

Rechtliche Aspekte des Lohnstandard-CH (ELM) und des Leistungsstandard-CH (KLE)

Auftraggeber:
Verein Swissdec
Fluhmattstrasse 1
6004 Luzern

Zürich, im Mai 2024

IT & Law Consulting GmbH
mag. iur. Maria Winkler
Sternenstrasse 18
8002 Zürich

Inhaltsverzeichnis

1.	Ziel und Zweck des Dokuments und Abgrenzung	4
2.	Die Entstehung des Vereins Swissdec und des Lohnstandard-CH (ELM) sowie des Leistungsstandard-CH (KLE).....	4
2.1	Ausgangslage	4
2.2	Das Projekt Lohnstandard-CH (ELM).....	4
2.3	Das Projekt Leistungsstandard-CH (KLE).....	5
2.4	Der Verein Swissdec	5
2.4.1	Die Vereinsgründung	5
2.4.2	Organigramm.....	6
2.4.3	Dienstleistungen des Vereins Swissdec.....	7
2.5	Verhältnis Datenempfänger – Vereinsmitglieder - Verein Swissdec.....	8
2.6	Verhältnis zum Datensender	8
3.	Der Lohnstandard-CH (ELM)	8
3.1	Elemente des Lohnstandard-CH (ELM)	8
3.2	Die Standardisierung der Deklaration von Lohnmeldungen.....	10
3.3	Die Standardisierung des Verfahrens	10
3.4	Der Distributor.....	10
3.4.1	Begriff und Aufgaben.....	10
4.	Der Leistungsstandard-CH (KLE)	12
4.1	Elemente des Leistungsstandard-CH (KLE)	12
4.2	Übersicht Leistungsstandard-CH (KLE)	13
4.2.1	Anmeldung eines Ereignisses	13
4.2.2	Austausch von Parts/Stories im Fallverlauf.....	14
4.2.3	Daten des Versicherers an den Betrieb	15
4.2.4	Dialogaustausch	16
4.2.5	Ereignis-Registrierung	17
5.	Datenschutzrechtliche Aspekte.....	18
5.1	Vorbemerkungen	18
5.2	Datenlieferanten	18
5.3	Datenempfänger	18
5.3.1	Grundsatz	18
5.3.2	Suva.....	18
5.3.3	Ausgleichskassen.....	19
5.3.4	Bundesamt für Statistik.....	19
5.3.5	Kantonale Steuerbehörden.....	19
5.3.6	Versicherungsanstalten des privaten Rechts	19
5.4	Daten	19
5.4.1	Art und Inhalt	19
5.4.2	Klassifizierung der Daten.....	20
5.4.3	Fazit	21
5.5	Datenfluss Lohnstandard-CH (ELM)	21
5.6	Datenfluss Leistungsstandard-CH (KLE)	23
5.7	Rechtmässigkeit der Datenbearbeitung	23
5.7.1	Allgemeines	23
5.7.2	Lohnstandard-CH (ELM)	24
5.7.3	Leistungsstandard-CH (KLE).....	25
5.8	Outsourcing der Datenbearbeitung	25
5.8.1	Allgemein	25
5.8.2	Outsourcing des Datenempfangs an den Verein Swissdec	25
5.8.3	Outsourcing des Vereins Swissdec an Dritte	26

5.8.4	Gesetzliche oder vertragliche Geheimhaltungspflichten	27
5.9	Verhältnismässigkeitsgrundsatz	28
5.9.1	Allgemein	28
5.9.2	Lohnstandard-CH (ELM)	28
5.9.3	Leistungsstandard-CH (KLE).....	30
5.10	Grundsatz der Zweckbindung.....	30
5.10.1	Allgemein	30
5.10.2	Lohnstandard-CH (ELM) und Leistungsstandard-CH (KLE)	30
5.11	Prinzip der Integrität	31
5.11.1	Allgemein	31
5.11.2	Lohnstandard-CH (ELM) und Leistungsstandard-CH (KLE)	31
5.12	Datensicherheit.....	31
5.12.1	Allgemein	31
5.12.2	Lohnstandard-CH (ELM)	31
5.12.3	Leistungsstandard-CH (KLE).....	33
5.12.4	Fazit	33
6.	Haftung.....	33

1. Ziel und Zweck des Dokuments und Abgrenzung

Das vorliegende Dokument dient dem Zweck, interessierten Kreisen Informationen zu den folgenden Themen rund um den Verein Swissdec und den Lohnstandard-CH (ELM) sowie dem Leistungsstandard-CH (KLE) zur Verfügung zu stellen:

- Die Organisation des Vereins Swissdec und seine Dienstleistungen
- Das Konzept des Lohnstandard-CH (ELM) und des Leistungsstandard-CH (KLE)
- Datenschutzrechtliche Aspekte des Lohnstandard-CH (ELM) und des Leistungsstandard-CH (KLE).

Ziel ist es, Transparenz über die Ziele und die Dienstleistungen des Vereins Swissdec und den Lohnstandard-CH (ELM) sowie den Leistungsstandard-CH (KLE) zu schaffen.

Die Erläuterungen beziehen sich ausschliesslich auf den Verein Swissdec als Organisation sowie auf die Dienstleistungen, welche dieser gemäss den Vereinsstatuten oder auf der Basis von Verträgen gegenüber Vereinsmitgliedern und Dritten erbringt und die daher in seinem Verantwortungsbereich liegen. (Siehe dazu die Ausführungen in Ziffer 2.4.3).

2. Die Entstehung des Vereins Swissdec und des Lohnstandard-CH (ELM) sowie des Leistungsstandard-CH (KLE)

2.1 Ausgangslage

Lohndeklarationen, welche die Unternehmen regelmässig an Behörden und Versicherungen (Suva, AHV, Steuerbehörden, etc.) weiterzuleiten haben, verursachen sowohl auf der Seite der Unternehmen als auch auf Seiten der Empfänger einen sehr **grossen administrativen Aufwand**. Der Grund liegt unter anderem darin, dass wegen der Vielfalt von Organisationsformen im Sozialversicherungsbereich und der dezentralen Organisation der staatlichen Verwaltung zahlreiche **unterschiedliche Vorschriften betreffend die Durchführung der Lohndeklaration** bestehen.

Ungefähr 80% der schweizerischen Unternehmen mit mehr als 10 Mitarbeitenden (rund 48'000 Unternehmen) erledigen ihre administrativen Aufgaben mit Hilfe von zeitgemässen IT-Lösungen. Der Grossteil aller für die Lohndeklarationen nötigen Daten ist deshalb in den Unternehmen bereits heute in elektronischer Form vorhanden.

2.2 Das Projekt Lohnstandard-CH (ELM)

Das Bundesamt für Statistik, die Schweizerische Steuerkonferenz SSK, der Schweizerische Versicherungsverband SVV, die Suva sowie die im Verein eAHV/IV vertretenen Ausgleichskassen (im Folgenden «Vereinsmitglieder» genannt) strebten mit dem im Jahr 2003 lancierten Projekt Lohnstandard-CH (ELM) die **Standardisierung der Deklaration und Übermittlung der Lohndaten** von Unternehmen an Behörden und Versicherungen an. Ziel des Projekts war es, die Lohndaten von den Unternehmen bereits in elektronischer Form sowie in guter Qualität zu erhalten. Für die Unternehmen sollten die Lohnmeldungen vereinfacht werden. Sie sollten die Lohnmeldungen an alle Empfänger mittels einer einzigen Transaktion vornehmen können. Durch Vermeidung von Medienbrüchen und die Reduktion des Aufwands für die interne Revision sowie für die Aufbereitung der Lohndaten in unterschiedlichen Formulare sollten so Einsparungen auf beiden Seiten realisiert werden.

