Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO

digitastic.plus Gesellschaft für digitale Lösungen mbH & CO. KG, nachstehend “Auftragsverarbeiter“, und die Gegenpartei, die diesen Bedingungen zustimmt ("Verantwortlicher"), haben eine Vereinbarung zur Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO geschlossen.

Präambel

Zwischen dem Verantwortlichen und dem Auftragsverarbeiter besteht ein Auftragsverhältnis im Sinne des Art. 28 der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, „**DSGVO**“).

Dieser Auftragsverarbeitungsvertrag einschließlich aller Anlagen (nachfolgend gemeinsam als „**Vereinbarung**“ bezeichnet) konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien aus dem zugrundeliegenden Vertrag, der Leistungsvereinbarung und/oder Auftragsbeschreibung einschließlich aller Anlagen (nachfolgend gemeinsam als „**Hauptvertrag**“ bezeichnet). Sofern Bezug auf die Regelungen des Bundesdatenschutzgesetzes (nachfolgend „**BDSG**“) genommen wird, so ist damit das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 in der zum Zeitpunkt ab dem 25. Mai 2018 geltenden Fassung gemeint.

Der Auftragsverarbeiter verpflichtet sich gegenüber dem Verantwortlichen zur Erfüllung des Hauptvertrages und dieser Vereinbarung nach Maßgabe der folgenden Bestimmungen:

§ 1 Anwendungsbereich und Begriffsbestimmungen

(1) Die nachfolgenden Bestimmungen finden Anwendung auf alle Leistungen der Auftragsverarbeitung im Sinne des Art. 28 DSGVO, die der Auftragsverarbeiter auf Grundlage des Hauptvertrages gegenüber dem Verantwortlichen erbringt.

(2) Sofern in dieser Vereinbarung der Begriff „Datenverarbeitung“ oder „Verarbeitung“ von Daten benutzt wird, ist darunter allgemein die Verwendung von personenbezogenen Daten zu verstehen. Datenverarbeitung oder das Verarbeiten von Daten bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(3) Auf die weiteren Begriffsbestimmungen in Art. 4 DSGVO wird verwiesen.

§ 2 Gegenstand und Dauer der Datenverarbeitung

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag und nach Weisung des Verantwortlichen.

(2) Gegenstand des Auftrags ist die Nutzung von Lösung im Bereich der Beleg- und Datenverarbeitung in der Steuerberatung im Rahmen des mit dem Auftragsverarbeiter vereinbarten Umfangs, gemäß dem Hauptvertrag.

(3) Die Dauer dieser Vereinbarung ist an die Dauer des ihr zugrundeliegenden Hauptvertrags geknüpft. Diese Vereinbarung endet automatisch mit Beendigung und vollständiger Abwicklung des Hauptvertrags, ohne dass es einer Kündigung bedarf. Das beiderseitige Recht zur außerordentlichen, fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

§ 3 Art und Zweck der Datenverarbeitung

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter ergeben sich aus dem Hauptvertrag.

§ 4 Kategorien betroffener Personen

Die Kategorien der durch den Umgang mit den personenbezogenen Daten im Rahmen dieser Vereinbarung betroffenen Personen umfasst Testkunden sowie Bestandskunden.

§ 5 Art der personenbezogenen Daten

Von der Auftragsverarbeitung sind folgende Datenarten betroffen:

- Personenstammdaten (Name, Anrede, Titel/akademischer Grad, Geburtsdatum)
- Kontaktdaten (E-Mail-Adresse, Telefonnummer, Anschrift)
- Vertragsdaten (Vertragsdetails, Leistungen, Kundennummer)
- Kundenhistorie
- Vertragsabrechnungsdaten und Zahlungsinformationen (Rechnungsdetails, Bankverbindung, Kreditkarteninformationen)
- Daten aus gescannten Dokumenten insbesondere Belegen

§ 6 Rechte und Pflichten des Verantwortlichen

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie zur Wahrung der Rechte der Betroffenen ist allein der Verantwortliche zuständig und somit für die Verarbeitung Verantwortlicher im Sinne des Art. 4 Nr.7 DSGVO.

(2) Der Verantwortliche ist berechtigt, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Mündliche Weisungen sind auf Verlangen des

Verantwortlichen unverzüglich vom Auftragsverarbeiter schriftlich oder in Textform (z.B. per E-Mail) zu bestätigen.

