Product Service

Mehr Sicherheit.
Mehr Wert.

Gutachten
Nr. 028-713180861-000 Rev. 0

Datenschutz-Gutachten

Anwendung von Software-Systemen

für das Lohnbüro “Lohndirekt”

Gegenstand	Datenschutz-Gutachten der Software des Lohnbüros “Lohndirekt”
Prüfungsart	Gutachten
Grundlage	TÜV SÜD Prüfkatalog zur Qualität von Anwendungs-Software auf der Basis anerkannter Anforderungen und Standards
Prüfspezifikationen	TÜV SÜD Product Service Prüfgrundsätze, basierend auf PPP 13011B:2018
Zeitraum der Gutachten-Erstellung	April 2020 - Juni 2020
Berichtsdatum	02.06.2020
Unternehmen / Auftraggeber	Lohndirekt GmbH (einfach effizient)
Auftrags-Nr.	713180861
Straße / Postfach	Lise-Meitner-Straße 14a
PLZ / Ort	24941 Flensburg
Ansprechpartner	Thomas Petersen (Geschäftsführer)
TÜV-Sachverständiger	Tuan Khai Hoang
Unterauftragnehmer	Hans-Ulrich Bierhahn (Produktspezialist Datenschutz, Datensicherheit)
Ergebnis	Die Anforderungen der Prüfgrundlage sind erfüllt

Hinweis:

Dieser Bericht darf nur in vollständigem Wortlaut wiedergegeben werden. Die Verwendung zu Werbezwecken bedarf der schriftlichen Genehmigung. Er enthält das Ergebnis einer einmaligen Untersuchung an dem zur Prüfung vorgelegten Entwicklungsstand und stellt kein zeitlich unbegrenztes Urteil über Eigenschaften des Produkts dar.

Telefon: + 49 (0)89 50 08 - 268
Telefax: + 49 (0)89 50 08 - 45 10
www.tuev-sued.de
E-Mail: tuankhai.hoang@tuev-sued.de

TÜV SÜD Product Service GmbH
Daimlerstrasse 11
85748 Garchuing
Deutschland

1 Anlass, Auftrag

Es wird eine Revisionsprüfung für das Datenschutz-Gutachten der Anwendung von Software-Systemen für das Lohnbüro „Lohndirekt“ durchgeführt. Die Evaluation bezieht sich auf die Einhaltung datenschutzrechtlicher Bestimmungen beim Betrieb der Software durch die Lohndirekt GmbH.

2 Unternehmen

Durch die Lohndirekt GmbH wird das Lohnbüro „Lohndirekt“ betrieben, das aktuell mit 82 Mitarbeitern für monatlich ca. 2.800 Firmen ca. 45.000 Lohnabrechnungen durchführt. Die Dienstleistung des Lohnbüros „Lohndirekt“ umfasst den gesamten Abrechnungsvorgang als Komplettpaket auf der Basis der gesetzlichen Bestimmungen nach den Vorgaben der Auftraggeber.

Die Datenverarbeitung erfolgt auf der Basis der Software Sage Personalabrechnung der Sage GmbH (nachfolgend als Sage GmbH bezeichnet), für die durch die Lohndirekt GmbH eine Lizenz erworben wurde.

Die Software wird durch die Sage GmbH im Rahmen eines ASP-Hostings betrieben. Dafür nutzt die Sage GmbH Technik der Netz 16 GmbH, die in deren eigenem Rechenzentrum läuft.

Die Ergebnisse der Abrechnung werden den Auftraggebern durch Lohndirekt wahlweise in Papierform oder in elektronischer Form übergeben.

3 Prüfgegenstand

Bei dem Prüfgegenstand handelt es sich um die Anwendung von Software-Systemen für die Realisierung des Lohnbüros Lohndirekt.

<u>Abgrenzung:</u>
Fragen der Funktionalität sowie der Datensicherheit, die keinen Bezug zum Datenschutz haben, werden nicht betrachtet.

Software-Entwicklungsprozesse waren kein Gegenstand der Untersuchung, da das Gutachten einmalig einen konkreten gegenwärtigen Zustand widerspiegeln sollte.

Die Begutachtung erfolgt ausschließlich anhand der zum Zeitpunkt des Gutachtens geltenden Rechtsvorschriften.

4 Maßstäbe, Anforderungen

Zusammenfassend können die Anforderungen folgendermaßen formuliert werden:

Bietet Lohndirekt die Voraussetzungen, die in Deutschland geltenden Datenschutz-Bestimmungen einzuhalten und sind die internen Prozesse bei der Lohndirekt GmbH so beschaffen, dass sie den Datenschutz für die im Rahmen von Lohndirekt erhobenen und verarbeiteten personenbezogenen Daten gewährleisten?

5 Prüfkonzept

Entsprechend dem Auftrag und dem Prüfgegenstand geht es um ein Datenschutz-Gutachten zu Lohndirekt, das eine Aussage darüber treffen soll, ob alle technischen und organisatorischen Maßnahmen getroffen wurden, um die in Deutschland geltenden Datenschutzbestimmungen zu erfüllen.

Grundlage der Begutachtung waren hauptsächlich

- die EU-Datenschutzgrundverordnung - DSGVO - in der berichtigten Fassung vom 19.04.2018 und
- das Bundesdatenschutzgesetz -BDSG-.

Die Beurteilung der wirksamen Umsetzung der gesetzlichen Anforderungen für die Informationssicherheit erfolgte anhand des IT-Grundschutzkompendiums des Bundesamtes für Sicherheit in der Informationstechnik -BSI-.

