Anlage zum Vertrag über Software-as-a-Service-Leistungen (SaaS) betreffend das Optiziser-Webtool:

Auftrag zur Verarbeitung personenbezogener Daten

– nachstehend bezeichnet als **AV-Vertrag** –

zwischen **dem Partner**

– nachstehend bezeichnet als **Auftraggeber** –

und der

Name/Fa.:	optisizer ag
Straße Nr.:	Hauptstrasse 33
PLZ, Ort, Land:	9053 Teufen, Schweiz
Geschäftsführer:	Stefan Merz

– nachstehend bezeichnet als **Auftragnehmerin** –

– Auftragnehmer und Auftraggeber werden nachstehend auch als **Vertragsparteien** bezeichnet. –

1. Gegenstand des Auftrags, Zwecksetzung, Datenkategorien, Betroffene, Art und Umfang der Verarbeitung

1.1. Gegenstand und Zweck der Auftragsverarbeitung

Der Gegenstand des AV-Vertrages, die im Rahmen des Auftrags verarbeiteten personenbezogenen Daten nachfolgend kurz „**Daten**“), die von der Verarbeitung betroffene Personen (nachfolgend kurz „**Betroffene**“) sowie Art, Umfang und Zwecke der Verarbeitung, werden durch den „Vertrag über Software-as-a-Service-Leistungen (SaaS) betreffend das Optiziser-Webtool“ zwischen den Vertragsparteien bestimmt (nachstehend bezeichnet als **Hauptvertrag**).

Die Auftragnehmerin bietet das Online-Webtool „Optisizer“ zur Messung, Analyse und Optimierung des Einsatzes von Photovoltaikanlagen sowie Vermittlungsleistungen zwischen den Nutzern des Webtools und Anbietern von Solarstromlösungen an. Der Auftraggeber kooperiert mit der Auftragnehmerin und bietet die Leistungen des Optisizer-Webtools gegenüber eigenen Kunden und Interessenten an, was mit der Übermittlung von personenbezogenen Messwerten an die Auftragnehmerin einher gehen kann (z.B. bei Übermittlung von Messwerten von Privatpersonen/ Freiberuflern, etc.). Die personenbezogenen Messwerte werden entsprechend der folgenden Regelungen durch die Auftragnehmerin verarbeitet.

Die Regelungen dieses AV-Vertrages gelten gegenüber dem Hauptvertrag vorrangig.

1.2. Art der Daten:

☒ Bestandsdaten (z.B., Namen, Adressen).

☒ Kontaktdaten (z.B., E-Mail, Telefonnummern).

☒ Inhaltsdaten (z.B., Textliche Mitteilungen, Messdaten).

☒ Meta-/Kommunikationsdaten (z.B., Geräte-IDs, IP-Adressen, Standortdaten).

1.3. Kategorien der Betroffenen:

☒ Kunden / Interessenten / Geschäftspartner des Auftraggebers.

2. Verantwortlichkeit und Weisungsrecht

2.1. Der Auftraggeber ist als **Verantwortlicher** für die Einhaltung der datenschutzrechtlichen Vorgaben, insbesondere für die Auswahl der Auftragnehmerin, die an diese übermittelten Daten sowie erteilte Weisungen verantwortlich.

2.2. Die Auftragnehmerin darf Daten nur im Rahmen des Hauptvertrages sowie der Weisungen des Auftraggebers verarbeiten (was insbesondere auch für deren Berichtigung, Löschung oder Einschränkung der Verarbeitung gilt) und nur insoweit die Verarbeitung hierzu erforderlich ist, außer wenn die Auftragnehmerin zu der Verarbeitung durch das geltende Recht verpflichtet ist; in einem solchen Fall teilt die Auftragnehmerin dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

2.3. Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen im Hinblick auf die Verarbeitung der Daten und die Sicherheitsmaßnahmen zu erteilen.

2.4. Ist die Auftragnehmerin der Ansicht, dass eine Weisung des Auftraggebers gegen geltendes Datenschutzrecht verstößt, wird sie den Auftraggeber unverzüglich darauf hinweisen. In diesem Fall ist die Auftragnehmerin berechtigt, die Ausführung der Weisung bis zur Bestätigung der Weisung durch den Auftraggeber auszusetzen und im Fall offensichtlich rechtswidriger Weisungen abzulehnen.