(3) Weisungen des Verantwortlichen müssen in Einklang mit gesetzlichen Bestimmungen erfolgen. Der Verantwortliche wahrt durch eigene Maßnahmen die Einhaltung gesetzlicher Bestimmungen. Wenn der Verantwortliche den Auftragsverarbeiter zur Löschung von Daten anweist, die einer gesetzlichen Aufbewahrungsfrist unterliegen, bestätigt der Verantwortliche dem Auftragsverarbeiter zusammen mit der Weisungserteilung, dass auf anderem Wege für die Einhaltung der Aufbewahrungsfristen Sorge getragen wird.

(4) Soweit es der Verantwortliche für erforderlich hält, können weisungsberechtigte Personen benannt werden. Diese wird der Verantwortliche dem Auftragsverarbeiter schriftlich oder in Textform mitteilen. Für den Fall, dass sich diese weisungsberechtigten Personen bei dem Verantwortlichen ändern, wird dies dem Auftragsverarbeiter unter Benennung der jeweils neuen Person schriftlich oder in Textform mitgeteilt.

(5) Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter festgestellt werden.

§ 7 Pflichten des Auftragsverarbeiters

(1) Datenverarbeitung

Der Auftragsverarbeiter wird personenbezogene Daten ausschließlich nach Maßgabe dieser Vereinbarung und/oder des zugrundeliegenden Hauptvertrages sowie nach den Weisungen des Verantwortlichen zu verarbeiten.
Außerhalb der Weisungen des Verantwortlichen ist der Auftragsverarbeiter zur Verarbeitung der personenbezogenen Daten des Verantwortlichen berechtigt, soweit er hierzu durch das Recht der Europäischen Union oder ihrer Mitgliedstaaten verpflichtet ist. Der Auftragsverarbeiter teilt dem Verantwortlichen diese rechtlichen Anforderungen vor Verarbeitung mit, wenn nicht das betreffende Recht eine solche Mitteilung aufgrund eines wichtigen öffentlichen Interesses verbietet. Dem Auftragsverarbeiter ist zudem gestattet, die personenbezogenen Daten des Verantwortlichen zu anonymisieren und in anonymisierter Form für eigene Zwecke zu verarbeiten

(2) Betroffenenrechte

a. Der Auftragsverarbeiter wird den Verantwortlichen bei der Erfüllung der Rechte der Betroffenen, insbesondere im Hinblick auf Berichtigung, Einschränkung der Verarbeitung und Löschung, Benachrichtigung und Auskunftserteilung, im Rahmen seiner Möglichkeiten unterstützen. Sollte der Auftragsverarbeiter die in § 5 dieser Vereinbarung genannten personenbezogenen Daten im Auftrag des Verantwortlichen verarbeiten und sind diese Daten Gegenstand eines Verlangens auf Datenportabilität gem. Art. 20 DSGVO, wird der Auftragsverarbeiter dem Verantwortlichen den betreffenden Datensatz innerhalb einer

angemessen gesetzten Frist, im Übrigen innerhalb von sieben Arbeitstagen, in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung stellen.

b. Der Auftragsverarbeiter hat auf Weisung des Verantwortlichen die in § 5 dieser Vereinbarung genannten personenbezogenen Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder die Verarbeitung einzuschränken. Das Gleiche gilt, wenn diese Vereinbarung eine Berichtigung, Löschung oder Einschränkung der Verarbeitung von Daten vorsieht.

c. Soweit sich eine betroffene Person unmittelbar an den Auftragsverarbeiter zwecks Berichtigung, Löschung oder Einschränkung der Verarbeitung der in § 5 dieser Vereinbarung genannten personenbezogenen Daten wendet, wird der Auftragsverarbeiter dieses Ersuchen binnen einer angemessen Frist nach Erhalt an den Verantwortlichen weiterleiten.

(3) Kontrollpflichten

a. Der Auftragsverarbeiter stellt durch geeignete Kontrollen sicher, dass die im Auftrag verarbeiteten personenbezogenen Daten ausschließlich nach Maßgabe dieser Vereinbarung und/oder des Hauptvertrages und/oder den entsprechenden Weisungen verarbeitet werden.

b. Der Auftragsverarbeiter wird sein Unternehmen und seine Betriebsabläufe so gestalten, dass die Daten, die er im Auftrag des Verantwortlichen verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind.

c. Der Auftragsverarbeiter bestätigt, dass er gem. Art. 37 DSGVO und, sofern anwendbar, gemäß § 38 BDSG einen Datenschutzbeauftragten bestellt hat und die Einhaltung der Vorschriften zum Datenschutz und zur Datensicherheit unter Einbeziehung des Datenschutzbeauftragten überwacht. Datenschutzbeauftragter des Auftragsverarbeiters ist derzeit:

Iryna Krasna
Firma Isico Datenschutz GmbH
Am Hamburger Bahnhof 4, 10557 Berlin

(4) Informationspflichten

a. Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich darauf aufmerksam machen, wenn eine von dem Verantwortlichen erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

b. Der Auftragsverarbeiter wird den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützen. Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen im Rahmen des Erforderlichen und Zumutbaren auf Verlangen bei der Erfüllung der Informationspflichten gegenüber der jeweils zuständigen

Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen nach Art. 33 und 34 DSGVO. Der Aufwand des Auftragsverarbeiters für diese Unterstützung des Verantwortlichen ist von dem Verantwortlichen zu vergüten, wenn nicht der Auftragsverarbeiter die Verletzung des Schutzes personenbezogener Daten zu vertreten hat.
Der Auftragsverarbeiter unterstützt den Auftragnehmer unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen im Rahmen des Erforderlichen und Zumutbaren auf Verlangen bei Datenschutzfolgenabschätzungen iSd. Art. 35 DSGVO. Im Falle der Notwendigkeit einer vorherigen Konsultation der zuständigen Aufsichtsbehörde iSd. Art. 36 DSGVO unterstützt der Auftragnehmer den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen im Rahmen des Erforderlichen und Zumutbaren auf Verlangen auch hierbei. Der Aufwand des Auftragsverarbeiters für diese Unterstützung des Verantwortlichen ist von dem Verantwortlichen zu vergüten.

(5) Ort der Datenverarbeitung

Die Verarbeitung der Daten findet entsprechend § 146 Abs. 2 AO im Gebiet der Bundesrepublik Deutschland statt.

(6) Löschung der personenbezogenen Daten nach Auftragsbeendigung

Nach Beendigung des Hauptvertrages wird der Auftragsverarbeiter alle im Auftrag verarbeiteten personenbezogenen Daten nach Wahl des Verantwortlichen entweder löschen oder zurückgeben, sofern der Löschung dieser Daten keine gesetzlichen Aufbewahrungspflichten des Auftragsverarbeiters entgegenstehen. Die datenschutzgerechte Löschung ist zu dokumentieren und gegenüber dem Verantwortlichen auf Anforderung zu bestätigen.

(7) Verpflichtung zur Wahrung des Berufsgeheimnisses

§ 8 Kontrollrechte des Verantwortlichen

(1) Der Verantwortliche ist berechtigt, nach rechtzeitiger vorheriger Anmeldung von min. 7 Tagen zu den üblichen Geschäftszeiten ohne Störung des Geschäftsbetriebes des Auftragsverarbeiters oder Gefährdung der Sicherheitsmaßnahmen für andere Verantwortliche und auf eigene Kosten, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang selbst oder durch einen von ihm auf eigene Kosten beauftragten, zur Verschwiegenheit gegenüber Dritten verpflichteten Prüfer ausüben, sofern es sich nicht um einen Wettbewerber des Auftragnehmers oder ein mit einem solchen verbundenes Unternehmen handelt.. Die Kontrollen können auch durch Zugriff auf vorhandene branchenübliche Zertifizierungen des Auftragsverarbeiters aktuelle Testate oder Berichte einer unabhängigen Instanz (wie z.B. Wirtschaftsprüfer, externer Datenschutzbeauftragter, Revisor oder externer Datenschutzauditor) oder Selbstauskünfte

durchgeführt werden. Der Auftragsverarbeiter wird die notwendige Unterstützung zur Durchführung der Kontrollen anbieten.

(2) Der Auftragsverarbeiter wird den Verantwortlichen über die Durchführung von Kontrollmaßnahmen der Aufsichtsbehörde informieren, soweit die Maßnahmen oder Datenverarbeitungen betreffen können, die der Auftragsverarbeiter für den Verantwortlichen erbringt.

§ 9 Unterauftragsverhältnisse

(1) Der Verantwortliche ermächtigt den Auftragsverarbeiter weitere Auftragsverarbeiter gemäß den nachfolgenden Absätzen in § 9 dieser Vereinbarung in Anspruch zu nehmen. Diese Ermächtigung stellt eine allgemeine schriftliche Genehmigung i. S. d. Art. 28 Abs. 2 DSGVO dar.

(2) Der Auftragsverarbeiter arbeitet derzeit bei der Erfüllung des Auftrags mit den in der **Anlage 2** benannten Unterauftragnehmern zusammen, mit deren Beauftragung sich der Verantwortliche einverstanden erklärt.

(3) Der Auftragsverarbeiter ist berechtigt, weitere Auftragsverarbeiter zu beauftragen oder bereits beauftragte zu ersetzen. Der Auftragsverarbeiter wird den Verantwortlichen spätestens einen Monat vorab über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines weiteren Auftragsverarbeiters informieren. Der Verantwortliche kann gegen eine beabsichtigte Änderung Einspruch erheben.