6 Durchführung

Die Revisionsprüfung für das Datenschutz-Gutachten erstreckte sich über den Zeitraum vom April 2020 bis Juni 2020.

Auf Grund der Corona-bedingten Einschränkungen wurde zur Beurteilung der räumlichen und technischen Rahmenbedingungen für den Betrieb der Software auf die Ergebnisse der Vor-Ort-Überprüfungen der Revisionsprüfung 2018 zurückgegriffen. Das war möglich, da es in den bereits überprüften Standorten Flensburg, Berlin und Leipzig keine Veränderungen der räumlichen oder technischen Rahmenbedingungen gab.

Seit der Revisionsprüfung 2018 ist als neuer Standort die Niederlassung in Norderstedt hinzugekommen. Eine Vor-Ort-Überprüfung dieses Standortes wird unverzüglich nachgeholt, wenn die Aufhebung der Corona-bedingten Beschränkungen dies gestattet.

7 Begriffe

Die Beseitigung aller mit der **Klasse 1** gekennzeichneten Abweichungen ist die Voraussetzung für die Bestätigung der Datenschutz-Konformität. Solange diese Abweichungen nicht beseitigt sind, kann das Gutachten nur einen unzureichenden Datenschutz bescheinigen.

Die mit der **Klasse 2** versehenen Feststellungen kennzeichnen unvollständige Umsetzungen von Datenschutz-Bestimmungen. Das Gutachten wird unter der Auflage erstellt, dass diese innerhalb von 6 Monaten behoben werden.

Hinweise (**Klasse 3**) dienen der weiteren Optimierung, müssen jedoch nicht umgesetzt werden. Zusätzlich werden zu den Ergebnissen Anmerkungen und ggf. Lösungsvorschläge aufgeführt.

„OK“ kennzeichnet Punkte, deren Anforderungen mit positivem Ergebnis (keine Abweichung, keine Feststellung) überprüft wurden.

„Erl.“ kennzeichnet eine nachträgliche Anpassung gemäß den gegebenen Anforderungen, die im Zuge einer Nachprüfung ein positives Ergebnis ergab.

8 Vorgelegte Dokumente

- Anlage zum Leistungsschein 2011/799/9080 vom 28.02.2011
- Aufstellung Dienstleistungsverträge Stand 07.04.2020
- Auftrag Daten-CDs vor Datenlöschung vom 16.01.2020
- Auftrag zur Datenlöschung und Aktenvernichtung
- Auskunftsrecht von Betroffenen gem. Art. 15 DSGVO vom 25.06.2018
- Bericht Penetrationstest durch TÜV SÜD vom 02.11.2018
- Checkliste Ausscheiden eines Mitarbeiters vom 05.03.2018
- Checkliste Datenlöschung Kündiger vom 06.02.2020
- Checkliste IT-ToDos Jahreswechsel vom 20.01.2020
- Datenschutzbericht 2019
- Datenschutzfolgenabschätzung vom 20.03.2019
- Datenschutz- und Datensicherheitskonzept Rev. 2.1 vom 16.01.2020
- Google Ads Data Processing Terms Stand 16.04.2018
- Infopflichten Mitarbeiter vom 04.06.2019
- Informationen zum Datenschutz nach DSGVO vom 26.06.2019
- ISO 27001 Zertifikat Netz 16, gültig bis 05.09.2020
- IT-Richtlinie vom 06.06.2019
- ITSG-Zertifikat für Software der Sage HR Solutions AG, gültig bis 31.10.2020
- Löschkonzept vom 27.04.2020
- Nachweise durchgeführter Datenschutz-Schulungen 2019
- Richtlinie zur Nutzung von Internet und Email vom 13.02.2018
- Speicherung, Sperrung und Löschung der Daten von Interessenten, Nichtinteressenten und Kunden im CRM-System, dem Lohnabrechnungssystem, dem Drucksystem und in Papierform vom 16.01.2020
- Speicherung und Löschung der Logs für Zutrittskontrolle vom 06.06.2019
- Standardvertrag Auftragsverarbeitung nach DSGVO vom 13.02.2018
- Technische und organisatorische Maßnahmen Elektronische Personalakte vom 07.02.2020
- Technische und organisatorische Maßnahmen Lohndirekt vom 06.02.2019
- TÜV-Zertifikat Qualitätsmanagement nach ISO9001:2008, gültig vom 21.06.2019
- Übersicht Datenschutzvorfälle 2018-01/2020
- Übersicht über Zugriffsrechte auf Server 16.01.2020

Fortsetzung nächste Seite

Fortsetzung vorgelegte Dokumente

- Verfahrensanweisung zur Ansprechpartnerverwaltung inkl. Neuanlage von Ansprechpartnern / Änderung oder Löschung von Ansprechpartnern, Neuanlage, Änderung, Löschung sowie Verschlüsselung von Kennwörtern vom 16.01.2020
- Vereinbarung über Auftragsverarbeitung (Lohndirekt als Auftraggeber) vom 13.02.2018
- Verpflichtungserklärung auf das Datengeheimnis vom 05.06.2019
- Verschwiegenheitsverpflichtung für externe Dienstleister vom 04.06.2019
- Vertrag über Auftragsverarbeitung mit der Sage GmbH vom 02.05.2018
- Verzeichnis der Verarbeitungstätigkeiten Stand 30.04.2020

9 Gutachten

9.1 Ausgangssituation

Durch die Lohndirekt GmbH Flensburg wird das Lohnbüro Lohndirekt betrieben, das als Dienstleistung den gesamten Abrechnungsvorgang als Komplettpaket auf der Basis der gesetzlichen Bestimmungen nach den Vorgaben der Auftraggeber durchführt.

