

Vertrag zur Auftragsverarbeitung

gemäß Art. 28 DSGVO

zwischen dem Lizenznehmer

- Verantwortlicher -

nachstehend Auftraggeber genannt

und der

Solar-Log GmbH

Fuhrmannstraße 9, 72351 Geislingen-Binsdorf

- Auftragsverarbeiter -

nachstehend Auftragnehmer genannt

zusammen auch im Folgenden als die „Parteien“ bezeichnet.

Präambel

Dieser Vertrag zur Auftragsverarbeitung regelt die Rechte und Pflichten bezüglich der weisungsgebundenen Datenverarbeitung der Parteien im Rahmen der Leistungserbringung durch den Auftragnehmer. Der Auftraggeber hat den Auftragnehmer sorgfältig ausgewählt und insbesondere sichergestellt, dass der Auftragnehmer hinreichende Garantien dafür bietet, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung personenbezogener Daten durch ihn im Einklang mit den für ihn geltenden datenschutzrechtlichen Vorgaben erfolgt und den Schutz der Rechte der von der Verarbeitung betroffenen Personen gewährleistet.

1. Gegenstand und Dauer des Auftrags

1.1 Gegenstand

Der Gegenstand des Auftrags ergibt sich aus dem Lizenzvertrag für das Solar-Log WEB Enerest™ Portal, auf den hier verwiesen wird (im Folgenden Leistungsvereinbarung)

1.2 Ort der Verarbeitung durch den Auftragnehmer

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet auch außerhalb eines Mitgliedsstaates der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt.

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

Das angemessene Schutzniveau in der Schweiz

- ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DSGVO);
- wird hergestellt durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m. 47 DSGVO);

1.3 Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Lizenzvertrages.

Der Auftrag ist unbefristet erteilt und kann gemäß den Lizenzvertragsbedingungen gekündigt werden.

- 1.4 Der Auftraggeber kann diesen Vertrag als auch das zugrundeliegende Rechtsverhältnis nach Ziffer 1.1 jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar. 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.
- 1.5 Die Beauftragung des Auftragnehmers entbindet den Auftraggeber nicht von seiner Verpflichtung, die für ihn geltenden datenschutzrechtlichen Vorgaben, insbesondere im Hinblick auf die Rechtmäßigkeit der Verarbeitung sowie der Wahrung der Rechte der betroffenen Personen (Art. 12 bis 22 DSGVO) zu wahren. Vor diesem Hintergrund bleibt der Auftraggeber für die Datenverarbeitung Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO.

2. Konkretisierung des Auftragsinhalts

2.1 Art der vorgesehenen Verarbeitung gem. Art. 4 Nr. 2 DSGVO

Im Rahmen der Auftragsverarbeitung sind folgende Arten von Verarbeitungen vorgesehen:

- Erheben
- Erfassen
- Organisation
- Ordnen
- Speicherung
- Anpassung oder Veränderung
- Auslesen
- Abfragen
- Berechnen

- Anonymisieren
- Verwendung
- Offenlegung durch Übermittlung
- Verbreitung oder eine andere Form der Bereitstellung
- Abgleich oder die Verknüpfung
- Einschränkung
- Löschen

2.2 Zweck der vorgesehenen Verarbeitung von Daten

Die Verarbeitung wird zu folgenden Zwecken durchgeführt:

Siehe: [Datenschutzinformation für Solar-Log WEB Enerest™](#)

2.3 Art der personenbezogenen Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- Personenstammdaten
- Kommunikationsdaten (z. B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Sonstige anfallende Daten aus der Erfüllung unserer vertraglichen und gesetzlichen Verpflichtung

2.4 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden
- Deren Beschäftigte
- Alle Nutzer von Solar-Log WEB Enerest™

3. Weisungsbefugnis des Auftraggebers

- 3.1 Der Auftragnehmer und jede von ihm zur Verarbeitung personenbezogener Daten befugte Person darf die im Auftrag verarbeiteten Daten nur nach dokumentierten Weisungen des Auftraggebers verarbeiten. Eine Verarbeitung für andere als in diesem Vertrag festgelegte Zwecke ist nicht gestattet.

Weisungsempfänger beim Auftragnehmer sind alle festen und freien Mitarbeiter der Solar-Log GmbH.

- 3.2 Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Die Einzelweisungen sind vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren.