(4) Der Einspruch gegen die beabsichtigte Änderung ist innerhalb von 2 Wochen nach Zugang der Information über die Änderung gegenüber dem Auftragsverarbeiter zu erheben. Im Fall des Einspruchs kann der Auftragsverarbeiter nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder einen alternativen weiteren Auftragsverarbeiter vorschlagen und mit dem Verantwortlichen abstimmen. Sofern die Erbringung der Leistung ohne die beabsichtigte Änderung dem Auftragsverarbeiter nicht zumutbar ist – etwa aufgrund von damit verbundenen unverhältnismäßigen Aufwendungen für den Auftragsverarbeiter – oder die Abstimmung eines weiteren Auftragsverarbeiters fehlschlägt, können der Verantwortliche und der Auftragsverarbeiter diese Vereinbarung sowie den Hauptvertrag mit einer Frist von einem Monat zum Monatsende kündigen.

(5) Bei Einschaltung eines weiteren Auftragsverarbeiters muss stets ein Schutzniveau, welches mit demjenigen dieser Vereinbarung vergleichbar ist, gewährleistet werden. Der Auftragsverarbeiter ist gegenüber dem Verantwortlichen für sämtliche Handlungen und Unterlassungen der von ihm eingesetzten weiteren Auftragsverarbeiter verantwortlich.

§ 10 Vertraulichkeit

(1) Der Auftragsverarbeiter ist bei der Verarbeitung von Daten für den Verantwortlichen zur Wahrung der Vertraulichkeit verpflichtet.

(3) Der Auftragsverarbeiter verpflichtet sich bei der Erfüllung des Auftrags nur Mitarbeiter oder sonstige Erfüllungsgehilfen einzusetzen, die auf die Vertraulichkeit im Umgang mit überlassenen personenbezogenen Daten verpflichtet und in geeigneter Weise mit den Anforderungen des Datenschutzes vertraut gemacht worden sind. Die Vornahme der Verpflichtungen wird der Auftragsverarbeiter dem Verantwortlichen auf Nachfrage nachweisen.

(4) Der Auftragnehmer verpflichtet sich und seine Mitarbeiter zur Wahrung des Berufsgeheimnisses der Rechtsanwälte und Steuerberater nach §§ 203 und 204 StGB (siehe Anlage 3). Auf die Belehrungen durch den Auftraggeber in Anlage 3 wird explizit hingewiesen

(5) Sofern der Verantwortliche anderweitigen Geheimnisschutzregeln unterliegt, wird er dies dem Auftragsverarbeiter mitteilen. Der Auftragsverarbeiter wird seine Mitarbeiter entsprechend den Anforderungen des Verantwortlichen auf diese Geheimnisschutzregeln verpflichten.

§ 11 Technische und organisatorische Maßnahmen

(1) Die in **Anlage 1** beschriebenen technischen und organisatorischen Maßnahmen werden als angemessen vereinbart. Der Auftragsverarbeiter kann diese Maßnahmen aktualisieren und ändern, vorausgesetzt dass das Schutzniveau durch solche Aktualisierungen und/oder Änderungen nicht wesentlich herabgesetzt wird.

(2) Der Auftragsverarbeiter beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung gemäß Art 32 i.V.m Art. 5 Abs. 1 DSGVO. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen. Er wird alle erforderlichen Maßnahmen zur Sicherung der Daten bzw. der Sicherheit der Verarbeitung, insbesondere auch unter Berücksichtigung des Standes der Technik, sowie zur Minderung möglicher nachteiliger Folgen für Betroffene ergreifen. Die zu treffenden Maßnahmen umfassen insbesondere Maßnahmen zum Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Maßnahmen, die die Kontinuität der Verarbeitung nach Zwischenfällen gewährleisten. Um stets ein angemessenes Sicherheitsniveau der Verarbeitung gewährleisten zu können, wird der Auftragsverarbeiter die implementierten Maßnahmen regelmäßig evaluieren und ggf. Anpassungen vornehmen.

§ 12 Haftung/ Freistellung

(1) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen gemäß den gesetzlichen Regelungen für sämtliche Schäden durch schuldhafte Verstöße gegen diese Vereinbarung sowie gegen die ihn treffenden gesetzlichen Datenschutzbestimmungen, die der Auftragsverarbeiter, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung verursachen. Eine Ersatzpflicht des Auftragsverarbeiters besteht nicht, sofern der Auftragsverarbeiter nachweist, dass er die ihm überlassenen Daten des Verantwortlichen ausschließlich nach den Weisungen des Verantwortlichen verarbeitet und seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus der DSGVO nachgekommen ist.