2.5. Gehen ergänzende Weisungen des Auftraggebers über die Leistungspflicht der Auftragnehmerin nach dem Hauptvertrag hinaus und beruhen sie nicht auf einem Fehlverhalten der Auftragnehmerin, dann hat der Auftraggeber der Auftragnehmerin den dadurch entstehenden Mehraufwand gesondert zu vergüten.

2.6. Die Vertragsparteien können zum Erteilen und Empfangen von Weisungen berechtigte Personen benennen (insbesondere, wenn diese sich nicht bereits aus dem Hauptvertrag ergeben) und sind verpflichtet deren Änderung unverzüglich mitzuteilen.

3. Sicherheitskonzept und diesbezügliche Pflichten

3.1. Die Auftragnehmerin wird die innerbetriebliche Organisation in ihrem Verantwortungsbereich entsprechend den gesetzlichen Anforderungen gestalten und wird insbesondere technische und organisatorische Maßnahmen (nachfolgend bezeichnet als „**TOMs**“) zur angemessenen Sicherung, insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit von Daten dem Auftraggeber, unter Beachtung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen treffen sowie deren Aufrechterhaltung sicherstellen. Zu den TOMs gehören insbesondere die Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle, Trennungskontrolle und die Sicherung der Betroffenenrechte. Die TOMs der Auftragnehmerin werden im Einzelnen in dem Anhang „Technische und organisatorische Maßnahmen“ zu diesem AV-Vertrag aufgeführt.

3.2. Die TOMs dürfen entsprechend dem technischen Fortschritt weiterentwickelt und durch adäquate Schutzmaßnahmen ersetzt werden, sofern sie das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschreiten und wesentliche Änderungen dem Auftraggeber mitgeteilt werden.

3.3. Die Auftragnehmerin stellt sicher, dass die zur Verarbeitung der Daten des Auftraggebers befugten Personen auf Vertraulichkeit und Verschwiegenheit verpflichtet und in die gesetzlichen Schutzbestimmungen eingewiesen worden sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

3.4. Die im Rahmen des AV-Vertrages überlassene Daten sowie Datenträger und sämtliche hiervon gefertigten Kopien verbleiben im Eigentum des Auftraggebers, sind durch die Auftragnehmerin sorgfältig zu verwahren, vor Zugang durch unberechtigte Dritte zu schützen und dürfen nur mit Zustimmung des Auftraggebers, und dann nur datenschutzgerecht, vernichtet werden. Kopien von Daten dürfen nur erstellt werden, wenn sie zur Erfüllung der Leistungshaupt- und Nebenpflichten der Auftragnehmerin gegenüber dem Auftraggeber erforderlich sind (z.B. Backups).

4. Informationspflichten und Mitwirkungspflichten

4.1. Betroffenenrechte sind gegenüber dem Auftraggeber wahrzunehmen, wobei die Auftragnehmerin den Auftraggeber hierbei unterstützt und ihn insbesondere über die bei ihr eingehenden Anfragen Betroffener informiert.

4.2. Der Auftraggeber hat die Auftragnehmerin unverzüglich und vollständig zu informieren, wenn der Auftraggeber im Hinblick auf die Verarbeitung der Daten Fehler oder Unregelmäßigkeiten im Hinblick auf die Einhaltung der Bestimmungen dieses AV-Vertrages oder einschlägiger Datenschutzvorschriften feststellt.

4.3. Für den Fall, dass die Auftragnehmerin Tatsachen feststellt, welche die Annahme begründen, dass der Schutz der für der Auftraggeber verarbeiteten Daten verletzt worden ist, hat die Auftragnehmerin den Auftraggeber unverzüglich und vollständig zu informieren, unverzüglich erforderliche Schutzmaßnahmen zu ergreifen, und bei der Erfüllung der dem Auftraggeber obliegenden Melde- oder Anzeigepflichten zu unterstützen.

4.4. Sollte die Sicherheit der Daten des Auftraggebers durch Maßnahmen Dritter (z.B. Gläubiger, Behörden, Gerichte, etc.) gefährdet sein (Pfändung, Beschlagnahme, Insolvenzverfahren, etc.) wird die Auftragnehmerin die Dritten unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich bei dem Auftraggeber liegen und nach Rücksprache mit dem Auftraggeber, sofern erforderlich, entsprechende Schutzmaßnahmen ergreifen (z.B. Widersprüche, Anträge, etc. stellen).