Bis dahin diente den Herstellern von ERP-Systemen die von der Suva herausgegebene «Anleitung für Programmhersteller und Anwender» als Grundlage für die Berechnung der beitragspflichtigen Löhne für die UV, die AHV/IV/EO und die ALV. Wenn das Lohnprogramm die Anforderungen der Anleitung erfüllte, wurde das Label «Suva-geprüft» erteilt. Im Rahmen des Projekts Lohnstandard-CH (ELM) wurden die Richtlinien zum Lohnstandard-CH (ELM) erarbeitet sowie um die Module Versicherungen, Statistik, Steuern und BVG sowie Quellensteuer ergänzt und neu in einem einheitlichen Format dargestellt.

Die Standardisierung betrifft die Berechnung der beitragspflichtigen Löhne für AHV/IV/EO, ALV, FAK, UVG, UVGZ, KTG und BVG, die Deklaration von Lohnmeldungen und das Verfahren der Übermittlung, weshalb der Lohnstandard-CH (ELM) sich aus verschiedenen Richtlinien zusammensetzt¹. Lohnprogramme bzw. ERP-Systeme, welche den **Lohnstandard-CH (ELM)** erfüllen und sich vom Verein Swissdec zertifizieren lassen, erhalten das Label «swissdec certified basic».

2.3 Das Projekt Leistungsstandard-CH (KLE)

Der Leistungsstandard ermöglicht den Unternehmen und den Versicherern, **alle mit einer Schadensabwicklung (Unfall oder Krankheit) verbundenen Prozessschritte** von der Ereignismeldung durch das Unternehmen bis zum Fallabschluss **über denselben Kanal abzuwickeln**. Der Leistungsstandard-CH (KLE) greift aber nicht in die internen Prozesse des Versicherers ein. Er legt also nicht durchgehend fest, welche Prozessschritte wann gemacht oder welche Daten in einem einzelnen Prozessschritt genau übermittelt werden müssen.

2.4 Der Verein Swissdec

2.4.1 Die Vereinsgründung

Von 2003 bis August 2007 arbeiteten die Vereinsmitglieder auf der Basis von Einzelverträgen zusammen, welche aufeinander abgestimmt waren. Die Suva trat dabei als Generalunternehmerin auf.

Diese Projektorganisation eignete sich allerdings nicht für eine langfristige Zusammenarbeit aller beteiligten Behörden und Versicherer, weshalb sich diese entschieden, für die weitere Zusammenarbeit einen Verein zu gründen.

Für die Gründung eines Vereins sprachen insbesondere die folgenden Punkte:

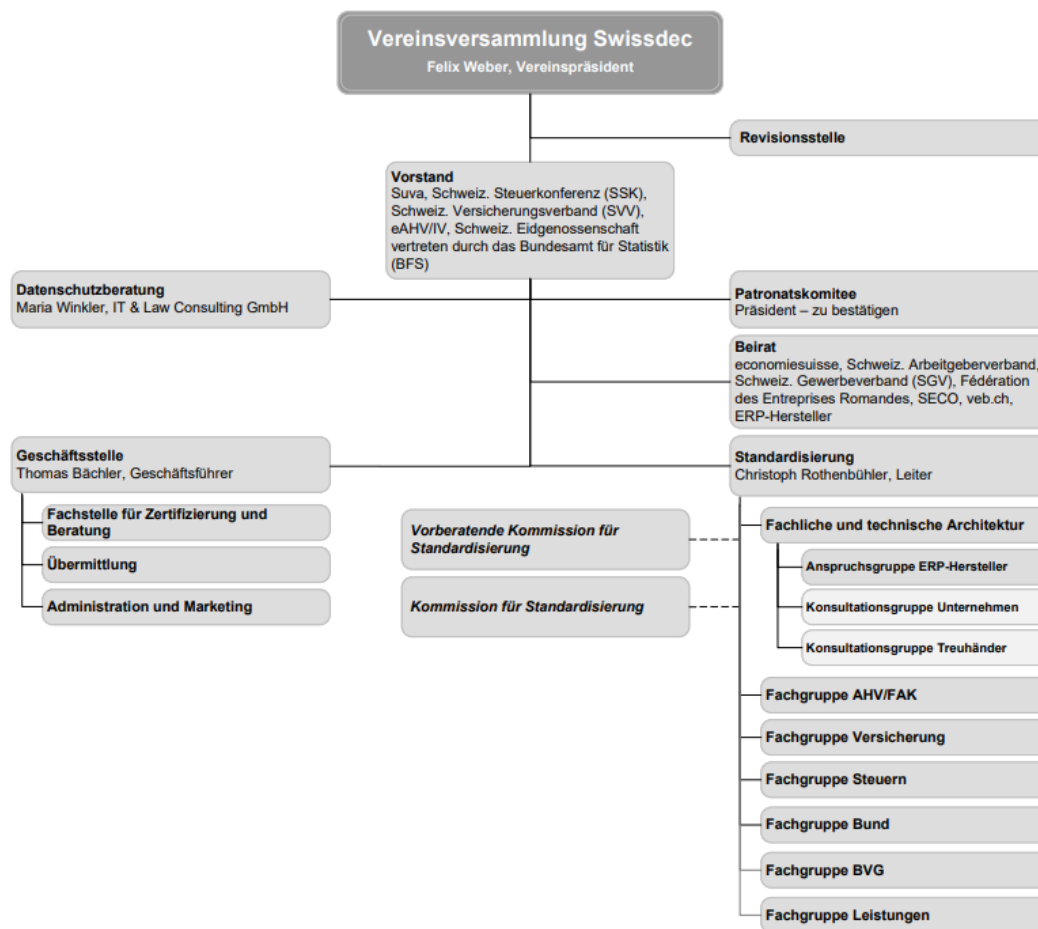
- Die **Gründung** ist einfach und erfolgt durch die Erstellung von Statuten. Es ist **kein Mindestkapital** erforderlich.
- Der Verein kann Träger von Rechten und Pflichten sein. Die **Urheberrechte an Swissdec-Standards** konnten auf den Verein übertragen werden.
- Für die **Verbindlichkeiten** des Vereins haftet nur das **Vereinsvermögen**, welches aus den Mitgliederbeiträgen besteht, sofern die Mitgliederbeiträge in den Statuten summenmässig bestimmt sind.
- Der Verein eignet sich im Gegensatz zu anderen Rechtsformen zur **Verfolgung von nichtwirtschaftlichen Zwecken**.

Im August 2007 wurde der **Verein Swissdec** gegründet. Gründungsmitglieder waren die Suva, die Schweizerische Steuerkonferenz SSK sowie der Schweizerische Versicherungsverband SVV. Im Jahr 2008 trat der Verein eAHV/IV dem Verein Swissdec als Vollmitglied bei. Das BFS hat mit dem Verein Swissdec seit dem Jahr 2008 zusammengearbeitet und ist am 1. Januar 2021 dem Verein Swissdec als Vollmitglied beigetreten.

