QUICK-LOHN®
Das Lohnprogramm
für kleine und mittlere Betriebe.

Vereinbarung zur Auftragsverarbeitung für die Quick-Lohn Software Testversion

Vereinbarung

Zwischen der

Quick-Lohn Software GmbH
Wiesenstr. 32
16230 Britz

-nachstehend **Auftragnehmer** genannt-

und

_____

_____

_____

(Bitte tragen Sie hier Ihren Namen und Ihre Anschrift ein.)

-nachstehend **Auftraggeber** genannt-

Britz, den 30.10.19

Präambel

Neben unserer Software ist es insbesondere unsere Kundenbetreuung, die unser Produkt auszeichnet. Sie können innerhalb des Nutzungszeitraums der Testversion unsere Kundenbetreuung vollumfänglich und kostenlos testen. Diese Vereinbarung begründet keine Kosten.

Diese Vereinbarung wird geschlossen, um den datenschutzrechtlichen Anforderungen des Bundesdatenschutzgesetzes (BDSG) und der Datenschutzgrundverordnung (DSGVO), insbesondere des Art. 28 III DSGVO, bei der Bereitstellung und Inanspruchnahme des Dienstes "hinter der Software", der Kundenbetreuung, sowie bei der Verarbeitung von personenbezogenen Daten durch die Kundenbetreuung, gerecht zu werden. Diese Vereinbarung garantiert Ihnen, dass Sie bereits in der Testversion von der Quick-Lohn Software Ihre Löhne und Gehälter mit Echtdaten datenschutzkonform abrechnen und unseren Kundenservice dabei in Anspruch nehmen können.

1 Gegenstand des Auftrages

Gegenstand des Auftrages zur Verarbeitung von personenbezogenen Daten im Bereich der Kundenbetreuung ist insbesondere die Durchführung folgender Aufgaben durch den Auftragnehmer:

- Kundenbetreuung / Support und Fernwartung,

- Kundendatendiagnose

2 Arten und Zwecke der Verarbeitungen

Die aufgrund dieser Vereinbarung getätigten Verarbeitungen von personenbezogenen Daten werden vom Auftragnehmer durchgeführt, um dem Auftraggeber den Service der Kundenbetreuung bei der Nutzung der Testversion von Quick-Lohn, die den Interessenten an der Quick-Lohn-Software beim Erstellen von Lohn- und Gehaltsabrechnungen unterstützt, zur Verfügung stellen zu können. Die von diesem Auftrag umfassten Verarbeitungstätigkeiten ergeben sich in Art, Form, Umfang und zugrunde liegenden Zwecken aus Anlage Nr. 3 und dieser Vereinbarung. Der Auftragnehmer darf diese Verfahren einseitig anpassen, solange und soweit er den Auftraggeber über wesentliche Änderungen dieser Verfahren im Voraus in Textform informiert und eine vierzehntägige Widerspruchsfrist einräumt. Dem Zweckbindungsgrundsatz ist Rechnung zu tragen.

3 Kategorien der betroffenen personenbezogenen Daten und Personen

Während einer Kundenbetreuung per Telefon besteht stets die Möglichkeit, dass der Kundenbetreuer von Quick-Lohn Kenntnis von personenbezogenen Daten aus den Gehalts- und Lohnabrechnungen des Auftraggebers erhält, die in der Testversion von Quick-Lohn gespeichert sind. Bei einer Kundenbetreuung per Fernwartung verarbeitet der Kundenbetreuer von Quick-Lohn zwangsläufig diese personenbezogene Daten. So werden bei der Durchführung des hier zugrunde liegenden Auftrags temporär alle personenbezogenen Daten der Personen aus den Gehalts- und Lohnabrechnungen des Auftraggebers verarbeitet, die in der Testversion von Quick-Lohn gespeichert sind. Insofern der Arbeitgeber die Löhne und Gehälter selbst abrechnet, sind ausschließlich personenbezogene Daten von dem Arbeitgeber und den Arbeitnehmern betroffen. Wurde die Lohnabrechnung an einen Dritten ausgelagert, sind zusätzlich noch personenbezogene Daten dieses Dritten, der abrechnende Stelle, betroffen.