4.5. Die Auftragnehmerin wird der Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde gegenüber der Auftragnehmerin tätig wird und deren Tätigkeit die für der Auftraggeber verarbeiteten Daten betreffen kann. Die Auftragnehmerin unterstützt der Auftraggeber bei der Wahrnehmung ihrer Pflichten (insbesondere zur Auskunfts- und Duldung von Kontrollen) gegenüber Aufsichtsbehörden.

4.6. Die Auftragnehmerin stellt dem Auftraggeber Informationen betreffend die Verarbeitung von Daten im Rahmen dieses AV-Vertrages, die für dessen Erfüllung von gesetzlichen Pflichten (zu denen insbesondere Anfragen Betroffener oder Behörden und die Einhaltung ihrer Rechenschaftspflichten, als auch die Durchführung einer Datenschutz-Folgenabschätzung gehören können) notwendig sind, zur Verfügung, sofern der Auftraggeber diese Informationen nicht selbst beschaffen kann. Die Informationen müssen der Auftragnehmerin zur Verfügung stehen und müssen nicht von Dritten beschafft werden, wobei Mitarbeiter, Beauftragte und Subunternehmer der Auftragnehmerin nicht als Dritte gelten.

5. Kontrollbefugnisse

5.1. Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorgaben und der Regelungen dieses AV-Vertrages, insbesondere der TOMs, bei der Auftragnehmerin jederzeit im erforderlichen Umfang zu kontrollieren.

5.2. Vor-Ort-Kontrollen erfolgen innerhalb üblicher Geschäftszeiten, sind von dem Auftraggeber mit einer angemessenen Frist (mindestens 14 Tage, außer in Notfällen) anzumelden und durch die Auftragnehmerin zu unterstützen (z.B. durch Bereitstellung von Personal).

5.3. Die Kontrollen sind auf den erforderlichen Rahmen beschränkt und müssen auf Betriebs- und Geschäftsgeheimnisse der Auftragnehmerin sowie den Schutz von personenbezogenen Daten Dritter (z.B. anderer Kunden oder Mitarbeiter der Auftragnehmerin) Rücksicht nehmen. Zur Durchführung der Kontrolle sind nur fachkundige Personen zugelassen, die sich legitimieren können und im Hinblick auf die Betriebs- und Geschäftsgeheimnisse sowie Prozesse der Auftragnehmerin und personenbezogene Daten Dritter zur Verschwiegenheit verpflichtet sind.

5.4. Statt der Einsichtnahmen und der Vor-Ort-Kontrollen, darf die Auftragnehmerin den Auftraggeber auf eine gleichwertige Kontrolle durch unabhängige Dritte (z.B. neutrale Datenschutzauditoren), Einhaltung genehmigter Verhaltensregeln oder geeignete Datenschutz- oder IT-Sicherheitszertifizierungen verweisen. Dies gilt insbesondere dann, wenn Betriebs- und Geschäftsgeheimnisse der Auftragnehmerin oder personenbezogene Daten Dritter durch die Kontrollen gefährdet wären.

6. Unterauftragsverhältnisse

6.1. Nimmt Die Auftragnehmerin die Dienste eines Unterauftragsverarbeiters (d.h. Unterauftragnehmer oder Subunternehmer) in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen dem Auftraggeber auszuführen, dann muss sie dem Unterauftragsverarbeiter im Wege eines Vertrags oder eines zulässigen anderen Rechtsinstruments dieselben Datenschutzpflichten zu denen sich die Auftragnehmerin in diesem AV-Vertrag verpflichtet hat, auferlegen (insbesondere im Hinblick auf die Befolgung von Weisungen, Einhaltung der TOMs, Erteilung von Informationen und Duldung von Kontrollen). Ferner hat die Auftragnehmerin den Unterauftragsverarbeiter sorgfältig auszuwählen, auf dessen Zuverlässigkeit zu prüfen und diese, als auch dessen Einhaltung der vertraglichen und gesetzlichen Vorgaben zu überwachen.

