



Product Service

**Mehr Sicherheit.
Mehr Wert.**

**Gutachten
Nr. 028-71395067-000 Rev. 0**

**Datenschutz-Gutachten
Anwendung von Software-Systemen
für das Lohnbüro "lohndirekt"**

Gegenstand	Datenschutz-Gutachten
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 13011:2008
Zeitraum der Gutachten-Erstellung	27. September 2011 bis 11. Januar 2012
Berichtsdatum	17.01.2012
Datum des Audits	25.10.2011
Unternehmen / Auftraggeber	Lohndirekt GmbH
Auftrags-Nr./ Kunden-Nr.	71395067/ 5010032539
Straße / Postfach	Lise-Meitner-Straße 14a
PLZ / Ort	24941 Flensburg
Ansprechpartner	Thomas Petersen (Geschäftsführer)
TÜV-Sachverständige	Ina Zumbruch (TÜV SÜD Product Service – Softwarequalität)
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.



1 Anlass, Auftrag

Es wird ein Datenschutz-Gutachten der Anwendung von Software-Systemen für das Lohnbüro „lohn*direkt*“ 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 „lohn*direkt*“ betrieben, das aktuell für monatlich 2.500 Firmen ca. 30.000 - 33.000 Lohnabrechnungen durchführt. Die Dienstleistung von lohn*direkt* 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 HR Solutions AG, die als ASP-Hosting auf Technik der Cronon AG Berlin (Tochterfirma der Strato AG) 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 lohn*direkt*.

Abgrenzung:

Fragen der Funktionalität sowie der Datensicherheit, die keinen Bezug zum Datenschutz haben, werden nicht betrachtet.

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

4 Maßstäbe, Anforderungen

Zusammenfassend können die Anforderungen folgendermaßen formuliert werden:

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

5 Prüfkonzzept

Entsprechend dem Auftrag und dem Prüfgegenstand geht es um ein Datenschutz-Gutachten zu lohn*direkt*, 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 das Bundesdatenschutzgesetz -BDSG-, das Telemediengesetz -TMG- sowie das Telekommunikationsgesetz -TKG-. Zur Beurteilung der wirksamen Umsetzung der gesetzlichen Anforderungen wurden die Kriterien der IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik -BSI- herangezogen.

6 Durchführung

Die Prüfung erstreckte sich über den Zeitraum vom September 2011 bis zum Januar 2012. Die Rahmenbedingungen für den Betrieb der Software zur Realisierung von lohn*direkt* wurden am 25. Oktober 2011 vor Ort bei der Lohndirekt GmbH überprüft.

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 der gegebenen Anforderungen, die im Zuge einer Nachprüfung ein positives Ergebnis ergab.

8 Ergebnisse

8.1 Vorgelegte Dokumente

- Anlage zum Leistungsschein 2011/799/9080 vom 28.02.2011
- AP Hosting-Vertrag mit Sage vom 04.04.2007
- Auftrag an Firma Veolia vom 21.11.2011
- Auftrag zur Datenlöschung und Aktenvernichtung
- Checkliste Datenlöschung
- Datenschutz- und Datensicherheitskonzept Rev. 1.0
- Interne Verfahrensbeschreibung nach §4g Abs. 2 BDSG
- ITSG-Zertifikat für Software der Sage HR Solutions AG
- Lohndirekt Firmen-Stammbblatt Version 10
- Lohndirekt Mitarbeiter-Stammbblatt Version 11
- Netzwerkdiagramm
- Öffentliches Verfahrensverzeichnis nach §4g Abs. 2 BDSG
- Speicherung, Sperrung und Löschung der Daten von Interessenten, Nichtinteressenten und Kunden im CRM-System, dem Lohnabrechnungssystem, dem Drucksystem und in Papierform
- Speicherung und Löschung der Logs für Zutrittskontrolle vom 21.11.2011
- TÜV-Zertifikat Qualitätsmanagement nach ISO2001:2008 vom 11.07.2011
- Urkunde ISO 2001:2005 der Strato Rechenzentrum AG
- Verschwiegenheitsverpflichtung für Mitarbeiter
- Verschwiegenheitsverpflichtung für externe Dienstleister
- Vertrag über Auftragsdatenverarbeitung mit der Firma Veolia vom 09.12.2011

