Vertragliche Regelungen und Vereinbarungen zur Auftragsverarbeitung (AVs)

gemäß Artikel 28 DSGVO

ENGLISH VERSION BELOW – starting on page 20

Vertrag zur Auftragsverarbeitung

Auftraggeber	**Auftragnehmer**
„Kunde"	Echo PRM GmbH Krokusweg 5 a D-87488 Betzigau

Dieser Vertrag zur Auftragsverarbeitung wird dem Auftraggeber vor Vertragsbeginn zur Prüfung zur Verfügung gestellt.
Der Abschluss/die Genehmigung erfolgt durch den Auftraggeber über eine Bestätigungslösung innerhalb der ECHO PRM Software beim ersten Login.

Vertragliche Regelungen und Vereinbarungen zur Auftragsverarbeitung (AVs)

gemäß Artikel 28 DSGVO

Inhaltsverzeichnis

Hinweis bzgl. geschlechtsneutraler Formulierung

Eine gleichstellungsgerechte Gesellschaft erfordert eine geschlechterneutrale Sprache. Im folgenden Text werden, soweit möglich und sinnvoll, entsprechende Formulierungen genutzt (z. B. Paarformeln, Ableitungen). Personenbezeichnungen, bei denen es sich um Fachbegriffe, Definitionen, Zitate o. ä. handelt, werden im Text nicht durch Paarformeln ersetzt. Entsprechende Begriffe sind im Sinne der Gleichbehandlung geschlechtsneutral zu interpretieren.

Wenn aus Gründen der leichteren Lesbarkeit bei personenbezogenen Substantiven und Pronomen nur ein Geschlecht dargestellt wird, impliziert dies ebenfalls keine Benachteiligung der anderen Geschlechter, sondern soll im Sinne der sprachlichen Vereinfachung als geschlechtsneutral verstanden werden.

Vertragliche Regelungen und Vereinbarungen zur Auftragsverarbeitung (AVs)

gemäß Artikel 28 DSGVO

1. Allgemeines

1.1. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dieser Vertrag enthält nach dem Willen der Parteien und insbesondere des Auftraggebers den schriftlichen Auftrag zur Auftragsverarbeitung i. S. d. Artikel 28 EU-Datenschutzgrundverordnung (DSGVO) und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Datenverarbeitung.

1.2. Sofern in diesem Vertrag der Begriff „Datenverarbeitung" oder „Verarbeitung" (von Daten) benutzt wird, wird die Definition der „Verarbeitung" i. S. d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

2. Gegenstand der Vereinbarung

2.1. Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen:

Gegenstand der Vereinbarung ist das Vertragsverhältnis zwischen den Parteien über die entgeltliche Überlassung zur zeitlich unbegrenzten, nicht ausschließlichen Nutzung der Software „ECHO PRM" (SaaS-Anwendung), sowie die Speicherung der Daten des Auftraggebers im Rahmen der Zur-Verfügung-Stellung von Speicherplatz in der Cloud des Auftragnehmers. Beinhaltet sind ebenfalls die Pflegeleistungen für die Software sowie die Unterstützungsleistungen im Rahmen von Supportdienstleistungen. Im Rahmen der Softwarenutzung erhält der Auftraggeber Zugriff über einen oder mehrere Backend-User.

Folgende Auftragsverarbeitung wird vom Auftragnehmer konkret erbracht, wobei die Möglichkeit der Einsicht und Kenntnisnahme in die personenbezogenen Daten des Auftraggebers besteht:

- Speicherung der Daten des Auftraggebers in der Cloud des Auftragnehmers, um die Daten vorzuhalten.
- Supportdienstleistungen, um Fehleranalysen und Problembehebungen im Rahmen der Nutzung der Software durchzuführen.

2.2. Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

- Stammdaten des Auftraggebers und von Personen, die im Namen des Auftraggebers agieren (Vorname, Nachname, Adressangaben, Kontaktdaten, Benutzercodes und-namen, Berechtigungen).
- Anwenderbezogene Änderungsprotokolle.
- Ggf. personenbezogene Daten von Dritten - je nach Ausgestaltung der Inhalte durch den Auftraggeber.

2.3. Kreis der von der Datenverarbeitung betroffenen Personen:

- Geschäftspartner des Auftraggebers (Kunden, Lieferanten)
- Mitarbeiter des Auftraggebers.

3. Rechte und Pflichten des Auftraggebers

3.1. Der Auftraggeber ist Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Die Beurteilung der Zulässigkeit der Datenverarbeitung obliegt allein dem Auftraggeber. Dem Auftragnehmer steht nach Ziff. 4 Abs. 6 das Recht zu, den Auftraggeber auf seiner Meinung nach rechtlich unzulässigen Datenverarbeitungen hinzuweisen.

3.2. Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn betroffene Personen ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.

3.3. Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit zu überzeugen. Der Auftraggeber wird das Ergebnis in geeigneter Weise dokumentieren.

3.4. Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen können

- schriftlich
- per E-Mail
- per Telefon

erfolgen. Der Auftraggeber soll mündliche Weisungen, sofern diese in diesem Vertrag für Weisungen zulässig sind, unverzüglich in Textform (z. B. per E-Mail) gegenüber dem Auftragnehmer bestätigen.

3.5. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

3.6. Der Auftraggeber kann weisungsberechtigte Personen benennen. Die weisungsberechtigten Personen werden dem Auftragnehmer nach Vertragsschluss benannt.
Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer schriftlich oder in Textform mitteilen.

3.7. Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

3.8. Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

4. Rechte und Pflichten des Auftragnehmers

4.1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Zweck, Art und Umfang der Datenverarbeitung richten sich ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat. Der Auftragnehmer verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen.

4.2. Nicht mehr benötigte Unterlagen mit personenbezogenen Daten und Dateien dürfen erst nach vorheriger Zustimmung durch den Auftraggeber datenschutzgerecht vernichtet werden.

4.3. Der Auftragnehmer bestätigt, dass er einen betrieblichen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Die Pflicht zur Bestätigung kann im Ermessen des Auftraggebers entfallen, wenn der Auftragnehmer nachweisen kann, dass er gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu bestellen und der Auftragnehmer nachweisen kann, dass betriebliche Regelungen bestehen, die eine Verarbeitung personenbezogener Daten unter Einhaltung der gesetzlichen Vorschriften, der Regelungen dieses Vertrages sowie etwaiger weiterer Weisungen des Auftraggebers gewährleisten.

4.4. Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu.

4.5. Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Der Auftragnehmer wird Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, vorab mit dem Auftraggeber abstimmen.