Vereinszweck ist die Standardisierung, Vereinheitlichung und Vereinfachung der (elektronischen) Übermittlung von Daten (insbesondere Lohn Daten), welche Unternehmen und Arbeitgeber aufgrund einer gesetzlichen Pflicht oder einer vertraglichen Vereinbarung zur gesetzeskonformen Weiterbearbeitung an Behörden oder Versicherungen zu liefern haben².

^{1,2} Die aktuellen Richtlinien können jeweils von der Website des Vereins Swissdec unter www.swissdec.ch/richtlinien heruntergeladen werden.

2.4.2 Organigramm



- Das oberste Organ des Vereins Swissdec ist die **Vereinsversammlung**, welche jährlich bis zum 30. April stattfindet. Die operativen Geschäfte leitet der Vorstand, der sich aus je einem Vertreter / einer Vertreterin der Vereinsmitglieder zusammensetzt.
- Der Vorstand führt seine Geschäfte über die Geschäftsstelle, welche durch den **Geschäftsführer** geleitet wird. Diese setzt insbesondere die Beschlüsse des Vorstands um, betreibt das Marketing, führt die Buchhaltung, überwacht die Einhaltung von Verträgen mit Dritten und ist verantwortlich für die Weiterentwicklung der Distributor-Applikation und der Standards.
- Der Verein Swissdec verfügt als Träger eines e-Government-Projekts über kein eigenes Personal. Die **Geschäftsstelle** des Vereins Swissdec ist das operative Organ des Vereins und wird im Auftrag des Vereins Swissdec durch die Suva geführt. Sie ist unter anderem verantwortlich für das Marketing und das Vereinssekretariat. Sie bereitet auch die Geschäfte des Vorstands vor.
- Die **Revisionsstelle** ist verantwortlich für die Rechnungsprüfung.
- Die Mitglieder des **Patronatskomitees** sind Persönlichkeiten aus Politik, Wirtschaft, Verwaltung und Versicherungswesen, welche die Digitalisierung und Automatisierung von Prozessen in Unternehmen und Verwaltungen fördern. Sie sind Botschafter/innen, die helfen, den Bekanntheitsgrad und die Anerkennung der Swissdec Standards in der Öffentlichkeit zu erweitern.
- Im **Beirat** sind Interessensverbände und Organisationen, die im Verein beratend mitwirken, aber nicht die Rechte und Pflichten von Mitgliedern haben (z.B. Economiesuisse, Arbeitgeberverband, etc.). Die Mitglieder des Beirats sind berechtigt, an der Vereinsversammlung und im Vorstand Anträge zu stellen und an den Sitzungen der Kommission für Standardisierung teilzunehmen und ihre Standpunkte einzubringen.

- Die **Fachstelle für Zertifizierung und Beratung** ist zuständig für die Zertifizierung und Beratung der Lohnbuchhaltungssysteme der ERP-Hersteller. Zudem nimmt sie die Kopplungen der Endempfänger vor.
- Das **Geschäftsfeld Übermittlung** verantwortet den ordnungsgemässen Betrieb des Distributors.
- Die **Organisationseinheit Standardisierung** ist zuständig für die Pflege und Weiterentwicklung der bestehenden Swissdec Standards. Projekte zu neuen Standards laufen ebenfalls in dieser Organisationseinheit.
- Die **Vorberatende Kommission für Standardisierung** behandelt Anliegen der Fachgruppen, der Anspruchsgruppe ERP-Hersteller und der Konsultationsgruppen. Sie bereitet Geschäfte für die Kommission für Standardisierung sowie für den Vorstand vor und gibt Empfehlungen zum Projektportfolio ab.
- Die **Kommission für Standardisierung** überprüft die Anträge der Fachgruppen. Sie bindet die Anspruchsgruppe ERP-Hersteller und die Konsultationsgruppen ein. Die Kommission für Standardisierung setzt die Swissdec Standards in Kraft.
- Die **fachliche und technische Architektur** verantwortet über alle Domänen hinweg harmonisierte Standards, die für ERP-Hersteller sowohl fachlich wie technisch umsetzbar sind.
- Die **Anspruchsgruppe ERP-Hersteller** ist das Bindeglied zwischen der Kommission für Standardisierung und den ERP-Herstellern, welche die Standards von Swissdec umsetzen.
- Die **Konsultationsgruppe Unternehmen** ermöglicht Anwendern, die mit Swissdec-zertifizierten ERP-Systemen arbeiten, ihre Erfahrung in der Praxis in die Weiterentwicklungen von Swissdec einfließen zu lassen.
- Die **Konsultationsgruppe Treuhänder** bietet Treuhändern eine Plattform, um ihr Expertenwissen und ihre Erfahrungen im Zusammenhang mit Swissdec aus der Praxis in die Weiterentwicklungen einfließen zu lassen.
- Für die Pflege und Weiterentwicklung der einzelnen Fachmodule des Lohnstandard-CH (ELM) und Leistungsstandard-CH (KLE) sind die jeweiligen **Fachgruppen** zuständig. Sie verantworten alle fachlichen Anforderungen in ihrer Domäne.
- Die **Datenschutzberaterin** übt eine beratende und kontrollierende Funktion aus. Sie rapportiert direkt an den Vorstand und ist in verschiedenen Vereinsgremien vertreten. Die Aufgaben und Kompetenzen der Datenschutzberaterin sind in einem Pflichtenheft dokumentiert. Die Datenschutzberaterin des Vereins Swissdec ist beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten gemeldet und erfüllt die gesetzlich geforderten Fachkenntnisse. Die Unabhängigkeit der Datenschutzberaterin ist einerseits dadurch gewährleistet, dass es sich um eine externe Person handelt, mit der ein Vertrag besteht und andererseits dadurch, dass diese im Organigramm als Stabsstelle direkt dem Vorstand unterstellt ist.

Weitere spezialisierte Dienstleistungen bezieht der Verein Swissdec bei externen Unternehmen auf der Basis von Verträgen. Dabei handelt es sich um die Unternehmen itServe AG (Informatikdienstleistungen) und Swisscom (Rechenzentrum).

2.4.3 Dienstleistungen des Vereins Swissdec

Der Verein Swissdec erbringt die folgenden Dienstleistungen an seine Vereinsmitglieder und an Dritte:

- **Standardisierung:** Definition, Pflege und Weiterentwicklung des Lohnstandard-CH (ELM) und des Leistungsstandard-CH (KLE)
- **Zertifizierung:** Zertifizierung von Lohnprogrammen im Hinblick auf deren Konformität mit dem Lohnstandard-CH (ELM) bzw. Leistungsstandard-CH (KLE)
- **Abnahme:** Überprüfung der Systeme der Datenempfänger auf deren Übereinstimmung mit den End-Receiver-Anforderungen
- **Übermittlung:** Empfang, Filterung und Übermittlung von Daten mit der Distributor-Applikation
- Nicht im Verantwortungsbereich des Vereins Swissdec liegen die Datenbearbeitungen durch die Datensender (Unternehmen) sowie durch die Datenempfänger (Behörden und Versicherer, welche an den Distributor gekoppelt sind).

2.5 Verhältnis Datenempfänger – Vereinsmitglieder - Verein Swissdec

Der Verein Swissdec übernimmt die oben unter 2.4.3 genannten Aufgaben im Auftrag seiner Vereinsmitglieder.

