Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 Abs. 3 DSGVO

zwischen

Kunden-Nr:

– Verantwortlicher – nachstehend Auftraggeber genannt -

und dem

institut für finanzdienstleistungen e.V. *(iff)*

– Auftragsverarbeiter – nachstehend Auftragnehmer genannt

1. Präambel

Das institut für finanzdienstleistungen e.V. (iff) bietet Schuldnerberatungsstellen die Software CAWIN – Volllizenzen und Update-Verträge – für die Bearbeitung ihrer Fälle sowie Support beim Einsatz der Software CAWIN über Remote Control Systeme an. Darüber hinaus wertet das iff von teilnehmenden Schuldnerberatungsstellen deren anonymisierte Daten aus und veröffentlicht die aggregierten anonymisierten Daten in Form eines jährlichen Überschuldungsreports oder gegebenenfalls anlässlich anderer wissenschaftlicher Forschungsprojekte des iff. Personenbezogene Daten erhält das iff dabei nicht. Lediglich in in Einzelfällen kann es bei dem Support der genutzten Software CAWIN dazu kommen, dass Mitarbeiter des iff personenbezogene Daten erhalten oder über Remote Control Systeme Einsicht in personenbezogene Daten erhalten. Um diese Fälle abzudecken, wird die folgende Vereinbarung zur Wahrung der Anforderungen gem. Art. 28 DSGVO geschlossen, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

2. Gegenstand und Dauer des Auftrags

(1) Der Gegenstand des Auftrags ergibt sich aus dem jeweiligen CAWIN-Lizenzvertrag (Kauf einer Vollversion, Abschluss von Updateverträgen) zwischen den Parteien und der unentgeltlichen Zurverfügungstellung von anonymisierten Daten aus der Schuldnerberatung (im Folgenden Hauptvertrag genannt).

(2) Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Hauptvertrags, d.h. sie endet mit der Wirksamkeit der Kündigung des Hauptvertrages.

(3) Der Auftragnehmer verarbeitet personenbezogene Daten des Auftraggebers ausschließlich im Auftrag und auf dokumentierte Weisung des Auftraggebers. Umfang und Zweck der Datenverarbeitung bestimmt der Auftraggeber und ergeben sich aus dem Hauptvertrag zwischen den Parteien. Dem Auftraggeber obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

3. Art und Zweck der vorgesehenen Verarbeitung von Daten

(1) Der Auftragsnehmer verarbeitet im Rahmen der Ausführung des Hauptvertrages, dessen Gegenstand das Zurverfügungstellung einer Software nebst Update und Wartung per Fernzugriff ist, in der Regel keine personenbezogenen Daten vom Auftraggeber. Im Einzelfall kann der Auftragsnehmer personenbezogene Daten des Auftraggebers beispielsweise im Rahmen des Supports durch Remote Control Systeme und durch die Zusendung von E-Mails durch den Auftraggeber verarbeiten. Der konkrete Zugriff durch Remote Control Systeme wird in **Anlage 1** beschrieben.

(2) Bei dem Kreis der von der Datenverarbeitung nach Absatz 1 betroffenen Personen handelt es sich um die Ratsuchenden und Beschäftigte des Auftraggebers im Rahmen der Schuldnerberatung. Die Daten können neben den

institut für finanzdienstleistungen e.V. *(iff)* | Vorstand: Claudia Rutt, Prof. Dr. Ingrid Größl | Geschäftsführende Direktorin: Dr. Sally Peters
Grindelallee 100, 20146 Hamburg +49 (0)40 30 96 91-0 +49 (0)40 30 96 91-22 www.iff-hamburg.de institut@iff-hamburg.de
USt-IdNr. DE 118713543 | AG Hamburg VR 13836 | Hamburger Sparkasse | IBAN DE62 2005 0550 1238 1229 21 | BIC HASPDEHHXXX
Gläubiger-ID: DE39ZZZ00000988279 | GLS Bank | IBAN DE15 4306 0967 1255 4537 00 | BIC GENODEM1GLS

personenbezogenen Stammdaten (Vor- und Nachname, Adresse, Emailadresse, IP-Daten) zusätzlich bei den Ratsuchenden der Schuldberatung Angaben zu Gläubigern und deren Ansprechpartner, Schuldenhöhe, Haushalts- und Einkommenssituation der Schuldner sowie den Bearbeitungsstatus der Schuldnerberatungsstelle beinhalten.