4.6. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

4.7. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

4.8. Für den Fall, dass der Auftragnehmer feststellt oder Tatsachen die Annahme begründen, dass von ihm für den Auftraggeber verarbeitete

- besondere Arten personenbezogener Daten (Art. 9 DSGVO) oder
- personenbezogene Daten, die einem Berufsgeheimnis unterliegen oder
- personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen oder (auch i. S. v. Art. 10 DSGVO)
- personenbezogene Daten zu Bank- oder Kreditkartenkonten

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, hat der Auftragnehmer den Auftraggeber unverzüglich und vollständig über Zeitpunkt, Art und Umfang des Vorfalls/der Vorfälle in Schriftform oder Textform (E-Mail) zu informieren. Die Information muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung enthalten. Die Information soll zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung beinhalten. Der Auftragnehmer ist darüber hinaus verpflichtet, unverzüglich mitzuteilen, welche Maßnahmen durch den Auftragnehmer getroffen wurden, um die unrechtmäßige Übermittlung bzw. unbefugte Kenntnisnahme durch Dritte künftig zu verhindern.

Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei entsprechenden Meldepflichten unterstützen.

4.9. Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Benachrichtigungspflicht nach Art. 34 DSGVO bestehen kann. Der Auftragnehmer wird den Auftraggeber dabei entsprechend unterstützen.

4.10. Die Verarbeitung von Daten im Auftrag des Auftraggebers außerhalb von Betriebsstätten oder innerhalb von Privatwohnungen des Auftragnehmers oder Subunternehmern ist zulässig. Für die Voraussetzungen und die nähere Ausgestaltung wird auf Ziff. 11 dieses Vertrages verwiesen.

4.11. Der Auftragnehmer wird die Daten, die er im Auftrag für den Auftraggeber verarbeitet, auf geeignete Weise kennzeichnen. Sofern die Daten für verschiedene Zwecke verarbeitet werden, wird der Auftragnehmer die Daten mit dem jeweiligen Zweck kennzeichnen.

4.12. An der Erstellung des Verzeichnisses der Verarbeitungstätigkeiten durch den Auftraggeber hat der Auftragnehmer mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

4.13. Der Auftragnehmer soll dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Diese Personen werden dem Auftraggeber nach Vertragsschluss mitgeteilt.

4.14. Hat eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zu Folge, so hat der Auftraggeber eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen. Der Auftragnehmer hat bei der Durchführung mitzuwirken und dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

4.15. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei der Erstellung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO und einer etwaigen vorherigen Konsultation der Aufsichtsbehörde nach Art. 36 DSGVO zu unterstützen.

5. Kontrollbefugnisse

5.1. Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.

5.2. Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i. S. d. Absatzes 1 erforderlich ist.

5.3. Der Auftraggeber kann eine Einsichtnahme in die vom Auftragnehmer für den Auftraggeber verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen.

5.4. Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören.

5.5. Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i. S. d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten, die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

6. Unterauftragsverhältnisse

6.1. Die Beauftragung von Subunternehmen durch den Auftragnehmer ist nur mit Zustimmung des Auftraggebers zulässig. Der Auftragnehmer wird alle bereits zum Vertragsschluss bestehenden Unterauftragsverhältnisse in der **„Anlage 1"** zu diesem Vertrag angeben.

Änderungen betreffend der in Anlage 1 aufgelisteten Subunternehmer werden dem Auftraggeber über eine Benachrichtigung mitgeteilt, die der Auftraggeber dann über eine Bestätigungslösung innerhalb der Software genehmigen kann.

6.2. Der Auftragnehmer hat den Subunternehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Subunternehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln. Der Auftragnehmer ist verpflichtet, sich vom Subunternehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten i. S. d. Art. 37 DSGVO bestellt hat es sei denn dieser ist nicht bestellpflichtig.

6.3. Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzenden Weisungen des Auftraggebers auch gegenüber den Subunternehmern gelten. Der Auftragnehmer hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren.

6.4. Der Auftragnehmer hat mit dem Subunternehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Dem Auftraggeber ist der Auftragsverarbeitungsvertrag mit dem Subunternehmer auf Anfrage in Kopie zu übermitteln. Der Auftragnehmer stellt sicher, dass dem Unterauftragnehmer dabei dieselben Datenschutzpflichten auferlegt werden, die in diesem Vertrag festgelegt sind.

6.5. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass bei dem jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gemäß den Artikeln 44 ff. DSGVO gewährleistet ist.

Dies kann insbesondere in Ländern außerhalb des EWR-Raumes und ohne Vorhandensein eines Angemessenheitsbeschlusses der EU-Kommission, durch den Abschluss einer Vereinbarung auf Basis der EU-Standardvertragsklauseln, vorhanden Binding Corporate Rules oder eines Code of Conduct erfolgen.

Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

6.6. Nicht als Unterauftragsverhältnisse i. S. d. Absätze 1 bis 5 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Wartungs- und Prüfungsleistungen stellen zustimmungspflichtige Unterauftragsverhältnisse dar, soweit die Wartung und Prüfung solche IT-Systeme betreffen, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber

genutzt werden. Die Parteien sind sich darüber einig, dass vorgenannte Wartungs- und Prüfleistungen eine „Auftragsverarbeitung" i. S. d. Art. 28 DSGVO darstellen.

7. Datenschutzbeauftragter des Auftragnehmers

Beim Auftragnehmer ist als fachkundiger Datenschutzbeauftragter benannt:

Herr Sven Lenz
Datenschutzkanzlei Lenz GmbH & Co. KG
Bahnhofstraße 50
87435 Kempten
Telefon: +49831930653 - 00
E-Mail: lenz@deutsche-datenschutzkanzlei.de

Der Fachkundenachweis über die Qualifikation des Datenschutzbeauftragten kann bei Bedarf angefordert werden.

Ein Wechsel des Datenschutzbeauftragten ist dem Verantwortlichen unverzüglich mitzuteilen. Auf Anfrage des Verantwortlichen ist der aktuelle Fachkundenachweis zur Verfügung zu stellen.

8. Vertraulichkeitsverpflichtung

8.1 Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.

8.2 Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und diese auf die Wahrung der Vertraulichkeit verpflichtet. Sofern der Auftragnehmer im Zusammenhang mit Leistungen für den Auftraggeber an der Erbringung geschäftsmäßiger Telekommunikationsdienste mitwirkt, ist er verpflichtet, die hieran beteiligten Beschäftigten schriftlich auf das Fernmeldegeheimnis i. S. d. § 88 TKG zu verpflichten.

8.3 Der Auftragnehmer wird alle Beschäftigten, die Leistungen im Zusammenhang mit dem Auftrag des Auftraggebers erbringen, in schriftlicher Form verpflichten, alle Daten des Auftraggebers, insbesondere die für den Auftraggeber verarbeiteten personenbezogenen Daten vertraulich zu behandeln. Diese Verpflichtung der Beschäftigten ist auf Anfrage dem Auftraggeber nachzuweisen.

9. „Home-Office"-Regelung

Homeoffice, auch Telearbeit genannt, ist eine flexible Arbeitsform, bei der die Beschäftigten ihre Arbeit vollumfänglich oder teilweise aus dem privaten Umfeld heraus ausführen.

9.1 Der Auftragnehmer darf seinen Beschäftigten, die mit der Verarbeitung von personenbezogenen Daten für den Auftraggeber beauftragt sind, die Verarbeitung von personenbezogenen Daten in Privatwohnungen („Home-Office") erlauben.