6.2. Der Auftraggeber erklärt sich unbeschadet etwaiger Einschränkungen durch den Hauptvertrag ausdrücklich damit einverstanden, dass die Auftragnehmerin im Rahmen der Auftragsverarbeitung Unterauftragsverarbeiter einsetzen darf.

6.3. Die Auftragnehmerin informiert den Auftraggeber im Hinblick auf Änderungen bei den Unterauftragsverarbeitern, die für die Auftragsverarbeitung maßgeblich sind. Die Information erfolgt mit einem angemessenen zeitlichen Vorlauf, der grundsätzlich 10 Werktage nicht unterschreiten darf. Der Auftraggeber macht von seinem Recht auf Einspruch im Hinblick auf die Änderungen oder neue Unterauftragsverarbeiter nur unter Beachtung der Grundsätze von Treu und Glauben sowie der Angemessenheit und Billigkeit Gebrauch.

6.4. Die bereits zum Abschluss dieses AV-Vertrages bestehenden Unterauftragsverhältnisse, werden von der Auftragnehmerin nachfolgend angegeben und gelten als von der Auftraggeberin genehmigt:

- merz familie ag, Herisauer Strasse 70, 9015 St. Gallen / Bereitstellung von IT-Infrastruktur, Personal, und Büro- sowie Verwaltungsleistungen auf Grundlage eines Auftragsverarbeitungsvertrages.

6.5. Vertragsverhältnisse, bei denen die Auftragnehmerin die Leistungen Dritter als reine Nebenleistung in Anspruch nimmt, um ihre geschäftliche Tätigkeit auszuüben (z.B. Reinigungs-, Bewachungs- oder Transportleistungen) stellen keine Unterauftragsverarbeitung im Sinne der vorstehenden Regelungen dieses AV-Vertrages dar. Gleichwohl hat die Auftragnehmerin sicher zu stellen, z.B. durch vertragliche Vereinbarungen oder Hinweise und Instruktionen, dass hierbei die Sicherheit der Daten nicht gefährdet wird und die Vorgaben dieses AV-Vertrages und der Datenschutzvorschriften eingehalten werden.

7. Verarbeitung in Drittländern

7.1. Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in der Schweiz, einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt.

7.2. Die Auftragsverarbeitung in einem Drittland (d.h. einem anderen als in Ziffer 7.1 genannten Land), auch durch Unterauftragsverarbeiter, bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die gesetzlichen Voraussetzungen gewahrt sind, insbesondere das Datenschutzniveau hinreichende gesichert ist, außer wenn die Auftragnehmerin zu der Verarbeitung im Drittland gesetzlich verpflichtet ist; in einem solchen Fall teilt die Auftragnehmerin dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

8. Dauer des Auftrags, Vertragsbeendigung und Datenlöschung

8.1. Dieser AV-Vertrag wird mit dessen Abschluss gültig, wird auf unbestimmte Zeit geschlossen und endet spätestens mit der Laufzeit des Hauptvertrags.

8.2. Das Recht auf außerordentliche Kündigung bleibt den Vertragsparteien vorbehalten, insbesondere im Fall eines schwerwiegenden Verstoßes gegen die Vorgaben dieses AV-Vertrages und geltendes Datenschutzrecht. Der außerordentlichen Kündigung hat grundsätzlich eine Abmahnung der Verstöße mit angemessener Frist vorauszugehen, wobei sie nicht erforderlich ist, wenn nicht damit zu rechnen ist, dass die beanstandeten Verstöße behoben werden oder diese derart schwer wiegen, dass ein Festhalten am AV-Vertrag der kündigenden Vertragspartei nicht zuzumuten ist.

8.3. Nach Abschluss der Erbringung der Verarbeitungsleistungen im Rahmen dieses AV-Vertrages, wird die Auftragnehmerin alle personenbezogenen Daten und deren Kopien (sowie sämtliche im Zusammenhang mit dem Auftragsverhältnis in ihren Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände), nach Wahl dem Auftraggeber entweder innerhalb eines Monats löschen oder zurückgeben, sofern nicht eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Die Einrede eines Zurückbehaltungsrechts, wird hinsichtlich der

verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen. Im Hinblick auf die Löschung oder Rückgabe, gelten die Auskunfts-, Nachweis und Kontrollrechte dem Auftraggeber entsprechend diesem AV-Vertrag.