(3) 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 Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(4) Der Auftraggeber erklärt sich damit einverstanden, dass die dem Auftragnehmer in anonymisierter Form zur Verfügung gestellten Daten auch für Zwecke verwendet werden dürfen, die über diesen Vertrag hinausgehen. Diese Zwecke sind die Erstellung des jährlichen Überschuldungsreports sowie wissenschaftliche und statistische Zwecke.

4. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer stellt die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO her. Sie ergeben sich aus der **Anlage 2**. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus insbesondere hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit und der Belastbarkeit der Systeme. Dabei sind 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 DSGVO zu berücksichtigen.

(2) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das vertraglich vereinbarte Sicherheitsniveau nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(3) Beschäftigte, die auf besondere Kategorien personenbezogener Daten oder auf Daten von Berufsgeheimnisträger zugreifen können, sind nach § 203 Abs. 4 StGB belehrt und verpflichtet worden.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO.

(2) Der Auftragnehmer bestätigt, dass er – soweit eine gesetzliche Verpflichtung hierzu besteht – einen Datenschutzbeauftragten bestellt hat. Die Kontaktdaten des Datenschutzbeauftragten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt

(3) Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

(4) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, 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.

institut für finanzdienstleistungen e.V. (iff) | Vorstand: Claudia Rutt, Prof. Dr. Ingrid Größl | Geschäftsführende Direktorin: Dr. Sally Peters
Grindelallee 100, 20146 Hamburg +49 (0)40 30 96 91-0 +49 (0)40 30 96 91-22 www.iff-hamburg.de institut@iff-hamburg.de
USt-IdNr. DE 118713543 | AG Hamburg VR 13836 | Hamburger Sparkasse | IBAN DE62 2005 0550 1238 1229 21 | BIC HASPDEHHXXX
Gläubiger-ID: DE39ZZZ00000988279 | GLS Bank | IBAN DE15 4306 0967 1255 4537 00 | BIC GENODEM1GLS

6. Unterauftragsverhältnisse

(1) Die vertraglich vereinbarte Leistung über Remote Control Systeme kann auf Wunsch des Auftraggebers mittels der Software TeamViewer der TeamViewer GmbH, Jahnstr. 30, 73037 Göppingen, erfolgen. Der Auftragnehmer hat diesen Anbieter der Fernwartungssoftware sorgfältig nach deren Eignung und Zuverlässigkeit ausgewählt. Soweit möglich stellt der Auftragnehmer sicher, dass der Auftraggeber seine Rechte aus dieser Vereinbarung direkt gegenüber den Subunternehmern wahrnehmen kann. Der Auftragnehmer weist bezüglich der Speicherung von personenbezogenen Daten durch TeamViewer GmbH auf deren Datenschutzbestimmungen hin: https://www.teamviewer.com/de/datenschutzerklaerung/. Auf eine Speicherung und Verarbeitung von Daten durch den Anbieter dieser Fernwartungssoftware während des Fernzugriffs hat der Auftragnehmer im Übrigen keinen Einfluss. Soweit der Auftraggeber keinen Zugriff über Remote Control Systeme wünscht, hat er dies dem Auftragnehmer schriftlich mitzuteilen. Der Support des Auftragnehmers erfolgt in dem Fall dann ausschließlich telefonisch oder auf Wunsch des Auftraggebers persönlich vor Ort. Die Mehrkosten bei einem Support vor Ort hat der Auftraggeber dem Auftragnehmer gesondert zu vergüten.

(2) Weitere Unterauftragnehmer setzt der Auftragnehmer aktuell nicht ein. Der Auftragnehmer darf weitere Unterauftragnehmer nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. In diesem Fall hat der Auftragnehmer dafür Sorge zu tragen, dass die in diesem Vertrag vereinbarten Regelungen des Auftraggebers auch gegenüber den von ihm beauftragten Subunternehmen gelten und dem Auftraggeber sämtliche Kontrollrechte gegenüber dem Subunternehmer einzuräumen sind. Der Auftragnehmer hat die Einhaltung der Pflichten regelmäßig zu kontrollieren.