Eine Firma, welche die Lohnabrechnung über Lohndirekt abwickeln möchte, muss im Rahmen der Vertragsanbahnung zunächst ihre Firmen-Stammdaten einschließlich der Kontaktdaten von Ansprechpartnern mittels Checklisten an die Lohndirekt GmbH (nachfolgend Lohndirekt genannt) übergeben. Durch Lohndirekt werden diese Daten in einem selbst entwickelten, auf PostgreSQL basierenden CRM-System erfasst.

Nach Vertragsabschluss übergibt die beauftragende Firma (nachfolgend Auftraggeber genannt) detailliertere Daten zur eigenen Firma mit Hilfe eines Firmenstammbogens an Lohndirekt. Die relevanten Daten der eigenen Mitarbeiter werden vom Auftraggeber mit Hilfe von Mitarbeiter-Stammbögen bzw. Mitarbeiter-Bewegungsdatenbögen an Lohndirekt übergeben.

Die Verarbeitung der übergebenen Daten durch Lohndirekt erfolgt auf der Basis der Software Sage Personalabrechnung der Sage GmbH (nachfolgend Sage GmbH genannt), für welche Lohndirekt eine Lizenz erworben hat. Zum Zeitpunkt des Gutachtens wird mit dem System Sage HR Suite 2019.4.1 gearbeitet.

Die Software läuft in Form eines ASP-Hostings, mit dessen Durchführung Lohndirekt die Sage GmbH beauftragt hat.

Zur Realisierung des ASP-Hostings nutzt die Sage GmbH im Rahmen eines Unterauftragsverhältnisses Technik eines Unterauftragnehmers in dessen eigenem Rechenzentrum. Bei diesem Unterauftragnehmer handelt es sich um die Netz 16 GmbH.

Die Ergebnisse der Abrechnung werden den Auftraggebern durch Lohndirekt wahlweise in Papierform oder in elektronischer Form übergeben.

Lohndirekt ist nach ISO 9001 zertifiziert.

Das Rechenzentrum der Netz 16 GmbH, in dem die technische Verarbeitung der Daten erfolgt, ist ebenfalls nach ISO 27001 zertifiziert.

Lohndirekt betreibt Niederlassungen in Berlin, Leipzig und Norderstedt. Von allen diesen Niederlassungen aus wird über VPN auf das interne Netz von Lohndirekt in Flensburg und von dort auf die o.g. Systeme zugegriffen. Eine Datenspeicherung erfolgt in diesen Niederlassungen nicht. Auch der Internet-Zugang dieser Niederlassung wird via VPN über die Zentrale in Flensburg hergestellt.

9.2 Zulässigkeit

Lohndirekt gehört im Sinne des Bundesdatenschutzgesetzes - BDSG - zum nicht öffentlichen Bereich.

Bei der Bewertung der datenschutzrechtlichen Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch Lohndirekt müssen das CRM-System und das Lohnbüro gesondert betrachtet werden.

9.2.1 CRM-System

Rechtliche Einordnung

Im CRM-System können sich personenbezogene Daten in Form der Kontaktdaten der Ansprechpartner bei den Interessenten bzw. bei den Auftraggebern befinden. Diese umfassen neben dem Namen, der Firmenadresse und eventuell der Funktion des Ansprechpartners dessen Telefon- und Faxnummern sowie Mailadressen. Die Daten werden ausschließlich durch Lohndirekt und ausschließlich zur Vertragsanbahnung bzw. Vertragsdurchführung genutzt. Eine Übermittlung der Daten an Dritte erfolgt nicht.

Wenn kein Vertrag zustande kommt, werden die personenbezogenen Daten der Interessenten durch Überschreiben mit dem Buchstaben „X“ gelöscht. Damit stellen die verbliebenen Daten keine personenbezogenen Daten i.S.d. Art. 4 Ziff. 1. DSGVO mehr dar und ihre Verarbeitung fällt gem. Art. 3 DSGVO nicht mehr in den Geltungsbereich der DSGVO.

Kommt ein Vertrag zustande, werden die Daten der Auftraggeber nach Ablauf der gesetzlichen Aufbewahrungsfristen im CRM-System durch Überschreiben mit dem Buchstaben „X“ gelöscht. Damit stellen die verbliebenen Daten im CRM-System keine personenbezogenen Daten i.S.d. Art. 4 Ziff. 1. DSGVO mehr dar und ihre Verarbeitung fällt gem. Art. 3 DSGVO nicht mehr in den Geltungsbereich der DSGVO.

Rechtsgrundlagen der Erhebung, Verarbeitung und Nutzung

Die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten im CRM-System erfolgen zum Zwecke der Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dem (potentiellen oder tatsächlichen) Auftraggeber.

Die Zulässigkeit ergibt sich aus Art. 6 Abs. 1 lit. f DSGVO.

9.2.2 Lohnbüro

Rechtliche Einordnung

Durch Lohndirekt erfolgt im Rahmen des Lohnbüros keine Verarbeitung personenbezogenen Daten für eigene Zwecke. Die Verarbeitung der Mitarbeiterdaten des Auftraggebers erfolgt ausschließlich im Auftrag des Auftraggebers, welcher der Verantwortliche i.S.d. Art. 4 Ziff. 7 DSGVO ist. Die Mitarbeiter-Daten werden durch den Verantwortlichen mit Hilfe der Mitarbeiter-Bögen an Lohndirekt übergeben.