Die Vereinsmitglieder (Suva, SSK, SVV, BFS und Verein eAHV/IV) wiederum handeln im Vereinsvorstand und an der Vereinsversammlung im Namen der Mitglieder ihres Verbandes (d. h. sie handeln für die angeschlossenen Versicherungen, Steuerverwaltungen, Ausgleichskassen etc.) und damit im Namen der Datenempfänger.

Die Datenempfänger (Versicherer und Behörden)

- sind folglich im Verein Swissdec über ihren jeweiligen Verband (Vereinsmitglied) vertreten.
- **sind deshalb direkt oder indirekt für die Instruktion und Kontrolle des Vereins Swissdec verantwortlich.**
- lagern die oben genannten Aufgaben an den Verein Swissdec im Rahmen eines Outsourcings nach Art. 9 DSG aus (siehe hierzu Ziff. 5.8).

2.6 Verhältnis zum Datensender

Die Datensender stehen mit dem Verein Swissdec in keiner Vertragsbeziehung. Der Verein Swissdec handelt im (direkten bzw. indirekten) Auftrag der Datenempfänger.

Eine direkte **Rechtsbeziehung der Datensender (Unternehmen) besteht nur mit den Datenempfängern**. Die Verantwortung für die Information und Instruktion der Datensender obliegt deshalb auch den Datenempfängern.

3. Der Lohnstandard-CH (ELM)

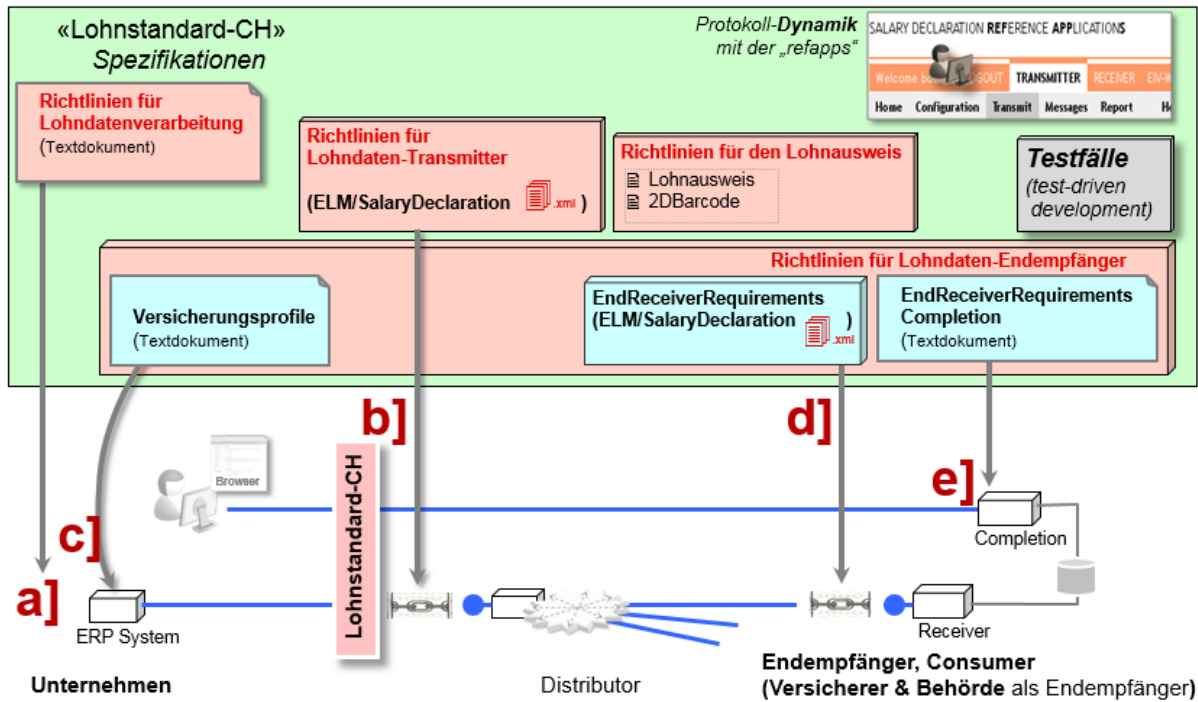
3.1 Elemente des Lohnstandard-CH (ELM)

Der Lohnstandard-CH (ELM) setzt sich aus der fachlichen Dokumentation (Richtlinien für Lohndatenverarbeitung (RL-LDV)) und der technischen Dokumentation (Richtlinien für die Lohndatenübermittlung (RL-LDÜ³)) des Vereins Swissdec zusammen. Der Begriff Lohnstandard-CH (ELM) umfasst im vorliegenden Dokument sowohl die fachliche als auch die technische Dokumentation. Lohnprogramme, welche den Lohnstandard-CH (ELM) erfüllen, können sich zertifizieren lassen und erhalten dann das Recht, das Label «swissdec certified basic» zu verwenden.

Die Elemente des Lohnstandard-CH (ELM) werden im Folgenden grafisch dargestellt.

³ Die Richtlinien für die Lohndatenübermittlung sind gegliedert in die Richtlinie für Transmitter (RL-LDT), Richtlinie für Empfänger (RL-LDE) und die Richtlinie zum Lohnausweis: Abrufbar unter www.swissdec.ch/richtlinien.

Übersicht Lohnstandard-CH (ELM)



a) bis g) Beschreibung

RL-LDV

a) Richtlinien für Lohndatenverarbeitung

Fachliche Anforderungen für eine zertifizierte Lohnbuchhaltung
Technische Anforderung RL-LDÜ (Richtlinien für Lohndatenübermittlung)

RL-LDT

b) Richtlinien für Lohndaten Transmitter

Technische Anforderungen für den Transmitter einer zertifizierten Lohnbuchhaltung
Lohnstandard-CH Version M.m wsdl: SalaryDeclarationService.wsdl
Namespace www.swissdec.ch/schema/sd/yyyymdd/SalaryDeclarationService

RL-LDE

c) Richtlinien für Lohndaten Endempfänger

Technische Anforderungen für Endempfänger Institutionen, Consumer

d) Versicherungsprofile

Konfigurationsdaten zur Adressierung, Versicherungsprodukte (Code), ...

e) EndReceiverRequirements

Anforderungen an die Standardkopplung für eine Endempfänger-Institution
Lohnstandard-CH Version M.m wsdl: SalaryDeclarationConsumerService.wsdl
Namespace: www.swissdec.ch/schema/sd/yyyymdd/SalaryDeclarationConsumerService

f) EndReceiverReqCompletion

Maskenbeschreibung für die Internet-Applikation zur Freigabe der Lohnmeldung

RL-LDX

g) Richtlinien für Lohnausweis / Barcode

Transformation von XML-Lohndaten in ein PDF-Dokument (den Lohnausweis)
Schema und Stylesheet für die Erstellung des 2D-Barcodes auf dem Lohnausweis

3.2 Die Standardisierung der Deklaration von Lohnmeldungen

Die auf der Basis des Lohnstandard-CH (ELM) erstellten Lohnmeldungen werden in einem einheitlichen Format ELM/Salary Declaration, einem sogenannten XML-Schema elektronisch dargestellt und übermittelt. ERP-Hersteller müssen somit nunmehr eine Schnittstelle programmieren und unterhalten.

