

Vereinbarung zur Auftragsverarbeitung

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 14.01.19

Präambel

Diese Vereinbarung wird als ergänzende Regelung zum Hauptvertrag zur Einhaltung der datenschutzrechtlichen Vorgaben des Bundesdatenschutzgesetzes (BDSG) und der Datenschutzgrundverordnung (DSGVO), insbesondere des Art. 28 III DSGVO, geschlossen.

Der Hauptvertrag ist der Nutzungsvertrag zur Durchführung der Lohnabrechnung mit Quick-Lohn, den beide Parteien geschlossen haben.

1 Gegenstand des Auftrages

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

- Datenübermittlungsverfahren per Quick-Lohn-Meldecenter (M),
- Aufbewahrung der übermittelten Meldungen (M),
- Kundenbetreuung / Support und Fernwartung,
- Kundendatendiagnose
- Online-Datensicherung (D)

(M) betrifft nur diejenigen Auftraggeber, die das Meldecenter nutzen.

(D) betrifft nur diejenigen Auftraggeber, die die Online-Datensicherung in Anspruch nehmen.

Die Verfahren aus den Bereichen Meldecenter und Online-Datensicherung werden zusammen als Online-Dienste bezeichnet.

2 Arten und Zwecke der Verarbeitungen

Die aufgrund dieser Vereinbarung getätigten Verarbeitungen von personenbezogenen Daten werden vom Auftragnehmer durchgeführt, um dem Auftraggeber das Erstellen von Lohn- und Gehaltsabrechnungen zu erleichtern und zu ermöglichen. Die von diesem Auftrag umfassten Verarbeitungstätigkeiten ergeben sich in Art, Form, Umfang und zugrunde liegenden Zwecken aus Anlage Nr. 3, dem Hauptvertrag 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

Die von diesem Auftrag betroffenen personenbezogenen Daten können den Personen zugeordnet werden, die an der zugrunde liegenden Lohn- und Gehaltsabrechnungen beteiligt 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 im Hauptvertrag geregelten Dienste ausschließlich im Auftrag und gemäß den Weisungen des Auftraggebers, die in dieser Vereinbarung und dem Hauptvertrag oder anderen Leistungsbeschreibungen hinsichtlich der Zwecke und des Umfangs bestimmt sind, es sei denn höherrangiges Recht gebietet eine anderweitige Verarbeitung durch den Auftragnehmer. Im Weiteren gilt Art. 28 III lit. a) DSGVO.

4.2 Vertraulichkeit

Der Auftragnehmer behandelt personenbezogene Daten des Auftraggebers absolut vertraulich.

Alle im Kreise des Auftragnehmers tätigen 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 i.S.d. Art. 30 II DSGVO.

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 Auftrages verstoße gegen Datenschutzvorschriften.

Über eventuelle Fehler des Datenübermittlungsverfahrens in den Bereichen der Online-Dienste informiert der Auftragnehmer den Auftraggeber per Telefax oder mit Rückmeldungen, die direkt in Quick-Lohn dem Auftraggeber angezeigt werden.

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

Zur Erteilung von einzelnen Aufträgen in den Bereichen der Online-Dienste sind auf Seiten des Auftraggebers ausschließlich die Personen weisungsbefugt, die sich erfolgreich in Quick-Lohn

authentifizieren können und über das erforderliche Passwort und die entsprechende Kundennummer verfügen.

Die Kundenbetreuung und die Kundendatendiagnose kann von jedem beim Auftragnehmer registrierten Ansprechpartner des Auftraggebers beansprucht werden.

5.2 Verfügbarkeit des Datenübermittlungsverfahrens (M) (D)

Die Daten können an sieben Tagen in der Woche zu jeder Uhrzeit an die Online Dienste eingeliefert werden. Die Weiterleitung der Daten vom Meldecenter an die Finanzbehörden und Sozialversicherungsträger erfolgt arbeitstäglich. Eine zeitweise Nichtverfügbarkeit des Servers kann sich aufgrund von Störungen im Bereich der Telekom oder des Internet-Providers o.ä. ergeben. In diesem Fall werden vom Auftragnehmer alle möglichen Anstrengungen unternommen, um die Störung zu beseitigen.