(2) Der Verantwortliche stellt den Auftragsverarbeiter von allen Ansprüchen Dritter und ersetzt ihm – unabhängig von einem Vertreten müssen und jeweils auf erstes Anfordern – sämtliche dem Auftragsverarbeiter in diesem Zusammenhang entstehenden Aufwendungen, Kosten und Schäden. Die Ersatzverpflichtung besteht insbesondere für sämtliche Aufwendungen des Auftragsverarbeiter für die Abwehr solcher Ansprüche bzw. Bußgelder, ob sich diese als begründet herausstellen oder nicht. Rechtsanwaltsvergütungen sind insoweit auf Basis eines angemessenen Stundensatzes zu erstatten. Es bestehen keine Zurückbehaltungsrechte des Verantwortlichen gegen die vorstehenden Freistellungs- und Ersatzverpflichtungen. Die Haftung des Auftragnehmers richtet sich nach dem Hauptvertrag.

§ 13 Sonstiges

(1) Im Falle von Widersprüchen zwischen den Bestimmungen in dieser Vereinbarung und den Regelungen des Hauptvertrages gehen die Bestimmungen dieser Vereinbarung vor.

(2) Änderungen und Ergänzungen dieser Vereinbarung setzen die beidseitige Zustimmung der Vertragsparteien voraus unter konkreter Bezugnahme auf die zu ändernde Regelung dieser Vereinbarung und sie bedürfen zu ihrer Rechtswirksamkeit der Textform; dies gilt auch für den Verzicht auf dieses Formerfordernis. Mündliche Nebenabreden bestehen nicht und sich auch für künftige Änderungen dieser Vereinbarung ausgeschlossen.

(3) Diese Vereinbarung unterliegt deutschem Recht unter Ausschluss des UN-Kaufrechts und aller internationaleren Kollisionsnormen. Gerichtsstand ist - soweit gesetzlich zulässig - Berlin.

(4) Sofern der Zugriff auf die Daten, die der Verantwortliche dem Auftragsverarbeiter zur Datenverarbeitung übermittelt hat, durch Maßnahmen Dritter (z.B. Maßnahmen eines Insolvenzverwalters, Beschlagnahme durch Finanzbehörden, etc.) gefährdet wird, hat der Auftragsverarbeiter den Verantwortlichen unverzüglich hierüber zu benachrichtigen.

(5) Sollte eine Bestimmung dieser Vereinbarung unwirksam oder nicht durchsetzbar sein oder werden, so bleiben die übrigen Bestimmungen dieser Vereinbarung hiervon unberührt. Die unwirksame oder nicht durchsetzbare Bestimmung ist durch eine wirksame und durchsetzbare Bestimmung zu ersetzen, welche dem Zweck der ersetzenden Bestimmung am nächsten kommt.

Anlagenverzeichnis

Anlage 1 Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung

Anlage 2 Unterauftragsverhältnisse gemäß § 9 der Vereinbarung zur Auftragsverarbeitung

Anlage 3 Vereinbarung über die Verpflichtung zur Wahrung des Berufsgeheimnisses nach §§ 203 und 204 StGB einschließlich Belehrung über die strafrechtlichen Folgen einer Pflichtverletzung
(§ 62a StBerG)

Anlage 1

Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung

Der Auftragsverarbeiter sichert zu, folgende technische und organisatorische Maßnahmen getroffen zu haben:

A. Maßnahmen zur Pseudonymisierung

Maßnahmen, die den unmittelbaren Personenbezug während der Verarbeitung in einer Weise reduzieren, dass nur mit Hinzuziehung zusätzlicher Informationen eine Zuordnung zu einer spezifischen betroffenen Person möglich ist. Die Zusatzinformationen sind dabei durch geeignete technische und organisatorische Maßnahmen von dem Pseudonym getrennt aufzubewahren.

Beschreibung der Pseudonymisierung:

Eine intern erstellte Kunden ID dient als grundlegende Maßnahme der Pseudonymisierung. Eine weitere direkte Pseudonymisierung können nicht vorgenommen werden. Passwörter müssten mindestens 7-stellig und 3 von 4 Kategorien (Großbuchstaben, Kleinbuchstaben, Zahlen oder Sonderzeichen) erfüllen. Diese werden verschlüsselt gespeichert. Es findet eine Randomisierung bei der Session Verwaltung statt. Als Standardhashwertfahren wird SHA-2 verwendet.