9.2 Der Auftragnehmer hat sicherzustellen, dass die Einhaltung der vertraglich vereinbarten technischen und organisatorischen Maßnahmen auch im „Home-Office" der Beschäftigten des Auftragnehmers

gewährleistet ist. Abweichungen von einzelnen vertraglich vereinbarten technischen und organisatorischen Maßnahmen sind vorab mit dem Auftraggeber abzustimmen und von diesem in Textform zu genehmigen.

9.3 Der Auftragnehmer trägt insbesondere Sorge dafür, dass bei einer Verarbeitung von personenbezogenen Daten im „Home-Office" die Speicherorte so konfiguriert werden, dass eine lokale Speicherung von Daten auf IT-Systemen, die im „Home-Office" verwendet werden, ausgeschlossen ist. Sollte dies nicht möglich sein, hat der Auftragnehmer Sorge dafür zu tragen, dass die lokale Speicherung ausschließlich verschlüsselt erfolgt und andere im Haushalt befindliche Personen keinen Zugriff auf diese Daten erhalten.

9.4 Der Auftragnehmer ist verpflichtet, Sorge dafür zu tragen, dass eine wirksame Kontrolle der Verarbeitung personenbezogener Daten im Auftrag im „Home-Office" durch den Auftraggeber möglich ist. Dabei sind die Persönlichkeitsrechte der Beschäftigten sowie der weiteren im jeweiligen Haushalt lebenden Personen angemessen zu berücksichtigen.

10. Wahrung von Betroffenenrechten

10.1 Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich.

10.2 Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten – insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung – durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen.

10.3 Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

11. Geheimhaltungspflichten

11.1 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.

11.2 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.

12. Vergütung

Die Vergütung des Auftragsnehmers wird gesondert vereinbart.

13. Technische und organisatorische Maßnahmen zur Datensicherheit

13.1 Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind.

13.2 Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als **„Anlage 2"** zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Vorwege mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

13.3 Der Auftragnehmer wird die von ihm getroffenen technische und organisatorische Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird der Auftragnehmer den Auftraggeber informieren.

13.4 Der Auftragnehmer wird dem Auftraggeber die von ihm nach Art. 32 DSGVO getroffenen technischen und organisatorischen Maßnahmen zur Gewährleistung des nach Art. 32 DSGVO und des in diesem Vertrag geregelten Schutzniveaus in dokumentierter Form und in geeigneter Weise zur Verfügung stellen. Sofern die Parteien nicht gesondert vereinbaren, dass die in der „**Anlage 2"** aufgeführten technischen und organisatorischen Maßnahmen durch die nach diesem Absatz neu zur Verfügung gestellte Dokumentation der technischen und organisatorischen Maßnahmen zur Datensicherheit ersetzt werden, bleiben die in „Anlage 2" genannten Maßnahmen Vertragsbestandteil und sind vom Auftragnehmer entsprechend zu erfüllen.

14. Dauer des Auftrages

14.1 Der Vertrag ist für die Dauer der Laufzeit des Hauptvertrages gültig.

14.2 Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

15. Beendigung

15.1 Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen. Die Datenträger des Auftragnehmers sind danach physisch zu löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Die Löschung ist in geeigneter Weise zu dokumentieren. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder physisch zu löschen.

15.2 Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Auftraggeber angekündigt werden.

16. Zurückbehaltungsrecht

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

17. Schlussbestimmungen

17.1 Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

17.2 Für Nebenabreden ist die Schriftform erforderlich.

17.3 Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Dieser Vertrag wird digital innerhalb der ECHO PRM Software abgeschlossen und dokumentiert.

Anlage 1: Unterauftragnehmer

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von folgenden Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer"):

Unterauftragnehmer	**Zweck der Verarbeitung**	**Geeignete Garantien, wenn Daten in Drittland verarbeitet werden**
Google Cloud EMEA Limited Velasco Clanwilliam Place Dublin 2 IRLAND	Betrieb der Saas-Anwendung „ECHO PRM", Erfüllung des Vertrags; Hosting der personenbezogenen Daten des Auftraggebers.	Abschluss der Standardvertragsklauseln, Abschluss eines Auftragsverarbeitungsvertrages
Netcup GmbH, Daimlerstr. 25, 76185 Karlsruhe DE	Betrieb der Saas-Anwendung „ECHO PRM", Erfüllung des Vertrags; Domainverwaltung;	
Uberspace.de Jonas Pasche, Kaiserstr. 15, 55116 Mainz DE	Betrieb der Saas-Anwendung „ECHO PRM", Erfüllung des Vertrags; Statische Daten für das Erscheinungsbild der Website.	

Anlage 2: Technische und organisatorische Maßnahmen des Auftragnehmers

INHALT

Vertragliche Regelungen und Vereinbarungen zur Auftragsverarbeitung (AVs)

gemäß Artikel 28 DSGVO

1 Einleitung

Datensicherheit ist ein wichtiger integrierter Part im Datenschutz. Über Datensicherheit werden die technischen und organisatorischen Maßnahmen geregelt, die erforderlich sind, um den Schutz von personenbezogenen Daten bei automatisierter Verarbeitung, also in Systemen oder Programmen, zu gewährleisten.

Im Fall des Einbezugs von Auftragsverarbeitern müssen diese ebenfalls auf die Einhaltung von Datensicherheit geprüft werden (Art. 28 DSGVO).

Die Europäische Datenschutzgrundverordnung (DSGVO) enthält in Art. 32 Abs. 1 DSGVO Vorgaben darüber, dass personenbezogene Daten über adäquate technische und organisatorische Maßnahmen sicher verarbeitet werden müssen. Die Umsetzung der Schutzziele (= Maßnahmen) bleibt dabei dem Verantwortlichen*, „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 des Risikos für die Rechte und Freiheiten natürlicher Personen*"(Art. 32 DSGVO) selbst überlassen.

Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

Für eine automatisierte Verarbeitung (also vor allem per Hard- und Software) nennt die DSGVO verschiedene Kontrollbereiche, die jeweils verschiedene Unterpunkte beinhalten:

(1) Pseudonymisierung und Verschlüsselung wo immer möglich
(2) Vertraulichkeit
(3) Integrität
(4) Verfügbarkeit und Belastbarkeit
(5) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Für nicht-automatisierte Verarbeitungen von personenbezogenen Daten sind die oben genannten Kontrollbereiche nach dem Gesetzeswortlaut nicht direkt anwendbar. Es wird jedoch empfohlen, für einen bestmöglichen Schutz auch in diesen Fällen die Datensicherheit in Anlehnung an die Kontrollbereiche zu organisieren.

2 Organisatorisches

Die ECHO PRM GmbH gewährleistet die schriftliche Dokumentation des aktuellen Datenschutzniveaus und gibt den Mitarbeitern schriftliche Vorgaben in Form von Arbeitsanweisungen, Richtlinien und Merkblätter für die Einhaltung. Die bei der Datenverarbeitung eingesetzten Mitarbeiter sind auf die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b), 29, 32 Abs. 4 DSGVO verpflichtet.