3.1 Personenbezogene Daten der Arbeitnehmer

Bei den Kategorien von personenbezogenen Daten, die den Arbeitnehmern zugerechnet werden können deren Löhne und Gehälter abgerechnet werden sollen, sind folgende Kategorien aufzuzählen.

Vorname, Name, Adresse, Kontaktdaten, Beschäftigungszeiträume und -verhältnisse, Krankenkasse, Personalnummer, Steueridentifikationsnummer und Steuerdaten, Sozialversicherungsnummer, Sozialdaten, Geburtsdatum, Geburtsort, Geburtsland, Wohnort, Kirche, bestimmte Angaben zur Gesundheit, Familienstand, Steuerklasse, alle Details zu Lohn und Gehalt, Urlaub, Urlaubsgelder, Überstunden und Bank- bzw. Kontodaten. Die Informationen, die mit der Gesundheit in Verbindung stehen (Gesundheitsdaten) und die Religionszugehörigkeit, sind besonders sensible Kategorien personenbezogener Daten i.S.d. Art. 9 I DSGVO.

3.2 Personenbezogene Daten des Arbeitgebers (z.B. Unternehmer)

Darüber hinaus werden Kategorien von personenbezogenen Daten des Arbeitgebers verarbeitet. Hierzu zählen: Name, Adresse, Firma, E-Mail-Adresse, Telefonnummer, Ansprechpartner, Betriebsnummer, Steuernummer, Konto- und Bankdaten, Urlaubskassen sowie Berufsgenossenschaftszugehörigkeit.

3.3 Personenbezogene Daten einer Dritten abrechnenden Stelle (z.B. Lohnbüro)

Falls die Lohn- und Gehaltsabrechnung an einen anderen ausgelagert wurde, werden zudem personenbezogene Daten dieser Stelle verarbeitet. Zu diesen personenbezogenen Daten zählen Name des Bearbeiters sowie dessen Kontaktdaten.

4 Rechte und Pflichten des Auftragnehmers

4.1 Weisungsgebundenheit

Der Auftragnehmer ist an die Weisungen des Auftraggebers gebunden. Der Auftragnehmer verarbeitet personenbezogene Daten im Rahmen der hier geregelten Aufträge ausschließlich gemäß den Weisungen des Auftraggebers, es sei denn höherrangiges Recht gebietet eine anderweitige Verarbeitung durch den Auftragnehmer. Im Weiteren gilt Art. 28 III lit. a) DSGVO. Die zugrunde liegenden Weisungen werden unter anderem in dieser Vereinbarung und den Leistungsbeschreibungen hinsichtlich der Zwecke und des Umfangs der Verarbeitung konkretisiert.

4.2 Vertraulichkeit

Der Auftragnehmer behandelt personenbezogene Daten des Auftraggebers absolut vertraulich.

Alle im Kreise des Auftragnehmers tätigenden Personen, die Verarbeitungen von personenbezogenen Daten dieses Auftrages wahrnehmen, sind in einer angemessenen Form und Weise zur Verschwiegenheit und Vertraulichkeit verpflichtet.

4.3 Dokumentierung der Weisungen

Der Auftragnehmer dokumentiert die vom Auftraggeber erhaltenen Weisungen in einem von ihm zu führenden Verzeichnis.

4.4 Mitwirkungspflichten

Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der gesetzlichen Ansprüche der Betroffenen gem. Kapitel III, Art. 12 – 22 DSGVO.

Der Auftragnehmer unterstützt den Auftraggeber in einer angemessenen Art und Weise bei der Einhaltung der in den Artikel 32 bis 36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen und vorherigen Konsultationen.

4.5 Informationspflichten

Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung des Auftrags verstoße gegen Datenschutzvorschriften.

4.6 Zustimmung zur Telearbeit

Der Auftraggeber gestattet dem Auftragnehmer, unter Einhaltung der gesetzlichen Bestimmungen, zur Verarbeitung von personenbezogenen Daten dieses Auftrages auch Angestellte einzusetzen, die von Zuhause aus arbeiten.

5 Rechte und Pflichten des Auftraggebers

5.1 Weisungsrecht

Die Kundenbetreuung und die Kundendatendiagnose kann von jedem beim Auftragnehmer registrierten Ansprechpartner des Auftraggebers beansprucht werden, der sich erfolgreich authentifizieren kann.