B. Maßnahmen zur Verschlüsselung

Maßnahmen oder Vorgänge, bei denen ein klar lesbarer Text / Information mit Hilfe eines Verschlüsselungsverfahrens (Kryptosystem) in eine unleserliche, das heißt nicht einfach interpretierbare Zeichenfolge (Geheimtext) umgewandelt wird:

Ein Zugriff kann nur durch das interne Netzwerk über IP-Sec VPN mit AES 256 GCM bzw. AES128 CBC Verschlüsselung erfolgen. Alle Unternehmenscomputer haben eine Festplattenverschlüssellung; Jeder Anwender hat hierbei ein persönliches zugewiesenes SSL Zertifikat. Der Zugriff auf Web-Anwendungen ist ausschließlich per SSL (https) möglich. Jede Datenübertragung ist damit SSL verschlüsselt. Passörter werden nur verschlüsselt im System abgelegt. Die API für den externen Zugriff kann nur durch eine OAuth2 Authentifizierung erfolgen.

C. Maßnahmen zur Sicherung der Vertraulichkeit

1. Zutrittskontrolle

Maßnahmen, die unbefugten Personen den Zutritt zu IT-Systemen und Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, sowie zu vertraulichen Akten und Datenträgern physisch verwehren:

Alle Daten werden in einem deutschen Rechenzentrum auf eigenen Servern gespeichert. Das Rechenzentrum betreibt eigene High-End in Deutschland, in denen sämtliche unserer Server untergebracht sind. Die Rechenzentren sorgen mit optimaler Netzanbindung, unterbrechungsfreier Stromversorgung (USV), Klimatisierung, Zugangskontrolle sowie Videoüberwachung und vielem mehr für den reibungslosen Betrieb der Server-Infrastruktur. Vertrauliche Ordner mit Informationen werden separat in einem abgeschlossenen Schrank aufbewahrt. Zugriff du diesem Schrank haben nur berechtigte Personen.-Arbeiten nur auf Terminalservern, welche auf den Servern im Rechenzentrum betrieben werden, mit persönlichen Accounts. Sämtliche PC-Arbeitsplätze sind passwortgeschützt und werden nach Beendigung der Arbeit heruntergefahren. Auf Datenträgern befindlich Daten jeglicher Art werden sachgerecht vernichtet.

2. Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte datenschutzrechtlich geschützte Daten verarbeiten oder nutzen können.

Beschreibung des Zugangskontrollsystems:

Bei häufigen Fehlversuchen kommt es zu einer automatischen Passwortsperre. Berechtige sind angewiesen Ihre Passwörter geheim zu halten und gewisse Passwort Sicherheitsstandards zu nutzen. Die Speicherung von personenbezogenen Daten und Dokumenten auf lokalen Laufwerken ist verboten. Es erfolgt ein automatisches Abmelden nach 15 Minuten.

Zum Schutz der Software dient eine PSENSE Firewall und zum Schutz der Hardware eine Sonicwall, sowie der Einsatz von der Antivirensoftware AVAST Enterprise auf allen Rechnern und Servern.

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können, so dass Daten bei der Verarbeitung, Nutzung und Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Beschreibung des Zugriffskontrollsystems:

Zur Rechteverwaltung wird eine LDAP bzw. Active Directory Nutzung verwendet. Grundsätzlich findet ein Logging von Zugriffen auf Backend und Datenbanken statt. Zudem ein Logging inkl. automatisches, dezentrales Reporting in Echtzeit von administrativen Zugriffen auf Serverinfrastruktur. Im Allgemeinen findet eine Einweisung des Personals bei Dienstantritt in den Datenschutz durch Vorgesetzten statt.

4. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden und so von anderen Daten und Systemen getrennt sind, dass eine ungeplante Verwendung dieser Daten zu anderen Zwecken ausgeschlossen ist.

Beschreibung des Trennungskontrollvorgangs:

Alle Mitarbeiter von digitastic wurde auf das Datengeheimnis und Vertraulichkeit hingewiesen und geschult. Zudem besteht ein Rollenzugriffskonzept, welches den Datenzugriff auf einzelne

Personen beschränkt. DSGVO-konforme Verträge zur Auftragsverarbeitung wurden mit allen Subunternehmern geschlossen.

D. Maßnahmen zur Sicherung der Integrität

1. Datenintegrität

Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden:

Das Einspielen neuer Releases und Patches erfolgt mit einem Release-/Patchmanagement. Zudem erfolgen vollständige Funktionstests des Releases / Patches von Installation bis Nutzung durch die IT- Abteilung. Im gesamten System findet ein Logging statt.

2. Übertragungskontrolle

Maßnahmen, die gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können:

Alle Daten durchlaufen ein Logging, welches eine Nachvollziehbarkeit der Übertragung ermöglicht.

3. Transportkontrolle

Maßnahmen, die gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden:

Beschreibung der Transportkontrolle:

Der Zugriff auf das das interne Netzwerk ist nur über IP-Sec VPN mit AES 256 GCM bzw. AES128 CBC Verschlüsselung möglich. Der externe Zugriff erfolgt über API mit OAuth2.