Lohndirekt erwirbt keinerlei Rechte an im Rahmen des Lohnbüros erhobenen und verarbeiteten personenbezogenen Daten.

Die Zwecke und die Mittel der Verarbeitung werden von den Auftraggebern vorgegeben und durch Lohndirekt entsprechend dieser Vorgaben im System umgesetzt. Bei der Anwendung der Vorgaben hat Lohndirekt keinerlei Entscheidungsspielräume.

Rechtsgrundlagen der Erhebung, Verarbeitung und Nutzung
Lohndirekt ist Auftragsverarbeiter i.S.d. Art. 4 Ziff. 8 DSGVO.

Seitens Lohndirekt ist die Verarbeitung zulässig, soweit diese im Rahmen des Auftrages durch den Auftraggeber erfolgen und die weitergehenden Anforderungen aus der Auftragsverarbeitung (siehe 9.3.) erfüllt werden.

9.3 Erfüllung rechtlicher Datenschutzanforderungen

9.3.1 Anforderungen aus der Auftragsdatenverarbeitung

Lohndirekt als Auftragnehmer

Auf Grund der Tatsache, dass Lohndirekt gegenüber den Auftraggebern ein Auftragsverarbeiter im Sinne des Art. 4 Ziff. 8 ist, obliegen Lohndirekt folgende Rechtspflichten:

- Gewährleistung hinreichender Garantien, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit der DSGVO erfolgt und der Schutz der betroffenen Personen gewährleistet wird (Art. 28 Abs. 1 DSGVO)
- Beauftragung von weiteren Auftragsverarbeitern nur mit Genehmigung der Verantwortlichen (Art. 28 Abs. 2 DSGVO)
- Verarbeitung auf der Grundlage eines Vertrages mit dem Auftraggeber, der den Festlegungen des Art. 28 Abs. 3 DSGVO entspricht.
- Verarbeitung der Daten ausschließlich entsprechend der Weisungen des Auftraggebers (Art. 29 DSGVO)
- Gewährleistung, dass alle unterstellten Personen auf das Datengeheimnis verpflichtet sind und darüber belehrt wurden, dass sie die Daten ausschließlich auf Weisung des Auftraggebers verarbeiten dürfen (Art. 29 i.V.m. Art. 32 Abs. 4 DSGVO)
- Gewährleistung technischer und organisatorischer Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus gemäß Art. 32 DSGVO
- Umsetzung aller Vorgaben des Auftraggebers entsprechend Art. 28 Abs. 3 lit.a DSGVO
- unverzügliche Meldung von Verletzungen des Schutzes personenbezogener Daten an den Auftraggeber
- Benennung eines Datenschutzbeauftragten (Art. 37 DSGVO i.V.m. §38 BDSG)

Die Erfüllung dieser Rechtspflichten durch Lohndirekt ist gewährleistet. Die entsprechenden Maßnahmen sind schriftlich angewiesen und dokumentiert.

Die Beschäftigten werden bei Beginn ihrer Tätigkeit für Lohndirekt mit den Datenschutzanforderungen vertraut gemacht und auf das Datengeheimnis verpflichtet. Alle Beschäftigten nehmen darüber hinaus an den jährlichen Datenschutzschulungen teil.

Die technischen und organisatorischen Maßnahmen sind in einem Sicherheitskonzept sowie einer vertiefenden Darstellung beschrieben, das den Auftraggebern zur Verfügung steht. Weitere Angaben zu den technischen und organisatorischen Maßnahmen sind im Abschnitt 9.4 aufgeführt.

Es ist ein Datenschutzbeauftragter benannt. Weitere Angaben dazu sind im Abschnitt 9.3.2 aufgeführt.

Lohndirekt als Auftraggeber

Mit dem Betrieb der Software im Rahmen eines ASP-Hostings hat Lohndirekt die Sage GmbH beauftragt. Damit wird

- Lohndirekt gegenüber der Sage GmbH zum Auftraggeber
- die Sage GmbH gegenüber Lohndirekt zum Auftragnehmer
- die Sage GmbH gegenüber den Auftraggebern (Kunden) von Lohndirekt zum Unterauftragnehmer

Aus der rechtlichen Stellung von Lohndirekt als Auftraggeber gegenüber der Sage GmbH als Auftragnehmer ergeben sich für Lohndirekt folgende Rechtspflichten:

- der Sage GmbH müssen dieselben Datenschutzpflichten auferlegt werden, die Lohndirekt aus dem Vertrag mit den Auftraggebern (Kunden) auferlegt werden (Art. 28 Abs. 4 DSGVO)
- Gewährleistung, dass die Vorgaben der Auftraggeber (Kunden) von Lohndirekt im vollen Umfang auch durch die Sage GmbH umgesetzt werden

Diese Rechtspflichten wurden und werden durch Lohndirekt im vollen Umfang erfüllt.

9.3.2 Datenschutzbeauftragter

Entsprechend Art. 37 DSGVO i.V.m. §38 BDSG ist durch Lohndirekt ein Datenschutzbeauftragter zu benennen, der die Anforderungen des Art. 37 Abs. 5 DSGVO erfüllt und entsprechend der Art. 38 und 39 DSGVO tätig wird.

Als Datenschutzbeauftragter ist eine juristische Person, die compolicy GmbH, schriftlich benannt. Diese berichtet direkt an die Geschäftsführung, ist gemäß Art. 38 DSGVO in die Prozesse eingebunden und nimmt die Aufgaben entsprechend Art. 39 DSGVO wahr.

