Vertrag über die Verarbeitung von Daten im Auftrag

Geltungsbereich: FP Digital Business Solutions GmbH

Zwischen

- Auftraggeber -

und

FP Digital Business Solutions GmbH
Barbara-McClintock-Str. 11
12489 Berlin

- Auftragnehmer –

1 Allgemeines

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz- Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

(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 des Auftrags

Der Auftragnehmer stellt für den Auftraggeber folgenden Gegenstand zur Verfügung:

☐ **FP SIGN**

Gegenstand der Verarbeitung ist die elektronische Erstellung, Übermittlung, Unterzeichnung und Archivierung von Dokumenten mittels der Signaturlösung FP Sign. Dabei werden insbesondere personenbezogene Daten verarbeitet, die zur Identifizierung der unterzeichnenden Personen sowie zur Durchführung und Dokumentation des Signaturprozesses erforderlich sind.

Zweck der Verarbeitung ist die rechtssichere Abwicklung digitaler Signaturvorgänge, einschließlich der Authentifizierung der Unterzeichner, der Sicherstellung der Integrität und Nachvollziehbarkeit der Dokumente sowie der Bereitstellung eines revisionssicheren Nachweises über den Abschluss der Signatur. Die Verarbeitung dient zudem der Effizienzsteigerung und Digitalisierung von Geschäftsprozessen.

☐ **FP eBO Online**

Im Rahmen des ERV-Portals erfolgt die Verarbeitung personenbezogener Daten zur Bereitstellung, Durchführung und Absicherung des elektronischen Rechtsverkehrs. Gegenstand der Verarbeitung ist insbesondere die Entgegennahme, Übermittlung und Speicherung von Dokumenten sowie die damit verbundenen Kommunikations- und Protokolldaten.

Die Verarbeitung dient dem Zweck, eine rechtskonforme, sichere und nachvollziehbare elektronische Kommunikation zwischen den beteiligten Parteien zu gewährleisten. Dies umfasst insbesondere die Authentifizierung der Nutzer, die Sicherstellung der Integrität und Vertraulichkeit übermittelter Inhalte sowie die Dokumentation von Transaktionen zur Erfüllung gesetzlicher Nachweispflichten.

☐ **FP Justiz Connect (eBO Edition)**

Das FP Justiz Connect (eBO Edition) dient der technischen Abwicklung und Steuerung elektronischer Kommunikationsprozesse, insbesondere im Bereich digitaler Nachrichtenübermittlung mit der bestehenden E-Mail-Infrastruktur beim Auftraggeber. Gegenstand der Verarbeitung ist die Erfassung, Weiterleitung und Protokollierung der zur Durchführung dieser Kommunikationsdienste erforderlichen Daten.

Die Verarbeitung dient dem Zweck, eine rechtskonforme, sichere und nachvollziehbare elektronische Kommunikation zwischen den beteiligten Parteien zu gewährleisten. Dies umfasst insbesondere die Authentifizierung der Nutzer, die Sicherstellung der Integrität und Vertraulichkeit übermittelter Inhalte sowie die Dokumentation von Transaktionen zur Erfüllung gesetzlicher Nachweispflichten.

☐ **FP Justiz Connect (beBPO Edition)**

Das FP Justiz Connect (bePBO Edition) dient der technischen Abwicklung und Steuerung elektronischer Kommunikationsprozesse, insbesondere im Bereich digitaler Nachrichtenübermittlung mit der bestehenden E-Mail-Infrastruktur beim Auftraggeber. Gegenstand der Verarbeitung ist die Erfassung, Weiterleitung und Protokollierung der zur Durchführung dieser Kommunikationsdienste erforderlichen Daten.

Die Verarbeitung dient dem Zweck, eine rechtskonforme, sichere und nachvollziehbare elektronische Kommunikation zwischen den beteiligten Parteien zu gewährleisten. Dies umfasst insbesondere die Authentifizierung der Nutzer, die Sicherstellung der Integrität und Vertraulichkeit übermittelter Inhalte sowie die Dokumentation von Transaktionen zur Erfüllung gesetzlicher Nachweispflichten.

Die Art der personenbezogenen Daten und die Kategorien der betroffenen Personen werden in der **Anlage 1** weiter beschrieben. Die **Anlage 1** ist Bestandteil dieser Vereinbarung zur Auftragsverarbeitung.

3 Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DS-GVO DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 5 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte

gegenüber dem Auftragnehmer geltend machen.

(3) Der Auftraggeber hat das Recht, ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung (Kenntnisnahme bei Wartungsarbeiten an den eingesetzten IT-Systemen) gegenüber dem Auftragnehmer zu erteilen. Weisungen können in Textform (z.B. E-Mail) erfolgen.