4. Eingabekontrolle

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

Beschreibung des Eingabekontrollvorgangs:

Es findet eine Protokollierung sämtlicher Systemaktivitäten, insbesondere 24/7-Logging-Kontrolle von administrativen Server-Zugriffen, statt. Die Aufbewahrung dieser Protokolle ist mindestens drei Jahren. 24/7-Logging-Kontrolle von administrativen Server-Zugriffen

E. Maßnahmen zur Sicherung der Verfügbarkeit und Belastbarkeit

1. Verfügbarkeitskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Beschreibung des Verfügbarkeitskontrollsystems:

Es findet eine komplette Nutzung von digitalen Systemen auf Basis redundanter, DSGVO-konformer Cloud-Technologien in einem deutschen zertifizierten Rechenzentrum statt. Die Erstellung von Backups verläuft automatisiert nach dem Generationenprinzip. Zudem wird das System regelmäßig auf einem lokalen, räumlich getrennten Medium durch einen verschlüsselten Backup (Vollsicherung) gesichert. Des Weiteren finden weitere regelmäßige Sicherungen auf einem separaten Desaster-Server in einem anderen deutschen zertifizierten Rechenzentrum statt. Die Technologie RAID6 ist Grundlage aller Festplattensicherungen.

2. Rasche Wiederherstellbarkeit

Maßnahmen, die die Fähigkeit sicherstellen, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Beschreibung der Maßnahmen zur raschen Widerherstellbarkeit:

Durch eine 24/7-Server-Überwachung mit dezentralen SMS/Emails-Notifikation im Eskalationsfall können sofort Maßnahmen zur Wiederherstellbarkeit eingeleitet werden. Es erfolgt durchgängig eine katastrophensichere Datenhaltung im Rechenzentrum.

3. Zuverlässigkeit

Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden:

Beschreibung der Maßnahmen zur Zuverlässigkeit:

Ein speziell ausgearbeitet Notfallplan sorgt für eine Meldung von Fehlfunktionen und leitet entsprechende Maßnahmen ein.

F. Maßnahmen zur regelmäßigen Evaluation der Sicherheit der Datenverarbeitung

1. Überprüfungsverfahren

Maßnahmen, die die datenschutzkonforme und sichere Verarbeitung sicherstellen.

Beschreibung der Überprüfungsverfahren:

Ein Datenschutzmanagement ist die Grundlage für regelmäßigen Evaluation der Sicherheit der Datenverarbeitung. Dabei werden besondere Datenschutzvorfälle durch formalisierte Prozesse abgesichert. Es erfolgen regelmäßige Prüfungen durch einen externen Datenschutzbeauftragten.

2. Auftragskontrolle

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

Beschreibung der Maßnahmen zur Auftragskontrolle:

Alle Weisungen des Auftragsgebers werden dokumentiert. Dabei wird ein formalisiertes Auftragsmanagement betrieben.

3. Weitere Maßnahmen

Die Datenschutzrichtlinien werden direkt bei der Entwicklung von neuen Lösungen und Ideen mit eingebunden.

Anlage 2

Unterauftragsverhältnisse gemäß § 9 der Vereinbarung zur Auftragsverarbeitung

Der Auftragsverarbeiter arbeitet derzeit bei der Erfüllung des Auftrags mit den folgenden weiteren Auftragsverarbeitern zusammen, mit deren Beauftragung sich der Verantwortliche einverstanden erklärt.

1. finAPI GmbH
Name/Firma: finAPI GmbH
Funktion/Tätigkeit: Finanzdienstleister
Sitz [Stadt, Land]: München, Deutschland

1. fino run GmbH
Name/Firma: fino run GmbH
Funktion/Tätigkeit: Digialisierungsdienstleister
Sitz [Stadt, Land]: Kassel, Deutschland

Anlage 3

Vereinbarung über die Verpflichtung zur Wahrung des Berufsgeheimnisses nach §§ 203 und 204 StGB einschließlich Belehrung über die strafrechtlichen Folgen einer Pflichtverletzung (§ 62a StBerG)

I.) Der Veranwortliche belehrt den Auftragsverarbeiter gem. § 62a Abs. 3 Satz 2 Nr. 1 Steuerberatungsgesetz (StBerG) über die strafrechtlichen Folgen aus §§ 203 und 204 Strafgesetzbuch (StGB) wie folgt:

1. Offenbart der Auftragsverarbeiter ein in Ausübung oder bei Gelegenheit der Auftragsverarbeitung bekannt gewordenes fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, welches den Berufsträgern des Auftraggebers anvertraut wurde, kann dies mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft werden (§ 203 Abs. 1, Abs. 4 Satz 1 StGB). Die Strafandrohung gilt auch für Personen, die für den Auftragsverarbeiter an der Auftragsverarbeitung mitwirken (§ 203 Abs. 4 Satz 1 StGB).