- 3.3 Soweit der Auftragnehmer der Auffassung ist, dass Weisungen gegen anwendbares Recht verstoßen, wird er den Auftraggeber hierüber unverzüglich informieren. In diesem Fall ist der Auftragnehmer berechtigt, die Umsetzung der Weisung so lange auszusetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde. Eine von den Weisungen des Auftraggebers abweichende Verarbeitung ist nur zulässig, sofern der Auftragnehmer durch das Recht der Union oder der Mitgliedsstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

4. Verpflichtung auf die Vertraulichkeit

Bei der Datenverarbeitung durch den Auftragnehmer ist es dessen beschäftigten Personen 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 entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Beschäftigten und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

5. Technische und organisatorische Maßnahmen (TOM)

- 5.1 Der Auftragnehmer hat seine innerbetriebliche Organisation so gestaltet, dass alle von ihm als Auftragsverarbeiter zu beachtenden, besonderen datenschutzrechtlichen Anforderungen gewahrt werden.
- 5.2 Er hat in diesem Zusammenhang insbesondere die in der Anlage 1 genannten technischen und organisatorischen Maßnahmen nach Art. 28 Abs. 3 lit. c, 32 DSGVO getroffen, die erforderlich sind, um die Anforderungen an die Sicherheit der Verarbeitung zu gewährleisten. Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen wird der Auftragnehmer den Auftraggeber bestmöglich bei der Einhaltung der vom Auftraggeber zu treffenden technischen und organisatorischen Maßnahmen sowie dessen Pflichten nach Art. 32 DSGVO unterstützen.
- 5.3 Eine Aufstellung der von ihm getroffenen technischen und organisatorischen Maßnahmen hat der Auftragnehmer dem Auftraggeber vor Abschluss dieses Vertrages zur Prüfung übergeben.
- 5.4 Die vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Vor diesem Hintergrund ist es dem Auftragnehmer gestattet, neue Technologien oder technische Werkzeuge einzusetzen, mit denen der Schutz der von ihm verarbeiteten personenbezogenen Daten verbessert werden kann. Das Sicherheitsniv-

eau der im Rahmen dieses Vertrags festgelegten Maßnahmen darf dabei jedenfalls nicht unterschritten werden.

- 5.5 Wesentliche Änderungen wird der Auftragnehmer dokumentieren und dem Auftraggeber in diesem Zusammenhang unaufgefordert in einer entsprechend angepassten Anlage vorlegen.
- 5.6 Auf Anfrage legt der Auftragnehmer geeignete Nachweise dafür vor, dass er alle erforderlichen technischen und organisatorischen Maßnahmen umgesetzt hat. Zum Nachweis der getroffenen technischen und organisatorischen Maßnahmen kann der Auftragnehmer aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung (z.B. nach Art. 42 DSGVO) durch ein IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) vorlegen.
- 5.7 Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate (auch Back-Ups) der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.
- 5.8 Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

6. Pflichten des Auftragnehmers

- 6.1 Der Auftragnehmer gewährleistet die ordnungsgemäße Führung eines den Vorgaben des Art. 30 Abs. 2 DSGVO entsprechenden Verzeichnisses von Verarbeitungstätigkeiten.

An der Erstellung und Aktualisierung des Verzeichnisses von Verarbeitungstätigkeiten durch den Auftraggeber hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

- 6.2 Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, wenn er der Auffassung ist, dass dieser Vertrag oder Teile davon nicht den Anforderungen an einen Vertrag zur Auftragsverarbeitung nach den relevanten Vorschriften der DSGVO und/oder etwaigen Leitlinien, Empfehlungen oder sonstigen Stellungnahmen der Aufsichtsbehörden, insbesondere der Datenschutzkonferenz, der ehem. Art. 29 Datenschutzgruppe oder des Europäischen Datenschutzausschusses entspricht. In einem solchen Fall werden sich die Parteien gemeinsam um die erforderlichen Anpassungen dieses Vertrages bemühen.
- 6.3 Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, falls die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden. Der Auftrag-

nehmer wird alle in diesem Zusammenhang Beteiligten unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlichem im Sinne der DSGVO liegen.

6.4 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 Auftraggeber unverzüglich in Schriftform oder Textform informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

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

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.