(3) Eine Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z.B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen sowie Leistungen, die der Auftragnehmer für die eigene Wartung seiner IT-Systeme, die Entsorgung von Datenträgern sowie für sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. 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 sowie Kontrollmaßnahmen zu ergreifen.

7. Weisungsbefugnis des Auftraggebers

(1) Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen mit Blick auf die Datenverarbeitung berechtigt.

(2) Die weisungsberechtigen Personen und der Ansprechpartner des Auftragnehmers für Weisungen ergeben sich aus Nr. 13.

(3) Alle erteilten Weisungen sind sowohl vom Auftragnehmer wie vom Auftraggeber zu dokumentieren.

(4) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(5) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

8. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten dieses Vertrages erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

institut für finanzdienstleistungen e.V. (iff) | Vorstand: Claudia Rutt, Prof. Dr. Ingrid Größl | Geschäftsführende Direktorin: Dr. Sally Peters
Grindelallee 100, 20146 Hamburg +49 (0)40 30 96 91-0 +49 (0)40 30 96 91-22 www.iff-hamburg.de institut@iff-hamburg.de
USt-IdNr. DE 118713543 | AG Hamburg VR 13836 | Hamburger Sparkasse | IBAN DE62 2005 0550 1238 1229 21 | BIC HASPDEHHXXX
Gläubiger-ID: DE39ZZZ00000988279 | GLS Bank | IBAN DE15 4306 0967 1255 4537 00 | BIC GENODEM1GLS

2) Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt.

(3) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen. Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit.

9. Anfragen und Rechte Betroffener

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der in den Artikeln 12 bis 22 DSGVO und in den Artikeln 32 bis 36 der DSGVO genannten Pflichten.

(2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbständig, sondern verweist den Betroffenen unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

10. Haftung

(1) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragnehmer allein der Auftraggeber gegenüber dem Betroffenen verantwortlich.

(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen entstanden ist, verantwortlich ist.

11. Mitteilung bei Verstößen des Auftragnehmers

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder Textform informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch eine Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

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

(2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung nachteiliger Folgen der Betroffenen, informiert hierüber den Auftraggeber und ersucht um weitere Weisungen.

(3) Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) Der Auftragnehmer führt ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DSGVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

(5) Der Auftragnehmer unterstützt den Auftraggeber darüber hinaus bei der Einhaltung der Informationspflichten des Auftraggebers nach Möglichkeit.

institut für finanzdienstleistungen e.V. *(iff)* | Vorstand: Claudia Rutt, Prof. Dr. Ingrid Größl | Geschäftsführende Direktorin: Dr. Sally Peters
Grindelallee 100, 20146 Hamburg +49 (0)40 30 96 91-0 +49 (0)40 30 96 91-22 www.iff-hamburg.de institut@iff-hamburg.de
USt-IdNr. DE 118713543 | AG Hamburg VR 13836 | Hamburger Sparkasse | IBAN DE62 2005 0550 1238 1229 21 | BIC HASPDEHHXXX
Gläubiger-ID: DE39ZZZ00000988279 | GLS Bank | IBAN DE15 4306 0967 1255 4537 00 | BIC GENODEM1GLS

(6) Für Unterstützungsleistungen, die nicht in dem Hauptvertrag enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

12. Zusammenarbeit mit der zuständigen Datenschutz-Aufsichtsbehörde

Der Auftraggeber und der Auftragnehmer und gegebenenfalls deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

13. Löschung und Rückgabe von personenbezogenen Daten

(1) Der Auftragnehmer wird personenbezogene Daten unmittelbar nach Beendigung des Zwecks der Datenverarbeitung löschen. Die Löschung der personenbezogenen Daten erfolgt ebenso nach Aufforderung durch den Auftraggeber, spätestens mit Beendigung des Hauptvertrages. Der Auftragnehmer hat in dem Fall sämtliche in seinen Besitz gelangten personenbezogenen Daten dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Die Löschung personenbezogener Daten bezieht sich auf sämtliche Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen. Nicht umfasst sind anonymisierte Daten nach Ziffer 3 Abs. 2 des Vertrages.