5.2 Zusammenarbeit bei Anfragen der Aufsichtsbehörden

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

5.3 Kontrollrechte

Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer, Überprüfungen hinsichtlich der hier geregelten Verpflichtungen des Auftragnehmers durchzuführen. Er kann sich nach rechtzeitiger Anmeldung von der Einhaltung dieser Vereinbarung durch den Auftragnehmer vor Inanspruchnahme einer hier bestimmten Leistung und sodann regelmäßig in angemessener Weise überzeugen. Der Auftragnehmer ist berechtigt dem Auftraggeber etwaig anfallende Kosten, die in Verbindung mit den Kontrollmaßnahmen stehen, in Rechnung zu stellen.

5.4 Fernwartung

Der Auftraggeber verpflichtet sich sämtliche Anwendungen, Ordner und Programme außer Quick-Lohn während und vor eines Fernwartungszugriffes aus Datenschutzgründen zu schließen bzw. geschlossen zu halten.

Der Auftraggeber hat den gesamten Fernwartungszugriff zu überwachen. Der Auftraggeber hat stets das Recht und die Pflicht die Fernwartung zu beenden, falls Vorgänge nicht nach seiner Vorstellung verlaufen.

6 Löschung und Rückgabe von personenbezogenen Daten

Spätestens 6 Monate nach Abschluss der Erbringung der Verarbeitungsleistungen oder früher nach Aufforderung durch den Auftraggeber – hat der Auftragnehmer sämtliche eventuell noch in seinem Besitz befindlichen personenbezogenen Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten, soweit die Daten nicht dem Nachweis der auftrags- und ordnungsgemäßen Leistungserbringung oder gesetzlichen Aufbewahrungspflichten unterliegen oder der Auftraggeber explizit in die fortdauernden Speicherung eingewilligt hat.

7 Haftung

7.1 Gesamtschuldnerische Haftung

Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner.

7.2 Schäden aufgrund unzulässigen oder unrichtigen Datenverarbeitung

Für den Ersatz von Schäden, die eine betroffene Person wegen einer nach dem geltenden Datenschutzrecht unzulässigen oder unrichtigen Verarbeitung von Auftraggeber-Daten im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragnehmer alleine der Auftraggeber verantwortlich.

7.3 Verschuldensnachweis

Der Auftraggeber verpflichtet sich, den Auftragnehmer im Innenverhältnis von allen Ansprüchen Dritter frei zu stellen, solange und soweit er nicht nachweist, dass der Auftragnehmer seinen speziell den Auftragnehmer treffenden Pflichten aus der DSGVO nicht nachgekommen ist oder unter Nichtbeachtung einer rechtmäßig erteilten Weisung des Auftraggebers oder gegen eine rechtmäßig erteilte Weisung gehandelt hat.

7.4 Geldbuße aufgrund Weisung des Auftraggebers

Sollte eine Datenschutzbehörde oder ein Gericht gegen den Auftragnehmer eine Geldbuße aufgrund einer Datenverarbeitung des Auftragnehmers verhängen, die auf einer Weisung des Auftraggebers beruht, hat der Auftraggeber dem Auftragnehmer den entsprechenden Betrag auf schriftliche Mitteilung hin in voller Höhe innerhalb von 30 Tagen ab der schriftlichen Mitteilung zu erstatten.

7.5 Kostenerstattung

Der Auftraggeber hat dem Auftragnehmer sämtliche sich aus der von ihm zu vertretenden Rechtsverletzung gemäß Absatz 3 und 4 ergebenden Kosten zu erstatten, einschließlich der Kosten der Rechtsverfolgung.

7.6 Unbeschränkte Haftung

Der Auftragnehmer haftet unbeschränkt für Vorsatz und grobe Fahrlässigkeit, bei Verletzung einer vertraglich gewährten Garantie sowie nach Maßgabe des Produkthaftungsgesetzes. Für leichte Fahrlässigkeit haftet der Auftragnehmer bei Schäden aus der Verletzung des Lebens, des Körpers und der Gesundheit von Personen. Im Übrigen gilt folgende beschränkte Haftung: Bei leichter Fahrlässigkeit haftet der Auftragnehmer nur im Falle der Verletzung einer wesentlichen Vertragspflicht des Hauptvertrages, deren Erfüllung die ordnungsgemäße Durchführung des Hauptvertrages überhaupt erst ermöglicht und auf deren Einhaltung der Auftraggeber regelmäßig vertrauen darf (Kardinalpflicht). Die Haftung für leichte Fahrlässigkeit ist der Höhe nach beschränkt auf die bei Vertragsschluss vorhersehbaren Schäden, mit deren Entstehung typischerweise gerechnet werden muss.