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

6.5 Soweit gesetzlich vorgeschrieben, hat der Auftragnehmer einen Datenschutzbeauftragten benannt oder wird einen Datenschutzbeauftragten benennen, der die ihm gem. Art. 38, 39 DSGVO obliegenden Aufgaben wahrnimmt. Die Kontaktdaten des Datenschutzbeauftragten hat der Auftragnehmer der für ihn zuständigen Datenschutz-Aufsichtsbehörde mitgeteilt. Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten/Ansprechpartners für den Datenschutz oder eine Erstbenennung ist dem Auftraggeber unverzüglich mitzuteilen.

6.6 Soweit der Auftraggeber seinerseits einer Kontrolle der Datenschutz-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.

7. Unterauftragsverhältnisse (siehe [Datenblatt Subunternehmer](#))

7.1 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, Post-/Transportdien-

stleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. 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.

- 7.2 Der Auftraggeber stimmt der Beauftragung der in dem [Datenblatt Subunternehmer](#) aufgeführten Unterauftragnehmer unter den folgenden Bedingungen zu.
- Die Auslagerung auf Unterauftragnehmer oder der Wechsel eines bestehenden Unterauftragnehmers ist zulässig, soweit der Auftragnehmer dies dem Auftraggeber eine angemessene Zeit vorab 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 erhebt.
- 7.3 Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
- 7.4 Sofern eine Einbeziehung von Unterauftragnehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Unterauftragnehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Unterauftragnehmern nachweisen.
- 7.5 Sämtliche vertragliche Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen. Die Parteien halten klarstellend fest, dass der Auftragnehmer dem Auftraggeber stets für die Einhaltung der Pflichten des Unterauftragnehmers haftet. Im Falle einer Verletzung der Pflichten aus der Vereinbarung mit dem Auftragnehmer oder eines Verstoßes gegen relevante gesetzliche Vorgaben durch den Unterauftragnehmer bleibt der Auftragnehmer dem Auftraggeber voll verantwortlich.

8. Unterstützungspflichten des Auftragnehmers

- 8.1 Der Auftragnehmer wird den Auftraggeber bestmöglich bei der Erfüllung seiner Pflichten zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Personen (i. S. d. Art. 12–22 DSGVO) in Bezug auf ihre personenbezogenen Daten unterstützen.

Der Auftragnehmer wird den Auftraggeber unverzüglich insbesondere über alle Auskunfts-, Berichtigungs-, Lösch-, Einschränkung- und Datenübertragungsverlangen betroffener Personen informieren. Entsprechende Anträge und Ersuchen wird der Auftragnehmer unverzüglich an den Auftrag-

geber weiterleiten. Der Auftragnehmer ist nicht befugt betroffenen Personen oder Dritten Auskunft über die im Auftrag verarbeiteten personenbezogenen Daten zu geben.

- 8.2 Der Auftragnehmer wird den Auftraggeber bestmöglich bei der Erfüllung seiner gesetzlichen Verpflichtungen nach Art. 32 bis 36 DSGVO unterstützen. Soweit erforderlich, wird der Auftragnehmer in diesem Zusammenhang daher insbesondere
- ein angemessenes Schutzniveau durch technische und organisatorische Maßnahmen sicherstellen, 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,
 - die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden,
 - den Auftraggeber im Rahmen seiner Informationspflicht gegenüber den betroffenen Personen unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung stellen,
 - den Auftraggeber bei der Durchführung einer Datenschutz-Folgenabschätzung unterstützen,
 - den Auftraggeber im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde unterstützen.
- 8.3 Der Auftragnehmer wird den Auftraggeber unverzüglich über alle Kontrollhandlungen und Maßnahmen einer Datenschutz-Aufsichtsbehörde informieren. Dies gilt auch, wenn eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten beim Auftragnehmer ermittelt.
- 8.4 Soweit sich der Auftraggeber Kontrollen der Aufsichtsbehörden, einem Ordnungswidrigkeits- oder Strafverfahren, Ansprüchen einer betroffenen Person nach Art. 82 DSGVO, Ansprüchen eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt sieht, wird der Auftragnehmer den Auftraggeber hierbei bestmöglich unterstützen.
- 8.5 Die Parteien verpflichten sich, etwaige im Rahmen der Prüfung von Aufsichtsbehörden festgestellte und mit diesem Vertrag im Zusammenhang stehende Mängel unverzüglich zu beheben.