Einige diesen Bereich betreffende Sicherungsmaßnahmen der folgenden Prüfliste sind nicht gesondert ausgewiesen, da sie entweder in die Verantwortung von Auftragsverarbeitern fallen und daher gesondert geregelt und geprüft werden oder da aus Gründen der Vertraulichkeit nicht alle Details veröffentlicht werden sollen.

3 Sicherungsmaßnahmen

Die folgenden Punkte beschreiben die technischen und organisatorischen Maßnahmen, die von der ECHO PRM GmbH betrieben werden.

4 Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a) DSGVO)

Wo immer möglich, werden personenbezogene Daten ausschließlich pseudonymisiert (also ohne direkte Erkennbarkeit einer betroffenen Person) verarbeitet. Zudem sollten Daten, wo immer möglich, ausschließlich verschlüsselt versendet oder gespeichert werden. Dabei gilt das Prinzip der Verhältnismäßigkeit.

5 Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO)

5.1.1 Zutrittskontrolle

Die Zutrittskontrolle umfasst Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren:

Maßnahmen	Bemerkung
Die Verteilerräume der Gebäudetechnik sind gegen unbefugten Zutritt gesichert.	
Es gibt Sicherungsmaßnahmen gegen Überfälle.	
Es existieren angemessene, nicht maschinelle Zutrittskontrollen zu dem Gebäude.	
Die Netzwerkkomponenten befinden sich in dafür vorgesehenen zutrittskontrollierten Räumen.	
Die eingerichteten Schutzmaßnahmen der Zutrittskontrolle werden regelmäßig einem eingehenden Test unterzogen, um festzustellen, ob sie noch den gewünschten Schutzzweck erfüllen.	

5.1.2 Zugangskontrolle

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

Maßnahmen	Bemerkung
Es gibt ein formales Freigabeverfahren, welche Systeme und Applikationen mit personenbezogenen Daten zu durchlaufen haben, bevor diese Netzwerkzugang bekommen dürfen.	

Das WLAN ist vor unbefugtem Zugang gesichert.	

5.1.3 Zugriffskontrolle

Maßnahmen, die 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.

Maßnahmen	Bemerkung
Die Benutzer stellen sicher, dass ihre DV-Ausstattung, falls unbeaufsichtigt, ausreichend geschützt ist.	
Es wird der Grundsatz des aufgeräumten Schreibtischs und des leeren Bildschirms gelebt (Clean Desk Policy).	
Es gibt Anweisungen, wie mit nicht mehr benötigten Datenträgern (einschließlich beschriebenem oder bedrucktem Papier) umzugehen ist.	
Die Entsorgung oder Weiterverwendung von Geräten, die mit Speichermedien ausgerüstet sind, ist geregelt.	

5.1.4 Trennungsgebot

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

Maßnahmen	Bemerkung
Personenbezogene Daten auf den Systemen werden logisch voneinander getrennt (unterschiedliche Datensätze in einer einheitlichen Datenbank werden je nach Zweck markiert (softwareseitige Unterscheidbarkeit)).	
Die im Unternehmen eingesetzten Systeme sind mandantenfähig.	
Die Mandantenfähigkeit für die davon betroffenen Verfahren ist durchgängig realisiert.	
Office-, Entwicklungs-, Test- und Wirksysteme befinden sich in klar voneinander getrennten Netzsegmenten, wo möglich sogar physikalisch voneinander getrennt.	

6 Integrität (Art. 32 Abs. 1 lit. b) DSGVO)

6.1.1 Weitergabekontrolle

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.

Maßnahmen	Bemerkung
Alle Personen, die mit der Verarbeitung/Nutzung personenbezogener Daten beschäftigt sind, sind zur Einhaltung der Vertraulichkeit verpflichtet.	
Allen neuen Mitarbeitern werden bei der Verpflichtung zur Vertraulichkeit Informationen zum Datenschutz ausgehändigt.	
Die Mitarbeiter, die personenbezogene Daten verarbeiten/nutzen, werden durch Datenschutzschulungen auf datenschutzgerechtes Verhalten am Arbeitsplatz geschult worden.	
Es ist sichergestellt, dass Daten nur an die vom Auftraggeber festgelegten oder der Zweckbestimmung nach richtigen Adressaten übermittelt werden.	
Bei der Weitergabe von Daten wird, soweit möglich, von den Möglichkeiten der Anonymisierung/Pseudonymisierung Gebrauch gemacht.	

6.1.2 Eingabekontrolle

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

Maßnahmen	Bemerkung
Die protokollierten Daten unterliegen einer strengen Zweckbestimmung.	
Die protokollierten Daten sind gegen unbefugte Einsicht oder Manipulation geschützt.	
Es werden digitale Signaturverfahren zur Manipulationserkennung eingesetzt.	

7 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b) und c) DSGVO)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

Maßnahmen	Bemerkung
Die Strom Versorgungsleitungen verlaufen unterirdisch.	
Ein Frühwarnsystem mit automatischen Brandmeldern ist installiert.	
Das Brandmeldesystem wird regelmäßig gewartet.	
Es sind ausreichend geeignete Feuerlöscher sowie das richtige Löschmittel im Einsatz und dabei wird auf Einheitlichkeit geachtet.	
Es findet eine regelmäßige Wartung und Überprüfung der Rauchmelder und Handfeuerlöscher statt.	
Es werden regelmäßige Backups durchgeführt.	
Die Backups sind verschlüsselt.	
Es wird Antivirensoftware eingesetzt und werden immer auf dem aktuellsten Stand gehalten	
Es wird ein IDS (intrusion detection system) bzw. IPS (intrusion prevention system) eingesetzt.	

8 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 25 Abs. 1 DSGVO; Art. 32 Abs. 1 lit. d) DSGVO)

8.1.1 Organisatorische Sicherheitskriterien

Organisatorische Sicherheit beschreibt alle organisatorische Maßnahmen (Handlungsanweisungen, Vorgehensweisen, etc.) zur Gewährleistung und Verbesserung der Sicherheit.

Maßnahmen	Bemerkung
Ein Datenschutz-Managementsystem (DSMS) ist eingeführt und beinhaltet die wichtigsten datenschutzrechtlichen Vorgaben und eine umfassende Struktur zur Abbildung der Datenschutzmaßnahmen.	
Es wurde freiwillig ein externer Datenschutzbeauftragter benannt	
Eine regelmäßige Aufklärung und Sensibilisierung der Mitarbeiter und Führungskräfte werden durchgeführt.	

8.1.2 Auftragskontrolle

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

Mitarbeiter, die als Administratoren Zugriff auf die Systeme haben, sind alle hinsichtlich des Datenschutzes belehrt, auf die Wahrung der Vertraulichkeit verpflichtet und haben als Bestandteil ihres Arbeitsvertrags entsprechende Verschwiegenheits- und Geheimhaltungsvereinbarungen akzeptiert.