8 Gebühren für die Aufträge zur Datenverarbeitung

Für die Inanspruchnahme der Kundenbetreuung von Quick-Lohn und aller hier geregelten Aufträge entstehen während des Nutzungszeitraums der Testversion keine Kosten.

9 Geltungsdauer

Diese Vereinbarung ist an die Testversion von Quick-Lohn gekoppelt. Sie gilt solange die Testversion von Quick-Lohn genutzt werden kann. Endet die Nutzungserlaubnis für die Testversion, verliert auch diese Vereinbarung ihre Geltung. Eine Kündigung der Testversion oder dieser Vereinbarung ist nicht notwendig.

10 Datenübermittlungen an einen Drittstaat

Die Datenverarbeitung durch den Auftragnehmer findet ausschließlich im Bereich der Bundesrepublik Deutschland statt. Jede Verlagerung in ein sonstiges Land bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers und hat im Falle der Datenübermittlung in einen nicht EU-Mitgliedstaat unter den besonderen Bestimmungen der DSGVO zu erfolgen.

11 Subauftragsverhältnisse

Als Subauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen und bei denen eine Verarbeitung von personenbezogenen Daten aus dem hier bestimmten Auftragsverhältnis stattfindet, diese aber nicht vom Auftraggeber persönlich erbracht wird.

Der Auftraggeber erteilt hiermit dem Auftragnehmer die grundsätzliche Ermächtigung weitere Subauftragnehmer für die Verarbeitung von personenbezogenen Daten einzuschalten. Jedoch hat der Auftragnehmer den Auftraggeber zuvor zu informieren und zu belehren. Die Belehrung und Information durch den Auftragnehmer über das neue Auftragsverhältnis erfolgt unter Angabe von Name, Anschrift, sowie vorgesehener Tätigkeit des Subauftragnehmers. Dem Auftraggeber wird eine zweiwöchige Frist ab Zugang dieser Information und Belehrung über das neue Unterauftragsverhältnis eingeräumt, um der Beauftragung des Subauftragnehmers zu widersprechen. Der Widerspruch muss begründet werden und hat in Textform zu erfolgen. Erst nach Ablauf der Frist gilt die Genehmigung des Auftraggebers als erteilt.

Mit der Zustimmung zu dieser Vereinbarung erlaubt der Auftraggeber dem Auftragnehmer die in Anlage Nr. 2 aufgeführten Subauftragnehmer zur Erfüllung der dort definierten Aufgaben / Leistungen und Verarbeitungen i.S.d. Art. 4 Nr. 2 DSGVO für die Erbringung der Hauptleistung zu beauftragen.

12 Technische und organisatorische Maßnahmen

Der Auftragnehmer wird seine innerbetriebliche Organisation so gestalten, dass die Datensicherheit gem. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO nach allgemein anerkannten Regeln der Wissenschaft und Technik sichergestellt wird.

Die technischen und organisatorischen Maßnahmen (TOMs) zum angemessenen Schutz der im Auftrag des Auftraggebers verarbeiteten Daten für die Datensicherheit werden von dem Auftragnehmer eingerichtet und dokumentiert. Die TOMs werden dem Auftraggeber zur Prüfung vorgelegt (Anlage Nr. 1 - Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO). Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftragnehmer unverzüglich.

Der Auftragnehmer darf die getroffenen Maßnahmen für die Datensicherheit jederzeit ändern sofern sichergestellt ist, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Die aktuellste Version der Maßnahmen zur Datensicherheit kann durch den Auftraggeber jederzeit angefordert werden und wird ihm durch den Auftragnehmer binnen vierzehn Tagen zur Verfügung gestellt.

