens (wenn personenbezogen), Name der verantwortlichen sachverständigen Person (Vorname, Nachname, Titel, etc.), Beraternummer, Straße und Hausnummer, Postleitzahl, Stadt, Telefonnummer, Faxnummer, E-Mail-Adresse (wenn nicht unternehmensbezogen)

☒ Daten zum Fördervorhaben (wenn personenbezogen), die der Verwaltung und Steuerung der Prüfung dienen, z. B. Geschäftspartner- und (KfW-) Darlehenskontonummer bzw. Zuschussreferenznummer, Zusagebetrag, Name der Ansprechpersonen bei BAFA oder KfW (Vorname, Nachname, Titel, etc.)

☒ Rechnungsdaten

☒ Vertragsabrechnungs- und Zahlungsdaten (z. B. Daten der Kontoverbindung, Verwendungszwecke, Transferbeträge, Kreditkartenummer)

☒ Planungs- und Steuerungsdaten

☒ Bilddaten (z. B. Gebäude außen und innen, Anlagentechnik, Einzelaspekte Herstellungsprozesse, Fuhrpark)

☒ Score-Werte (z. B. Prüfungsdaten, Prüfunterlagen, Prüfberichte, Korrespondenz)

☒ Textdaten bzw. Inhaltsdaten

☒ Auskunftsdaten (z. B. Qualifikationsunterlagen wie Zeugnisse, Nachweise und Zertifikate, Lebenslauf)

☒ Zeiterfassung

☒ Einwilligung(en) (z. B. zum Zweck der Verarbeitung von Daten, soweit noch nicht vorliegend)

2.5 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

☒ Antragstellende/Fördernehmende: Unternehmen und deren Projektverantwortliche/Mitarbeiter (Umfang vgl. Anzahl der geplanten Förderprüfungen in der Leistungsbeschreibung)

☒ Vertragspartner und deren Ansprechpartner der Antragstellenden/Fördernehmenden wie

- Berater, Sachverständige
- Contractinggeber, Dienstleister, Lieferanten, Handwerksbetriebe
- Behörden, Institutionen

☒ Ansprechpartner der Durchführer für die Antragstellenden/Fördernehmenden: Mitarbeiter, externe Beschäftigte und ehem. Mitarbeiter sowie ehem. externe Beschäftigte von BAFA und KfW

☒ Mitarbeiter und ehem. Mitarbeiter der dena

☒ Vertragspartner der dena: Mitarbeiter / externe Beschäftigte und ehem. Mitarbeiter / externe Beschäftigte von Auftragnehmenden der dena

2.6 Ort der Datenverarbeitung

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

Jede Verlagerung der Dienstleistung oder von Teilarbeiten in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

3 Weisungsrecht

3.1 Der Auftragnehmer darf personenbezogene Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers verarbeiten; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

3.2 Die dena hat jederzeit das Recht, umfassend Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten, sofern berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen. Die Weisungen werden anfänglich durch diese AVV festgelegt und können von der dena danach schriftlich oder in einem dokumentierten elektronischen Format (z.B. per E-Mail) an die vom Auftragnehmer bezeichnete Stelle durch

einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren.

3.3 Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, nach einem entsprechenden Hinweis gegenüber dem Auftraggeber, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

3.4 Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

3.5 Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

4 Weisungsberechtigte des Auftragsgebers, Weisungsempfänger des Auftragnehmers

Weisungsberechtigte Personen des Auftraggebers sind neben den vertretungsberechtigten Personen der dena:
Elisabeth Gebhard (IME), Elisabeth.Gebhard@dena.de, Tel. +49 30 66 777-214;

Johannes Wiedemann (IME), johannes.wiedemann@dena.de, Tel. +49 30 66 777-299;

Dr. Daniel Vallentin (IME), Daniel.Vallentin@dena.de, Tel. +49 30 66 777-134

(Vorname, Name, Bereich, Telefon, E-Mail-Adresse)

Weisungsempfänger beim Auftragnehmer ist/sind:

_____

(Vorname, Name, Bereich, Telefon, E-Mail-Adresse)

Für Weisung zu nutzende Kommunikationskanäle:

_____

(genaue postalische Adresse und/oder E-Mail und/oder Telefonnummer)

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpersonen sind der anderen Vertragspartei unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger/-in bzw. die Vertretung mitzuteilen.

Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

5 Schutzmaßnahmen des Auftragnehmers

5.1 Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

5.2 Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes und der Datensicherheit gerecht wird. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DSGVO, insbesondere mindestens die in der **Anlage** aufgeführten technischen und organisatorischen Maßnahmen der Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle, Trennungskontrolle.

5.3 Das Datenschutzkonzept des Auftragnehmers stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT- Systeme und Verarbeitungsprozesse beim Auftragnehmer dar. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist das Datenschutzkonzept einvernehmlich anzupassen und die Anpassung umzusetzen, ohne dass ein zusätzlicher Vergütungsanspruch entsteht.

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

5.5 Beim Auftragnehmer ist als betriebliche/-r Datenschutzbeauftragte/-r bzw. als Ansprechperson für den Datenschutz (sofern ein/-e Datenschutzbeauftragte/-r nach Art. 37 Abs. 1 DSGVO nicht bestellt werden muss) bestellt:

(Vorname, Name, Organisationseinheit, Telefon)

Der Auftragnehmer veröffentlicht die Kontaktdaten des/der Datenschutzbeauftragten auf seiner Internetseite und teilt sie der Aufsichtsbehörde mit. Veröffentlichung und Mitteilung weist der Auftragnehmer auf Anforderung des Auftraggebers in geeigneter Weise nach.

5.6 Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden Mitarbeiter genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen. Diese Verpflich-

tungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

5.7 Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist nur mit Zustimmung des Auftraggebers gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen. Die Maßnahmen nach Art. 32 DSGVO sind auch in diesem Fall sicherzustellen.

5.8 Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. e und f DSGVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an die unter Ziff. 4 genannte weisungsberechtigte Person und an die betriebliche Datenschutzbeauftragte der dena (datenschutz@dena.de) weiterzuleiten.

5.9 Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind.

6 Informationspflichten des Auftragnehmers

6.1 Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder Textform informieren. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;

b) eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 (= Weisungsberechtigte und Weisungsempfänger) dieses Vertrages durchführen.

6.2 Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Auftraggeber und ersucht um weitere Weisungen.

6.3 Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Ziff. 6.1. betroffen sind.

6.4 Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem" im Sinne der DSGVO liegen.

6.5 Über wesentliche Änderung der Sicherheitsmaßnahmen nach § 6 Abs. 2 hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

6.6 Ein Wechsel in der Person des/der betrieblichen Datenschutzbeauftragte/-n bzw. der Ansprechperson für den Datenschutz ist dem Auftraggeber unverzüglich mitzuteilen.

6.7 Der Auftragnehmer und gegebenenfalls sein/-e Vertreter/-in führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DSGVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

6.8 An der Erstellung des Verarbeitungsverzeichnisses durch den Auftraggeber hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

7 Kontrollrechte der dena

7.1 Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig einmal im Quartal von den technischen und organisatorischen Maßnahmen des Auftragnehmers. Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

7.2 Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.

7.3 Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

7.4 Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

7.5 Der Auftragnehmer weist dem Auftraggeber die Verpflichtung der Mitarbeiter/-innen nach Ziff. 5.6. auf Verlangen nach.

