Erweiterte Datenschutzerklärung

gem. Art. 28 DSGVO

zwischen

Firma: _____
Straße: _____
PLZ / Ort: _____

- Auftraggeber -

und

SOLVIS GmbH

Grotrian-Steinweg-Straße 12
38112 Braunschweig

- Auftragnehmer –

1. Allgemeines

(1) Der Auftraggeber installiert Heizungsanlagen, die er zu diesem Zweck beim Auftragnehmer erworben hat. Im Zusammenhang mit dem Liefervorgang ist nicht ausgeschlossen, dass der Auftragnehmer Kenntnis von personenbezogenen Daten erhalten kann.

(2) Diese Vereinbarung hat nur den Umgang des Auftragnehmers mit personenbezogenen Daten zum Gegenstand und gilt vorrangig vor anderen Regelungen, die die Parteien ggf. miteinander vereinbart haben.

2. Pflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, bei der Erbringung seiner Leistungen für den Auftraggeber die geltenden datenschutzrechtlichen Vorschriften, insbesondere die der Datenschutz-Grundverordnung (DSGVO) einzuhalten.

(2) Sofern den Auftragnehmer eine gesetzliche Pflicht trifft, ist dieser zur Bestellung eines Datenschutzbeauftragten verpflichtet. Dieser hat über das gesetzlich erforderliche Fachwissen und Qualifikation zu verfügen.

(3) Der Auftragnehmer verpflichtet sich, die personenbezogenen Daten, von denen er im Zusammenhang mit dem Liefervorgang für den Auftraggeber Kenntnis erlangt, vertraulich zu behandeln und nicht an Dritte weiterzugeben. Eine weitergehende Verwendung der Da-

ten, insbesondere eine solche zu eigenen Zwecken des Auftragnehmers oder zu Zwecken Dritter, ist unzulässig.

3. Technische und organisatorische Maßnahmen zur Datensicherheit

Der Auftragnehmer ist verpflichtet, alle erforderlichen technischen und organisatorischen Maßnahmen i.S.d. Art. 32 DSGVO zu treffen und diese auf Anfrage gegenüber dem Auftraggeber nachzuweisen.

4. Vertraulichkeit

Der Auftragnehmer verpflichtet sich zum vertraulichen Umgang mit Informationen und personenbezogenen Daten, die im Zusammenhang mit der Tätigkeit für den Auftraggeber zur Kenntnis gelangen.

5. Unterauftragnehmer

(1) Die Einschaltung von Unterauftragnehmern durch den Auftragnehmer für Leistungen, die für den Auftraggeber ausgeführt werden, bedarf der vorherigen Zustimmung des Auftraggebers in Textform (z.B. E-Mail/Fax).

(2) Der Auftragnehmer verpflichtet sich, den Unterauftragnehmer unter besonderer Berücksichtigung der von diesem getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO sorgfältig auszuwählen. Der Auftragnehmer ist verpflichtet, die Pflichten aus dieser Vereinbarung in gleicher Weise gegenüber Unterauftragnehmer verpflichtend zu regeln. Dies gilt insbesondere hinsichtlich der Einhaltung der Vertraulichkeit im Umgang mit personenbezogenen Daten.

(3) Soweit diese Vereinbarung Kontrollrechte des Auftraggebers gegenüber dem Auftragnehmer vorsieht, hat der Auftragnehmer im Falle der Beauftragung eines Unterauftragnehmers dafür Sorge zu tragen, dass die Kontrollrechte des Auftraggebers auch direkt gegenüber dem Unterauftragnehmer wirken und insoweit vertragliche Regelungen zwischen Auftragnehmer und Unterauftragnehmer bestehen. Der Auftragnehmer wird das Vorliegen entsprechender Kontrollrechte auf Anfrage des Auftraggebers beim Unterauftragnehmer durch Vorlage einer vertraglichen Vereinbarung beim Auftraggeber auf Anfrage des Auftraggebers nachweisen. Erfolgt der Nachweis nicht, kann der Auftraggeber die Zustimmung des Auftraggebers zur Beauftragung des Unterauftragnehmers verweigern oder zurückziehen. Die Parteien sind sich darüber einig, dass dem Auftragnehmer im Falle einer Verweigerung oder einer Zurückziehung der Genehmigung der Beauftragung eines Unterauftragnehmers keine Schadensersatzansprüche gegenüber dem Auftraggeber zustehen.

6. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, den Auftragnehmer hinsichtlich der von diesen getroffenen Maßnahmen zur Einhaltung der Pflichten aus der DSGVO sowie aus diesem Ver-

trag jederzeit zu überprüfen. Dies kann durch das Einholen von Auskünften oder durch Vor-Ort-Kontrollen erfolgen.

(2) Sofern der Auftragnehmer Daten im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber außerhalb der Geschäftsräume des Auftraggebers verarbeitet, müssen Vor-Ort-Kontrollen vom Auftraggeber grundsätzlich mit angemessener Frist im Voraus angekündigt werden. In dringenden Fällen kann eine Vor-Ort-Kontrolle auch ohne Frist durchgeführt werden. Der Auftragnehmer hat die Kontrollen im erforderlichen Umfang zu dulden.

7. Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

8. Informationspflichten

Der Auftragnehmer wird den Auftraggeber bei Datenschutzverletzungen oder anderen Unregelmäßigkeiten im Umgang mit personenbezogenen Daten unverzüglich informieren. Die Information soll in Textform (z.B. E-Mail) erfolgen.

