Anlage

„Technisch-organisatorische Maßnahmen“

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 diese Anlage.

§ 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.	▪ Während der Vor-Ort-Kontrollen führt die Prüferin/ der Prüfer das Tablet ständig mit sich. ▪ Ansonsten verwahrt die Prüferin/ der Prüfer das Tablet in einem verschlossenen Behältnis oder einer anderen Schutzvorrichtung, die gegen Wegnahme besonders gesichert ist.

2.	**Zugangskontrolle** Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	▪ Zugang zum Tablet nur durch Berechtigte und nur mit Kennwort, das den Komplexitätsanforderungen der dena-Sicherheitsrichtlinie entspricht. ▪ Das Tablet wird bei Nichtnutzung sofort gesperrt. ▪ Einsatz von Anti-Viren-Software je nach Anforderung durch die dena. ▪ Einsatz von Firewall-System je nach Anforderung durch die dena.
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.	▪ Während der Vor-Ort-Kontrollen führt die Prüferin/ der Prüfer das Tablet ständig mit sich. ▪ Zugriff auf Daten nur durch den Auftraggeber der Prüferin oder des Prüfers und die dena aufgrund der Datenübertragung per E-Mail. ▪ Prüfung der ein- und ausgehenden Daten und E-Mails durch Firewall-System inkl. Virenschutz je nach Installationsvorgaben der dena.
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.	▪ Während der Vor-Ort-Kontrollen führt die Prüferin/ der Prüfer das Tablet ständig mit sich. ▪ Der von der dena zur Verfügung gestellte Webmail-Account ist SSL-verschlüsselt. ▪ Die alternative Datenübertragung über die sog. dena-Cloud ist ebenfalls SSL-verschlüsselt. ▪ Die Excel-Dateien werden darüber direkt passwortgeschützt an die dena übermittelt (E-Mails verlassen die dena nicht). ▪ Es werden bei technischen Problemen ausschließlich von der dena autorisierte Personen involviert.
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.	Der Zugriff auf das Tablet, das zur Datenverarbeitung genutzt wird, ist aufgrund des Passwortschutzes nur der Prüferin/ dem Prüfer möglich.

6.	**Auftragskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können.	▪ Schriftlicher Vertrag gem. Vorgaben Art. 28 Abs. 3 DSGVO. ▪ Daten werden gem. den Anweisungen des Auftraggebers verarbeitet. ▪ Dem Auftraggeber werden Weisung- und Kontrollrechte gem. Hauptvertrag und Auftragsverarbeitungsvereinbarung eingeräumt.
7.	**Verfügbarkeitskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	▪ Alle relevanten Daten werden sofort nach Erfassung per Mail versendet und sind daher über das Backup der dena gesichert. ▪ Die störungsfreie Stromversorgung wird geprüft. ▪ Die Software ist nach Weisung der dena aktuell zu halten, Updates sind nach Aufforderung durchzuführen.
8.	**Trennungskontrolle** Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	▪ Die Prüferin/ der Prüfer verwendet das Tablet ausschließlich zum Zweck der Datenaufnahme im Rahmen der Vor-Ort-Kontrollen. Somit ist eine Trennung von Daten, die zu anderen Zwecken erhoben werden, gegeben. ▪ Verwendung der benötigten Software auf aktuellem Stand und entsprechend den Anforderungen der dena bzw. des Auftraggebers der Prüferin/des Prüfers.
	Datenlöschung	▪ Nach Aufforderung durch die dena in Textform werden mit entsprechender Software alle personenbezogenen Unterlagen auf dem Tablet sicher gelöscht und der freie Speicher mehrfach überschrieben, so dass eine Wiederherstellung ausgeschlossen ist.

(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) Das Meldesystem für (IT-)Sicherheitsvorfälle und Datenpannen ist einzuhalten. Vorfälle sind zu protokollieren.