8.2 Gutachten

8.2.1 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 HR Solutions AG. Die Software wurde durch Lohndirekt erworben und läuft als ASP-Hosting auf Technik der Cronon AG Berlin (Tochterfirma der Strato AG) in deren eigenem Rechenzentrum, welches nach ISO 27001 zertifiziert ist.

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

Lohndirekt ist nach ISO 9001 zertifiziert.

In einem Datenschutz-Check durch die TÜV SÜD Product Service GmbH sollte überprüft werden, ob die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten für das Lohnbüro lohndirekt durch die Lohndirekt GmbH den deutschen Datenschutzbestimmungen entspricht.

8.2.2 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.

8.2.2.1. 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. Die nicht personenbezogenen Daten werden nicht gelöscht.

Kommt ein Vertrag zustande, werden die Daten der Auftraggeber nach Ablauf der gesetzlichen Aufbewahrungsfristen gelöscht.

Die Löschung der personenbezogenen Daten im CRM-System erfolgt durch Überschreiben dieser mit dem Buchstaben „X“.

Rechtsgrundlagen der Erhebung, Verarbeitung und Nutzung

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

Die Zulässigkeit ergibt sich aus §28 Abs. 1 Ziff. 2 BDSG bzw. (wenn die Daten öffentlich zugänglich sind) aus §28 Abs. 1 Ziff. 3 BDSG.

8.2.2.2 Lohnbüro

Rechtliche Einordnung

Durch Lohndirekt erfolgt im Rahmen des Lohnbüros keine **Erhebung** personenbezogener Daten für eigene Zwecke. Die Erhebung der Mitarbeiterdaten des Auftraggebers erfolgt ausschließlich im Auftrag des Auftraggebers auf Basis der vom Auftraggeber übergebenen Mitarbeiter-Bögen.

Im Rahmen des Lohnbüros erfolgt durch Lohndirekt keine **Verarbeitung** personenbezogener Daten für eigene Geschäftszwecke. Die Verarbeitung erfolgt ausschließlich im Auftrag der Auftraggeber.

Eine **Nutzung** personenbezogener Daten aus dem Lohnbüro erfolgt ausschließlich durch die Auftraggeber oder durch Dritte, an welche die Daten im Auftrag der Auftraggeber durch Lohndirekt übermittelt wurden.

Lohndirekt erwirbt keinerlei Rechte an im Rahmen des Lohnbüros erhobenen und verarbeiteten personenbezogenen Daten. Alle Fragen der Erhebung und Verarbeitung wie z.B. die zu erhebenden Einzelangaben, die Logik ihrer Verknüpfung, Art und Reihenfolge der Verarbeitung usw. 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 als Auftragnehmer führt im Rahmen des Lohnbüros eine Auftragsdatenverarbeitung im Sinne des § 11 BDSG für die Auftraggeber durch. Damit ist der Auftraggeber für die Zulässigkeit der Erhebung, Verarbeitung und Nutzung verantwortlich.

Seitens Lohndirekt ist die Erhebung und Verarbeitung zulässig, soweit diese im Rahmen des Auftrages durch den Auftraggeber erfolgen und die weitergehenden Anforderungen aus der Auftragsdatenverarbeitung (siehe 8.2.3) erfüllt werden.



Eventuelle weitere Zulässigkeits-Tatbestände

Es findet keine Datenspeicherung zum Zwecke der Übermittlung statt. Demzufolge treffen die entsprechenden Voraussetzungen für die Zulässigkeit einer solchen Datenverarbeitung nicht auf Lohndirekt zu.

Alle weiteren Zulässigkeitstatbestände des BDSG sind für das betrachtete Lohnbüro auf Grund seines Zwecks und seines Inhaltes von vornherein gegenstandslos.