9. Rückgabe von Daten / Löschung von Daten

(1) Der Auftragnehmer hat nach Abschluss der vertragsgegenständlichen Leistungen die ihm vom Auftraggeber überlassenen Daten oder die Daten, die er im Zusammenhang mit der Tätigkeit für den Auftraggeber verarbeitet oder genutzt hat, in einem mit dem Auftraggeber abzustimmenden Format auszuhändigen und nach der vorherigen schriftlichen Freigabe durch den Auftraggeber datenschutzkonform zu löschen, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Auf Verlangen hat der Auftragnehmer dem Auftraggeber das Löschungsprotokoll vorzulegen. Dem Auftraggeber steht es frei, statt der Aushändigung der Daten nur eine Löschung der Daten vom Auftragnehmer zu verlangen.

10. Schlussbestimmungen

(1) Es gilt das Recht der Bundesrepublik Deutschland, wobei die Geltung des UN-Kaufrechts ausgeschlossen wird.

(2) Ausschließlicher Gerichtsstand für alle Streitigkeiten aus dem Vertragsverhältnis ist der Sitz des Auftragnehmers.

(3) Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein oder werden, so berührt dies die Wirksamkeit der übrigen Bestimmungen nicht.

_____, den _____	Braunschweig, den
Ort Datum	Ort Datum
	
	Markus Kube Geschäftsführer Solvis GmbH
_____	_____
- Auftraggeber -	- Auftragnehmer –

Technische und organisatorische Maßnahmen

i.S.d. Art. 32 DSGVO

der

Solvis GmbH
Grotrian-Steinweg Straße 12
38112 Braunschweig

1. Zutrittskontrolle

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

- Zutrittskontrollsystem mit persönlichem Mitarbeiterschlüssel.
- Schlüsselausgabe wird dokumentiert, eine entsprechende Richtlinie ist vorhanden
- Separater Serverraum, ständig verschlossen. Zugang hat nur der Leiter IT und dessen Vertreter.
- Besucher werden nur begleitet geführt.

2. Zugangskontrolle

Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Die Arbeitsplätze sind mit persönlichen, zeitlich begrenzten Kennwörtern gesichert. Jeder Mitarbeiter wird bei Einstellung informiert, dass bei Verlassen des Arbeitsplatzes die Arbeitsstation zu sperren ist. Zusätzlich sperrt eine Richtlinie den Arbeitsplatz automatisch nach 5 Minuten.
- Benutzer werden entsprechend ihrem Aufgabenbereich in Gruppen mit Berechtigungen aufgenommen.
- Es existiert eine Richtlinie für die Vergabe von starken Kennwörtern
- Mobile Geräte sind verschlüsselt
- Die Systeme werden zusätzlich mittels Anti-Viren Software geschützt.
- WLan ist mit WPA2 gesichert.

3. Zugriffskontrolle

Maßnahmen, die geeignet sind, 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.

- Es existiert für alle eingesetzten Systeme ein dediziertes Rechtesystem. Eine Zuteilung von Berechtigungen erfolgt erst nach Prüfung und Freigabe durch den Vorgesetzten. Die Berechtigungen werden regelmäßig überprüft.
- Accounts ausscheidender Mitarbeiter werden unmittelbar gesperrt.
- Datenträger und Papierunterlagen werden durch professionellen Aktenvernichter zerstört.

4. Weitergabekontrolle

Maßnahmen, die geeignet sind, 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.

- Mitarbeiterdaten sind getrennt von Kunden- und Projektdaten
- kein unbefugtes Lesen, Kopieren, verändern oder Entfernen bei elektronischer Übertragung oder Transport

5. Eingabekontrolle

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

- Versionsverwaltung von Dokumenten.
- Protokollierung der Zugriffe auf IT-Systeme.
- Überwachung der Änderungen innerhalb der IT-Systeme.

6. Auftragskontrolle

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

- Auswahl der AN erfolgt unter Berücksichtigung von Zertifizierungen bzw. Gütesiegeln
- Angaben der AN werden persönlich geprüft und dokumentiert

7. Verfügbarkeitskontrolle

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

- Daten werden regelmäßig gesichert (Vollsicherung am Wochenende, unter der Woche täglich inkrementell. Monatssicherungen (extern) werden beim Systembereitsteller gelagert.
- Interne Sicherung auf NAS und HDD in feuerfestem Safe
- Die Systeme werden an getrennten USVs betrieben und sind gegen Spannungsschwankungen abgesichert
- In den Serverräumen befinden sich unabhängige Klimaanlagen und Rauchmelder

- Alle Systeme befinden sich hinter einer Hardware-Firewall und sind ggf. durch weitere Software-Firewall zusätzlich geschützt
- Es kommt eine Antivirus-Lösung eines namhaften Herstellers zum Einsatz. Die Software wird ständig aktualisiert
- Ein Notfall- bzw. Wiederanlaufplan ist vorhanden.

8. Trennungsgebot

Maßnahmen, die geeignet sind, zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Personenbezogene Daten werden gesondert von Daten anderer Natur gesichert. Die Trennung ist durch ein Berechtigungskonzept mit Gruppen und Benutzern gewährleistet.
- Der IT stehen, sofern notwendig, Testsysteme zur Verfügung bzw. werden kurzfristig eingerichtet. Der Einsatz von Testsystemen bei Kundenprojekten erfolgt in Kundenabsprache.