XML ist ein Satz an Regeln für die Erstellung von Textformaten zur Strukturierung solcher Daten. XML erleichtert es einem Computer, Daten zu generieren oder zu lesen und sorgt dafür, dass eine bestimmte Datenstruktur eindeutig bleibt («XML in 10 Punkten» www.w3.org/XML/1999/XML-in-10-points). XML ist somit keine Programmiersprache und keine Software.

3.3 Die Standardisierung des Verfahrens

Die Standardisierung des Verfahrens beinhaltet die Spezifizierung des Protokolls, das den Datenaustausch zwischen einem Transmitter (ERP-System des Unternehmens) und einem Receiver (Server z.B. einer Steuerverwaltung, einer Sozialversicherung oder Privatversicherung) beschreibt.

Die Standardisierung bezieht sich auf folgende Verfahrensvarianten:

- **Prozessintegriertes Verfahren (PIV)**
Dieses Verfahren beinhaltet die direkte Übermittlung der Lohndaten durch Verwendung der Swissdec-Technology Stack (WSDL (Web Services Description Language), XSD (XML-Schema Definition), SOAP (Simple Object Access Protocol), WSS (Web Services Security) usw.).
- **Export/Import-Verfahren (EIV)**
Dieses Verfahren beinhaltet den Export von Lohnmeldedaten aus einem ERP-System und das verschlüsselte File-Uploading dieser Daten auf den Swissdec-Distributor Receiver (Server).

3.4 Der Distributor

3.4.1 Begriff und Aufgaben

Nicht alle Datenempfänger benötigen zur Erfüllung ihrer Aufgaben genau dieselben Daten. Der sogenannte «Distributor» des Vereins Swissdec, über welchen die Daten an die Datenempfänger weitergeleitet werden, filtert die erhaltenen Daten nach den Datenempfängern.

Jeder Datenempfänger ist jedoch selbst verantwortlich, dass er nur solche Daten erhält und bearbeitet, zu denen er aufgrund eines Gesetzes oder Vertrages berechtigt ist. Sie bzw. ihre Vertreter im Verein Swissdec haben für jedes abgefüllte Datenfeld, das sie erhalten wollen, das Vorliegen einer genügenden gesetzlichen oder vertraglichen Grundlage – welche sie zum Empfang der Daten berechtigt – zu prüfen und dies in der sogenannten «Datenschutzerklärung» gegenüber dem Verein Swissdec zu bestätigen. Aufgrund dieser Datenschutzerklärungen verteilt der Distributor des Vereins Swissdec die Daten an die Datenempfänger.

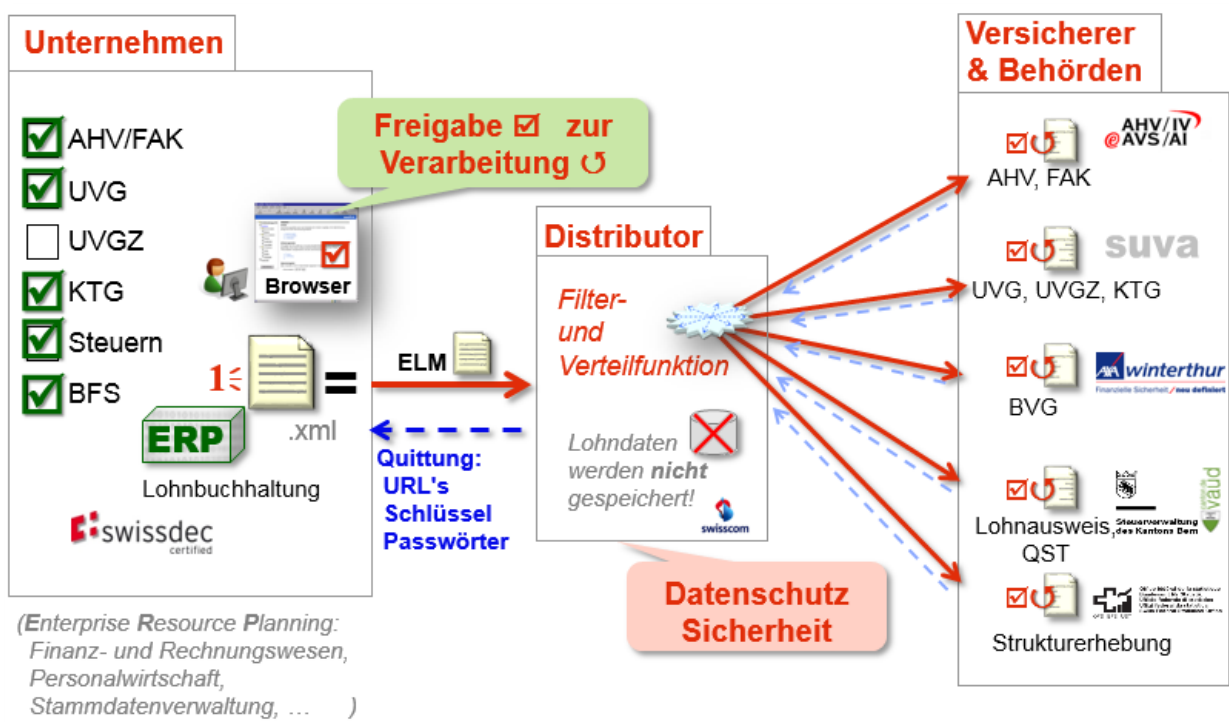
Damit wird einerseits sichergestellt, dass die Unternehmen die Daten den verschiedenen Empfängern **mit einer einmaligen Sendung** übermitteln können und andererseits, dass die Datenempfänger nur die Daten erhalten, welche sie zur Erfüllung ihres (gesetzlichen oder vertraglichen) Auftrages benötigen. Für jede dieser Sendungen wird zuerst nach einer Empfängeradresse gesucht, dann die Übermittlung durchgeführt und schliesslich eine eingegangene Rückmeldung verarbeitet.

Der Distributor besteht aus einer Softwareapplikation mit Betriebsumgebung. Die Aufgaben und die Funktionsweise des Distributors, die mit dem Betrieb verbundenen Kosten und Risiken werden in den AGB auf der Website ausführlich dargestellt.

Der Distributor erfüllt somit im Wesentlichen die folgenden Funktionen:

1. Er empfängt die Daten aus den Swissdec-zertifizierten Lohnbuchhaltungen der Unternehmen (Datensender).
2. Er überprüft die erhaltenen Daten im Hinblick auf deren Validität und Plausibilität.
3. Er filtert die Daten und leitet sie an die berechtigten Empfänger weiter.
4. Er speichert die Antworten der angeschlossenen Empfänger und gibt sie gesammelt an den Sender zurück.
5. Nach der erfolgreichen Übermittlung werden sämtliche Daten gelöscht. Es werden keine Personendaten gespeichert.

Die Funktion des Distributors zeigt die folgende grafische Darstellung – Swissdec Lösung:



Die Distributor-Applikation wird im Rechenzentrum eines spezialisierten Anbieters⁴ (im Folgenden «Betreiber») betrieben, der nach ISO 27001:2013 zertifiziert ist. Zwischen dem Verein Swissdec und dem Betreiber besteht ein Vertrag, welcher den Anforderungen gemäss Art. 9 DSG entspricht. Der Betreiber ist insbesondere verpflichtet, die übermittelten Daten nicht für eigene Zwecke zu verwenden und die Datensicherheit zu gewährleisten. Er rapportiert monatlich an die Geschäftsstelle des Vereins Swissdec. Zudem finden regelmässig externe Audits betreffend die Datensicherheit statt.