13 Schlussbestimmungen

Sollten eine Bestimmung oder Teile dieser Vereinbarung unwirksam sein, wird die Wirksamkeit der übrigen Bestimmungen davon nicht berührt. Die Parteien verpflichten sich, anstelle der unwirksamen Bestimmung eine der unwirksamen Bestimmung möglichst nahekommende, wirksame Bestimmung zu vereinbaren.

Gerichtsstand ist Eberswalde.

Die nachfolgend aufgezählten Anlagen werden je nach Auftrag zum Bestandteil dieser Vereinbarung. Der Auftraggeber kann aktuelle Versionen dieser Anlagen auf Anfrage hin beim Auftragnehmer einsehen.

- Anlage Nr. 1 Technische und organisatorische Maßnahmen nach Art. 32 DSGVO
- Anlage Nr. 2 Subauftragnehmer
- Anlage Nr. 3 Verarbeitungsbeschreibungen

Anlage Nr. 1 - Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Der Auftragsverarbeiter bestätigt dem Auftraggeber die Einhaltung der in dieser Anlage aufgeführten technischen und organisatorischen Maßnahmen zur Datensicherheit.

1 Verschlüsselung

Jede Verarbeitungstätigkeit wird daraufhin überprüft, ob sich ihr Zweck auch ohne unmittelbaren Personenbezug realisieren lässt. Ist dies der Fall, werden lesbare Informationen mit Hilfe eines Verfahrens in eine nicht ohne weiteres interpretierbare Zeichenfolge umgewandelt, soweit diese Maßnahme mit verhältnismäßigen Mitteln und Aufwand umsetzbar ist.

2 Vertraulichkeit (Art. 32 I lit. B DSGVO)

Für die Vertraulichkeit Ihrer personenbezogenen Daten ergreifen wir folgende Maßnahmen:

2.1 Zutrittskontrolle

Der Auftragsverarbeiter verhindert, dass Unberechtigte Zutritt zu Datenverarbeitungsanlagen erlangen können; dies erfolgt bei den von Quick-Lohn eingesetzten Subauftragnehmern durch:

- die Zertifizierung der TeamViewer und NFON Server gemäß ISO 27001,
- andere von Quick-Lohn genutzte Datenverarbeitungsanlagen unterliegen Zutrittsregeln, wie bspw. einem Berechtigungskonzept hinsichtlich der genutzten Schließanlagen.

2.2 Zugangskontrolle

Der Auftragnehmer verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können; dies erfolgt bei Quick-Lohn durch:

- festgelegte und kontrollierte interne Passwortregeln,
- die Verwendung von TeamViewer bei Fernwartungen, das die Eingabe eines EinmalPasswortes und zugehörigen Nutzer-ID vor der Sitzung erforderlich macht,
- eine bereitgestellte Zugangskontrolle in der Quick-Lohn Software, die durch den Auftraggeber aktiviert werden kann,
- die Verpflichtung auf Vertraulichkeit und zur Verschwiegenheit aller uns unterstellen Personen bei Erfüllung der von ihnen erteilten Aufträge im Umgang mit personenbezogenen Daten,
- die schrittweise und kundenfreundliche Authentifizierung bei der Kundenbetreuung und unmittelbar vor der Fernwartung,

2.3 Zugriffskontrolle

Der Auftragnehmer trägt dafür Sorge, dass ausschließlich die zur Nutzung des System Berechtigten, nur auf die ihrer Zugriffsberechtigung unterliegenden Daten, zugreifen können und dass die Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können; dies erfolgt bei Quick-Lohn durch:

- ein differenziertes Berechtigungskonzeptes mit vier Sicherheitsstufen,
- mit dem Authentifizieren durch ein VPN-Zertifikat.

2.4 Trennungskontrolle

Der Auftragnehmer stellt sicher, dass zu unterschiedlichen Zwecken bzw. von unterschiedlichen Auftraggebern erhobene personenbezogene Daten getrennt verarbeitet werden können.