(2) Der Auftragnehmer hat dafür ein Löschkonzept, beachtet die gesetzlichen Vorgaben auf das Recht auf Vergessenwerden, auf Berichtigung und auf Auskunft und wird dies entsprechend dokumentieren.

(3) Kopien oder Duplikate der personenbezogenen 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.

(4) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

14. Schlussbestimmungen

(1) Änderungen, Ergänzungen und die Aufhebung dieses Vertrags bedürfen der Schriftform. Gleiches gilt für eine Änderung oder Aufhebung des Schriftformerfordernisses

(2) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt.

institut für finanzdienstleistungen e.V. *(iff)* | Vorstand: Claudia Rutt, Prof. Dr. Ingrid Größl | Geschäftsführende Direktorin: Dr. Sally Peters
Grindelallee 100, 20146 Hamburg +49 (0)40 30 96 91-0 +49 (0)40 30 96 91-22 www.iff-hamburg.de institut@iff-hamburg.de
USt-IdNr. DE 118713543 | AG Hamburg VR 13836 | Hamburger Sparkasse | IBAN DE62 2005 0550 1238 1229 21 | BIC HASPDEHHXXX
Gläubiger-ID: DE39ZZZ00000988279 | GLS Bank | IBAN DE15 4306 0967 1255 4537 00 | BIC GENODEM1GLS

15. Zuständige Datenschutz-Aufsichtsbehörden und Ansprechpartner

Zuständige Datenschutz-Aufsichtsbehörde des Auftragnehmers	Zuständige Datenschutz-Aufsichtsbehörde des Auftraggebers
Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit Ludwig-Erhard-Straße 22 20459 Hamburg	
Ansprechpartner des Auftragnehmers	**Ansprechpartner des Auftraggebers**
Andrea Hollweg institut für finanzdienstleistungen e.V. Grindelallee 100 20146 Hamburg Tel. 040/309691-25 E-Mail: andrea.hollweg@iff-hamburg.de	

_____ _____

Ort, Datum Ort, Datum

_____ _____

Stempel, rechtsverbindliche Unterschrift rechtsverbindliche Unterschrift)

Auftraggeber **Auftragnehmer *(iif)***

institut für finanzdienstleistungen e.V. *(iff)* | Vorstand: Claudia Rutt, Prof. Dr. Ingrid Größl | Geschäftsführende Direktorin: Dr. Sally Peters
Grindelallee 100, 20146 Hamburg +49 (0)40 30 96 91-0 +49 (0)40 30 96 91-22 www.iff-hamburg.de institut@iff-hamburg.de
USt-IdNr. DE 118713543 | AG Hamburg VR 13836 | Hamburger Sparkasse | IBAN DE62 2005 0550 1238 1229 21 | BIC HASPDEHHXXX
Gläubiger-ID: DE39ZZZ00000988279 | GLS Bank | IBAN DE15 4306 0967 1255 4537 00 | BIC GENODEM1GLS

Anlage 1 – Fernwartung mittels Remote Control Software

§ 1 Hintergrund

Der Auftraggeber nutzt die Schuldnerberatungssoftware CAWIN des Auftragnehmers. Im Rahmen der Nutzung bietet der Auftragnehmer die technische Unterstützung dem Auftraggeber im Wege der Fernwartung an.

§ 2 Zugriffsrechte

Der Auftraggeber darf den Auftragnehmer im Rahmen des Lizenzvertrags bei technischen Fragen konsultieren. Dabei wird dem Auftragnehmer der Zugriff auf die CAWIN-Installation, inklusive Zugriff auf die gesamte Installationsumgebung (CAWIN-Programmverzeichnis, Windows-Verzeichnis, Windows-Benutzerverzeichnis, Registry) eingeräumt. In den zwischen den Mitarbeitern der Vertragspartner vorab abgesprochenen Ausnahmefällen darf der Auftragnehmer zudem auf die CAWIN-Datenbank im SQL-Server zugreifen.