⁴ Swisscom.

4. Der Leistungsstandard-CH (KLE)

4.1 Elemente des Leistungsstandard-CH (KLE)

Der Verein Swissdec hat den Leistungsstandard-CH (KLE) entwickelt und stellt dem Versicherer Infrastruktur für die elektronische Kommunikation mit seinen Kunden zur Verfügung (sogenannter „Distributor“). Der Leistungsstandard-CH (KLE) ermöglicht dem Versicherer eine standardisierte elektronische Abwicklung von Ereignismeldungen im Bereich UVG, UVGZ und KTG basierend auf einem Swissdec-zertifizierten ERP-System. Die Standardisierung umfasst die beiden folgenden Bereiche:

- Standardisierung der Datenübermittlung aus einem ERP-System eines Unternehmens an den Versicherer und
- Standardisierung des Prozesses der Schadenabwicklung im Sinn einer Festlegung der zu erledigenden Prozessschritte.

Eine **Standardisierung** der Datenübermittlung erfolgt nur dort, wo sie auch bestimmt werden kann. Auch in diesen Fällen sind aber nicht immer alle Datenfelder genau festgelegt. Vielmehr gibt es Muss- und Kann-Felder. Dies ist beispielsweise der Fall bei

- Ereignismeldungen
- Mutationsmeldungen betreffend die Arbeitsunfähigkeit (AUF)
- Mutationsmeldungen betr. den behandelnden Arzt / das Spital
- Mutation betr. den Jahreslohn
- Mutation betr. die Zahlungsverbindung
- Etc.

Da die Informationen, die zur Schadenabwicklung ausgetauscht werden müssen, von Fall zu Fall variieren, besteht im Leistungsstandard zudem die Möglichkeit, **elektronische Nachrichten** (Dialoge) auszutauschen.

4.2 Übersicht Leistungsstandard-CH (KLE)

4.2.1 Anmeldung eines Ereignisses

Die Anmeldung eines Ereignisses startet mit der Übermittlung eines «Declares». Der Versicherer gibt die Schadennummer zurück, sofern die Anlage des gemeldeten Ereignisses erfolgreich war.

Nach der erfolgreichen Registrierung erfolgt die Synchronisation, die durch das Unternehmen angestoßen wird. Das heisst, der Versicherer kann im Rahmen des Synchronisierungsprozesses die aus seiner Sicht notwendigen Datenpakete (Parts/Stories) beim Versicherer automatisch einverlangen, die er für die Fallbearbeitung benötigt, falls sie nicht schon direkt übermittelt wurden.

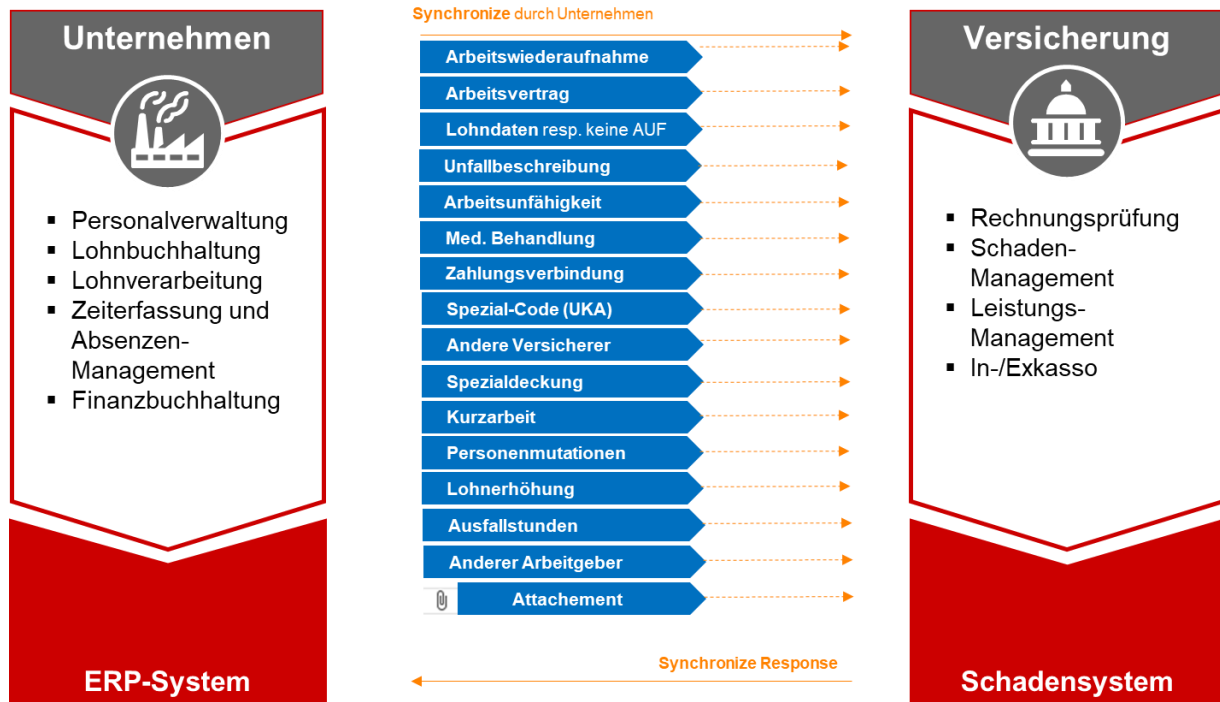
Die folgende Grafik zeigt die Übersicht aller vorgesehenen Datenpakete auf:



4.2.2 Austausch von Parts/Stories im Fallverlauf

Grundsätzlich kann der Versicherer auch im Fallverlauf Datenpakete (Parts/Stories) vom Arbeitgeber im Rahmen des Synchronisierungsprozesses bestellen. Welche Datenpakete der Versicherer bestellt, ist abhängig von seinen internen Schadenprozessen.