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

(5) Der Auftraggeber kann weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt werden sollen, werden diese unter Kontaktdaten benannt. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer in Textform mitteilen.

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

(7) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

4 Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten 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.

(2) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

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

(4) 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.

(5) 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 so lange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

(6) Die Verarbeitung von Daten im Auftrag des Auftraggebers außerhalb von Betriebsstätten des Auftragnehmers oder Subunternehmern ist ausgeschlossen. Nur in besonderen Ausnahmefällen, wie z.B. Pandemien, darf diese nur mit schriftlicher Zustimmung des Auftraggebers und zusätzlicher Telearbeitsregelungen und Verpflichtungen der Beschäftigen der Auftragsnehmers erfolgen.

(7) Der Auftragnehmer wird die Daten, die er im Auftrag für den Auftraggeber verarbeitet, getrennt von anderen Daten verarbeiten. Eine physische Trennung ist nicht zwingend erforderlich.

(8) Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Sofern weisungsempfangsberechtigte Personen benannt werden sollen,

werden diese unter Kontaktdaten benannt. Für den Fall, dass sich die weisungsempfangsberechtigten Personen beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Auftraggeber in Textform mit- teilen.

5 Datenschutzbeauftragter des Auftragnehmers

(1) Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt.

Datenschutzbeauftragte: Norbert Bornemann, Danny Lindner

Kontakt: datenschutz@fp-dbs.com

6 Meldepflichten des Auftragnehmers

(1) 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. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.

(2) 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.

(3) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich, spätestens aber binnen 48 Stunden ab Kenntnis des Zugriffs mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

7 Mitwirkungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen von Ziff. 11 dieses Vertrages.

(2) Der Auftragnehmer unterstützt bei Bedarf den Auftraggeber bei der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten. Er teilt dem Auftraggeber die erforderlichen Angaben auf Anfrage mit.

(3) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

8 Kontrollbefugnisse

(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 im erforderlichen Umfang zu kontrollieren.

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

(3) Der Auftraggeber kann Informationen über die vom Auftragnehmer verwendeten Datenverarbeitungssysteme anfordern.

(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) 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.

9 Unterauftragsverhältnisse

Der Auftragnehmer bedient sich derzeit keiner Unterauftragnehmer und beabsichtigt nach derzeitigem Stand auch künftig keinen Einsatz von Unterauftragnehmern. Für den Fall, dass dennoch Unterauftragnehmer eingesetzt werden, sind die nachfolgenden Bestimmungen verbindlich zu beachten.

(1) Die Beauftragung von Subunternehmern ist nur mit Zustimmung des Auftraggebers im Einzelfall zugelassen. Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Der Auftragsverarbeiter reicht den Antrag für die gesonderte Genehmigung schriftlich oder in Textform mindestens vier Wochen vor der Beauftragung des betreffenden Subunternehmers zusammen mit den Informationen ein, die die Verantwortliche benötigt, um über die Genehmigung zu entscheiden.

(2) Die Zustimmung ist nur möglich, wenn dem Subunternehmer vertraglich mindestens Datenschutzpflichten auferlegt wurden, die den in diesem Vertrag vereinbarten vergleichbar sind. Der Vertrag mit dem Subunternehmer muss berücksichtigen, dass es sich um eine Subbeauftragung im Auftrag handelt. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmer und Subunternehmer.

(3) Die Rechte des Auftraggebers müssen auch gegenüber dem Subunternehmer wirksam ausgeübt werden können. Insbesondere muss der Auftraggeber berechtigt sein, in dem hier festgelegten Umfang Kontrollen auch bei Subunternehmern durchzuführen oder durch Dritte durchführen zu lassen.

(4) Der Einsatz von Subunternehmern in Drittländern ist nur zulässig, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. SCC, Angemessenheitsbeschluss, TIA).

Der Auftragsverarbeiter darf mit der Datenübermittlung in das Drittland erst beginnen, wenn alle Voraussetzungen schriftlich dokumentiert und nachweisbar erfüllt sind.

(5) Der Auftragsverarbeiter führt eine Liste der Subunternehmer und stellt dem Verantwortlichen auf Anfrage Nachweise zur Verfügung. Der Verantwortliche kann die Einhaltung prüfen.

(6) Der Auftragsverarbeiter haftet nach Maßgabe der gesetzlichen Bestimmungen der DSGVO dafür, dass die von ihm eingesetzten Subunternehmer die datenschutzrechtlichen Pflichten gemäß DSGVO und diesem Vertrag einhalten. Die Beauftragung eines Subunternehmers entbindet den Auftragsverarbeiter nicht von seiner Verantwortlichkeit gegenüber dem Verantwortlichen.