Lohndirekt erbringt keinerlei Telekommunikationsdienstleistungen im Sinne des Telekommunikationsgesetzes - TKG -. Die Datenschutzbestimmungen des TKG sind für Lohndirekt daher nicht relevant.

Telekommunikationsdienste im Sinne des Telemediengesetzes - TMG - werden im Rahmen des Lohnbüros nicht erbracht.

8.2.3 Allgemeine Datenschutzanforderungen

Anforderungen aus der Auftragsdatenverarbeitung

Auf Grund der Tatsache, dass Lohndirekt Auftragnehmer im Sinne des §11 BDSG ist, obliegen Lohndirekt folgende Rechtspflichten:

- Gewährleistung eines Grundniveaus technischer und organisatorischer Maßnahmen gemäß §9 BDSG i.V.m. der Anlage zu §9 Satz 1 BDSG, das den Auftraggebern eine Entscheidung gemäß §11 Abs. 2 BDSG ermöglicht
- Duldung von Kontrollen des Auftraggebers und Mitwirkung bei diesen entsprechend der vertraglichen Regelungen auf Basis von §11 Abs. 2 BDSG
- Informationspflichten gegenüber dem Auftraggeber gemäß §11 Abs. 3 BDSG
- Verpflichtung der Mitarbeiter auf das Datengeheimnis gemäß §5 BDSG
- Bestellung eines / einer Datenschutzbeauftragten gemäß §§ 4f und 4g BDSG
- Umsetzung aller Vorgaben des Auftraggebers entsprechend §11 Abs. 3 BDSG

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

Die technischen und organisatorischen Maßnahmen sind in einem Sicherheitskonzept beschrieben, das den Auftraggebern zur Verfügung steht.

Es ist ein Datenschutzbeauftragter bestellt. Weitere Angaben dazu sind im nachfolgenden Abschnitt aufgeführt.



Datenschutzbeauftragter

Entsprechend §4f BDSG i.V. mit §11 Abs. 4 Ziff. 3 BDSG ist durch Lohndirekt ein Datenschutzbeauftragter zu bestellen, der die Anforderungen dieses Paragraphen erfüllt und entsprechend der Paragraphen §f und 4g BDSG tätig wird.

Es ist ein Datenschutzbeauftragter schriftlich bestellt. Ein Exemplar der Bestellsurkunde ist im Besitz der Datenschutzbeauftragten, ein Exemplar im Besitz von Lohndirekt.

Der Datenschutzbeauftragte hat die erforderliche Sachkunde in Lehrgängen des Unabhängigen Landeszentrums für Datenschutz Schleswig Holstein erworben. Er verfügt über langjährige Erfahrungen als Datenschutzbeauftragter.

Für die Tätigkeit als Datenschutzbeauftragten steht ihm ausreichend Arbeitszeit zur Verfügung. Er verfügt über kein eigenes Budget, bekommt die erforderlichen finanziellen und materiellen Mittel aber problemlos zur Verfügung gestellt.

Der Datenschutzbeauftragte ist der Geschäftsführung direkt unterstellt, nimmt seine Aufgaben entsprechend den §§ 4f und 4g BDSG wahr und ist in der Ausübung dieser Tätigkeit weisungsfrei.

Alle Mitarbeiter wurden durch den Datenschutzbeauftragten zu Datenschutz-Fragen geschult. Über die Teilnahme an den Schulungen wird ein schriftlicher Nachweis geführt. Für neu hinzukommende Mitarbeiter sind Nachschulungen geplant.

Über die Grundschulungen zum Datenschutz hinaus werden die Mitarbeiter zusätzlich zu speziellen Fragen wie z.B. Verschlüsselungen geschult.

Weitere Anforderungen aus dem BDSG

Es wurde geprüft, inwieweit es im Rahmen des Lohnbüros Zugriffe auf die hinterlegten Daten gibt, unter die Bestimmungen des § 10 BDSG fallen. Das ist nicht der Fall.