Die Benennung einer juristischen Person als Datenschutzbeauftragten wird als fragwürdig angesehen.

Durch die Regelungen des neuen BDSG wurden ergänzend zu Artikel 37 Abs. 1 DSGVO de facto die bisher geltenden Regelungen des alten BDSG übernommen, in dem ausdrücklich vom Datenschutzbeauftragten als Person die Rede war. Außerdem wird im neuen BDSG ausnahmslos von „dem Datenschutzbeauftragten oder der Datenschutzbeauftragten“ gesprochen, was sinnlos wäre, wenn sich die Aussagen nicht auf eine Person beziehen würden.

Die Formulierung des Artikel 37 Abs. 6 DSGVO, dass der Datenschutzbeauftragte seine Aufgaben auf Grundlage eines Dienstleistungsvertrages erfüllen kann, wird als keine hinreichende Begründung der Zulässigkeit der Benennung einer juristischen Person als Datenschutzbeauftragter angesehen. Sie ist nach dem Verständnis des Gutachters eine Fortführung des bisherigen Konstrukts der Bestellung einer Person außerhalb der verantwortlichen Stelle gem. §4f Abs. 2 Satz 3 BDSG (alt).

Unabhängig davon wird auf die Ausführungen des Kommentars zur DSGVO von Kühling/Buchner (Verlag C.H.BECK) zu diesem Thema verwiesen:

„Die Frage, ob juristische Personen als Datenschutzbeauftragte benannt werden dürfen, regelt das Gesetz nicht. Die in Abs. 5 genannten Anforderungen an die Qualifikation zeigen aber, dass der Gesetzgeber eine natürliche Person im Auge hatte, auch wenn letztlich die Frage offen bleiben muss. Im Hinblick auf die erhebliche Sanktionsdrohung sollte aber in den Fällen, in denen die Benennung verpflichtend ist, besser eine natürliche Person benannt werden."
(ebenda, Seite 666, Abschnitt 36)

Dieser Empfehlung schließt sich der Gutachter an. Es wird empfohlen, eine Person als Datenschutzbeauftragten zu benennen.

9.3.3 Datenschutz-Schulung der Beschäftigten

Alle Beschäftigten wurden zu Beginn ihrer Tätigkeit mit den Datenschutz-Vorschriften vertraut gemacht. Darüber hinaus finden für alle Beschäftigten jährliche Datenschutz-Schulungen statt, die schriftlich nachgewiesen werden.

9.3.4 Spezielle Anforderungen an den Webauftritt

Die Vertragsanbahnung wie auch andere Kommunikationen mit potentiellen Auftraggebern oder Auftraggebern erfolgen u.a. über die Webseiten von Lohndirekt. Diese nutzen neben einem technisch notwendigen Cookie auch Cookies für statistische und Marketing-Zwecke. Gemäß Urteil des EuGH vom 01.10.2019 muss für das Setzen technisch nicht notwendiger Cookies eine Einwilligung eingeholt und nachgewiesen werden, die den Bedingungen des Art. 7 DSGVO entspricht.

9.3.5 Anforderungen aus anderen Bestimmungen

Es gibt keine weiteren Datenschutz-Anforderungen an den Betrieb des Lohnbüros durch Lohndirekt.

Für die Auftraggeber von Lohndirekt können sich unter Umständen weitergehende Datenschutz-Anforderungen ergeben (z.B. in Bezug auf besondere Kategorien personenbezogene Daten gemäß Art. 9 DSGVO i.V.m. §22 BDSG). Lohndirekt ist in der Lage, solchen Anforderungen auf entsprechende Weisungen der Auftraggeber hin zu entsprechen.

Lohndirekt verfügt über alle technischen und organisatorischen Voraussetzungen, um im Rahmen des Tätigkeitsfeldes „Lohnbüro" Aufträge zur Erfüllung eventueller weitergehenden datenschutzrechtlicher Pflichten zu erfüllen.

9.3.6 Datenschutz-Dokumente

Aus den Datenschutzbestimmungen, die für die Auftragsverarbeitung durch Lohndirekt gelten, ergibt sich die Verpflichtung zum Führen der nachfolgend aufgeführten Datenschutz-Dokumente:

Dokument	Rechtsgrundlage	Status
Datenschutz- und Informationssicherheitskonzept	Art. 32 DSGVO	vorhanden
Nachweis der Verpflichtung auf das Datengeheimnis	Art. 29 i.V.m. Art. 32 Abs. 4 DSGVO	vorhanden
Verträge über die Auftragsverarbeitung durch Lohndirekt	Art. 28 Abs. 3 DSGVO	vorhanden
Vertrag über Auftrags-Verarbeitung durch die Sage GmbH	Art. 28 Abs. 3 DSGVO	vorhanden
Vertrag Auftragsverarbeitung (Aktenvernichtung) durch Veolia	Art. 28 Abs. 3 DSGVO	vorhanden
Lösch- / Anonymisierungs-Pseudonymisierungskonzept	Art. 32 Abs. 1 Buchst. a	vorhanden
Dokumentation der technischen und organisatorischen Maßnahmen	Art. 32 DSGVO	vorhanden

9.4 Einzelergebnisse zu technischen und organisatorischen Maßnahmen

Es wird den Auftraggebern ein Grundniveau technischer und organisatorischer Maßnahmen entsprechend Art. 32 DSGVO angeboten, der den Interessenten eine Entscheidung gemäß Art. 28 Abs. 1 DSGVO gestattet. Diese Maßnahmen waren Gegenstand des Audits.