Im Normalfall erfolgen keine Speicherung und keine Datenübertragung aus der CAWIN-Datenbank an den Auftragnehmer. Bei einigen Problemen kann es jedoch nötig sein, dass Haushalte aus CAWIN – in der Regel anonymisiert – exportiert und an den Auftragnehmer übertragen werden. Die Mitarbeiter des Auftragnehmers haben den Anweisungen der Mitarbeiter des Auftraggebers Folge zu leisten.

§ 3 Technische Umsetzung

Der Auftraggeber kontaktiert den Auftragnehmer über die durch den Auftragnehmer bereitgestellte Hotline. Wenn aufgrund des geschilderten Problems notwendig, bietet der Auftragnehmer die Fernwartung an. Ist der Auftraggeber damit einverstanden, wird zwischen Auftragnehmer und Auftraggeber eine Fernwartungsverbindung zwischen ihren Rechnern mittels der Software „TeamViewer“ hergestellt. Dazu wird eine eigene Benutzerkennung für den Rechner des Auftraggebers vergeben. Das dazugehörige Passwort wird bei jedem Start des Wartungsvorgangs geändert. Die Verbindung kann nur nach Starten der Software auf dem Rechner des Auftraggebers und Nennung des Passworts durch einen Mitarbeiter des Auftraggebers aufgebaut werden. Die Datenübertragung ist mittels der bereitgestellten Software durch eine AES-Verschlüsselung mit 256 Bit gesichert. Der Mitarbeiter des Auftragnehmers erhält durch die Verbindung Zugriff auf den Rechner des Auftraggebers mit den Berechtigungen des Mitarbeiters des Auftraggebers.

Der Auftraggeber wird dem Auftragnehmer für die Wartung nur solche Zugriffsmöglichkeiten eröffnen, die für die Hilfestellung bzw. Fehlerbehebung unbedingt erforderlich sind. Bei Aktionen, die erweiterte Rechte benötigen (z. B. Installationen), wird der Mitarbeiter des Auftraggebers sich als Windows-Benutzer mit den entsprechenden Rechten einloggen beziehungsweise Benutzernamen und Passwort selbst eingeben. Diese Vorgänge sind während der Abfrage am Bildschirm des Auftragnehmers nicht sichtbar. Der Auftraggeber überwacht die Fernwartung durch seine Mitarbeiter. Diese können die Wartungsarbeiten des Auftragnehmers am eigenen Bildschirm mitverfolgen und jederzeit durch Trennung der Verbindung abbrechen. Eine „stille“, das heißt, durch den Auftraggeber unbeobachtete Fernwartung ist durch die verwendete Fernwartungssoftware ausgeschlossen. Nach Abschluss der Wartungsarbeiten wird die Verbindung durch den Mitarbeiter des Auftraggebers oder des Auftragnehmers getrennt. Die Trennung der Verbindung ist für den Mitarbeiter des Auftraggebers ersichtlich.

§ 4 Behandlung der Daten

Der Auftragnehmer verpflichtet sich, übertragene Daten nur wenn notwendig und nur auf entsprechende Anweisung der Mitarbeiter des Auftraggebers zu speichern. Falls eine Übertragung personenbezogener Daten unbedingt erforderlich ist, werden diese Daten in der Fernwartungszentrale des Auftragnehmers nur temporär und auf einem vor dem zweckwidrigen Zugriff anderer Rechner im Netz geschützten Bereich gespeichert und anschließend, spätestens nach 14 Tagen, gelöscht. Zugriff auf den geschützten Bereich erhalten allein die mit der Fernwartung betrauten Personen des Auftragnehmers.

§ 5 Eingesetzte Mitarbeiter

Die Fernwartung wird durch die Mitarbeiter des Auftragnehmers durchgeführt.

institut für finanzdienstleistungen e.V. *(iff)* | Vorstand: Claudia Rutt, Prof. Dr. Ingrid Größl | Geschäftsführende Direktorin: Dr. Sally Peters
Grindelallee 100, 20146 Hamburg +49 (0)40 30 96 91-0 +49 (0)40 30 96 91-22 www.iff-hamburg.de institut@iff-hamburg.de
USt-IdNr. DE 118713543 | AG Hamburg VR 13836 | Hamburger Sparkasse | IBAN DE62 2005 0550 1238 1229 21 | BIC HASPDEHHXXX
Gläubiger-ID: DE39ZZZ00000988279 | GLS Bank | IBAN DE15 4306 0967 1255 4537 00 | BIC GENODEM1GLS