Anforderungen aus anderen gesetzlichen Bestimmungen

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

Für die Auftraggeber von Lohndirekt können sich aber weitergehende Datenschutz-Anforderungen (z.B. in Bezug auf besondere personenbezogene Daten i.S.d. §3 Abs. 9 BDSG) ergeben. Lohndirekt ist in der Lage, solchen Anforderungen auf entsprechende Weisungen der Auftraggeber hin zu entsprechen.

Lohndirekt verfügt über alle technischen und organisatorischen Voraussetzungen, um Aufträge zur Erfüllung eventueller weitergehenden datenschutzrechtlicher Pflichten zu erfüllen.

Datenschutz-Dokumente

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

Dokument	Rechtsgrundlage	Status
Schriftliche Bestellung des Datenschutzbeauftragten	§4f Abs. 1 Satz 1 BDSG	vorhanden
Öffentliches Verzeichnisse	§4g Abs. 2 Satz 1 BDSG i.V.m. §4e BDSG	vorhanden
interne Verzeichnisse	§4g Abs. 2 Satz 2 BDSG i.V.m. §4e BDSG	vorhanden
Verpflichtung auf das Datengeheimnis	§5 BDSG	vorhanden
Verträge über die Auftragsdatenverarbeitung im Lohnbüro durch Lohndirekt	§11 Abs. 2 BDSG	vorhanden
Vertrag über Aktenvernichtung durch Veolina	§11 Abs. 2 BDSG	vorhanden

8.3 Einzelergebnisse zu den technischen und organisatorischen Maßnahmen

Es wird den Auftraggebern ein Grundniveau technischer und organisatorischer Maßnahmen entsprechend §9 BDSG i.V.m. der Anlage zu §9 Satz 1 BDSG angeboten, der den Interessenten eine Entscheidung gemäß §11 Abs. 2 Satz 1 BDSG 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
8.3.1	Was	Zutrittskontrolle	OK
	Detail	<p>Der Zutritt zu den Geschäftsräumen von Lohndirekt ist nur mit Transponder oder die Eingabe eines Sicherheitscodes möglich. Der Serverraum ist durch eine Tür mit einem zusätzlichen Sicherheitsschloss gesichert.</p> <p>Die Tür zum (Papier-) Archiv, das sich in einem anderen Gebäude befindet, ist mit einem Sicherheitsschloss gesichert. Die Wände aller Räume einschließlich des Archivs weisen eine ausreichende Stabilität auf.</p> <p>Sowohl das Objekt von Lohndirekt als auch das Archiv sind über Alarmanlagen gesichert, die bei der Sicherheit Nord GmbH auflaufen. Jede Nacht erfolgen durch den Wachdienst mindestens 3 Kontrollen zu unregelmäßigen Zeitpunkten.</p> <p>Die Daten der Auftraggeber werden ausschließlich im Rechenzentrum der Cronon AG verarbeitet, in dem eine Zutrittskontrolle auf höchstem Niveau gegeben ist.</p>	
	Kommentar	Die Zutrittskontrolle ist im erforderlichen Maß gewährleistet	
8.3.2	Was	Zugangskontrolle	OK
	Detail	<p>Es werden die Windows-Standard-Richtlinien für Passworte umgesetzt. Die Passworte sind 90 Tage gültig.</p> <p>Root- und Administrator-Accounts sind nur den Administratoren bekannt und bei der Geschäftsführung schriftlich hinterlegt.</p> <p>Ein externer Zugang ist nur dem Geschäftsführer (auf Exchange) und dem Linux-Admin (auf das Linux-System) möglich. Dieser Zugang erfolgt über ein verschlüsseltes VPN (IPSEC 256)</p> <p>Die Daten der Auftraggeber werden ausschließlich im Rechenzentrum der Cronon AG gespeichert. Ein Zugang zu diesen Systemen ist nur über einen Citrix-Server möglich, zu dem eine VPN-Verbindung besteht.</p> <p>Die Bearbeitungsergebnisse werden im Rechenzentrum als XML-Dateien auf einem SFTP-Server bereitgestellt, von diesem durch Lohndirekt abgeholt und ausgedruckt.</p> <p>Konkrete Verfahrensweisen für die Gewährleistung der Zugangskontrolle sind im Datenschutz- und Sicherheitskonzept (Rev. 1.0 vom 20.04.2011) festgelegt, das zum Audit vorgelegt wurde.</p>	
	Kommentar	<i>Es ist mit ausreichender Sicherheit gewährleistet, dass die Datenverarbeitungssysteme nicht durch Unbefugte genutzt werden können.</i>	
8.3.3	Was	Zugriffskontrolle	OK
	Detail	<p>Für das Lohnbüro werden die Zugriffskontrollmechanismen der Sage-Software genutzt.</p> <p>Für das CRM-System ist ein eigenes Zugriffssystem realisiert.</p> <p>Jeder Mitarbeiter hat seinen eigenen Account, der einer Standardrolle zugewiesen ist.</p>	