8.4. Im Übrigen bleiben die Verpflichtungen aus diesem AV-Vertrag im Hinblick auf die im Auftrag verarbeiteten Daten auch nach Beendigung des AV-Vertrages bestehen.

9. Haftung

9.1. Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, haften im Innenverhältnis Auftragnehmerin und Auftraggeber entsprechend ihres jeweiligen Verursachungs- und Verschuldensanteils. Die Vertragsparteien stellen sich jeweils von der Haftung frei, wenn eine der Vertragsparteien nachweist, dass sie für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, nicht verantwortlich ist.

9.2. Im Übrigen bestimmt sich die Haftung nach dem Gesetz.

10. Schlussbestimmungen, Rangfolge, Änderungen, Kommunikationsform, Rechtswahl, Gerichtsstand

10.1. Änderungen, Nebenabreden und Ergänzungen dieses AV-Vertrages und seiner Anhänge bedürfen einer schriftlichen (oder soweit durch die Auftragnehmerin z.B. im Rahmen der Optisizer-Tool-Verwaltung bereitgestellt, einer elektronischen) Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieses AV-Vertrages handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

10.2. Vorbehaltlich einer Verpflichtung zur Schriftform, bzw. elektronischen Form in diesem AV-Vertrag und im Hauptvertrag, erfolgt die Kommunikation zwischen der Auftragnehmerin und dem Auftraggeber im Rahmen dieses AV-Vertrages (insbesondere im Hinblick auf Weisungen und Informationserteilung) zumindest in Textform (z.B. E-Mail). Eine geringere Form (z.B. mündlich) kann den Umständen nach statt der Textform zulässig sein (z.B. in Notfallsituation), muss jedoch unverzüglich zumindest in Textform bestätigt werden.

10.3. Es gilt das Recht der Schweiz und der daneben einschlägigen Gesetze (insbesondere der DSGVO). Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem AV-Vertrag ist der Sitz der Auftragnehmerin.

Anhang zum AV-Vertrag: „Technische und organisatorische Maßnahmen“

1. **Datenschutzkonzept, Betroffenenrechte, Technikgestaltung und Datenschutz auf Mitarbeiterebene**

Allgemeine Angaben zu einem Sicherheitskonzept:

- - Es besteht ein betriebsinternes Datenschutz-Management, dessen Einhaltung ständig überwacht wird sowie anlassbezogenen und mindestens halbjährlichen evaluiert wird.
- - Es besteht ein Konzept, welches die Wahrung der Rechte der Betroffenen (Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung, Datentransfer, Widerrufe & Widersprüche) innerhalb der gesetzlichen Fristen gewährleistet.
- - Es besteht ein Konzept, das eine unverzügliche und den gesetzlichen Anforderungen entsprechende Reaktion auf Verletzungen des Schutzes personenbezogener Daten (Prüfung, Dokumentation, Meldung) gewährleistet.
- Der Schutz von personenbezogenen Daten wird unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen bereits bei der Entwicklung, bzw. Auswahl von Hardware, Software sowie Verfahren, entsprechend dem Prinzip des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen berücksichtigt.
- Die eingesetzte Software wird stets auf dem aktuell verfügbaren Stand gehalten, ebenso wie Virenscanner und Firewalls.
- Mitarbeiter werden im Hinblick auf den Datenschutz auf Verschwiegenheit verpflichtet, belehrt und instruiert, als auch auf mögliche Haftungsfolgen hingewiesen. Sofern Mitarbeiter außerhalb betriebsinterner Räumlichkeiten tätig werden oder Privatgeräte für betriebliche Tätigkeiten einsetzen, existieren spezielle Regelungen zum Schutz der Daten in diesen Konstellationen.
- Die an Mitarbeiter ausgegebene Schlüssel, Zugangskarten oder Codes sowie im Hinblick auf die Verarbeitung personenbezogener Daten erteilte Berechtigungen, werden nach deren Ausscheiden aus dem Unternehmen, bzw. Wechsel der Zuständigkeiten eingezogen, bzw. entzogen.
- Das Reinigungspersonal, Wachpersonal und übrige Dienstleister, die zur Erfüllung nebengeschäftlicher Aufgaben herangezogen werden, werden sorgfältig ausgesucht und es wird sichergestellt, dass es den Schutz personenbezogener Daten beachtet.
- Es wurde ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung implementiert.