8 Unterauftragsverhältnisse

8.1 Begriffsbestimmung

Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen für den Auftragnehmer, Post-/Transportdienstleistungen, Reinigungsleistungen und Bewachungsdienste. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Unteraufträge dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

8.2 Zustimmungsvorbehalt

Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklich schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

Zutreffendes bitte ankreuzen:

a) ☐ Eine Unterbeauftragung ist nicht zulässig.

b) ☒ Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu, unter der Bedingung einer schriftlich abgefassten Vereinbarung zwischen dem Auftragnehmer und dem Unterauftragnehmer nach Maßgabe des Art. 28 Abs. 2-4, Abs. 9 DSGVO und den weiteren Voraussetzungen in dieser Vereinbarung:

Firma Unterauftragnehmer	Anschrift/Land	Leistung

c) ☒ Die spätere Auslagerung auf Unterauftragnehmer oder

☒ Wechsel der bestehenden Unterauftragnehmer sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer durchführt und dem Auftraggeber eine angemessene Zeit vorab (mind. 3 Wochen) schriftlich oder in Textform anzeigt **und**
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung/Änderung gem. Art. 28 Abs. 2 S. 2 DSGVO erhebt **und**
- eine schriftlich abgefasste Vereinbarung zwischen dem Auftragnehmer und dem Unterauftragnehmer nach Maßgabe des Art. 28 Abs. 2-4, Abs. 9 DSGVO und den weiteren Voraussetzungen in dieser Vereinbarung zugrunde gelegt wird.

8.3 Voraussetzungen für Unterauftragsverarbeitungsvereinbarung und Übermittlung personenbezogener Daten

Der Auftragnehmer muss dafür Sorge tragen, dass der Unterauftragnehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

Eine Beauftragung von Unterauftragnehmern, die die vereinbarte Leistung in Drittstaaten (also außerhalb der EU/des EWR) erbringt, darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Unterauftragnehmern gelten. In dem Vertrag mit dem Unterauftragnehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Unterauftragnehmers deutlich voneinander abgegrenzt werden. Werden mehrere Unterauftragnehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Unterauftragnehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Unterauftragnehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO).

Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung, insbesondere auch das Vorliegen einer Verpflichtung nach Art. 29 und Art. 32 Abs. 4 DSGVO, gestattet.

8.4 Überprüfung des und Haftung für den Unterauftragnehmer

Der Auftragnehmer hat insbesondere die Einhaltung der vertraglichen Vereinbarung sowie der Datenschutzbestimmungen durch den Unterauftragnehmer regelmäßig zu überprüfen und die dena unverzüglich über etwaige Unregelmäßigkeiten zu informieren. Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, insbesondere denjenigen Pflichten, die ihm durch den Auftragnehmer im Einklang mit diesem Vertrag auferlegt wurden.

8.5 Unterunterauftragsverhältnis

Zutreffendes bitte ankreuzen:

Eine weitere Auslagerung durch den Unterauftragnehmer

- ☒ ist nicht gestattet;
- ☐ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);
- ☐ bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform);

Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

9 Datenschutzkontrolle

Der Auftragnehmer verpflichtet sich, der/dem Datenschutzbeauftragten des Auftraggebers sowie der zuständigen Aufsichtsbehörde zur Erfüllung ihrer jeweiligen gesetzlichen zugewiesenen Aufgaben im Zusammenhang mit diesem Auftrag jederzeit Zugang zu den üblichen Geschäftszeiten zu gewähren. Der Auftragnehmer unterwirft sich zusätzlich zu der für sie bestehenden gesetzlichen Datenschutzaufsicht der Kontrolle der für den Verantwortlichen bestehenden Datenschutzaufsicht (hier: die/der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit) und der Kontrolle durch die/den Datenschutzbeauftragten des Verantwortlichen mit Ausnahme der Bereiche, die keinerlei Bezug zur Auftragserfüllung haben. Sie duldet insbesondere Betretungs-, Einsichts- und Fragerechte der Genannten einschließlich der Einsicht in durch Berufsgeheimnisse geschützte Unterlagen. Sie wird ihre Mitarbeiterinnen und Mitarbeiter anweisen, mit den Genannten zu kooperieren, insbesondere deren Fragen wahrheitsgemäß und vollständig zu beantworten. Die nach Gesetz bestehenden Verschwiegenheitspflichten und Zeugnisverweigerungsrechte der Genannten bleiben davon unberührt.