Sollte die ECHO PRM GmbH bei der Datenverarbeitung Auftragsverarbeiter einsetzen, werden bestimmte Vorgaben umgesetzt. Hierzu zählt die Sicherstellung der technisch-organisatorischen Maßnahmen der Auftragnehmer im Sinne Art. 28 DSGVO und Art. 32 Abs. 1 DSGVO.

Voraussetzungen für das Eingehen einer Auftragsverarbeitung ist grundsätzlich eine rechtliche Grundlage. Für einen Vertrag zur Auftragsdatenverarbeitung nach Art. 28 Abs. 3 DSGVO müssen alle geforderten Maßnahmen und Vorgaben eingehalten werden.

Maßnahmen	Bemerkung
Auftragsverarbeiter sind vollständig vertraglich verpflichtet.	

This document has been translated automatically from German into English. In the event of any discrepancies between the German and English versions, the German version shall prevail.

Contract for order processing

Client	**Contractor**
"Customer"	Echo PRM GmbH. Krokusweg 5 a 87488 Betzigau Germany

This contract for commissioned processing shall be made available to the Client for review prior to the commencement of the contract.
Completion/approval is done by the client via a confirmation solution within the ECHO PRM software at the first login.

Vertragliche Regelungen und Vereinbarungen zur Auftragsverarbeitung (AVs)

gemäß Artikel 28 DSGVO

Table of contents

Note regarding gender-neutral wording
A gender-equal society requires gender-neutral language. In the following text, appropriate formulations are used wherever possible and appropriate (e.g. pair formulas, derivations). Personal terms that are technical terms, definitions, quotations or similar are not replaced by pair formulas in the text. Corresponding terms are to be interpreted in a gender-neutral manner for the purpose of equal treatment. If, for reasons of easier readability, only one gender is shown for personal nouns and pronouns, this also does not imply any discrimination against the other genders, but should be understood as gender-neutral in the sense of linguistic simplification.

18. General

1.3. The Contractor processes personal data on behalf of the Client. According to the will of the parties and in particular the Customer, this contract contains the written order for commissioned processing within the meaning of Article 28 of the EU General Data Protection Regulation (GDPR) and regulates the rights and obligations of the parties in connection with the data processing.

1.4. Insofar as the term "data processing" or "processing" (of data) is used in this Agreement, the definition of "processing" within the meaning of Article 4 No. 2 of the GDPR shall apply.

19. Subject of the agreement

2.4th The Client's order to the Contractor shall include the following work and/or services:

The subject matter of the agreement is the contractual relationship between the parties concerning the provision for a fee of the software "ECHO PRM" (SaaS application) for unlimited, non-exclusive use, as well as the storage of the Customer's data within the scope of the provision of storage space in the Contractor's cloud. Also included are the maintenance services for the software as well as the support services within the scope of support services. Within the scope of the use of the software, the Customer shall receive access via one or more back-end users.

The following order processing is specifically provided by the Contractor, with the possibility of inspection and knowledge of the Client's personal data:

- Storage of the client's data in the contractor's cloud in order to keep the data available.
- Support services to perform error analysis and problem resolution in the course of using the Software.

2.5th The following types of data are regularly subject to processing:

- Master data of the client and of persons acting on behalf of the client (first name, last name, address details, contact details, user codes and names, authorizations).
- User-related change logs.
- If applicable, personal data of third parties - depending on the design of the content by the client.

2.6th Group of persons affected by the data processing:

- Business partners of the client (customers, suppliers)
- Employees of the client.

20. Rights and obligations of the client

3.9. The Client is the responsible party within the meaning of Art. 4 No. 7 DSGVO for the processing of data on behalf of the Contractor. The assessment of the permissibility of the data processing is the sole responsibility of the Client. Pursuant to Section 4 (6), the Contractor shall have the right to notify the Client of any data processing that it considers to be legally inadmissible.

3.10. As the responsible party, the Client is responsible for safeguarding the data subject rights. The Contractor shall inform the Client without delay if data subjects assert their data subject rights against the Contractor.

3.11. Prior to the commencement of data processing and thereafter on a regular basis, the Customer shall satisfy itself of compliance with the technical and organizational data security measures taken by the Contractor. The Customer shall document the result in a suitable manner.

3.12. The Client has the right to issue supplementary instructions to the Contractor at any time regarding the type, scope and procedure of data processing. Instructions can

- in writing
- by e-mail
- By phone

take place. The Customer shall immediately confirm verbal instructions to the Contractor in text form (e.g. by e-mail), insofar as these are permitted for instructions in this contract.

3.13. This shall be without prejudice to any provisions regarding the remuneration of additional expenses incurred by the Contractor as a result of supplementary instructions issued by the Client.

3.14. The Client may appoint persons authorized to issue instructions. The persons authorized to give instructions shall be named to the Contractor after conclusion of the contract.
In the event that the persons authorized to issue instructions change at the Client, the Client shall notify the Contractor thereof in writing or in text form.

3.15. Customer shall inform Contractor without undue delay if it detects any errors or irregularities in connection with the processing of personal data by Contractor.

3.16. In the event that there is an obligation to inform third parties pursuant to Art. 33, 34 DSGVO, the Client shall be responsible for compliance therewith.

21. Rights and obligations of the contractor

4.16. The Contractor shall process personal data exclusively within the scope of the agreements made and/or in compliance with any supplementary instructions issued by the Client. The purpose, type and scope of data processing shall be governed exclusively by this Agreement and/or the Client's instructions. The Contractor is prohibited from processing data in any other way, unless the Customer has given its written consent. The Contractor undertakes to carry out data processing on behalf of the Client only in member states of the European Union (EU) or the European Economic Area (EEA).

4.17. Documents with personal data and files that are no longer required may only be destroyed with the prior consent of the client in accordance with data protection regulations.

4.18. The Contractor confirms that it has appointed an operational data protection officer in accordance with Art. 37 DSGVO. The obligation to confirm may be waived at the discretion of the Customer if the Contractor can prove that it is not required by law to appoint a data protection officer and the Contractor can prove that operational regulations exist which ensure that personal data is processed in compliance with the statutory provisions, the provisions of this Agreement and any further instructions of the Customer.

4.19. In the area of the processing of personal data in accordance with the order, the Contractor warrants that all agreed measures will be carried out in accordance with the contract.

4.20. The Contractor shall be obliged to organize its company and its operating procedures in such a way that the data which it processes on behalf of the Customer are secured to the extent required in each case and protected against unauthorized access by third parties. The Contractor shall coordinate any changes in the organization of data processing on behalf of the Customer that are significant for the security of the data with the Customer in advance.

4.21. The Contractor shall inform the Customer without undue delay if, in its opinion, an instruction issued by the Customer violates statutory regulations. The Contractor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Customer.