11. **2. Zutrittskontrolle**

Maßnahmen, mit denen Unbefugten der Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird:

- Es wird ein „papierloses Büro“ geführt und Unterlagen werden grundsätzlich nur digital gespeichert und nur in Ausnahmefällen in Papierform aufbewahrt.
- Es werden, bis auf die Arbeitsplatzrechner und mobile Geräte, keine Datenverarbeitungsanlagen in den eigenen Geschäftsräumlichkeiten unterhalten. Die Daten werden bei externen Hosting-Anbieter gespeichert.
- Es bestehen Zutrittsregelungen für betriebsfremde Personen.

- Besucher müssen sich am Empfang melden, werden verzeichnet und von einem Mitarbeiter abgeholt.
- Die Besucher werden protokoliert.
- Der Zutritt zu den Datenverarbeitungsanlagen (EDV-Räumlichkeiten am Serverstandort) ist unbefugten Personen vollständig verwehrt und nur zutrittsberechtigten Mitarbeitern gewährt.
- Es ist eine Alarmanlage am Serverstandort installiert.
- Die Fenster sind gesichert (Falls Erdgeschoss oder sonst eine Einbruchgefahr besteht).
- Der Zugang ist durch ein Schließsystem mit Codesperre gesichert.
- Der Zugang ist durch ein manuelles Schließsystem gesichert.
- Es besteht eine Regelung für Schlüssel oder Zugangskarten (Protokollierung der Ausgabe).
- Die Zugänge am Serverstandort werden videoüberwacht.

12. **3. Zugangskontrolle**

Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert wird:

- Es gibt ein Rechtekonzept, bzw. ein Rollenkonzept, mit dem die Zutrittsberechtigungen der Mitarbeiter, Beauftragter und sonstiger Personen (z.B. Nutzer innerhalb des Systems) festgelegt werden und nur soweit reichen, wie sie für die vorgegebene Nutzung erforderlich sind.
- Sämtliche Datenverarbeitungsanlagen sind passwortgeschützt.
- Es gibt ein Passwortkonzept, dass festlegt, dass Passwörter eine dem Stand der Technik und den Anforderungen an Sicherheit entsprechende Mindestlänge und Komplexität haben müssen.
- Es wird eine Passwort-Management-Software verwendet.
- Anmeldungen in den Verarbeitungssystemen werden protokolliert.
- Es wird eine Anti-Viren-Software eingesetzt.
- Es werden Hardware-Firewalls eingesetzt.
- Es werden Software-Firewalls eingesetzt.
- Die Website und/oder Zugänge zu Online-Software-Angeboten sind durch eine aktuelle TLS/SSL-Verschlüsselung geschützt.
- Die internen Systeme werden per Firewall sowie Benutzername und Passwort und/oder Client-Zertifikate vor unberechtigten Zugriffen geschützt.
- Es gibt eine Begrenzung der Fehlversuche beim Login auf betriebsinterne Systeme (z.B. Sperrung von Logins oder IP-Adressen).
- Beim Zugriff auf betriebsinterne Systeme von außen (z.B. bei Fernwartung), werden verschlüsselte Übertragungstechnologien verwendet (z.B. VPN).
- Externe Schnittstellen sind gegen unberechtigte Hardwarezugriffe gesperrt (z.B. Sperrung von USB-Schnittstellen).
- Es werden Serversysteme und Dienste eingesetzt, die über Intrusion-Detection-Systeme verfügen.
- Mobile Datenträger werden verschlüsselt.