Weitergehende Forderungen von Auftraggebern in Bezug auf technische und organisatorische Maßnahmen, die über dieses Grundniveau hinausgehen, liegen aktuell nicht vor.

Ergebnisse			**Klasse**
9.4.1	Was	**Zutrittskontrolle**	**OK**
	Detail	Der Zutritt zu den Geschäftsräumen von Lohndirekt in Flensburg ist nur mit Transponder oder die Eingabe eines Sicherheitscodes möglich. Der Serverraum ist durch eine Tür mit einem zusätzlichen Sicherheitsschloss gesichert. Die Tür zum (Papier-) Archiv, das sich in einem anderen Gebäude befindet, ist mit einer elektronischen Zutrittskontrollanlage gesichert. Außerhalb der Geschäftszeiten ist das gesamte Gebäude, in dem sich das Archiv befindet, verschlossen. Die Wände aller Räume einschließlich des Archivs weisen eine ausreichende Stabilität auf. Sowohl das Objekt von Lohndirekt als auch das Archiv sind über Alarmanlagen gesichert, die bei der Sicherheit Nord GmbH auflaufen. Jede Nacht erfolgen darüber hinaus durch diesen Wachdienst mindestens 3 Kontrollen zu unregelmäßigen Zeitpunkten. Die Niederlassung Berlin ist durch ein Sicherheitsschloss gesichert. Außerhalb der Geschäftszeiten ist zusätzlich das gesamte Bürogebäude verschlossen und wird durch einen Wachdienst überwacht. Die Niederlassung Leipzig ist durch ein Sicherheitsschloss und eine Einbruchmeldeanlage gesichert, die Alarm bei einem Wachdienst aufweist. In beiden Niederlassungen wäre ein unbefugter Zutritt durch die Fenster nur mit einem unverhältnismäßig hohen Aufwand möglich. Die Daten der Auftraggeber werden ausschließlich im Rechenzentrum der Netz 16 GmbH verarbeitet, in dem eine Zutrittskontrolle auf höchstem Niveau gegeben ist.	
	Kommentar	*Die Zutrittskontrolle zum Standort Flensburg sowie zu den Niederlassungen Berlin und Leipzig ist im erforderlichen Maße gewährleistet.*	

Ergebnisse			Klasse
		Die Zutrittskontrolle zur Niederlassung Norderstedt wird Gegenstand einer Vor-Ort-Überprüfung, sobald die Corona-bedingten Einschränkungen das gestatten.	
9.4.2	Was	**Zugangskontrolle**	**OK**
	Detail	Es werden die Standard-Richtlinien von Windows 10 für Passwörter umgesetzt. Die Passwörter sind 90 Tage gültig. Root- und Administrator-Accounts sind nur den Administratoren bekannt und bei der Geschäftsführung schriftlich hinterlegt. Ein externer Zugang ist für den Geschäftsführer (auf Exchange) und den Linux-Admin (auf das Linux-System) eingerichtet. Diese Zugänge erfolgen über ein verschlüsseltes VPN (IPSEC 256) Darüber hinaus gibt es einen Zugang für die Niederlassung Berlin, der über ein mit 3DES verschlüsseltes VPN realisiert wird. Die Niederlassungen Leipzig und Norderstedt sind über ein verschlüsseltes VPN IPSec IKEv2 angebunden Die Daten der Auftraggeber werden ausschließlich im Rechenzentrum der Netz 16 GmbH gespeichert. Ein Zugang zu diesen Systemen ist nur über einen Citrix-Server möglich, zu dem eine VPN-Verbindung besteht. Die Bearbeitungsergebnisse werden im Rechenzentrum als XML-Dateien auf einem SFTP-Server bereitgestellt, von diesem durch Lohndirekt abgeholt und ausgedruckt. Konkrete Verfahrensweisen für die Gewährleistung der Zugangskontrolle sind im Datenschutz- und Sicherheitskonzept (Rev. 2.1 vom 16.01.2020) festgelegt, das zum Audit vorgelegt wurde.	
	Kommentar	*Es ist mit ausreichender Sicherheit gewährleistet, dass die Datenverarbeitungssysteme nicht durch Unbefugte genutzt werden können.*	
9.4.3	Was	**Zugangskontrolle**	**OK**
	Detail	Alle USB-Schnittstellen werden über DriveLock geschützt. Für den Malware-Schutz kommt ein System von TrendMicro zum Einsatz.	
	Kommentar	*Der Schutz der Systeme vor Malware- Angriffen ist nach dem aktuellen Stand der Technik gewährleistet.*	

