Vereinbarung zur Auftragsverarbeitung bei Serviceleistungen der ETL Datenservice GmbH

zwischen ETL Datenservice GmbH, Widdersdorfer Str. 415 · 50933 Köln (eingetragen im Handelsregister des Amtsgerichts Köln unter HRB 75439)

- als **Auftragsverarbeiter** -
- nachfolgend: **Auftragnehmer** -

und

ggf. Stempel

……

Name, Vorname / bei Gesellschaften: Firmierung *

……

Straße, Hausnummer, PLZ, Ort *

(Angaben nur erforderlich, soweit nicht in Stempel enthalten)*

……

Bei natürlichen Personen: Geburtsdatum
Bei Gesellschaften: ggf. Handelsregister und HR-Nummer

- als **Verantwortlichem** -
- nachfolgend: „**Auftraggeber**“ -

- Auftraggeber und Auftragnehmer einzeln jeweils „**Partei“**, zusammen „**Parteien“** -

Der Auftragnehmer verarbeitet für den Auftraggeber personenbezogene Daten nach Maßgabe der beigefügten

> Vertragsbedingungen zur Auftragsverarbeitung bei Serviceleistungen der ETL Datenservice GmbH

und den Anhängen hierzu:

- Anlage „Technische und organisatorische Maßnahmen“
- Anlage „Unterauftragnehmer“
- Anlage „Weisungen“

- Unterschriften -

Für den Auftraggeber:

_____

Ort, Datum

_____

Unterschrift

_____

Name in Druckbuchstaben

_____

Funktion

Auftragnehmer:

_____

Unterschrift

UDO J. HEUSCHMANN

_____

Name in Druckbuchstaben

Prokurist

_____

Funktion

Vertragsbedingungen zur Auftragsverarbeitung bei Serviceleistungen der ETL Datenservice GmbH

1. Gegenstand und Dauer des Auftrags

(1) Der Gegenstand des Auftrags ergibt sich aus dem jeweiligen IT-Dienstleistungsvertrag zwischen den Parteien (im Folgenden Leistungsvereinbarung), auf deren Grundlage der Auftragnehmer als Auftragsverarbeiter für den Auftraggeber als Verantwortlicher IT-Dienstleistungen in Gestalt von Service-Leistungen (z.B. Leistungen zur Analyse und Beseitigung von Störungen von Hardware oder Software, zur Erbringung von Support oder zur Entsorgung von Datenträgern gemäß der Leistungsbeschreibung „Fullservice“ zu Miet- oder Kaufgeräten) erbringt.

(2) Die Dauer und Kündbarkeit dieses Auftrags richten sich nach der Laufzeit und Kündbarkeit der jeweiligen Leistungsvereinbarung. Das Recht zur außerordentlichen Kündigung bleibt unberührt.

(3) Diese Vereinbarung gilt unbeschadet des vorstehenden Absatzes 2 so lange, wie der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet (einschließlich Backups).

(4) Soweit sich aus anderen Vereinbarungen zwischen Auftraggeber und Auftragnehmer anderweitige Abreden zum Schutz personenbezogener Daten ergeben, hat diese Vereinbarung zur Auftragsverarbeitung in ihrem Anwendungsbereich Vorrang, es sei denn die Parteien vereinbaren ausdrücklich etwas anderes.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber ergeben sich aus der jeweiligen Leistungsvereinbarung. Im Falle der Erbringung von Service-Leistungen gemäß der Leistungsbeschreibung „Fullservice“ handelt es sich um Leistungen zur Analyse und Beseitigung von Störungen von Hardware oder Software (auch remote), zur Erbringung von Support (auch remote) oder zur Entsorgung von Datenträgern gemäß der Leistungsbeschreibung „Fullservice“ zu Miet- oder Kaufgeräten, soweit bei der Erbringung der Leistungen jeweils personenbezogene Daten verarbeitet werden.

(2) Art der Daten

Gegenstand der vorgesehenen Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien: Bestandsdaten (z.B. Personen-Stammdaten, Namen oder Adressen); Kommunikationsdaten (z.B. E-Mail-Adressen und Telefonnummern); Inhaltsdaten (z.B. Texte, Bilddaten, Videodaten, Audiodaten); Nutzungsdaten (z.B. Zugriffszeiten und User-Account-Informationen); Meta-/Kommunikationsdaten (z.B. Geräte-Informationen, Endgerätedaten und IP-Adressen); Zugangs- und Authentifizierungsdaten (z.B. Passwörter); Berufsgeheimnisse. Besondere Kategorien personenbezogener Daten werden nicht bestimmungsgemäß verarbeitet.