Für die Richtigkeit der gemeldeten Daten ist allein der Kunde verantwortlich. Der Kunde muss die Daten mindestens vierundzwanzig Stunden vor dem jeweiligen Fälligkeitstermin einliefern.

5.3 Abholung der Quittierungen (M)

Der Auftraggeber ist verpflichtet, regelmäßig in Quick-Lohn zu prüfen, ob Rückmeldungen vom Finanzamt, den Sozialversicherungsträgern oder der Berufsgenossenschaft im Meldecenter vorliegen.

5.4 Datenschutzhinweis durch die Finanzverwaltung (M)

Mit dieser Software werden personenbezogene Daten im Sinne des Art. 4 Nr. 1 DSGVO und Art. 9 I DSGVO zum Zwecke der Verarbeitung erhoben. Hierzu zählen Daten, die zur Steuerveranlagung benötigt werden. Die Nutzung der Daten erfolgt im Rahmen des Art. 6 Abs. 1 UAbs. 1 Buchst. e i.V.m. Abs. 3 UAbs. 1 Buchst. b DSGVO i.V.m. bundes- bzw. landesgesetzlicher Steuergesetze durch die Finanzverwaltung und nur für den genannten Zweck.

Weitere Hinweise zur Datenerhebung durch die Finanzverwaltung finden sich in der [Allgemeine Informationen zur Umsetzung der datenschutzrechtlichen Vorgaben der Artikel 12 bis 14 der Datenschutz-Grundverordnung in der Steuerverwaltung.](#)

5.5 Zusammenarbeit bei Anfragen der Aufsichtsbehörden

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

5.6 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.

5.7 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.

5.8 Vertragsrückabwicklung (M)

Der Auftraggeber trägt im Falle einer Kündigung des Hauptvertrages dafür Sorge, dass er sich bei den Institutionen um- bzw. abmeldet, sodass keine weitere Rückmeldungen von den Institutionen im Meldecenter eingehen. Insofern der Auftraggeber dem nicht nachkommt, erteilt er dem Auftragnehmer die Weisung für eine ordnungsgemäße Rückabwicklung der Vertragsbeziehungen bzw. Meldebestände zu sorgen.

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

Die Gebühren für Aufträge richten sich nach Anlage Nr. 4.

9 Geltungsdauer

Laufzeit und Kündigung dieses Vertrags richten sich nach den Bestimmungen zu Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrages. Eine isolierte Kündigung dieses Vertrages ist ausgeschlossen.

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. 4 Gebühren für die Aufträge zur Datenverarbeitung

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.

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

Für die Vertraulichkeit Ihrer personenbezogenen Daten ergreifen wir folgende Maßnahmen:

2.1 Zugangskontrolle

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

- das Einführen und Kontrollieren interner Passwortregeln,
- das Schaffen der Möglichkeit einer Zugangskontrolle in Quick-Lohn durch den Auftraggeber,
- die Verpflichtung auf Vertraulichkeit und zur Verschwiegenheit aller uns unterstellten Personen bei Erfüllung der von ihnen erteilten Aufträge im Umgang mit personenbezogenen Daten,
- das Erfordernis, sich explizit vor jeder Datenübermittlung einzeln mit einem speziell dafür eingerichteten Passwort und Benutzernamen in Quick-Lohn zu authentifizieren,
- der Protokollierung von Zugriffsversuchen und Log-Ins in den Bereichen der Online-Dienste,
- die Begrenzung der Authentifizierungsmöglichkeiten,
- der schrittweise und kundenfreundliche Authentifizierung bei der Kundenbetreuung und unmittelbar vor der Fernwartung,

2.2 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:

- die Implementierung eines differenzierenden Berechtigungskonzeptes mit vier Sicherheitsstufen,
- mit dem Authentifizieren durch ein VPN-Zertifikat, auf höchster Sicherheitsstufe.