4.22. The Contractor is obliged to notify the Customer without undue delay of any breach of data protection regulations or of the contractual agreements made and/or the instructions issued by the Customer which has occurred in the course of the processing of data by the Contractor or other persons involved in the processing. Furthermore, the Contractor shall inform the Client without undue delay if a supervisory authority takes action against the Contractor pursuant to Art. 58 DSGVO and this may also concern a control of the Processing which the Contractor performs on behalf of the Client.

4.23. In the event that the Contractor establishes or facts justify the assumption that the goods processed by it for the Client are

- special types of personal data (Art. 9 GDPR) or
- personal data subject to professional secrecy, or
- personal data relating to criminal acts or administrative offences or the suspicion of criminal acts or administrative offences or (also within the meaning of Art. 10 GDPR)
- personal data on bank or credit card accounts

have been unlawfully transmitted or have otherwise come to the attention of third parties unlawfully, the Contractor shall inform the Client immediately and completely of the time, nature and extent of the incident(s) in writing or in text form (e-mail). The information must contain an explanation of the nature of the unlawful acquisition of knowledge. The information shall additionally include an explanation of possible adverse consequences of the unlawful acquisition of knowledge. In addition, the Contractor shall be obliged to inform immediately which measures have been taken by the Contractor to prevent the unlawful transmission or unauthorized disclosure by third parties in the future.

The Contractor is aware that the Client may have a reporting obligation pursuant to Art. 33 of the GDPR, which provides for a report to the supervisory authority within 72 hours after it becomes known. The Contractor shall support the Client in the corresponding reporting obligations.

4.24. The Contractor is aware that the Client may be subject to a notification obligation pursuant to Art. 34 of the GDPR. The Contractor shall support the Client accordingly.

4.25. The processing of data on behalf of the Client outside of business premises or within private residences of the Contractor or subcontractors is permitted. For the prerequisites and further details, please refer to Section 11 of this Agreement.

4.26. The Contractor shall mark the data that it processes on behalf of the Client in a suitable manner. If the data are processed for different purposes, the Contractor shall mark the data with the respective purpose.

4.27. The Contractor shall cooperate in the preparation of the list of processing activities by the Customer. The Contractor shall provide the Client with the required information in an appropriate manner.

4.28. The Contractor shall name to the Client the person(s) authorized to receive instructions from the Client. These persons shall be notified to the Client after the conclusion of the contract.

4.29. If a form of processing is likely to result in a high risk to the rights and freedoms of natural persons, the Customer shall conduct an assessment of the consequences of the intended processing operations for the protection of personal data. The contractor shall cooperate in the implementation and provide the client with the required information in an appropriate manner.

4.30. The Contractor shall be obliged to assist the Client in the preparation of a data protection impact assessment pursuant to Art. 35 DSGVO and any prior consultation with the supervisory authority pursuant to Art. 36 DSGVO.

22. Control powers

5.6. The Customer shall have the right to monitor the Contractor's compliance with the statutory provisions on data protection and/or compliance with the contractual provisions made between the Parties and/or compliance with the Customer's instructions at any time to the extent required.

5.7. The Contractor shall be obliged to provide the Client with information to the extent that this is necessary to carry out the inspection as defined in paragraph 1.

5.8. The Customer may request to inspect the data processed by the Contractor for the Customer and the data processing systems and programs used.

5.9. The Customer may carry out the inspection within the meaning of Paragraph 1 at the Contractor's premises during normal business hours after prior notification with a reasonable period of notice. In doing so, the Customer shall ensure that the inspections are only carried out to the extent necessary in order not to disproportionately disrupt the Contractor's operating processes as a result of the inspections.

5.10. In the event of measures taken by the supervisory authority vis-à-vis the Customer within the meaning of Article 58 of the GDPR, in particular with regard to information and control obligations, the Contractor shall be obliged to provide the Customer with the necessary information and to enable the respective competent supervisory authority to carry out an on-site inspection. The Principal shall be informed by the Contractor about corresponding planned measures.

23. Subcontracting relationships

6.7. The commissioning of subcontractors by the Contractor shall only be permissible with the consent of the Customer. The Contractor shall specify all subcontracting relationships already existing at the time of conclusion of the contract in **"Annex 1"** to this contract.

Changes regarding the subcontractors listed in Attachment 1 will be communicated to the Client via notification, which the Client can then approve via a confirmation solution within the software.

6.8. The Contractor shall carefully select the subcontractor and check prior to the assignment that the subcontractor can comply with the agreements made between the Client and the Contractor. In particular, the Contractor shall check in advance and regularly during the term of the contract that the subcontractor has taken the technical and organizational measures required under Art. 32 GDPR to protect personal data. The result of the control shall be documented by the Contractor and

communicated to the Customer upon request. The Contractor shall be obliged to obtain confirmation from the subcontractor that the latter has appointed a company data protection officer within the meaning of Art. 37 of the GDPR, unless such officer is not required to be appointed.

6.9. The Contractor shall ensure that the regulations agreed in this contract and, if applicable, supplementary instructions of the Customer also apply to the subcontractors. The Contractor shall regularly monitor compliance with these obligations.

6.10. The Contractor shall conclude a contract processing agreement with the subcontractor that complies with the requirements of Art. 28 GDPR. A copy of the order processing agreement with the subcontractor shall be provided to the Customer upon request. The Contractor shall ensure that the subcontractor is thereby subject to the same data protection obligations as set out in this contract.

6.11. If subcontractors in a third country are to be involved, the Contractor shall ensure that an adequate level of data protection is guaranteed at the respective subcontractor in accordance with Articles 44 et seq. GDPR is guaranteed.

In particular, this can be done in countries outside the EEA and without the existence of an adequacy decision by the EU Commission, by concluding an agreement based on the EU standard contractual clauses, existing Binding Corporate Rules or a Code of Conduct.

Upon request, the Contractor shall provide the Customer with evidence of the conclusion of the aforementioned agreements with its subcontractors.

6.12. Subcontracting relationships within the meaning of paragraphs 1 to 5 shall not include services which the Contractor uses from third parties as a purely ancillary service in order to carry out the business activity. These include, for example, cleaning services, pure telecommunication services without any specific reference to services provided by the Contractor to the Customer, postal and courier services, transport services, guarding services. The Contractor shall nevertheless be obliged to ensure that appropriate precautions and technical and organizational measures have been taken to ensure the protection of personal data, even in the case of ancillary services provided by third parties. Maintenance and testing services constitute subcontracting relationships subject to approval insofar as the maintenance and testing concern such IT systems that are also used in connection with the provision of services for the Customer. The Parties agree that the aforementioned maintenance and testing services constitute "commissioned processing" within the meaning of Art. 28 DSGVO.

24. Data protection officer of the contractor

The Contractor has been appointed as an expert data protection officer:

Mr. Sven Lenz
Data Protection Law Firm Lenz GmbH & Co KG
Station road 50
87435 Kempten
Phone: +49831930653 - 00
E-mail: lenz@deutsche-datenschutzkanzlei.de

The certificate of qualification of the data protection officer can be requested if required.