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen: Beschäftigte und sonstige Mitarbeiter, Mandanten bzw. Kunden, Interessenten, Dienstleister und Lieferanten, Ansprechpartner, Nutzer bzw. Anwender von IT-Systemen

3. Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer ergreift in seinem Verantwortungsbereich die erforderlichen und angemessenen technischen und organisatorische Maßnahmen gemäß Art. 28 Abs. 3 Satz 2 Buchst. c DS-GVO i.V.m. Art. 32 DS-GVO zum Schutz der personenbezogenen Daten zur Aufrechterhaltung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind insbesondere der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen. Die bei Abschluss dieser Vereinbarung aktuellen technisch und organisatorischen Maßnahmen sind in der Anlage „Technische und organisatorische Maßnahmen“ dokumentiert.

(2) Soweit aufgrund datenschutzrechtlicher Anforderungen oder auch aufgrund des technischen Fortschritts oder der Weiterentwicklung technischer Maßnahmen ein Anpassungsbedarf entsteht, wird der Auftragnehmer die erforderlichen Anpassungen vornehmen. Der Auftragnehmer ist zudem berechtigt, alternative angemessene technische und organisatorische Maßnahmen umzusetzen.

(3) Die Verarbeitung von personenbezogenen Daten nach dieser Vereinbarung ist in Privatwohnungen (Heim- und Telearbeit) und auch im Übrigen außerhalb der Geschäftsräume des Auftragnehmers nur unter Wahrung besonderer technischer und organisatorischer Maßnahmen gestattet, die den datenschutzrechtlichen Anforderungen unter Berücksichtigung des jeweiligen Orts der Verarbeitung genügen.

4. Rechte von betroffenen Personen

Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technischer und organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte. Er darf die personenbezogenen Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beauskunften, portieren,

berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten sind und auch nicht auf einem Fehlverhalten des Auftragnehmers beruhen, stehen dem Auftragnehmer eine angemessene Vergütung und die Erstattung von Aufwendungen zu, die der Auftragnehmer für erforderlich halten durfte.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer hat - zusätzlich zu der Einhaltung der Regelungen dieser Vereinbarung - eigene gesetzliche Pflichten gemäß der DS-GVO; insofern sorgt er insbesondere für die Einhaltung folgender Vorgaben:

a) Der Auftragnehmer wahrt die Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 Buchst. b, 29, 32 Abs. 4 DS-GVO. Er setzt bei der Verarbeitung personenbezogener Daten nur Personen ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.

b) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

c) Der Auftragnehmer informiert unverzüglich den Auftraggeber über Kontrollhandlungen und Maßnahmen einer Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeiten- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

d) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeiten- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten, einem anderen Anspruch oder einem Informationsersuchen im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, unterstützt ihn der Auftragnehmer in angemessenem Umfang.

e) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um dafür zu sorgen, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

f) Der Auftragnehmer weist dem Auftraggeber auf Wunsch die getroffenen technischen und organisatorischen Maßnahmen im Rahmen von dessen Kontrollbefugnissen nach Ziffer 8 dieser Vereinbarung nach.

g) Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber in der Weise, dass der Auftraggeber seinen gesetzlichen Pflichten, insbesondere nach Art. 33, 34 DS-GVO nachkommen kann. Er fertigt über den Vorgang eine Dokumentation an, die er dem Auftraggeber im erforderlichen Umfang für weitere Maßnahmen zur Verfügung stellt.

h) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich und angemessen im Rahmen bestehender Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen und stellt ihm in diesem Zusammenhang die erforderlichen Informationen innerhalb angemessener Frist zur Verfügung.

i) Soweit der Auftraggeber zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet ist, unterstützt ihn der Auftragnehmer unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Gleiches gilt im Falle einer Verpflichtung zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde.

(2) Diese Vereinbarung entbindet den Auftragnehmer nicht von der Einhaltung anderer Vorgaben der DS-GVO.