Anlage 2 – Technische und organisatorische Maßnahmen, die zusätzlich zur Anlage 1 bestehen

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

- Zutrittskontrolle
  Kein unbefugter Zutritt zum Büro des iff. Dokumentierte Schlüsselvergabe an Mitarbeiter und Maßnahmen bei Verlust (unverzüglicher Austausch des Schlosses). Besuch muss klingeln, wird an der Tür empfangen und bleibt während der Anwesenheit in Begleitung eines Mitarbeiters des Auftragnehmers. Ein externer Reinigungsdienst wird sorgfältig ausgewählt und geprüft.
- Zugangskontrolle
  Account-Passwörter werden vom Auftraggeber nach erstmaliger Inbetriebnahme der Software von ihm selbst geändert und sind dem Auftragnehmer nicht bekannt. Das Passwort zur Administrationsoberfläche wird vom Auftraggeber selbst vergeben. CAWIN-Daten sind beim Auftragnehmer ausschließlich auf einem speziell mit Passwort gesicherten Laufwerk gespeichert. Es werden nur als sicher anerkannte Kennwörter verwendet (verwendete Passwörter müssen Mindestlänge haben und werden in regelmäßigen Abständen erneuert). Alle Arbeitsgeräte, auf denen personenbezogene Daten verarbeitet werden, sind für den jeweiligen Benutzer des Auftragnehmers anhand seiner Berechtigung personalisiert, mit einem Passwort sowie einer automatischen Desktopsperre geschützt und verwenden ein aktuelles Betriebssystem. Der Auftragnehmer nutzt ein verschlüsseltes und zentral überwachtes WiFi nach aktuellem Stand der Technik, eine zentral administrierte Malwareprotection und zentral überwachte Firewall.
- Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte der Mitarbeiter des Auftragnehmers sowie die Protokollierung von Zugriffen in Log-Dateien, eine minimale Anzahl von Administratoren, die Benutzerrechte vergeben, regelmäßige Sicherheitsupdates und das sichere Aufbewahren von Datenträgern verhindern zudem unberechtigte Zugriffe. Ferner werden Papierdokumenten und Datenträger nach einem Löschkonzept ordnungsgemäß vernichtet und dies protokolliert.
- Datenträgerkontrolle
  Festplatten werden mit einem definierten Verfahren mehrfach überschrieben und dadurch gelöscht. Nach Überprüfung werden die Festplatten erneut eingesetzt. Defekte Festplatten, die nicht sicher gelöscht werden können, werden zerstört.
- Trennungskontrolle
  CAWIN-Daten, werden von zu anderen Zwecken erhoben Daten physisch oder logisch getrennt gespeichert und verarbeitet auf projektbezogen getrennten Systemen. Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.
- Pseudonymisierung und Anonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
  Die Anonymisierung zur Verfügung gestellter Daten für den Überschuldungsreport oder anderweitiger wissenschaftlicher Forschungsprojekte erfolgt durch den Auftraggeber. Soweit eine Anonymisierung nicht möglich ist, werden personenbezogene Daten durch den Auftraggeber pseudonymisiert.

§ 2 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- Weitergabekontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch Verschlüsselung. Möglichkeiten zur verschlüsselten Datenübertragung werden im Umfang der Leistungsbeschreibung des Hauptauftrages sowie der Anlage 1 zur Verfügung gestellt. Ebenso die Möglichkeit einer elektronischen Signatur. Alle Mitarbeiter des Auftragnehmers sind i.S.d. Art. 32 Abs.4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Datensicherzustellen. Eine Weiterleitung von Daten durch den Auftragnehmer erfolgt allenfalls in anonymisierter Form. Mit Vertragsbeendigung erfolgt eine datenschutzgerechte Löschung elektronischer Datenträger und die Vernichtung von Papierdokumenten.
- Eingabekontrolle
  Die Daten werden vom Auftraggeber selbst eingegeben, verändert oder entfernt, so dass die Eingabekontrolle dem Auftraggeber obliegt.