The data controller must be informed immediately of any change in the data protection officer. Upon request of the person responsible, the current certificate of professional competence shall be made available.

25. Confidentiality undertaking

25.1 When processing data for the Client, the Contractor shall be obliged to maintain confidentiality with regard to data that it receives or becomes aware of in connection with the order. The Contractor undertakes to observe the same secrecy rules as are incumbent upon the Client. The Client shall be obliged to inform the Contractor of any special rules for the protection of secrets.

25.2 The Contractor warrants that it is aware of the applicable data protection regulations and is familiar with their application. The Contractor further warrants that it will familiarize the employees engaged in the performance of the work with the data protection provisions applicable to them and that it will oblige them to maintain confidentiality. If the Contractor is involved in the provision of business telecommunication services in connection with services for the Customer, it shall be obliged to commit the employees involved in this in writing to the secrecy of telecommunications within the meaning of Section 88 of the German Telecommunications Act (TKG).

25.3 The Contractor shall oblige all employees who perform services in connection with the Client's order in writing to treat all data of the Client, in particular the personal data processed for the Client, confidentially. This obligation of the employees shall be proven to the Customer upon request.

26. "Home office" regulation

Home office, also known as telecommuting, is a flexible form of work in which employees perform all or part of their work from their private environment.

26.1 The Contractor may allow its employees who are tasked with processing personal data for the Client to process personal data in private residences ("home office").

26.2 The Contractor shall ensure that compliance with the contractually agreed technical and organizational measures is also guaranteed in the "home office" of the Contractor's employees. Deviations from individual contractually agreed technical and organizational measures must be agreed in advance with the Customer and approved by the latter in text form.

26.3 In particular, the Contractor shall ensure that if personal data is processed in the "home office", the storage locations are configured in such a way that local storage of data on IT systems used in the "home office" is excluded. If this is not possible, the Contractor shall ensure that local storage is exclusively encrypted and that other persons in the household do not have access to this data.

26.4 The Contractor shall be obliged to ensure that effective control of the processing of personal data on behalf of the Client in the "home office" is possible. In this context, the personal rights of the employees as well as of the other persons living in the respective household shall be adequately taken into account.

27. Safeguarding of data subject rights

27.1 The client is solely responsible for safeguarding the rights of the data subjects.

27.2 Insofar as the cooperation of the Contractor is required for the protection of data subject rights - in particular to information, correction, blocking or deletion - by the Client, the Contractor shall take the respective measures required in accordance with the Client's instructions.

27.3 This shall be without prejudice to any provisions regarding the remuneration of additional expenses incurred by the Contractor as a result of cooperation services in connection with the assertion of data subject rights vis-à-vis the Client.

28. Secrecy obligations

28.1 Both parties undertake to treat all information received in connection with the execution of this contract as confidential for an unlimited period of time and to use it only for the execution of the contract. Neither party shall be entitled to use this information in whole or in part for purposes other than those just mentioned or to make this information available to third parties.

28.2 The foregoing obligation shall not apply to information which one of the parties has demonstrably received from third parties without being obliged to maintain secrecy or which is publicly known.

29. Remuneration

The remuneration of the Contractor shall be agreed separately.

30. Technical and organizational data security measures

30.1 The Contractor undertakes vis-à-vis the Client to comply with the technical and organizational measures required to comply with the applicable data protection regulations.

30.2 The status of the technical and organizational measures existing at the time of conclusion of the contract is attached as **"Annex 2"** to this contract. The parties agree that changes to the technical and organizational measures may become necessary in order to adapt to technical and legal circumstances. The Contractor shall agree in advance with the Customer on any significant changes that may affect the integrity, confidentiality or availability of the personal data. Measures that involve only minor technical or organizational changes and do not negatively affect the integrity, confidentiality and availability of the personal data may be implemented by the Contractor without coordination with the Customer. The Customer may request an up-to-date version of the technical and organizational measures taken by the Contractor at any time.

30.3 The Contractor shall check the effectiveness of the technical and organizational measures it has taken on a regular basis and also on an ad hoc basis. In the event that there is a need for optimization and/or change, the Contractor shall inform the Customer.

30.4 The Contractor shall provide the Customer with the technical and organizational measures taken by it in accordance with Art. 32 DSGVO to ensure the level of protection regulated in accordance with Art. 32 DSGVO and the level of protection regulated in this Agreement in documented form and in a suitable manner. Unless the parties separately agree that the technical and organizational measures listed in "**Annex 2" are replaced** by the documentation of the technical and organizational measures for data security newly provided pursuant to this paragraph, the measures listed in "Annex 2" shall remain part of the contract and shall be fulfilled by the Contractor accordingly.

31. Duration of the order

31.1 The contract is valid for the duration of the main contract.

31.2 The Customer may terminate the contract at any time without notice if there is a serious breach by the Contractor of the applicable data protection provisions or of obligations under this contract, if the Contractor is unable or unwilling to carry out an instruction of the Customer or if the Contractor refuses access by the Customer or the competent supervisory authority in breach of the contract.

32. Termination

32.1 After termination of the contract, the Contractor shall hand over to the Client all documents, data and created processing or utilization results that have come into its possession and that are related to the contractual relationship. The Contractor's data carriers shall be physically deleted thereafter. This shall also apply to any data backups at the Contractor. The deletion shall be documented in a suitable manner. Test and reject material shall be destroyed or physically deleted without delay.

32.2 The Client has the right to check the complete and contractual return and deletion of the data at the Contractor's premises. This may also be done by an inspection of the data processing equipment at the Contractor's premises. The on-site inspection shall be announced by the Customer with reasonable notice.

33. Right of retention

The parties agree that the defense of the right of retention by the Contractor within the meaning of Section 273 of the German Civil Code (BGB) is excluded with regard to the processed data and the associated data carriers.

34. Final provisions

34.1 Should the property of the Client with the Contractor be endangered by measures of third parties (for example by seizure or attachment), by insolvency proceedings or by other events, the Contractor shall inform the Client without delay. The Contractor shall inform the creditors without undue delay of the fact that data processed on behalf is involved.

34.2 Additional agreements must be made in writing.

34.3 Should individual parts of this contract be invalid, this shall not affect the validity of the remaining provisions of the contract.

This contract is concluded and documented digitally within the ECHO PRM software.

Annex 1: Subcontractor

For the processing of data on behalf of the Client, the Contractor shall use the services of the following third parties who process data on its behalf ("Subcontractors"):

Subcontractor	**Purpose of processing**	**Appropriate safeguards when data are processed in third country**
Google Cloud EMEA Limited Velasco Clanwilliam Place Dublin 2 IRELAND	Operation of the Saas application "ECHO PRM", performance of the contract; hosting of the client's personal data.	Conclusion of the standard contractual clauses, conclusion of a processing contract
Netcup GmbH, Daimlerstr. 25, 76185 Karlsruhe DE	Operation of the Saas application "ECHO PRM", fulfillment of the contract; domain management;	
Uberspace.com Jonas Pasche, Kaiserstr. 15, 55116 Mainz DE	Operation of the Saas application "ECHO PRM", fulfillment of the contract; Static data for the appearance of the website.	