(3) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten sind und auch nicht auf einem Fehlverhalten des Auftragnehmers beruhen, stehen dem Auftragnehmer eine angemessene Vergütung und die Erstattung von Aufwendungen zu, die der Auftragnehmer für erforderlich halten durfte.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Vereinbarung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer als Unterauftragsverarbeiter nach vorheriger dokumentierter Zustimmung des Auftraggebers beauftragen.

(3) Der Auftraggeber stimmt der Beauftragung der in der Anlage „Unterauftragnehmer“ bezeichneten Unterauftragnehmer zu. Der Auftragnehmer sorgt dafür, dass Unterauftragsverarbeiter durch dokumentierte Verträge gebunden und dazu verpflichtet werden, zumindest das nach dieser Vereinbarung und nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO erforderliche Datenschutzniveau zu wahren. Die vertragliche Vereinbarung mit dem Unterauftragnehmer wird dem Auftraggeber auf dessen Wunsch vorgelegt, wobei geschäftliche Klauseln ohne datenschutzrechtlichen Bezug (wie z.B. die Höhe der Vergütung) hiervon ausgenommen sind.

(3) Der Austausch von gemäß der Anlage „Unterauftragnehmer“ bestehenden Unterauftragnehmern ist zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber in einer

angemessenen Zeit, die 14 Tage nicht unterschreiten darf, vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung geschlossen wird, die zumindest das nach dieser Vereinbarung und nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO erforderliche Datenschutzniveau wahrt.

(4) Der Auftragnehmer ist berechtigt, den Auftraggeber zu informieren, wenn er die Beauftragung weiterer Unterauftragnehmer oder den Austausch eines Unterauftragnehmers beabsichtigt. Der Auftraggeber ist berechtigt, gegen eine derartige Hinzuziehung oder einen derartigen Austausch Einspruch zu erheben. Der Einspruch gegen die beabsichtigte Änderung ist innerhalb von vier Wochen nach Zugang der Information gegenüber dem Auftragnehmer zu erheben. Im Fall des Einspruchs kann der Auftragnehmer nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder - sofern die Erbringung der Leistung ohne die beabsichtigte Änderung dem Auftragnehmer nicht zumutbar ist - die von der Änderung betroffene Leistung gegenüber dem Kunden unter Wahrung einer angemessenen Abwicklungsfrist außerordentlich kündigen.

(5) Die Weitergabe von personenbezogenen Daten an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Die Einhaltung und Umsetzung der technischen und organisatorischen Maßnahmen beim Unterauftragnehmer wird unter Berücksichtigung des Risikos beim Unterauftragnehmer vorab der Verarbeitung personenbezogener Daten und sodann regelmäßig durch den Auftragnehmer kontrolliert. Der Auftragnehmer stellt dem Auftraggeber die Kontrollergebnisse auf Anfrage zur Verfügung. Der Auftragnehmer stellt ferner sicher, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Kontrollrechte) auch direkt gegenüber den Unterauftragnehmern wahrnehmen kann.

(6) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(7) Die vorstehenden Bestimmungen gelten für die Beauftragung weiterer Unterauftragnehmer durch den Unterauftragnehmer entsprechend.

7. Internationale Datentransfers

(1) Jede Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation bedarf einer dokumentierten Weisung des Auftraggebers und bedarf der Einhaltung der Vorgaben zur Übermittlung personenbezogener Daten in Drittländer nach Kapitel V der DS-GVO. 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.

(2) Soweit der Auftraggeber eine Datenübermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung von Kapitel V der DS-GVO verantwortlich.

8. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber ist berechtigt, nach vorheriger Abstimmung mit dem Auftragnehmer – d.h. zumindest vorheriger Information und Gewährung der Gelegenheit zur Stellungnahme – Überprüfungen der Einhaltung dieser Vereinbarung zur Auftragsverarbeitung durchzuführen.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen, die erforderlich sind, um die Einhaltung dieser Vereinbarung zur Auftragsverarbeitung und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis der technischen und organisatorischen Maßnahmen zur Einhaltung der besonderen Anforderungen des Datenschutzes allgemein sowie solche, die den Auftrag betreffen, erfolgt vorrangig durch Zertifizierungen oder aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder Remote-Zugriffe oder Online-Meetings. Sofern der Auftraggeber auf Basis tatsächlicher Anhaltspunkte bei verständiger Würdigung Zweifel an der Aussagekraft hat oder besondere Vorfälle im Sinne von Art. 33 Abs. 1 DS-GVO im Zusammenhang mit der Durchführung der Auftragsverarbeitung für den Auftraggeber dies rechtfertigen, kann der Auftraggeber Vor-Ort-Kontrollen durchführen.