10 Vertraulichkeitsverpflichtung

(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.

(2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutz- rechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und zur Vertraulichkeit verpflichtet hat. Der Auftragnehmer sichert ferner zu, dass er ins- besondere die bei der Durchführung der Arbeiten tätigen Beschäftigten zur Vertraulichkeit verpflichtet hat und diese über die Weisungen des Auftraggebers informiert hat.

(3) Die Verpflichtung der Beschäftigten nach Absatz 2 sind dem Auftraggeber auf Anfrage nachzuweisen.

11 Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützten. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

(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 Maß- nahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maß- nahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

(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.

12 Geheimhaltungspflichten

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

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

13 Vergütung

Die Vergütung des Auftragnehmers wird gesondert vereinbart.

14 Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung daranzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

(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.

Der Auftragnehmer wird, die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren.

15 Dauer des Auftrags

(1) Der Vertrag beginnt mit Unterzeichnung und wird auf unbestimmte Zeit geschlossen.

(2) Er ist mit einer Frist von drei Monaten zum Quartalsende kündbar.

(3) 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.

16 Beendigung

(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, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt. Für Datenträger gilt, dass diese im Falle einer vom Auftraggeber gewünschten Löschung zu vernichten sind, wobei mindestens die Sicherheitsstufe 3 der DIN 66399 einzuhalten ist; die Vernichtung ist dem Auftraggeber unter Hinweis auf die Sicherheitsstufe gemäß DIN 66399 nachzuweisen.

(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.

17 Kontaktdaten

	Auftraggeber	Auftragnehmer
Datenschutzbeauftragter		Siehe Punkt Datenschutzbeauftragter des Auftragnehmers
Technisch Verantwortlicher		Für FP SIGN, ERV Portal und Mentana Gateway: Jürgen Ludyga j.ludyga@fp-dbs.com
Weisungsberechtigter (Auftragsgeber) / Weisungsempfänger (Auftragsnehmer)		Für FP SIGN, ERV Portal und Mentana Gateway: Sonya Kapoor s.kapoor@fp-dbs.com

18 Schlussbestimmungen

(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.

(2) Für Nebenabreden ist die Schriftform erforderlich.

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

_____, den	_____	Berlin
Ort	Datum	Ort

Sonya Kapoor-Herme

_____	FP Digital Business Solutions GmbH
- Auftraggeber -	- Auftragnehmer –

Anlage 1: Datenarten und Kategorien betroffener Personen (Art. 28 DSGVO)

1 Datenarten (Art der verarbeiteten personenbezogenen Daten)

- ☒ Stammdaten (z.B. Name, Anschrift, Geburtsdatum)
- ☒ Kontaktdaten (z.B. Telefon, E-Mail)
- ☒ Vertrags- und Auftragsdaten
- ☒ Abrechnungs- und Zahlungsdaten
- ☒ Kommunikationsdaten
- ☒ Nutzungs- und Metadaten (z. B. Logfiles, IP-Adressen)
- ☒ Inhaltsdaten (Dokumente, Dateien)
- ☐ Standortdaten
- ☐ Technische Gerätedaten
- ☐ Bild- und Tonaufnahmen
- ☐ Gesundheitsdaten
- ☐ Biometrische Daten
- ☐ Sonstige Datenarten: _____

2 Kategorien betroffener Personen

- ☒ Kunden / Auftraggeber
- ☒ Interessenten
- ☐ Nutzer von Online-Diensten
- ☐ Beschäftigte / Mitarbeiter
- ☐ Bewerber
- ☐ Lieferanten / Dienstleister
- ☐ Ansprechpartner bei Geschäftspartnern
- ☒ Mitglieder / Teilnehmer
- ☐ Patienten / Klienten
- ☐ Minderjährige
- ☐ Sonstige betroffene Personen: _____

Anlage 2: Technische und organisatorische Maßnahmen FP DBS GmbH - Sicherheit der Verarbeitung (Art. 32 DS-GVO)

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

- **Zutrittskontrolle**
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;

  ☒ Alarmanlage

  ☒ Absicherung von Gebäudeschächten

  ☒ Automatisches Zugangskontrollsystem

  ☒ Chipkarten-/Transponder-Schließsystem

  ☒ Schließsystem mit Codesperre

  ☒ Manuelles Schließsystem

  ☒ Videoüberwachung der Zugänge

  ☒ Lichtschranken / Bewegungsmelder

  ☒ Sicherheitsschlösser

  ☒ Schlüsselregelung (Schlüsselausgabe etc.)