Annex 2: Technical and organizational measures of the contractor

CONTENT

1 Introduction

Data security is an important integrated part of data protection. Data security regulates the technical and organizational measures required to ensure the protection of personal data during automated processing, i.e. in systems or programs.

In the case of the involvement of processors, these must also be checked for compliance with data security (Art. 28 GDPR).

The European General Data Protection Regulation (GDPR) contains requirements in Article 32 (1) GDPR that personal data must be processed securely using adequate technical and organizational measures. The implementation of the protection objectives (= measures) is left to the controller, *"taking into account the state of the art, the implementation costs and the nature, scope, circumstances and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons"* (Art. 32 GDPR).

The assessment of the adequate level of protection shall, in particular, take into account the risks associated with the processing, in particular through destruction, loss or alteration, whether accidental or unlawful, or unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed.

For automated processing (i.e., primarily via hardware and software), the GDPR lists various control areas, each of which contains different sub-items:

(6) Pseudonymization and encryption wherever possible
(7) Confidentiality
(8) Integrity
(9) Availability and resilience
(10) Procedures for regular review, assessment and evaluation

According to the wording of the law, the above-mentioned control areas are not directly applicable to non-automated processing of personal data. However, it is recommended that data security be organized along the lines of the control areas for the best possible protection in these cases as well.

2 Organizational

ECHO PRM GmbH ensures written documentation of the current level of data protection and provides written instructions to employees in the form of work instructions, guidelines and fact sheets for compliance. The employees involved in data processing are obligated to maintain confidentiality in accordance with Art. 28 para. 3 p. 2 lit. b), 29, 32 para. 4 DSGVO.

Some of the safeguards in the following checklist that relate to this area are not shown separately because they either fall under the responsibility of processors and are therefore regulated and audited separately, or because not all details are to be published for reasons of confidentiality.

3 Safeguarding measures

The following points describe the technical and organizational measures operated by ECHO PRM GmbH.

4 Pseudonymization and encryption (Art. 32 para. 1 lit. a) DSGVO)

Wherever possible, personal data is processed exclusively in pseudonymized form (i.e., without direct identifiability of a data subject). In addition, data should be sent or stored exclusively in encrypted form wherever possible. The principle of proportionality applies here.

5 Confidentiality (Art. 32 (1) (b) GDPR)

5.1.1 Access control

Access control comprises measures suitable for preventing unauthorized persons from gaining access to data processing systems with which personal data are processed or used:

Measures	Comment
The distribution rooms of the building services are secured against unauthorized access.	
There are safeguards against robberies.	
Adequate non-machine access controls to the building exist.	
The network components are located in designated access-controlled rooms.	
The access control protective measures that have been set up are regularly subjected to a thorough test to determine whether they still fulfill the desired protective purpose.	

5.1.2 Access control

Measures suitable for preventing data processing systems from being used by unauthorized persons:

Measures	Comment
There is a formal approval process for which systems and applications containing personal data must go through before they are allowed network access.	
The WLAN is secured against unauthorized access.	

5.1.3 Access control

Measures that ensure that those authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, modified or removed without authorization during processing, use and after storage.

Measures	Comment
Users shall ensure that their DP equipment, if unattended, is adequately protected.	
The principle of the tidy desk and the empty screen is lived (Clean Desk Policy).	
There are instructions on how to handle media (including written or printed paper) that is no longer needed.	
The disposal or further use of devices equipped with storage media is regulated.	

5.1.4 Separation requirement

Measures to ensure that data collected for different purposes can be processed separately.

Measures	Comment
Personal data on the systems are logically separated from each other (different data records in a uniform database are marked according to their purpose (software-based distinguishability)).	
The systems used in the company are multi-client capable.	
Multi-client capability for the processes affected by this is implemented throughout.	
Office, development, test and active systems are located in clearly separated network segments, where possible even physically separated from each other.	

6 Integrity (Art. 32 (1) b) GDPR)

6.1.1 Transfer control

Measures to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transmission or while being transported or stored on data media, and that it is possible to verify and establish to which entities personal data are intended to be transmitted by data transmission equipment.

Measures	Comment
All persons involved in the processing/use of personal data are obliged to observe confidentiality.	
All new employees are given information on data protection when they commit to confidentiality.	
Employees who process/use personal data have been trained in data protection-compliant behavior in the workplace through data protection training.	
It is ensured that data is only transmitted to the addressees specified by the customer or to the correct addressees according to the intended purpose.	
When passing on data, the possibilities of anonymization/pseudonymization are used as far as possible.	

6.1.2 Input control

Measures to ensure that it is possible to check and establish retrospectively whether and by whom personal data have been entered into data processing systems, modified or removed.

Measures	Comment
The logged data is subject to strict purpose limitation.	
The logged data is protected against unauthorized viewing or manipulation.	
Digital signature methods are used for tamper detection.	

7 Availability and resilience (Art. 32(1)(b) and (c) GDPR)

Measures to ensure that personal data is protected against accidental destruction or loss and can be quickly recovered in the event of a physical or technical incident.

Measures	Comment
The power supply lines run underground.	
An early warning system with automatic fire detectors is installed.	
The fire alarm system is maintained on a regular basis.	

There are enough suitable fire extinguishers and the right extinguishing agent in use, and attention is paid to uniformity.	
There is regular maintenance and inspection of smoke detectors and hand-held fire extinguishers.	
Regular backups are performed.	
The backups are encrypted.	
Antivirus software is used and are always kept up to date	
An IDS (intrusion detection system) or IPS (intrusion prevention system) is used.	

8 Procedures for regular review, assessment and evaluation (Art. 25(1) GDPR; Art. 32(1)(d) GDPR)

8.1.1 Organizational safety criteria

Organizational security describes all organizational measures (instructions, procedures, etc.) to ensure and improve security.

Measures	Comment
A data protection management system (DSMS) has been introduced and contains the most important data protection requirements and a comprehensive structure for mapping data protection measures.	
An external data protection officer was appointed voluntarily	
Regular education and sensitization of employees and managers are carried out.	

8.1.2 Order control

Measures to ensure that personal data processed on behalf of the client can only be processed in accordance with the client's instructions.

Employees who have access to the systems as administrators have all been instructed with regard to data protection, are obligated to maintain confidentiality, and have accepted corresponding confidentiality and non-disclosure agreements as part of their employment contract.

If ECHO PRM GmbH uses contractors for data processing, certain requirements will be implemented. This includes ensuring the technical-organizational measures of the contractors within the meaning of Art. 28 DSGVO and Art. 32 para. 1 DSGVO.

The prerequisite for entering into a commissioned processing agreement is, in principle, a legal basis. For a contract for commissioned data processing pursuant to Art. 28 (3) DSGVO, all required measures and specifications must be complied with.

Measures	Comment
Processors are fully bound by contract.	