2.3 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:

- die Implementierung von Identifizierungs- und Authentifizierungsmechanismen,
- der Festlegung des Empfängerkreises von Daten,
- Verschlüsselungsverfahren SSL Zertifikat zwischen Client und den Online-Diensten,
- bei der Übermittlung an die Finanzämter wird die vom Finanzamt vorgeschriebene Komponente zur Verschlüsselung benutzt,
- bei der Datenübertragung an und von den Sozialversicherungsträger wird ein SSL Zertifikat zur Verschlüsselung genutzt. Zur Authentifizierung von Quick-Lohn wird zusätzlich ein privates ITSG-Zertifikat genutzt. Weiterhin werden die Daten unter der zusätzlichen Anwendung eines öffentlichen ITSG-Zertifikats der Annahmestelle verschlüsselt und erneut signiert.
- gesamte interne Kommunikation auf SSL-Protokoll / OpenSSL verschlüsselt,

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 Protokollierung der Systemaktivitäten im Bereich Meldecenter

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:

- eine regelmäßige Anfertigung von Sicherungskopien, die auf einem räumlich getrennten Sicherungsmedium gespeichert werden,
- der Verwendung einer Firewall nach dem Stand der Technik,
- der Verwendung eines aktuellen Virenschutzprogramms nach dem Stand der Technik.

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 durchgeführt.

Anlage Nr. 2 - Subauftragnehmer

Quick-Lohn beauftragt die Firma ICA-NET GmbH mit dem Hosting von virtuellen Applikationsservern. Wir bedienen uns dieses Auftragsverarbeiters in den Bereichen der Online-Dienste, um einen von ICA zu Verfügung gestellten Server nutzen zu können.

ICA-NET GmbH / Brieseallee 39 / 16547 Birkenwerder / Tel.: 03303-59609400 / Fax: 03303-59609499 / E-Mail: info@ica-net.de

Nach einer bei Quick-Lohn stattfindenden Umstrukturierungsmaßnahme werden die Dienste, die zuvor von ICA-NET GmbH durchgeführt wurden, auf die TELTA Citynetz GmbH verlagert.

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

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

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 bei barum gespeichert.

barum internet-service GbR / Bergerstraße 105 / 16225 Eberswalde / Tel. 03334 818290 / Mail: info@barum.de

Nach einer bei Quick-Lohn stattfindenden Umstrukturierungsmaßnahme werden die Aufzeichnungen und Aufträge aus den Tätigkeiten einer Kundenbetreuung heraus zukünftig nicht mehr auf einem Server bei barum gespeichert, sondern in unserem CRM-System bei der TecArt GmbH verwahrt. Alle alten Aufzeichnungen aus der Kundenbetreuung, die auf einem Server bei barum gespeichert waren, werden über ihren Aufbewahrungszeitraum bei TELTA gespeichert. Nach Abschluss der Umstrukturierungen werden die personenbezogenen Daten aus den Aufzeichnungen der Kundenbetreuung ausschließlich über das CRM-System von TecArt gesichert.

TecArt GmbH / Fischmarkt 5 / 99084 Erfurt / Telefon: +49 361 302624-0 / E-Mail: info@tecart.de

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

Anlage Nr. 3 – Verarbeitungsbeschreibungen

1 Datenübermittlungsverfahren (M)

Die elektronischen Meldungen werden von Quick-Lohn, welches auf dem PC des Auftraggebers installiert ist, auf Weisung des Auftraggebers hin an das Meldecenter und den Auftragnehmer übertragen. Von dort aus werden die Meldungen an die vorgesehenen Institutionen weitergeleitet. Die Institutionen sind das Finanzamt und die Sozialversicherungsträger. Zu letzteren zählen die Sozial-, Kranken-, Renten, Arbeitslosen-, Pflege- und Unfallversicherungen.

Rückmeldungen von den Institutionen werden vom Meldecenter abgerufen, und dem Auftragnehmer direkt in Quick-Lohn, auf seinem PC, zur Verfügung gestellt.

Für die Datenübermittlung werden die Meldungen beim Auftragnehmer solange gespeichert, bis die dazugehörige Rückmeldung von den Institutionen beim Auftragnehmer eingegangen ist, sodass eine zweifelsfreie Zuordnung zu einzelnen Auftraggebern sichergestellt werden kann.

Das Datenübermittlungsverfahren beinhaltet folgende Verarbeitungen i.S.d. Art. 4 Nr. 2 DSGVO: Erfassen, Organisieren, Ordnen, Speichern, Offenlegung und Übermittlung.