  ☒ Personenkontrolle beim Pförtner / Empfang

  ☒ Protokollierung der Besucher

  ☒ Sorgfältige Auswahl von Reinigungspersonal

  ☒ Sorgfältige Auswahl von Wachpersonal

  ☒ Tragepflicht von Berechtigungsausweisen

- **Zugangskontrolle**
  Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;

  ☒ Zuordnung von Benutzerrechten

  ☒ Erstellen von Benutzerprofilen

  ☒ Passwortvergabe

  ☒ Authentifikation mit Benutzername / Passwort

  ☒ Zuordnung von Benutzerprofilen zu IT-Systemen

  ☒ Gehäuseverriegelungen

  ☒ Einsatz von VPN-Technologie

  ☒ Sperren von externen Schnittstellen (USB etc.)

  ☒ Sicherheitsschlösser

  ☒ Schlüsselregelung (Schlüsselausgabe etc.)

  ☒ Einsatz von Intrusion-Detection-Systemen

☒ Verschlüsselung von mobilen Datenträgern

☒ Verschlüsselung von Smartphone-Inhalten

☒ Einsatz von Anti-Viren-Software

☒ Verschlüsselung von Datenträgern in Laptops / Notebooks

☒ Einsatz einer Hardware-Firewall

☒ Einsatz einer Software-Firewall (Clients)

- **Zugriffskontrolle**
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;

  ☒ Erstellen eines Berechtigungskonzepts

  ☒ Verwaltung der Rechte durch Systemadministrator

  ☒ Anzahl der Administratoren auf das „Notwendigste“ reduziert

  ☒ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel

  ☒ Protokollierung von Zugriffen auf Anwendungen, insb. bei der Eingabe, Änderung und Löschung von Daten

  ☒ Sichere Aufbewahrung von Datenträgern

  ☒ physische Löschung von Datenträgern vor Wiederverwendung

  ☒ ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)

  ☒ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)

  ☒ Protokollierung der Vernichtung

  ☒ Verschlüsselung von Datenträgern

- **Trennungskontrolle**
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;

  ☒ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern

  ☒ Logische Mandantentrennung (softwareseitig)

  ☒ Erstellung eines Berechtigungskonzepts

  ☒ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden

  ☒ Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System

  ☒ Festlegung von Datenbankrechten

  ☒ Trennung von Produktiv- und Testsystem

- **Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)**
  Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern

diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

☒ Pseudonymisierung von Personaldaten (Personalnummern)

☒ Pseudonymisierung von Kundendaten (Kundennummern)

☒ Pseudonymisierung in Datenbankanwendungen (spezielle Tabellen für Personenbezogenen Daten und Informationen

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

- Weitergabekontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

  ☒ Einrichtungen von Standleitungen bzw. VPN-Tunneln

  ☒ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form

  ☒ E-Mail-Verschlüsselung

  ☒ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen

  ☒ Beim physischen Transport: sichere Transportbehälter/-verpackungen

  ☒ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –Fahrzeugen

- **Eingabekontrolle**
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

  ☒ Protokollierung der Eingabe, Änderung und Löschung von Daten

  ☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

  ☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

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

- Verfügbarkeitskontrolle
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;

- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

  ☒ Unterbrechungsfreie Stromversorgung (USV)

  ☒ Klimaanlage in Serverräumen

  ☒ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen

  ☒ Schutzsteckdosenleisten in Serverräumen

  ☒ Feuer- und Rauchmeldeanlagen

  ☒ Feuerlöschgeräte in Serverräumen

- ☒ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☒ Erstellen eines Backup- & Recovery-Konzeptes
- ☒ Testen von Datenwiederherstellung
- ☒ Erstellen eines Notfallplans
- ☒ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ☒ Serverräume nicht unter sanitären Anlagen
- ☒ In Hochwassergebieten: Serverräume über der Wassergrenze

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

- ☒ IT-Sicherheitsmanagementsystem-System im Einsatz (ISMS gem. BSI-Grundschutz)
- ☒ Überprüfung durch interne SiBe u. DSB (jährlich)
- ☒ Incident-Response-Managementsystem im Einsatz
- ☒ Überprüfung durch interne SiBe u. DSB (jährlich)

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

- ☒ Bei Anschaffung von Geräten und Software wird die Möglichkeit Privacy by Design / Privacy by Default als Auswahlkriterium mitberücksichtigt
- ☒ Bei der Einrichtung wird speziell nach Einstellmöglichkeiten gesucht um Privacy by Design / Privacy by Default umzusetzen