10 Anfragen und Rechte Betroffener

10.1 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. Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft sind nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

10.2 Macht eine betroffene Person Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich ihrer Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist die betroffene Person unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

11 Haftung und Vertragsstrafe

Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung. Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in

keinerlei Hinsicht für den Umstand, durch den der Schaden bei einer betroffenen Person eingetreten ist, verantwortlich ist.

Für den Fall, dass der Auftragnehmer, seine Beschäftigen oder sonstige Personen, für die der Auftragnehmer gemäß §§ 31, 278, 831 BGB einzustehen hat, Verpflichtungen aus dieser Vereinbarung schuldhaft verletzt, vereinbaren die Parteien die Zahlung einer Vertragsstrafe durch den Auftragnehmer an den Auftraggeber in angemessener Höhe, welche 5.001,00 EUR nicht unterschreiten und 100.000 EUR nicht überschreitet, wobei der Auftraggeber die Höhe nach billigem Ermessen i.S.v. § 315 BGB bestimmen wird und die Angemessenheit der Vertragsstrafe im Streitfall von dem zuständigen Gericht überprüft werden kann. Die Geltendmachung weiterer Ansprüche, wie auf Schadensersatz oder Unterlassung, bleibt der dena vorbehalten. Die Vertragsstrafe wird auf einen eventuell zu leistenden Schadensersatz angerechnet. Weitergehende Schadensersatzansprüche bleiben unberührt. Darüber hinaus ist die Vertragsstrafe auf maximal 1.000,00 € zu begrenzen, wenn es sich um einen nur geringfügigen Verstoß handelt. 348 HGB wird ausgeschlossen.

12 Außerordentliches Kündigungsrecht

Der Auftraggeber kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DSGVO vorsätzlich oder grob fahrlässig verletzt oder eine Weisung (im Sinne dieser AVV) des Auftraggebers nicht ausführen kann oder will. Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann.

13 Beendigung des Hauptvertrags

13.1 Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen. Zu entsorgende Unterlagen sind mit einem Aktenvernichter nach DIN 32757-1 zu vernichten. Zu entsorgende Datenträger sind nach DIN 66399 zu vernichten.

13.2 Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

13.3 Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

14 Verschwiegenheitsvereinbarung

Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln, soweit sie nicht aufgrund eines Gesetzes oder einer Anordnung zur Offenlegung verpflichtet sind. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

15 Angabe der zuständigen Datenschutz-Aufsichtsbehörde

15.1. Zuständige Aufsichtsbehörde für den Auftraggeber ist die Berliner Beauftragte für Datenschutz und Informationssicherheit.

15.2 Zuständige Aufsichtsbehörde für den Auftragnehmer ist [der/die Landesbeauftragte für den Datenschutz <Bundesland>].

ODER Der Auftragnehmer hat als Vertreter nach Art. 27 Abs. 1 DSGVO benannt: […].

15.3 Der Auftraggeber und der Auftragnehmer und gegebenenfalls deren Vertretung arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

16 Aufbewahrungspflichten

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Unterauftragnehmern) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

17 Schlussbestimmungen: Schriftform, kein Zurückbehaltungsrecht, Insolvenz, salvatorische Klausel, anwendbares Recht, Gerichtsstand

17.1 Mündliche oder schriftliche Nebenabreden zu dieser Auftragsverarbeitungsvereinbarung bestehen nicht. Änderungen und Ergänzungen dieser AVV bedürfen zu ihrer Wirksamkeit der Schriftform. Dies gilt auch für die Abbedingung oder den Verzicht auf das Schriftformerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

17.2 Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

17.3 Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

17.4 Sind oder werden einzelne Bestimmungen des Vertrages unwirksam, so wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. Die Vertragspartner werden in diesem Fall die ungültige Bestimmung durch eine andere ersetzen, die dem wirtschaftlichen Zweck der weggefallenen Regelung in zulässiger Weise am nächsten kommt. Das Gleiche gilt für das Vorliegen von Vertragslücken.

17.5 Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Berlin.

Anlage: Technische und organisatorische Maßnahmen des Auftragnehmers