Anhang „Technisch-organisatorische Maßnahmen“ zur Vereinbarung zur Auftragsverarbeitung

zwischen **Deutsche Energie-Agentur GmbH** (dena), Chausseestraße 128a, 10115 Berlin

und <**Dienstleister**, Adresse> (nachfolgend Auftragsverarbeiter)

Ziffer 5.2 der Vereinbarung zur Auftragsverarbeitung verweist zur Konkretisierung der technisch-organisatorischen Maßnahmen auf diesen Anhang.

§ 1 Technische und organisatorische Sicherheitsmaßnahmen

Die Vertragspartner sind verpflichtet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung der Daten im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Person in angemessener Form gewährleistet ist.

§ 2 Innerbetriebliche Organisation des Auftragsverarbeiters

Der Auftragsverarbeiter wird seine innerbehördliche oder innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes nach der DSGVO und dem BDSG gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden Daten oder Datenkategorien geeignet sind.

§ 3 Konkretisierung der Einzelmaßnahmen

(1) Im Einzelnen werden folgende Maßnahmen bestimmt, die der Umsetzung der Vorgaben des Art. 32 DSGVO dienen:

Nr.	Maßnahme	Umsetzung der Maßnahme
1.	**Zutrittskontrolle** Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.	*[Ergänzen]* ***Zum Beispiel:*** *Zutrittskontrollsystem, Ausweisleser, Magnetkarte, Chipkarte, Schlüssel, Schlüsselvergabe, Werkschutz, Pförtner, Überwachungseinrichtung, Alarmanlage, Türsicherung*

2.	**Zugangskontrolle** Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	***Zwingend erforderlich:*** • Zugang zu den Computersystemen nur mit personifizierten Nutzernamen/Kennwort • Passwortrichtlinie für Kennwörter • Einsatz von Anti-Viren-Software • Einsatz von Firewall-System • Verschlüsselung von Notebooks --- *Ggf. ergänzen, **zum Beispiel:** Technische und organisatorische Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren (Beispiele: Automatisches Sperren, Einrichtung eines Benutzerstammsatzes pro User, Verschlüsselung von Datenträgern)*
3.	**Zugriffskontrolle** Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	***Zwingend erforderlich:*** • Zugriffsrechte über Rollen / Gruppen • Protokollierung von Zugriffen und Änderungen auf Daten in zentralen Systemen --- *Ggf. ergänzen, **zum Beispiel**: Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren (Beispiele: differenzierte Berechtigungen wie Profile, Rollen etc. Auswertungen, Kenntnisnahme, Veränderung, Löschung)*

4.	**Weitergabekontrolle** Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.	*[Ergänzen]* ***Zum Beispiel:*** *Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren, elektronische Signatur*
5.	**Eingabekontrolle** Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	*[Ergänzen]* ***Zum Beispiel:*** *Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung gewährleisten, etwa durch Protokollierungs- und Auswertungssysteme*
6.	**Auftragskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können.	***Zwingend erforderlich:*** • Sofern Subunternehmende mit der Verarbeitung personenbezogener Daten beauftragt werden, werden diese schriftlich beauftragt und denselben Regelungen unterworfen • Alle Mitarbeitenden werden im Umgang mit personenbezogenen Daten geschult --- *Ggf. ergänzen,* ***zum Beispiel****: Abgrenzen der Kompetenz zwischen Verantwortlichem und Auftragsverarbeiter (Beispiel: eindeutige Vertragsgestaltung, Kriterien zur Auswahl des Auftragsverarbeiters, Kontrolle der Vertragsausführung)*

7.	**Verfügbarkeitskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	*[Ergänzen]* ***Zum Beispiel:*** *Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen, Maßnahmen zur Datensicherung (Beispiel: Backup-Verfahren, Spiegeln von Festplatten, unterbrechungsfreie Stromversorgung, Firewall, Notfallplan)*
8.	**Trennungskontrolle** Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	*[Ergänzen]* ***Zum Beispiel:*** *Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten, Mandantenfähigkeit, Funktionstrennung zwischen Produktion / Test*

(2) Es ist ein Verfahren zu etablieren, das eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der zum Einsatz kommenden technischen und organisatorischen Maßnahmen durch die Vertragsparteien ermöglicht.

(3) Ein/e Datenschutzbeauftragte/r ist schriftlich zu benennen.