2 Aufbewahrung der Meldungen (M)

Alle Meldungen und Rückmeldungen werden grundsätzlich drei Jahre nach erfolgter Übermittlung an die Institutionen aufbewahrt. Mit Hilfe dieser Daten kann der Auftragnehmer gegenüber dem Auftraggeber nachweisen welche Meldungen von Quick-Lohn für den Auftraggeber an die Institutionen weitergegeben wurden. Außerdem kann der Auftraggeber so ein transparentes, ordnungsgemäßes und zuverlässiges Meldeverfahren bereitstellen und im Falle eines Fehlers diesen i.S.d. Auftraggebers diagnostizieren und auflösen.

Darüber hinaus werden Elstam An-/Um- und Abmeldungen solange aufbewahrt, bis das hier zugrunde liegende Auftragsverhältnis endet. Grund dafür ist, dass der Quick-Lohn in diesen Fällen den Arbeitgeber ggf. teilautomatisiert beim Finanzamt abmeldet und dafür diese Meldungen benötigt.

Der Auftragnehmer greift auf die aufbewahrten Meldungen zu, um Nachfragen des Auftraggebers zu seinen Datensätzen nachkommen zu können und eine reibungslose Verarbeitung i.S.d. Auftrages zu gewährleisten.

Nach Ablauf der hier festgelegten Aufbewahrungsfristen werden die personenbezogenen Daten gelöscht. Es wird für keine anderen als die hier festgelegten Zwecke auf die Datenbanken zurückgegriffen.

Mit dem hier erteilten Auftrag gehen folgende Verarbeitungen i.S.d. Art. 4 Nr. 2 DSGVO einher: Speichern und Löschen, Offenlegung und Übermittlung.

3 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 gegenüber abgegebenen Aufträge aufbewahrt und verwaltet. Mitschnitte aus der Fernwartung heraus werden unverzüglich nach der Lösung des zugrunde liegenden Problems gelöscht. Von der Kundenbetreuung getätigte Mitschriften werden über die gesamte Dauer des Auftragsverhältnisses gespeichert.

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.

4 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 werden nach Ablauf der Regelspeicherfrist von zwei Jahre nach ihrem Eingang gelöscht.

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

5 Online-Datensicherung

Die Online-Datensicherung (ODS) beinhaltet die Speicherung von den personenbezogenen Daten aus der Quick-Lohn-Software der letzten fünf Jahre. Die ODS wird zum einen durchgeführt um dem Auftraggeber stets ein Back-Up seiner lohnabrechnungsrelevanten Daten auf Anfrage hin bereitstellen zu können. Ferner kann die ODS den Auftraggeber bei seinen Aufbewahrungspflichten von lohnabrechnungsrelevanten Daten unterstützen.

Der Kunde kann alle Datenpakete der Online-Datensicherung per Programmanweisung direkt aus der Software heraus löschen. Hilfsweise werden die Datenpakete nach einer maximalen Aufbewahrungsfrist von 10 Jahren nach Ablauf des Jahres ihres Eingangs beim Auftragnehmer gelöscht.

Der Auftraggeber kann die Datenpakete aus der ODS per Programmanweisung aus Quick-Lohn abholen.

Mithin geht die ODS mit den Verarbeitungen i.S.d. Art. 4 Nr. 2 DSGVO in Form des Speicherns, Löschens und Verwendens einher.

Anlage Nr. 4 – Leistung und Preise

1 Preise

Die aktuell gültige Preisliste finden Sie unter www.quick-lohn.de/preise.

2 Preisanpassungsklausel

Preise sind nicht feststehend und können von dem Auftragnehmer nach Vorankündigung in Textform mit einer Frist von einem Monat zum Halbjahresende verändert werden. Widerspricht der Auftraggeber einer Preisänderung binnen zwei Wochen, bleiben die alten Preise gültig. In diesem Falle ist der Auftragnehmer berechtigt, außerordentlich zu kündigen. Widerspricht der Auftraggeber nicht innerhalb oben genannter Frist, gelten die neue Preise ab dem in der Änderungsmitteilung genannten Datum.

3 Zahlungsverzug

Kommt der Auftraggeber seiner Zahlungsverpflichtung nach erfolgloser Mahnung nicht nach, so ist der Auftragnehmer berechtigt, sämtliche Dienstleistungen bis zum Ausgleich der fälligen Zahlungen einzustellen.