2. Geheimnisse sind alle Informationen, die nur einem beschränkten Personenkreis bekannt sind und an deren Geheimhaltung derjenige, den die Informationen betreffen (Geheimnisträger), ein sachlich begründetes Interesse hat. Hierzu gehören insbesondere alle Informationen über Mandatsverhältnisse zum Auftraggeber bzw. zu den Berufsträgern des Auftraggebers.

3. Handelt es sich beim Auftragsverarbeiter nicht um eine natürliche Person, trifft die Strafandrohung die für den Auftragsverarbeiter mitwirkenden natürlichen Personen.

4. Im Fall der Einschaltung Dritter (z. B. Subunternehmer) macht sich der Auftragsverarbeiter bzw. die für ihn handelnde Person bei Strafandrohung von Freiheitsstrafe bis zu einem Jahr oder Geldstrafe strafbar, wenn der Dritte unbefugt ein bei der Ausübung oder bei Gelegenheit seiner Tätigkeit bekannt gewordenes fremdes Geheimnis offenbart und der Auftragsverarbeiter nicht dafür Sorge getragen hat, dass der Dritte zur Geheimhaltung verpflichtet wurde (§ 203 Abs. 1, Abs. 4 Satz 2 Nr. 2 StGB).

5. Die angedrohte Strafe beträgt bis zu zwei Jahren oder Geldstrafe, wenn der Täter gegen Entgelt oder in der Absicht handelt, sich zu bereichern oder durch die Tat einen anderen zu schädigen (§ 203 Abs. 6 StGB). Gleiches gilt, wenn der Täter ein dem Berufsträger anvertrautes fremdes Geheimnis unbefugt verwertet (§ 204 StGB).

II.) Der Auftragsverarbeiter verpflichtet sich gegenüber dem Auftraggeber sowie den beim Auftraggeber tätigen Berufsgeheimnisträgern wie folgt:

1. Der Auftragsverarbeiter wirkt als Dienstleister an den Tätigkeiten der Berufsgeheimnisträger mit, die einer beruflichen Verschwiegenheitsverpflichtung unterliegen. Der Auftragsverarbeiter wahrt in Kenntnis der strafrechtlichen Folgen einer Verletzung der Verschwiegenheitspflicht fremde Geheimnisse, die ihm zugänglich gemacht werden.
2. Der Auftragsverarbeiter ist befugt, weitere Personen (Dritte) zur Erfüllung des Vertrages heranzuziehen. Beim Einsatz von Dritten (z. B. weitere Auftragsverarbeiter) verpflichtet sich der Auftragsverarbeiter, diese in Textform unter Belehrung über die strafrechtlichen Folgen einer Pflichtverletzung zur Verschwiegenheit zu verpflichten, soweit diese Dritten im Rahmen ihrer Tätigkeit Kenntnis von fremden Geheimnissen erlangen könnten. Der Auftragsverarbeiter informiert den Auftraggeber über jede beabsichtigte Hinzuziehung von weiteren Auftragsverarbeitern. Der Auftraggeber kann hierbei in begründeten Einzelfällen die Hinzuziehung untersagen.

3. Der Auftragsverarbeiter ist verpflichtet, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Vertragserfüllung erforderlich ist. Er wird angemessene organisatorische und technische Maßnahmen zum Schutz der fremden Geheimnisse und vertraulichen Informationen einhalten und dabei akzeptierte Sicherheitsstandards nach dem jeweils aktuellen Stand der Technik anwenden.

4. Die Pflicht zur Verschwiegenheit besteht auch nach Beendigung des Auftragsverhältnisses zeitlich unbegrenzt fort.

5. Die Pflicht zur Verschwiegenheit gemäß den vorstehenden Absätzen besteht nicht, soweit der Auftragsverarbeiter aufgrund einer behördlichen oder gerichtlichen Entscheidung zur Offenlegung von vertraulichen Informationen des Auftraggebers verpflichtet ist. Soweit dies im Einzelfall zulässig und möglich ist, wird der Auftragsverarbeiter den Auftraggeber über die Pflicht zur Offenlegung vorab in Kenntnis setzen.

6. Der Auftragsverarbeiter ist verpflichtet sicherzustellen, dass die Auftragsverarbeitung nur durch einen zur Verschwiegenheit verpflichteten Personenkreis durchgeführt wird.