(4) Sofern der Auftraggeber solche Vor-Ort-Kontrollen vornimmt, sind diese als Stichprobenkontrollen der für die Durchführung der Auftragsverarbeitung relevanten Bereiche auszugestalten und dem Auftragnehmer unter Wahrung einer angemessenen Vorlauffrist, mindestens aber vier Wochen im Voraus schriftlich anzumelden, soweit nicht besondere Umstände eine Ausnahme rechtfertigen. Entsprechendes gilt für anlasslose Vor-Ort-Kontrollen.

(5) Vor-Ort-Kontrollen erfolgen nur während der üblichen Geschäftszeiten. Der Auftraggeber wird die Vor-Ort-Kontrolle so durchführen, dass der Geschäftsbetrieb des Auftragnehmers nicht unangemessen beeinträchtigt wird. Soweit der Auftraggeber einen externen Prüfer zu der Kontrolle hinzuzieht, wird der Auftraggeber den Auftragnehmer vorab die erforderlichen Informationen erteilen. Der Auftraggeber darf keinen externen Prüfer hinzuziehen, der unmittelbar oder mittelbar mit dem Auftragnehmer oder mit i.S.v. §§ 15 ff. AktG mit dem Auftragnehmer verbundenen Unternehmen im Wettbewerb steht.

(6) Über Vor-Ort-Kontrollen erstellt der Auftraggeber auf eigene Kosten ein schriftliches Protokoll. Darin werden insbesondere Zeitpunkt, teilnehmende Personen,

Umfang, Inhalt und Dauer des Kontrolltermins festgehalten.

(7) Der Auftragnehmer ist berechtigt, Kontrollen des Auftraggebers von dem Abschluss einer Verschwiegenheitserklärung hinsichtlich von Geschäftsgeheimnissen des Auftragnehmers und von Dritten, personenbezogenen Daten, die nicht Gegenstand dieser Vereinbarung zur Auftragsverarbeitung sind, oder sonstigen vertraulichen Daten, die dem Auftraggeber nicht zustehen, und hinsichtlich der von dem Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen abhängig zu machen. Der Auftraggeber wird sämtliche im Zusammenhang mit der Kontrolle erhaltenen Informationen vertraulich behandeln und nicht an Dritte weitergeben, es sei denn, er ist gesetzlich dazu verpflichtet oder berechtigt oder dies ist zur Prüfung oder Durchsetzung von Ansprüchen und Rechten erforderlich.

(8) Jegliche Kontrollen dürfen nicht zu Beeinträchtigungen von Vertraulichkeit, Integrität oder Verfügbarkeit von Daten oder IT-Systemen zum Nachteil des Auftragnehmers führen oder Risiken hierfür begründen. Sie sind unverzüglich abzubrechen, soweit solche Beeinträchtigungen auftreten oder aufzutreten drohen.

(9) Die Installation von Software durch den Auftraggeber auf den Systemen des Auftragnehmers oder eines Unterauftragnehmers zu Zwecken der Prüfung ist unzulässig.

(10) Für Unterstützungsleistungen des Auftragnehmers, die nicht in der Leistungsbeschreibung enthalten sind und auch nicht auf einem Fehlverhalten des Auftragnehmers beruhen, stehen dem Auftragnehmer eine angemessene Vergütung und die Erstattung von Aufwendungen zu, die der Auftragnehmer für erforderlich halten durfte. Der Auftragnehmer wird dem Auftraggeber auf Wunsch vorab eine Aufwandsschätzung mitteilen.

9. Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf Basis dokumentierter Weisungen des Auftraggebers, es sei denn, er ist kraft Gesetzes zu einer Verarbeitung verpflichtet. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich zumindest in Textform. Die anfänglichen Weisungen des Auftraggebers werden durch diese Vereinbarung festgelegt.