9. Berichtigung, Einschränkung und Löschung von Daten

- 9.1 Der Auftragnehmer wird von ihm verarbeitete personenbezogene Daten des Auftraggebers nur nach dessen Weisung berichtigen oder löschen. Soweit eine datenschutzkonforme Löschung oder Einschränkung der Datenverarbeitung nicht möglich ist, kann der Auftraggeber den Auftragnehmer mit der datenschutzkonformen Vernichtung von Datenträgern und sonstigen Materialien beauftragen. Wendet sich eine betroffene Person zwecks Berichtigung, Löschung ihrer personenbezogenen Daten oder Auskunft zu ihren personenbezogenen Daten unmittelbar an den Auftragnehmer, wird er dieses Gesuch unverzüglich an den Auftraggeber weiterleiten.

- 9.2 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 und Datenträger sind nach DIN 66399 zu vernichten.
- 9.3 Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.
- 9.4 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.

10. Kontrollrechte des Auftraggebers

- 10.1 Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig 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.
- 10.2 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.
- 10.3 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.

- 10.4 Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

11. Haftung

Die Haftung der Parteien richtet sich nach den Haftungsregelungen des Art. 82 DSGVO.

12. Schlussbestimmungen

- 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.
- 12.2 Änderungen und Ergänzungen dieses Vertrags bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.
- 12.3 Sollten einzelne Bestimmungen dieses Vertrags ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.
- 12.4 Dieser Vertrag unterliegt dem Recht der Bundesrepublik Deutschland. Gerichtsstand ist – soweit zulässig – der Sitz des Auftragnehmers Solar-Log GmbH in Geislingen - Binsdorf.

ANLAGE 1:

Allgemeine technische und organisatorische Maßnahmen nach Art. 32 Abs. 1 DS-GVO

Der Auftragnehmer hat die nachfolgenden technischen und organisatorischen Maßnahmen getroffen.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle

Maßnahmen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- Zutrittskontrollsystem mit Chipkarte
- Schlüssel/ kontrollierte Schlüsselvergabe
- Türsicherung
- Empfang
- Beschränkte Videoüberwachung
- Kein unbefugter Zugang zu Datenverarbeitungseinrichtungen

Zugangskontrolle

Technische (Kennwort-/Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung

- Kennwortverfahren oder Key-Authentifizierung
- Automatische Sperrung der Hardware bei Nichtnutzung
- Einrichtung eines Benutzerstammsatzes pro User
- Teilweise Verschlüsselung von Datenträgern
- Erstellen von Benutzerprofilen
- Keine unbefugte Nutzung der Systeme zur Datenverarbeitung und -speicherung

Zugriffskontrolle

Maßnahmen, um 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, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte)
- Protokollierung von Zugriffen
- Auswertungen
- Kenntnisnahme
- Veränderung
- Löschung

Trennungskontrolle

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

- „Interne Mandantenfähigkeit“/ Zweckbindung
- Teilweise Sandboxing
- Funktionstrennung/Produktion/Test
- Physikalisch getrennte Speicherung
- Getrennte Verarbeitung und Speicherung von Daten je nach Zweck

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle

Maßnahmen, um 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.

- Verschlüsselung/Tunnelverbindung (VPN = Virtual Private Network)
- SSL-Zertifikate (Client-Server Zugriff), HTTPS
- Protokollierung
- Zusätzliche Passwortschutz bei sensiblen Dokumenten
- Interne Vorschriften und Verhaltensmaßnahmen

Eingabekontrolle

Maßnahmen, um zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Protokollierungs- und Protokollauswertungssysteme
- Dokumentenmanagement

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle

Maßnahmen, um zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Backup-Verfahren
- Teilweises Spiegeln von Festplatten, z. B. RAID-Verfahren
- Unterbrechungsfreie Stromversorgung (USV)
- Getrennte Aufbewahrung
- Virenschutz/Firewall
- Notfallplan
- Feuerlöschgeräte in Serverräumen
- Klimaanlage in Serverräumen
- Meldewege
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Datenschutz-Management

Aktives Datenschutzmanagement durch externe Experten

Definiertes Reaktionsmanagement

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen durch Doppel Opt-In Verfahren, temporär gültige Tokens

Auftragskontrolle

Maßnahmen, um zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Eindeutige Vertragsgestaltung
- Formalisierte Auftragserteilung (Auftragsformular)
- Kriterien zur Auswahl des Auftragnehmers
- Kontrolle der Vertragsausführung
- Auditierung durch Externe

ANLAGE 2

[Datenblatt Subunternehmer](#) (gemäß 7.2. des Vertrages)