Ergebnisse			Klasse
9.4.4	Was	**Zugangskontrolle**	**OK**
	Detail	Für die Nutzung des DATA-Terminals bietet Lohndirekt den Kunden darüber hinaus die Nutzung einer 2-Faktor-Authentisierung per Handy an.	
	Kommentar	*Es ist mit ausreichender Sicherheit gewährleistet, dass die Datenverarbeitungssysteme nicht durch Unbefugte genutzt werden können. Die angebotenen Maßnahmen entsprechen dem Stand der Technik.*	
9.4.5	Was	**Zugangskontrolle**	**OK**
	Detail	Sowohl der Penetration Test des TÜV SÜD als auch ein technischer Sicherheitstest im Rahmen der Begutachtung ergaben keine Anhaltspunkte für Schwachstellen mit mittlerem oder hohem Risiko für unbefugtes Eindringen aus dem öffentlichen Netz.	
	Kommentar	*Das unbefugte Eindringen in die Systeme aus dem öffentlichen Netz mit Hilfe von Hacker-Angriffen würde einen unverhältnismäßig hohen Aufwand erfordern. Es ist ein ausreichender Schutz gegen derartige Angriffe gegeben.*	
9.4.6	Was	**Zugriffskontrolle**	**OK**
	Detail	Für das Lohnbüro werden die Zugriffskontrollmechanismen der Sage-Software genutzt. Aktuell kommt Sage HR Suite 2019.4.1 zum Einsatz. Für das CRM-System ist ein eigenes Zugriffssystem realisiert. Jeder Mitarbeiter hat seinen eigenen Account, der einer Standardrolle zugewiesen ist. Details der Zugriffskontrolle sind im Datenschutz- und Sicherheitskonzept (Rev. 2.1 vom 16.01.2020) festgelegt, das zum Audit vorgelegt wurde	
	Kommentar	*Sowohl in Bezug auf die technischen Systeme als auch hinsichtlich der organisatorischen Festlegungen wurden alle Voraussetzungen dafür geschaffen, dass die befugten Mitarbeiter nur auf die Daten zugreifen können, für die sie eine Berechtigung besitzen.*	
9.4.7	Was	**Eingabekontrolle**	**OK**
	Detail	Sowohl im Lohnbüro als auch im CRM-System kann nachträglich überprüft und festgestellt werden, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind.	

Ergebnisse			Klasse
		Dafür werden die Standard-Funktionen der Sage-Software genutzt. Das CRM-System realisiert eine eigene Protokollierung aller Eingaben.	
	Kommentar	*Die Eingabekontrolle ist im erforderlichen Maß gewährleistet.*	
9.4.8	Was	**Weitergabekontrolle**	**OK**
	Detail	Auf die Daten des Lohnbüros, die ausnahmslos im Rechenzentrum der Netz 16 GmbH gespeichert sind, wird über Citrix-Server zugegriffen. Die Verbindung zu den Citrix-Servern erfolgt über ein verschlüsseltes VPN (IPSEC 256). Die Übermittlung der XML-Dateien mit den Abrechnungsergebnissen vom Rechenzentrum zu Lohndirekt erfolgt über einen SFTP-Server und ein verschlüsseltes VPN (IPSEC 256)	
	Kommentar	*Es kann überprüft und festgestellt werden, an welchen Stellen eine Übermittlung personenbezogener Daten mit Einrichtungen der Datenübertragung vorgesehen ist.* *Die Datenübertragungen sind exakt festgelegt und werden protokolliert und kontrolliert.* *Es ist mit ausreichender Sicherheit gewährleistet, dass die Daten während der Datenübertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.*	
9.4.9	Was	**Weitergabekontrolle**	**OK**
	Detail	Remote-Zugriffe auf Computer im Objekt von Lohndirekt sind nur bei vier Stellen möglich: Der Geschäftsführer kann remote auf Exchange zugreifen, und der Linux-Admin auf die Linus-Systeme. Diese Zugriffe erfolgen über ein verschlüsseltes VPN (IPSEC 256). Der Zugang der Niederlassung Berlin wird über ein mit 3DES verschlüsseltes VPN realisiert. Die Anbindung der Niederlassungen Leipzig und Norderstedt erfolgt über ein verschlüsseltes VPN IPSec IKEv2.	

Ergebnisse			Klasse
	Kommentar	*Remote-Zugriffe können nur über die definierten Schnittstellen und durch die definierten Personen erfolgen.* *Die Datenübertragungen über Remote-Zugriffe werden protokolliert und kontrolliert.* *Es ist mit ausreichender Sicherheit gewährleistet, dass die Daten während der Remote-Zugriffe nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.*	
9.4.10	Was	**Weitergabekontrolle**	**OK**
	Detail	Daten von Mitarbeitern (neue Stammdaten, Veränderungsdaten) werden durch die Auftraggeber in Papierform, als Fax oder per Email an Lohndirekt gesandt. Der Transport von Unterlagen in Papierform erfolgt auf dem Postweg. Für die Übersendung von Daten per Emails wird den Auftraggebern durch Lohndirekt dringend die Nutzung eines Verschlüsselungsverfahrens empfohlen. Dafür werden seitens Lohndirekt mehrere Alternativen angeboten. An allen Stellen, bei denen Kunden auf die Systeme zugreifen, erfolgt die Übermittlung über https. Datenübermittlungen von Lohndirekt an die Auftraggeber erfolgen entweder gegenständlich (Papierform / CD) oder per Email. Bei der gegenständlichen Übermittlung werden die Datenträger durch DHL zugestellt. Sowohl bei der Zusammenstellung der Datenträger als auch bei deren Bereitstellung für den Versand sind alle Voraussetzungen gegeben, dass nicht Unbefugte in den Besitz der Datenträger kommen. Bei der Übermittlung per Email wird den Auftraggebern durch Lohndirekt dringend empfohlen, sich die Mail verschlüsselt zusenden zu lassen. Dafür werden seitens Lohndirekt mehrere Alternativen angeboten.	
	Kommentar	*Die Stellen, an welchen Übermittlungen personenbezogener Daten mit Einrichtungen der Datenübertragung erfolgen, sind eindeutig definiert.* *Die Arten der Datenübertragungen sind exakt festgelegt und werden protokolliert und kontrolliert.* *Seitens Lohndirekt sind alle Voraussetzungen gegeben, um sichere Datenübertragungen entsprechend der Forderungen der Auftraggeber zu realisieren.*	