(2) Die Personen, die bei Abschluss dieser Vereinbarung für den Auftraggeber weisungsberechtigt und für den Auftragnehmer weisungsempfangsberechtigt sind, und das Verfahren zum Austausch oder zur Änderung werden in der Anlage „Weisungen“ festgelegt.

(3) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Auffassung ist, eine Weisung verstoße gegen Datenschutzvorschriften oder sonstige Gesetze. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis der Auftraggeber sie bestätigt oder geändert hat. Gesetzliche Berechtigungen des Auftragnehmers zur Verweigerung der Leistung bei Gesetzesverstößen bleiben unberührt.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens aber mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Papier und Datenträger mit Informationen, die dem Berufsgeheimnis (§ 43a Abs. 2 Satz 1 BRAO, § 203 Abs. 1 Nr. 3 StGB) unterliegen, sind nach DIN 66399 und mindestens nach Schutzklasse 3 und Sicherheitsstufe 4 zu vernichten.

11. Allgemeine Bestimmungen

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter, etwa durch Pfändung oder Beschlagnahmung oder durch sonstige Ereignisse gefährdet sein, wird der Auftragnehmer den Auftraggeber informieren. Der Auftragnehmer weist die Dritten darauf hin, dass die Verantwortlichkeit und das Eigentum an den Daten ausschließlich beim Auftraggeber liegen.

(2) Macht eine betroffene Person gegenüber einer Partei Schadenersatzansprüche wegen Verstoßes gegen datenschutzrechtliche Bestimmungen im Zusammenhang mit dieser Vereinbarung zur Auftragsverarbeitung geltend, so wird diese Partei, die andere Partei hierüber unverzüglich informieren.

(3) Die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.v. § 273 BGB hinsichtlich der verarbeiteten personenbezogenen Daten und der zugehörigen Datenträger ist ausgeschlossen.

(4) Auf die Vereinbarung findet das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts Anwendung.

(5) Ausschließlicher Gerichtsstand für alle sich aus oder im Zusammenhang mit Vereinbarungen mit Auftraggebern ergebenden Streitigkeiten zwischen dem Auftragnehmer und Auftraggebern, die Kaufleute, juristische Personen des öffentlichen Rechts oder öffentlich-rechtliche Sondervermögen sind, ist der jeweilige Sitz des Auftragnehmers. Die Vereinbarung über den Gerichtsstand gilt nicht, soweit für die Klage oder das jeweilige gerichtliche Verfahren durch Gesetz ein ausschließlicher Gerichtsstand begründet ist

Anlage „Technisch und organisatorische Maßnahmen“

1. Pseudonymisierung und Verschlüsselung (nach Art. 32 Abs. 1 Buchst. a DS-GVO)

1.1. Pseudonymisierung

Der Auftragnehmer beabsichtigt, personenbezogene Daten - soweit möglich, sachdienlich und mit angemessenem Aufwand umsetzbar - in pseudonymisierter Form zu verarbeiten.

1.2. Verschlüsselung

Mobile Datenträger werden unter Berücksichtigung des Stands der Technik verschlüsselt. Die Übertragung von Daten über Datenverbindungen erfolgt soweit möglich unter Nutzung von Verschlüsselungstechnologien unter Berücksichtigung des Stands der Technik.

2. Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit (nach Art. 32 Abs. 1 Buchst. b DS-GVO)

2.1. Vertraulichkeit

2.1.1. Zutrittskontrolle

Maßnahmen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren: Es erfolgen Maßnahmen zur Zutrittskontrolle zu den Geschäftsräumen des Auftragnehmers. Es sind Maßnahmen getroffen, um den unbefugten Zutritt zu den Räumen, in denen personenbezogene Daten verarbeitet und aufbewahrt werden, zu verhindern, insbesondere verschlossene Eingangstüren, Begleitung von Besuchern, Einbruchschutz (z.B. einbruchsichere Fenster, Lichtschächte am Keller gesichert). Für die Schlüsselvergabe bestehen organisatorische Maßnahmen (z.B. Arbeitsanweisungen zur Schlüsselvergabe, klar definierte Schlüsselkreise und Vergabe der Schlüssel auf Basis eines definierten Prozesses).