13. **4. Zugriffskontrolle, Eingabekontrolle und Integritätsschutz**

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung unterliegenden Daten zugreifen können, und dass

personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt, eingegeben, gelesen, kopiert, verändert oder entfernt werden können sowie Maßnahmen, die es erlauben die Verarbeitungsvorgänge nachträglich nachzuvollziehen:

- Es gibt ein Rechtekonzept, bzw. ein Rollenkonzept, mit dem die Zugriffsberechtigungen der Mitarbeiter, Beauftragter und sonstiger Personen (z.B. Nutzer innerhalb des Systems) festgelegt werden und nur soweit reichen, wie sie für die vorgegebene Nutzung erforderlich sind.
- Protokollierung jedes einzelnen Schrittes der Datenverarbeitung, insbesondere von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten.
- Die Zugriffe der Mitarbeiter auf Daten werden protokolliert. Sofern einzelne Zugriffe nicht protokolliert werden, wird sichergestellt, dass die nachvollziehbar ist, wer auf welche Daten wann Zugriff hatte (z.B. durch Protokollierung der Softwarenutzung oder Rückschluss aus den Zugriffszeiten und dem Berechtigungskonzept).
- Protokollierung jedes einzelnen Schrittes, insbesondere von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten.
- Datenträger werden sicher aufbewahrt.
- Es liegt ein Lösch- und Entsorgungskonzept entsprechend der DIN 66399 mit festgelegten Zuständigkeiten und Protokollierungspflichten vor. Mitarbeiter wurden über gesetzliche Voraussetzungen, Löschfristen und Vorgaben für die Datenvernichtung oder Gerätevernichtung durch Dienstleister unterrichtet.
- Die Verarbeitung von Daten die nicht gelöscht werden (z.B. in Folge der gesetzlichen Archivierungspflichten), wird durch Sperrvermerke und Aussonderung eingeschränkt.

14. **5. Weitergabekontrolle und Vertraulichkeit**

Maßnahmen, die 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:

- Es wird festgelegt für welchen Zeitraum der Zugriff auf die Daten möglich ist.
- Im Fall des Fernzugriffs auf Daten wird durch Protokollmaßnahmen gesichert, dass Datenübermittlungen oder Offenlegungen nachvollziehbar sind.
- Sofern erforderlich, möglich und zumutbar, werden Daten in anonymisierter Form bzw. in pseudonymisierter Form weitergegeben.

15. **6. Sicherung der Verfügbarkeit und Integrität von Daten sowie Belastbarkeit von Systemen**

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und die Integrität, Verfügbarkeit sowie die Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt ist, ebenso wie die Verfügbarkeit der personenbezogenen Daten, und dass der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden kann:

- Es werden ausfallsichere Serversysteme und Dienste eingesetzt, die doppelt, bzw. mehrfach ausgelegt sind, Belastbarkeitstests und Hardwaretests unterliegen, über einen DDoS-Schutz verfügen sowie eine unterbrechungsfreie Stromversorgung bieten (z.B. RAID, HA-Netzteile).

- Es werden Serversysteme und Dienste eingesetzt, die ein Backupsystem an anderen Orten, bzw. zumindest in anderen Brandabschnitten bieten, auf dem die aktuellen Daten vorgehalten werden und so ein lauffähiges System auch im Katastrophenfall zur Verfügung stellen.
- Es werden Serversysteme und Dienste eingesetzt, die über Feuchtigkeitsmelder verfügen, als auch über Feuer- und Rauchmeldeanlagen sowie entsprechende Feuerlöschvorrichtungen oder Feuerlöschgeräte im EDV- Raum verfügen.
- Es werden Serversysteme und Dienste eingesetzt, die ein zuverlässiges und kontrolliertes Backupkonzept & Recoverykonzept bieten. Backups erfolgen täglich.
- Die Verfügbarkeit der Datenverarbeitungssysteme wird permanent überwacht.

16. **Gewährleistung der Zweckbindung, der Anonymisierung, Pseudonymisierung und des Trennungsgebotes**

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Die Daten werden logisch getrennt (z.B. in unterschiedlichen Datenbanken oder durch Kennzeichnung mit entsprechenden Zweckattributen, oder Datenfeldern).
- Sofern erforderlich und technisch möglich sowie zumutbar, werden Daten pseudonymisiert und anonymisiert, wobei zur vorgenannten Zwecken insbesondere Verschlüsselungsmethoden eingesetzt werden.
- Ein Übergriff durch nichtberechtigte Personen oder Prozesse wird durch ein Berechtigungskonzept verhindert.
- Im Fall pseudonymisierter Speicherung, werden die Zuordnungsschlüssel getrennt von den Daten gespeichert und gegen eine unberechtigte oder nicht vom Verarbeitungsprozess vorgesehene Verknüpfung gesichert.
- Produktiv- und Testsysteme werden getrennt.