3 Integrität (Art. 32 I lit. B DSGVO)

Für die Integrität Ihrer personenbezogenen Daten ergreifen wir folgende Maßnahmen:

3.1 Weitergabekontrolle

Der Auftragnehmer stellt sicher, dass personenbezogene Daten 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; dies erfolgt bei Quick-Lohn durch:

- Identifizierungs- und Authentifizierungsmechanismen,
- einen festgelegten Empfängerkreis für verschiedene Datenkategorien,
- die SSL-Protokoll / OpenSSL Verschlüsselung der gesamten Kommunikation,
- eine zusätzliche Verschlüsselung des Datenpakets im Bereich der Kundendatendiagnose bei der Übermittlung per E-Mail,
- komplett gesicherte Datenkanäle bei einer TeamViewer-Sitzung, die unter anderem mit einem RSA Public/Private Key Exchange. aufgebaut werden und mit 256-Bit-AES verschlüsselt sind,
- die von uns eingesetzten Telekommunikationsdienstleister und deren Beschäftigten sind gem. § 88 TKG zur Verschwiegenheit verpflichtet.

Die Weitergabekontrolle wird von uns als eine der wichtigsten Schutzebenen angesehen, da sie inhaltlich eng mit der Tätigkeit der Übermittlung in Zusammenhang steht.

3.2 Auftragskontrolle

Der Auftragnehmer organisiert die Verarbeitung so, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können; dies erfolgt bei Quick-Lohn durch:

- die schriftliche Festlegung der Weisungen,
- Kontrolle der Subauftragnehmer,
- schriftliche fixierte und streng kontrollierte Verträge mit Subauftragnehmern,
- ein speziell festgelegtes Identifizierungsverfahrens des Auftraggebers vor Übermittlung von Steuerdaten,
- der Festlegung von Ansprechpartnern und Personen, die Auftraggeber sein können im Kreise aller Auftraggeber.

3.3 Eingabekontrolle

Der Auftragnehmer trägt dafür Sorge, dass nachträglich geprüft und festgestellt werden kann, ob, wann und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind; dies erfolgt bei Quick-Lohn durch:

- die interne Vorschrift, dass personenbezogene Daten aus der Auftragsverarbeitung durch Quick-Lohn nicht inhaltlich verändert werden dürfen, weil diese Verarbeitung dem Auftraggeber obliegt.

4 Verfügbarkeit und Belastbarkeit (Art. 32 I lit. B DSGVO)

Der Auftragnehmer schützt personenbezogene Daten gegen zufällige Zerstörung oder Verlust; dies erfolgt bei Quick-Lohn durch:

- das Verwenden einer Firewall nach dem Stand der Technik,
- das Verwenden eines aktuellen Virenschutzprogramms nach dem Stand der Technik,
- festgelegte Notfallpläne mit den Serveranbietern, sodass bei Serverproblemen schnell Abhilfe geschafft werden kann,
- eine unterbrechungsfreie Stromversorgung (USV) der Server von NFON und TeamViewer,
- die Server bei Mittwald für den Bereich der Kundendatendiagnose werden mittels RAID-Systemen, USV-Anlagen, Notstromaggregaten und Löschanlagen gesichert.

5 Maßnahmen zur Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Um die regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOMs sicherzustellen, werden regelmäßig Sicherheitsüberprüfungen und Sensibilisierungsmaßnahmen sowie Schulungen der Mitarbeitenden durchgeführt.

Anlage Nr. 2 - Subauftragnehmer

Im Bereich der Fernwartung nutzt Quick-Lohn den Dienst der Software “TeamViewer”.

TeamViewer GmbH / Jahnstr. 30 / 73037 Göppingen / Telefon: +49 (0)7161 60692 50 / Fax: 07161 60692 79

Die telefonischen Beratungsgespräche der Kundenbetreuung/Supports werden über die VoIP von NFON AG durchgeführt.

NFON AG / Machtlfingler Str. 7 / 81379 München / Tel.: +49 89 45 30000

Für die Speicherung des Datensatzes im Bereich der Kundendatendiagnose bedient sich Quick-Lohn des Unterauftragnehmers Mittwald, die hierfür den entsprechenden Server bereitstellen.

Mittwald CM Service GmbH & Co. KG / Königsberger Straße 4-6 / 32339 Espelkamp / Telefon: +49 (0) 5772-293-100 / Telefax: +49 (0) 5772-293-333

Die Aufzeichnungen aus den Tätigkeiten der Kundenbetreuer heraus werden auf dem Server der TELTA Citynetz GmbH aufbewahrt.