2.1.2. Zugangskontrolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme (DV) von Unbefugten genutzt werden können: Zugang zur DV erhalten ausschließlich berechtigte Personen. Um das Eindringen Unbefugter in die DV zu verhindern, kommen insbesondere folgende Maßnahmen in Betracht: ein geregeltes Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts); automatische Sperrung (z.B. Kennwort oder Pausenschaltung); Einrichten eines Benutzerstammsatzes pro User. Die Initiierung der Teleserviceverbindung für remote-Leistungen erfolgt durch den Auftraggeber. Für den Verbindungsaufbau des Teleservice sind grundsätzlich zwei Verbindungswege vorgesehen:

- Physikalische Teleserviceverbindung: Die Anbindung des Auftragnehmers an das Netzwerk des Auftraggebers erfolgt über das Internet.

- Logische Teleserviceverbindung: Die Kommunikation zwischen Auftraggeber und Auftragnehmer wird durch den Auftragnehmer initiiert und erfolgt über die Fernwartungssoftware TeamViewer.

2.1.3. Zugriffskontrolle

Maßnahmen um zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können: Der Zugriff wird administrativ mittels Benutzerauthentifizierung geregelt. Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen werden durch bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung protokolliert und verhindert. Hierzu kommen insbesondere folgende Maßnahmen in Betracht: Differenzierte Berechtigungen (Berechtigungskonzept, Profile, Rollen, Transaktionen und Objekte); Protokollierung und deren unregelmäßige Auswertung

2.1.4. Trennungskontrolle

Maßnahmen um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können: Daten, die zu unterschiedlichen Zwecken erhoben werden, werden auch getrennt verarbeitet. Hierzu kommen insbesondere folgende Maßnahmen in Betracht: Zweckbindung und Funktionstrennung; physische und logische Trennung von Daten

2.1.5. Organisationskontrolle

Der Auftragnehmer wählt sein Personal sorgfältig aus. Alle Mitarbeiter sind vom Auftragnehmer auf das Datengeheimnis in der jeweils aktuellen Fassung zu verpflichten. Ansprechpartner für alle technischen Fragen im Zusammenhang mit den Einzelheiten der im Rahmen dieser Vereinbarung zu erbringenden Leistungen sind: die Geschäftsführung des Auftraggebers und die Geschäftsführung des Auftragnehmers. Der Auftragnehmer hat dafür Sorge zu tragen, dass Weisungen des Auftraggebers zur Verarbeitung von Daten bei remote-Leistungen beachtet werden. Der Auftragnehmer sorgt dafür, dass im erforderlichen Umfang alle Kundendaten einschließlich Zugangsdaten geheim gehalten werden. Das Einspielen von Updates / Änderungen für das Betriebssystem und für systematische Software-Systeme des Auftraggebers wird im Rahmen des „Fullservice" auf Veranlassung des ETAX-Serviceteams. Für Auftraggeber, die nicht im Rahmen des Fullservice" versorgt werden, können abweichende Regelungen getroffen werden.

2.2. Integrität

2.2.1. Weitergabekontrolle

Maßnahmen um zu gewährleisten, dass personenbezogene Daten bei elektronischer Übertragung während des 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: Die Aspekte der Weitergabe personenbezogener Daten werden durch Maßnahmen bei Transport Übertragung und Übermittlung oder Speicherung auf Datenträgern (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung geregelt. Hierzu kommen insbesondere folgende Maßnahmen in Betracht: Verschlüsselung / Tunnelverbindung (VPN = Virtual Private Network); Protokollierung; Transportsicherung.

2.2.2. Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege wird durch Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind, gewährleistet. Die Eingabekontrolle dient der Gewährleistung der Nachverfolgbarkeit von (gewollten und ungewollten) Datenmanipulationen: Protokollierungs- und Protokollauswertungssysteme; Plausibilitätsprüfungen; Formatbeschränkungen; Nachvollziehbarkeit der Nutzereingaben durch Zeitstempel, Nutzernamen und andere nicht manipulierbare Werte in Systemen, Applikationen und Datenbanken