Ergebnisse			Klasse
		Details der Zugriffskontrolle sind im Datenschutz- und Sicherheitskonzept (Rev. 1.0 vom 20.04.2011) festgelegt, das zum Audit vorgelegt wurde	
	Kommentar	<i>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.</i>	
8.3.4	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. Dafür werden bei S+P die Standard-Funktionen dieser Software genutzt. Das CRM-System realisiert eine eigene Protokollierung aller Eingaben.	
	Kommentar	<i>Die Eingabekontrolle ist im erforderlichen Maß gewährleistet.</i>	
8.3.5	Was	Weitergabekontrolle	OK
	Detail	Auf die Daten des Lohnbüros, die ausnahmslos im Rechenzentrum der Cronon AG gespeichert sind, wird über Citrix-Server zugegriffen. Die Verbindung zu den Citrix-Servern wird über ein verschlüsseltes VPN (IPSEC 256) hergestellt. Die Übermittlung der XML-Dateien mit den Abrechnungsergebnissen vom Rechenzentrum zu Lohndirekt erfolgt über einen SFTP-Server und ein verschlüsseltes VPN (IPSEC 256)	
	Kommentar	<i>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.</i>	
8.3.6	Was	Weitergabekontrolle	OK
	Detail	Remote-Zugriffe auf Computer im Objekt von Lohndirekt sind nur zwei Personen möglich: Der Geschäftsführer kann remote auf Exchange zugreifen, und der Linux-Admin auf die Linus-Systeme. Beide Zugriffe erfolgen über ein verschlüsseltes VPN (IPSEC 256).	
	Kommentar	<i>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</i>	