§ 3 Verfügbarkeit, Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO) sowie rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

- Verfügbarkeitskontrolle

institut für finanzdienstleistungen e.V. *(iff)* | Vorstand: Claudia Rutt, Prof. Dr. Ingrid Größl | Geschäftsführende Direktorin: Dr. Sally Peters
Grindelallee 100, 20146 Hamburg +49 (0)40 30 96 91-0 +49 (0)40 30 96 91-22 www.iff-hamburg.de institut@iff-hamburg.de
USt-IdNr. DE 118713543 | AG Hamburg VR 13836 | Hamburger Sparkasse | IBAN DE62 2005 0550 1238 1229 21 | BIC HASPDEHHXXX
Gläubiger-ID: DE39ZZZ00000988279 | GLS Bank | IBAN DE15 4306 0967 1255 4537 00 | BIC GENODEM1GLS

Zum Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust hat der Auftragnehmer ein Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten. Der Auftragnehmer verwendet als Virenschutz Microsoft Defender sowie als Firewall Microsoft Firewall.
Ferner nutzt der Auftragnehmer eine AES-Verschlüsselung mit 256 Bit und den Office-365-Spam-Filter. Für die von der Vertragsdurchführung erfassten Server erfolgt eine Festplattenspiegelung sowie ein regelmäßiges Monitoring. Die Aufbewahrung von Datensicherungen erfolgt an einem sicheren Ort.

- Rasche Wiederherstellbarkeit
  Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen. Ferner greif der Auftragnehmer zur raschen Wiederherstellung von Daten und zur Pflege von Server und IT-Technik auf folgendes Unternehmen zurück: CTNM computertechnologie + neue medien, Neuer Pferdemarkt 13, 20359 Hamburg. Im Übrigen werden Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums aufbewahrt.

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

- Datenschutz-Management
  Eine Übersicht über die Verarbeitungstätigkeiten wird geführt. Die Mitarbeiter des Auftragnehmers sind auf Vertraulichkeit / Datengeheimnis verpflichtet und es bestehen Datenschutz-Richtlinien. Ferner existiert ein formalisierter Prozess zur Bearbeitung von Auskunfts-, Löschungs- und Datenübertragungsanfragen seitens Betroffener
- Incident-Response-Management
  Ein Prozess zur Erkennung, Meldung an die Betroffenen bzw. Aufsichtsbehörden, Umgang und Nachbearbeitung von Sicherheitsvorfällen / Datenpannen existiert und wird jeweils dokumentiert.
- Datenschutzfreundliche Voreinstellungen
  Bei der Auftragsdurchführung durch den Auftragsnehmer werden ausschließlich diejenigen Daten verarbeitet, die für den jeweiligen Zweck erforderlich sind, sowie nach den Grundsätzen der Datenminimierung und -sparsamkeit.
  - Auftragskontrolle

  Es erfolgt durch eine vorherige Prüfung der getroffenen Sicherheitsmaßnahmen und deren Dokumentation eine sorgfältige Auswahl des Auftragnehmers, mit welchem eine Vereinbarung zur Auftragsverarbeitung geschlossen wird. Aus der Vereinbarung ergeben sich unter anderem wirksame Kontrollrechte gegenüber dem Auftragnehmer, die Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen der Bestellpflicht sowie die Vernichtung von Daten nach der Beendigung. Die Kontrolle der Vertragsausführung erfolgt durch Weisungen eines hierfür bestimmten Mitarbeiters, laufende Überprüfungen und Nachkontrollen.

institut für finanzdienstleistungen e.V. *(iff)* | Vorstand: Claudia Rutt, Prof. Dr. Ingrid Größl | Geschäftsführende Direktorin: Dr. Sally Peters
Grindelallee 100, 20146 Hamburg +49 (0)40 30 96 91-0 +49 (0)40 30 96 91-22 www.iff-hamburg.de institut@iff-hamburg.de
USt-IdNr. DE 118713543 | AG Hamburg VR 13836 | Hamburger Sparkasse | IBAN DE62 2005 0550 1238 1229 21 | BIC HASPDEHHXXX
Gläubiger-ID: DE39ZZZ00000988279 | GLS Bank | IBAN DE15 4306 0967 1255 4537 00 | BIC GENODEM1GLS