2.2.3. Auftragskontrolle

Maßnahmen um zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können: Der Auftragnehmer wählt (Unter-)Auftragnehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus und schließt Verträge, derer Inhalt den Anforderungen des Art. 28 DS-GVO genügen. Der Auftragnehmer überzeugt sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der bei (Unter-)Auftragnehmern getroffenen technischen und organisatorischen Maßnahmen. Die weisungsgemäße Auftragsverarbeitung wird durch technische und organisatorische Maßnahmen zur Abgrenzung der Kompetenzen zwischen Auftraggeber und (Unter-)Auftragnehmer gewährleistet. Hierzu kommen insbesondere folgende Maßnahmen in Betracht: eindeutige Kriterien zur Auswahl von Auftragnehmern; formalisierte Auftragserteilung (Auftragsformular); eindeutige Vertragsgestaltung; Kontrolle der Vertragsausführung.

2.3. Verfügbarkeit und Belastbarkeit

Die Daten sind gegen zufällige oder mutwillige Zerstörung durch umfangreiche Backup-Strategien zu schützen. Hierzu kommen insbesondere folgende Maßnahmen in Betracht: regelmäßiges Backup aller relevanten Daten; räumlich getrennte Lagerung; unterbrechungsfreie Stromversorgung (USV) und Notstromgeneratoren; Schutz gegen Schadsoftware; Firewall; Meldewege und Notfallpläne.

3. Rasche Wiederherstellung (nach Art. 32 Abs. 1 Buchst. c DS-GVO)

Die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen ist bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen. Herzu kommen folgende Maßnahmen in Betracht: Durch den Einsatz einer virtuellen System Umgebung innerhalb einer redundanten Infrastruktur können personenbezogene Daten jederzeit rasch wiederhergestellt werden. Es gibt ein Datensicherungskonzept, dass auch das erfolgreiche Testen der raschen Wiederherstellung der Verfügbarkeit von und des Zugangs zu personenbezogenen Daten beinhaltet.

4. Verfahren zur regelmäßigen Überprüfung und Evaluierung (nach Art. 32 Abs. 1 Buchst. d und Art. 25 Abs. 1 DS-GVO)

Der Auftragnehmer stellt sicher, dass die von ihm eingesetzten Systeme unter Berücksichtigung des Stands der Technik ausgestaltet sind. Der Auftragnehmer trägt durch Richtlinien und/oder Anweisungen an die Beschäftigten dazu bei, dass eine Verarbeitung personenbezogener Daten in einer Weise gewährleistet ist, die den Anforderungen der DS-GVO entspricht. Dies beinhaltet insbesondere eine regelmäßige Überprüfung der Wirksamkeit der getroffenen Maßnahmen zum Schutz personenbezogener Daten und ggf. der Anpassung. Es ist insbesondere sichergestellt, dass Datenschutzvorfälle von allen Beschäftigten erkannt und unverzüglich dem Auftraggeber gemeldet werden, wenn dies Daten betrifft, die im Rahmen der Auftragsverarbeitung für den Auftraggeber verarbeitet werden. Der Auftragnehmer trifft unter Berücksichtigung der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen.

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

Etwaige weitere erforderliche Maßnahmen im Zusammenhang mit der Verarbeitung von personenbezogenen Daten durch den Auftraggeber sind vom Auftraggeber zu treffen bzw. durch ergänzende Weisungen des Auftraggebers an den Auftragnehmer festzulegen

Anlage „Unterauftragnehmer“

- hmd Software AG
- eurodata AG
- ETL Service GmbH
- ETL SCS AG
- B.A.D GmbH
- Hersteller der ETL Datenservice Standardprodukte bzw. Servicepartner dieser Hersteller
- Fox-on
- Dankow IT
- Elektrotechnik Hintze
- K2M IT Solutions GmbH

Anlage „Weisungen“

1. Weisungsberechtigte Person des Auftraggebers ist:

Name: _____

E-Mail: _____

Der Auftraggeber ist berechtigt, weitere Personen als weisungsberechtigt zu bestimmen; die Bestimmung bedarf zu ihrer Wirksamkeit der Textform. Der Auftraggeber ist berechtigt, eine derartige Bestimmung mit Wirkung für die Zukunft zu widerrufen oder zu ändern, dies aber mit Ausnahme des jeweiligen Geschäftsführers des Auftraggebers als weisungsberechtigter Person; derartige Erklärungen bedürfen zu ihrer Wirksamkeit ebenfalls der Textform.