Ergebnisse		Klasse
		<i>während der Datenübertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.</i>
8.3.7	Was	Weitergabekontrolle
	Detail	<p>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.</p> <p>Datenübermittlungen von Lohndirekt an die Auftraggeber erfolgen entweder gegenständlich (Papierform / CD) oder per Email. Bei der gegenständlichen Übermittlung werden die Datenträger durch DHL zugestellt.</p> <p>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.</p>
	Kommentar	<p><i>Es kann überprüft und festgestellt werden, an welchen Stellen eine Übermittlung personenbezogener Daten mit Einrichtungen der Datenübertragung vorgesehen ist.</i></p> <p><i>Die Datenübertragungen sind exakt festgelegt und werden protokolliert und kontrolliert.</i></p> <p><i>Seitens Lohndirekt sind alle Voraussetzungen gegeben, um sichere Datenübertragungen entsprechend der Forderungen der Auftraggeber zu realisieren.</i></p>
8.3.8	Was	Verfügbarkeitskontrolle
	Detail	Es erfolgt eine tägliche Komplettsicherung aller Systeme, Daten und Lizenzen. Dabei wird ein 5-Tage-Generationen-Prinzip verwirklicht.
	Kommentar	<i>Die Daten- und Systembackups erfüllen die Voraussetzungen, um die Daten vor zufälliger Zerstörung oder Verlust zu schützen.</i>
8.3.9	Was	Verfügbarkeitskontrolle
	Detail	<p>Für den Anschluss an das externe Netz ist nur eine Standleitung von T-Systems vorhanden. Ein Ausfall dieser Leitung ist gleichbedeutend mit dem Ausfall des Lohnbüros.</p> <p>Ausweichvarianten (z.B. im Notfall Nutzung anderer Räume mit einer funktionierenden Netzanbindung durch die Mitarbeiter) sind in der Diskussion, aber noch nicht umgesetzt.</p> <p>Derzeit wären bei Ausfall der Leitung ein Minimal-Zugriff auf Daten der Kunden über einen UMTS-Router möglich.</p> <p>Notfallvarianten für einen Komplettausfall aller elektronischen Kommunikationswege werden zur Zeit erarbeitet.</p>
	Kommentar	<p><i>Die derzeitigen Maßnahmen zur Gewährleistung der Verfügbarkeit können nur kurzzeitige und teilweise Ausfälle der elektronischen Kommunikationswege kompensieren.</i></p> <p><i>Es sind weitergehende Maßnahmen erforderlich, um bei längeren und/oder Komplettausfällen dieser Kommunikationswege die</i></p>

Ergebnisse			Klasse
		<i>Funktionsfähigkeit des Lohnbüros zu gewährleisten.</i>	
8.3.10	Was	Verfügbarkeitskontrolle	2
	Detail	Es existieren seitens Lohndirekt noch keine Mindeststandards zur Verfügbarkeit. Darüber hinaus wurde im Audit nicht klar, welchen speziellen Verfügbarkeitsanforderungen der Auftraggeber Lohndirekt entsprechen kann und welchen nicht.	
	Kommentar	<i>Mindeststandards für die Verfügbarkeit müssen definiert und den Kunden transparent gemacht werden.</i>	
8.3.11	Was	Auftragskontrolle	OK
	Detail	Die Verarbeitung erfolgt exakt nach den Vorgaben der Auftraggeber. Es existieren allen Voraussetzungen, um weitere Forderungen der Auftraggeber bezüglich der Verarbeitung (z.B. Forderungen nach Löschung von Daten) zu erfüllen.	
	Kommentar	<i>Die Auftragskontrolle entspricht den gesetzlichen Forderungen.</i>	
8.3.12	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	<i>Die Einhaltung des Trennungsgebotes ist im erforderlichen Maß gegeben.</i>	



9 Zusammenfassung

Es wurden die Voraussetzungen für die Gewährleistung des Datenschutzes bei der Anwendung von Software im Rahmen des Lohnbüros lohndirekt geprüft und auditiert. Es wurden die gesetzlichen Datenschutz- Anforderungen sowie die Maßnahme-Empfehlungen der IT-Grundschutzkataloge des BSI zu Grunde gelegt.

Das Ergebnis der Datenschutz-Prüfung der Software-Anwendung des Lohnbüros lohndirekt lautet wie folgt:

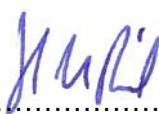
Die Anwendung der Software im Lohnbüro lohndirekt bietet alle technischen und organisatorischen Voraussetzungen für die Einhaltung des Datenschutzes. Die internen Prozesse des Betreibers Lohndirekt GmbH sind datenschutzkonform.

Es zeigten sich keine Abweichungen. Es wurden nur einzelne, untergeordnete Defizite festgestellt, die das Gesamtniveau des Datenschutzes nur geringfügig beeinträchtigen. Feststellungen sind vorhanden und sollen innerhalb der nächsten 6 Monate behoben werden.

München, den 17.01.2012

TÜV SÜD Product Service GmbH

Software-Qualität und Escrow Services

Prüfer: 

Hans-Ulrich Bierhahn

Review des Berichts 

Ina Zumbruch