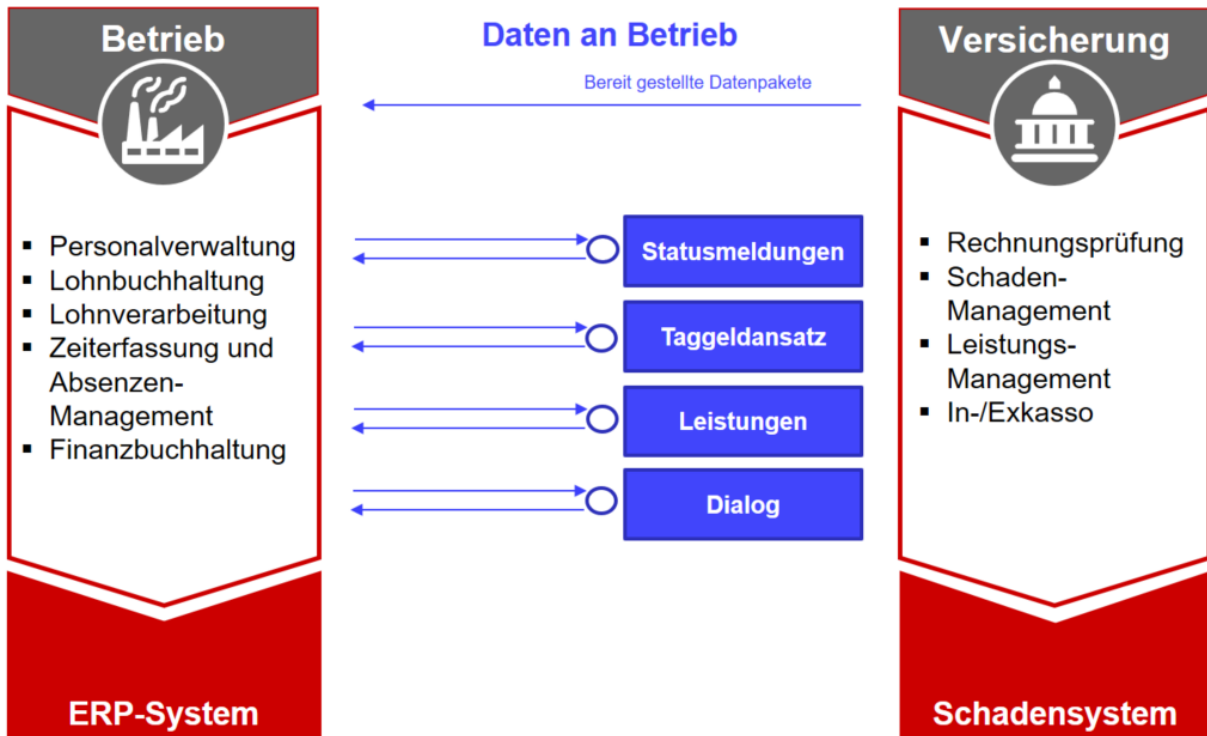
Die folgende Grafik zeigt auf, was aus Sicht eines Versicherers bestellt werden könnte. Mit Ausnahme der Arbeitswiederaufnahme kann das Unternehmen alle aufgeführten Parts/Stories auch von sich aus übermitteln.



4.2.3 Daten des Versicherers an den Betrieb

Sobald eine Ereignismeldung bei einem Versicherer erfolgreich registriert werden konnte, stellt der Versicherer dem Betrieb Informationen und Daten zur Verfügung.

Die folgende Grafik zeigt auf, um welche Informationen / Daten es sich handeln kann:

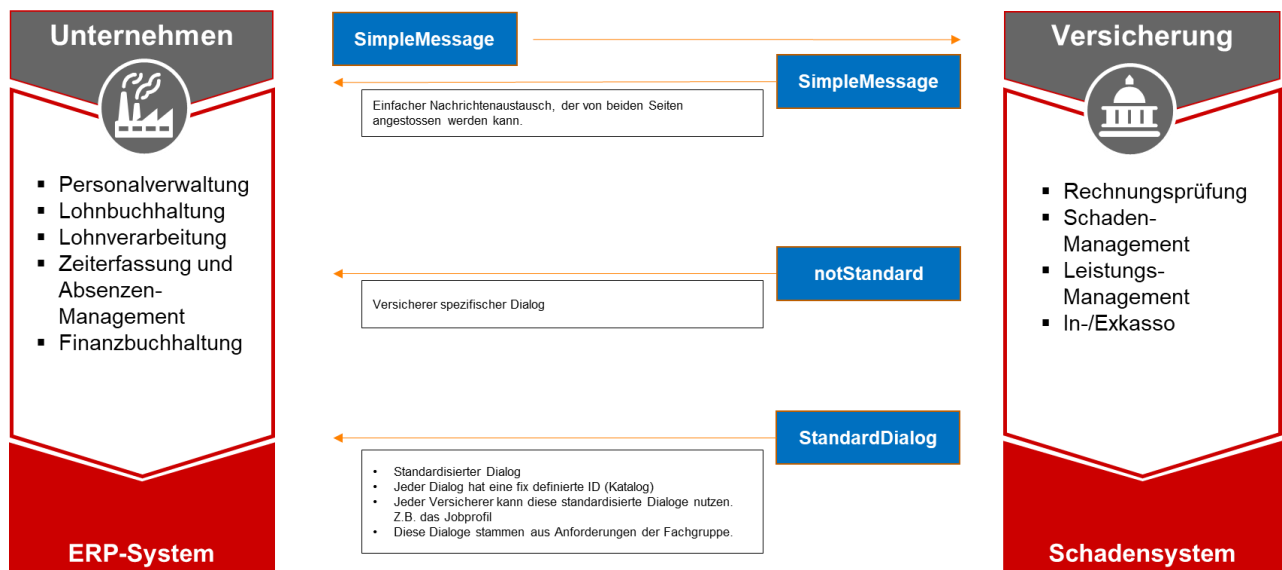


4.2.4 Dialogaustausch

Grundsätzlich wird der Dialog im Fallverlauf genutzt. Das heisst, es können vom Betrieb wie auch vom Versicherer Nachrichten übermittelt werden. Die Nachrichten können strukturiert wie auch unstrukturiert sein.

Die ausgetauschten Nachrichten (Dialoge) müssen sich jeweils auf das entsprechende Ereignis beziehen. Der Inhalt der Nachrichten soll so gehalten werden, als diese beim Versicherer in den Fallakten archiviert werden können.

Ein Dialog kann als Information als auch als Frage übermittelt werden, auf die eine Antwort erwartet wird. Die folgende Grafik zeigt die Varianten grob auf:



Sonderfall

Der Versicherer hat die Möglichkeit, mittels Dialogs den Betrieb darauf aufmerksam zu machen, eine neue Ereignismeldung vorzunehmen, die beim Versicherer benötigt wird, um ein Ereignis bearbeiten zu können.

4.2.5 Ereignis-Registrierung

Bereits beim Erfassen einer Ereignismeldung muss darauf geachtet werden, dass nur Datenkonstellationen übermittelt werden, die valide sind.

Mit einer Validierung der Daten vor der Übermittlung an den Versicherer ist sichergestellt, dass bereits zu Beginn im Meldeprozess keine Fehler entstehen und so die Verarbeitung weitgehend vollautomatisch, ohne manuelle Eingriffe für die Datenbereinigung, erfolgen kann.

Werden nicht valide Daten übermittelt, kann der Versicherer eine Rückweisung vornehmen unter Angabe des Rückweisungsgrundes.

Mögliche Rückweisungsgründe

- Partnernummer nicht korrekt
- Vertragsnummer nicht korrekt
- Betriebsteil nicht korrekt



5. Datenschutzrechtliche Aspekte

5.1 Vorbemerkungen

Im Folgenden werden datenschutzrechtliche Aspekte der Deklaration und Übermittlung von Daten mittels Lohnstandard-CH (ELM) sowie Leistungsstandard-CH (KLE) untersucht. Dabei werden im Wesentlichen die folgenden Fragestellungen beleuchtet:

- Datenlieferanten und Datenempfänger
- Klassifizierung der Daten und der Datenfluss
- Rechtmässigkeit der Deklaration und Übermittlung der Daten mittels Lohnstandard-CH (ELM) bzw. Leistungsstandard-CH (KLE)
- Outsourcing der Datenbearbeitung bei Verwendung des Distributors
- Verhältnismässigkeit bei der Deklaration und Übermittlung der Daten
- Prinzip der Zweckbindung
- Datensicherheit

Es wird weder die Datenbearbeitung durch die einzelnen Arbeitgeber noch durch die empfangenden Behörden und Versicherungen (inhouse) beleuchtet, da diese nicht im Verantwortungsbereich des Vereins Swissdec liegen.