Ergebnisse			Klasse
9.4.11	Was	**Weitergabekontrolle**	**OK**
	Detail	Eine Mailverschlüsselung nach verschiedenen Verschlüsselungsstandards wird mit Hilfe der aktuellen Version von CipherMail realisiert.	
	Kommentar	*Es kann mit den verschiedensten, bei den Kunden vorhandenen Mailverschlüsselungssystemen kommuniziert werden.*	
9.4.12	Was	**Verfügbarkeitskontrolle**	**OK**
	Detail	Es erfolgt eine tägliche Komplettsicherung aller Systeme, Daten und Lizenzen. Dabei wird ein 5-Tage-Generationen-Prinzip verwirklicht.	
	Kommentar	*Die Daten- und Systembackups erfüllen die Voraussetzungen, um die Daten vor zufälliger Zerstörung oder Verlust zu schützen.*	
9.4.13	Was	**Verfügbarkeitskontrolle**	**3**
	Detail	Der Anschluss an das externe Netz erfolgt standardmäßig über eine 200MBit-Glasfaserleitung von T-Systems. Als Backup dient eine von der Standleitung unabhängige 6MBit-ADSL-Leitung mit fester IP-Adresse. Bei einem Ausfall beider Leitungen wäre darüber hinaus immer noch ein Minimal-Zugriff auf Daten der Kunden über einen UMTS-Router möglich.	
	Kommentar	*Die derzeitigen Maßnahmen zur Gewährleistung der Verfügbarkeit können kurz- und mittelfristige Ausfälle einzelner elektronischer Kommunikationswege kompensieren.* *Es wird empfohlen, Notfallmaßnahmen für den mittelfristigen Komplettausfall aller elektronischen Kommunikationswege zu erarbeiten (z.B. manuelle Ersatzmethoden zur Ermittlung von Schätzwerten, provisorische Nutzung von Ausweichräumen usw.)*	
9.4.14	Was	**Verfügbarkeitskontrolle**	**OK**
	Detail	Für den Fall eines Komplettausfalles des Objektes von Lohndirekt können Räume der Nachbarfirma als Ausweichobjekt genutzt werden.	
	Kommentar	-	
9.4.15	Was	**Verfügbarkeitskontrolle**	**OK**
	Detail	Papierdokumente werden nach ca. einem Jahr gescannt und elektronisch archiviert.	

Ergebnisse			Klasse
		Papier-Dokumente aus dem alten Archivbestand werden ebenfalls schrittweise in die elektronische Archivierung überführt. Damit ist die Verfügbarkeit auch über lange Zeiträume gewährleistet.	
	Kommentar	*Die Speicherung des elektronischen Archivs erfolgt redundant, so dass die Daten auch bei Verlust einer Sicherungskopie noch zur Verfügung stehen.*	
9.4.16	Was	**Auftragskontrolle**	**OK**
	Detail	Die Verarbeitung erfolgt exakt nach den derzeitigen allgemeinen Vorgaben der Auftraggeber. Spezifische Vorgaben einzelner Auftraggeber gab es bisher nicht. Es existieren aber alle Voraussetzungen, um weitere Forderungen der Auftraggeber bezüglich der Verarbeitung (z.B. Forderungen nach Löschung von Daten) oder hinsichtlich weitergehender technischer und organisatorischer Maßnahmen zu erfüllen.	
	Kommentar	*Die Auftragskontrolle entspricht den gesetzlichen Forderungen.*	
9.4.17	Was	**Trennungsgebot**	**OK**
	Detail	Es erfolgt eine strikte Trennung der Daten nach Mandanten sowie – auf Anforderung des Auftraggebers – auch innerhalb eines Mandanten in verschiedene Gruppen. Elektronisch werden dafür die Mandanten-Fähigkeiten der Sage-Software genutzt. Darüber hinaus ist durch organisatorische Regelungen gesichert, dass die Daten verschiedener Auftraggeber im Lohnbüro strikt getrennt verarbeitet werden.	
	Kommentar	*Die Einhaltung des Trennungsgebotes ist im erforderlichen Maß gegeben.*	
9.4.18	Was	**Belastbarkeit**	**OK**
	Detail	Die technischen Systeme sind mit großen Reserven konzipiert, so dass auch deutlich größere Belastungen problemlos bewältigt werden können. Die Systeme weisen eine hohe Robustheit gegen Störungen (z.B. Stromschwankungen, Beeinträchtigungen des Datenverkehrs usw.) auf.	

10 Zusammenfassung

Es wurden die Voraussetzungen für die Gewährleistung des Datenschutzes bei der Anwendung von Software im Rahmen des Lohnbüros Lohndirekt geprüft und auditiert. Dabei wurden die gesetzlichen Datenschutz-Anforderungen sowie die Kriterien des IT-Grundschutzkompendiums des Bundesamtes für Sicherheit in der Informationstechnik -BSI- zu Grunde gelegt.

Das Ergebnis Datenschutz-Prüfung der Software-Anwendung im Lohnbüros Lohndirekt lautet wie folgt:

Die Anwendung der Software im Lohnbüro Lohndirekt bietet alle technischen und organisatorischen Voraussetzungen für die Einhaltung des Datenschutzes.

Die internen Prozesse des Betreibers Lohndirekt GmbH sind datenschutzkonform.

Es zeigten sich keine Abweichungen oder anderen Defizite.

Garching, den 02.06.2020

TÜV SÜD Product Service GmbH

Software-Qualität und Escrow Services

Prüfer: ……..

Hans-Ulrich Bierhahn

Review des Berichts ……..……

Tuan Khai Hoang