TELTA Citynetz GmbH / Bergerstr. 105 / 16225 Eberswalde / Tel.: 03334 277500 /Fax: 03334 277510 / E-Mail: info@telta.de

Anlage Nr. 3 – Verarbeitungsbeschreibungen

1 Kundenbetreuung und Fernwartung

Bei Fragen des Auftraggebers rund um die vom Auftragnehmer angebotenen Leistungen, sowie damit in Zusammenhang stehende Fragen bezüglich speziellen Themen zur Lohnabrechnung, steht der Kundenservice vom Auftragnehmer zur Verfügung. Dieser Service beinhaltet neben der Beratung des Auftraggebers, auch das Durchführen von Schulungen. Des Weiteren ist es Aufgabe der Kundenbetreuung die Ergebnisse aus der Kundendatendiagnose mit dem Auftraggeber einvernehmlich umzusetzen, insoweit es um eine inhaltliche Änderung oder Anpassung von personenbezogenen Daten geht. Wenn es zur Problemlösung im Einzelfall erforderlich ist, ist der Auftragnehmer dazu angewiesen und berechtigt eine Fernwartung bei dem Auftraggeber durchzuführen, solange und soweit der Auftraggeber dazu sein Einverständnis erteilt hat. Bei der Fernwartung ist sich der Software TeamViewer zu bedienen. Zu Zwecken der Aufklärung schwieriger Fallkonstellationen beim Auftraggeber ist der Auftragnehmer dazu berechtigt Aufzeichnungen aus den Wartungsgesprächen oder den Fernwartungen heraus vorzunehmen. Diese Aufzeichnungen werden ausschließlich für den Zweck der Problemlösung für den Kunden eingesetzt. Der Auftragnehmer darf mehreren Kundenbetreuern ermöglichen an den hier beschriebenen Tätigkeiten teilzunehmen. Ferner werden in der Kundenbetreuung alle vom Auftraggeber uns gegenüber abgegebenen Aufträge aufbewahrt und verwaltet. Falls von Quick-Lohn Aufzeichnungen über Lohn- oder Gehaltsabrechnungsdaten aus den Beratungsgesprächen der Kundenbetreuung angefertigt werden sollten, erfolgt eine unverzügliche Löschung dieser Daten direkt im Anschluss an das Gespräch, es sei die Daten werden weiterhin für eine Problemlösung im Auftrag des Kunden benötigt. Sodann erfolgt eine Löschung dieser Daten sobald das zugrunde liegende Problem des Kunden gelöst wurde und damit der Zweck der Aufbewahrung entfallen ist.

Mit dem hier erteilten Auftrag können folgende Verarbeitungen i.S.d. Art. 4 Nr. 2 DSGVO einhergehen: Verändern, Anpassung, Löschung, Speichern, Auslesen, Abfragen, Organisieren und Ordnen und die Verwendung.

2 Kundendatendiagnose

Eine Kundendatenanalyse beruht auf technischen Problemen oder Fehlern der Software, Übermittlungsproblemen der Online-Dienste, oder wird durchgeführt, um dem Auftraggeber beim Umgang mit den vom Auftragnehmer angebotenen Leistungen Hilfe zu leisten. Der Auftraggeber entscheidet im Einzelfall, ob eine Kundendatendiagnose durchgeführt werden soll. Im Falle der Durchführung werden alle Daten der letzten drei Jahre aus Quick-Lohn an den Auftragnehmer zu Diagnosezwecken weitergegeben. Der Upload darf aus Quick-Lohn heraus oder per Mail direkt an einen Analysten erfolgen. Die Diagnose wird durch einen Mitarbeitenden des Auftragnehmers durchgeführt. Hierbei wird neben der technischen, auch die inhaltliche Richtigkeit der Daten analysiert. Es werden keine inhaltlichen Änderungen an personenbezogenen Daten vorgenommen. Die Datenpakete aus der Kundendatendiagnose werden entsprechend einer Regelspeicherfrist von einem Jahr nach Ablauf des Jahres ihres Empfangs gespeichert und anschließend gelöscht.

Für eine Kundendatendiagnose ist es erforderlich die folgenden Verarbeitungen i.S.d. Art. 4 Nr. 2 DSGVO durchzuführen: Speichern, Löschung und das Verwenden.