5.2 Datenlieferanten

Zahlreiche Gesetze verpflichten die Arbeitgeber, regelmässig insbesondere die Lohndaten ihrer Angestellten an Behörden des Bundes und der Kantone sowie an Versicherungen bekanntzugeben. Die benötigten Daten werden in der Schweiz von den Unternehmen übermittelt. Datenlieferanten sind somit sämtliche in der Schweiz domizilierten Arbeitgeber. Bei den bekanntzugebenden Daten handelt es sich um Daten von in der Schweiz tätigen Arbeitnehmerinnen und Arbeitnehmern.

5.3 Datenempfänger

5.3.1 Grundsatz

Datenempfänger sind Verwaltungsbehörden, öffentlich-rechtliche Körperschaften des Bundes und der Kantone sowie privatrechtliche Versicherungen, welche berechtigt sind, die Lohndaten zur Erfüllung ihres gesetzlichen oder vertraglichen Auftrages zu bearbeiten. Die Datenempfänger sind, wie bereits erwähnt, teilweise durch ihre Interessensverbände (Schweizerischer Versicherungsverband SVV, Schweizerische Steuerkonferenz SSK, Verein eAHV/IV) im Verein Swissdec vertreten.

Im Folgenden werden die Kategorien der Datenempfänger aufgelistet und für jede Kategorie die massgebliche spezialgesetzliche Grundlage angegeben. Zusätzlich kommen noch das Datenschutzgesetz des Bundes (DSG) sowie die entsprechenden kantonalen Datenschutzgesetze zur Anwendung.

5.3.2 Suva

Die Suva ist eine selbständige Unternehmung des öffentlichen Rechts des Bundes mit Hauptsitz in Luzern. Sie versichert auf der Grundlage des Unfallversicherungsgesetzes die Mehrheit der Berufstätigen in der Schweiz gegen die Folgen von Unfällen und Berufskrankheiten. Die Suva erbringt für die Versicherten und die Unternehmen umfassende Leistungen in den Bereichen Prävention, Versicherung und Rehabilitation. Massgebende Rechtsgrundlage ist das Bundesgesetz über die Unfallversicherung (UVG) sowie das Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG).

5.3.3 Ausgleichskassen

Für die Durchführung und den direkten Kontakt mit den Versicherten und Arbeitgebern sind in erster Linie die Ausgleichskassen der Verbände, der Kantone und des Bundes mit ihren Zweigstellen zuständig. Sie setzen die Beiträge fest und ziehen sie ein. Sie berechnen die Leistungen der AHV und sind für deren Ausrichtung an die Versicherten verantwortlich. Die Gesetzgebung und die Aufsicht der AHV sind zentral organisiert. Das Bundesamt für Sozialversicherung sorgt für eine einheitliche Anwendung der gesetzlichen Vorschriften. Massgebende Rechtsgrundlage ist das Bundesgesetz über die Alters- und Hinterlassenenversicherung (AHVG) sowie das Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG).

5.3.4 Bundesamt für Statistik

Das Bundesamt für Statistik (BFS) ist das nationale Dienstleistungs- und Kompetenzzentrum für die statistische Beobachtung in wichtigen Bereichen von Staat und Gesellschaft, Wirtschaft und Umwelt. Massgebende Rechtsgrundlage ist das Bundesstatistikgesetz (BStatG).

5.3.5 Kantonale Steuerbehörden

Kantonale Steuerbehörden sind grundsätzlich für zwei Domänen als Datenempfänger vorgesehen – es handelt sich um den Lohnausweis sowie um die Quellensteuer.

Einige Kantone, wie z.B. der Kanton Bern, sehen vor, dass die Unternehmen die Lohndaten ihrer Mitarbeitenden direkt an das Kantonale Steueramt überweisen. Dies ist eine Ausnahme von dem in den meisten Kantonen vorherrschenden Prinzip der Selbstdeklaration, wonach die Mitarbeitenden den Lohnausweis von ihrem Arbeitgeber erhalten und diesen selbst bei der zuständigen Steuerbehörde einreichen. Eine elektronische Übermittlung von Lohndaten von Unternehmen an Steuerbehörden kann nur in solchen Kantonen erfolgen, in welchen die direkte Übermittlung der Lohndaten gesetzlich verankert ist. Die massgebenden gesetzlichen Grundlagen für die Datenbearbeitung finden sich in den kantonalen Steuergesetzen.

Die gesetzliche Grundlage für die Bearbeitung der Daten im Bereich der Quellensteuer findet sich im Bundesgesetz über die Harmonisierung der direkten Steuern der Kantone und Gemeinden (StHG; SR 642.14) sowie in den kantonalen Steuergesetzen. Die Daten zur Erhebung der Kirchensteuer, insbesondere die Konfession, sofern sie einer Landeskirche entspricht, erhalten nur die kantonalen Steuerbehörden, welche über eine entsprechende gesetzliche Grundlage verfügen⁵.

5.3.6 Versicherungsanstalten des privaten Rechts

Die privatrechtlichen Versicherungsanstalten erbringen im Rahmen der Personenversicherung unter anderem auch Leistungen der obligatorischen Unfallversicherung, sowie der Krankentaggeldversicherung und der beruflichen Vorsorge. Im Rahmen der obligatorischen Unfallversicherung üben diese Versicherungsanstalten eine öffentlich-rechtliche Aufgabe aus und sind an die massgeblichen gesetzlichen Grundlagen gebunden. Dabei handelt es sich um das Bundesgesetz über die Unfallversicherung (UVG). Ebenfalls anwendbar ist das Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG), sowie das Bundesgesetz über den Versicherungsvertrag (VVG) und das Bundesgesetz über die berufliche Alters-, Hinterlassenen- und Invalidenvorsorge (BVG).

5.4 Daten

5.4.1 Art und Inhalt

Die Daten, die im Rahmen des Lohnstandard-CH (ELM) bzw. des Leistungsstandard-CH (KLE) bearbeitet bzw. übermittelt werden, sind in den Richtlinien des Lohnstandard-CH (ELM) bzw. des Leistungsstandard-CH (KLE) detailliert ausgewiesen. Auf eine Auflistung der Daten wird daher an dieser Stelle verzichtet (siehe www.swissdec.ch/elm Datenfelder pro Domäne 20200220_20200602).

⁵ Diese sind in der Datenschutzerklärung Domäne Quellensteuer detailliert aufgelistet.

5.4.2 Klassifizierung der Daten

Das Datenschutzgesetz kennt Klassifizierungen von Daten. Unter dem allgemeinen Begriff Personendaten sind alle Angaben zu verstehen, die sich auf eine bestimmte oder bestimmbare Person beziehen (Art. 5 lit. a DSG). Nebst diesem allgemeinen Begriff der **Personendaten** kennt das Datenschutzgesetz den Begriff der **besonders schützenswerten Personendaten**. Dabei handelt es sich um Daten, bei deren Bearbeitung ein erhöhtes Gefährdungspotential für Persönlichkeitsverletzungen der betroffenen Personen besteht.

Welche Personendaten als besonders schützenswert zu bezeichnen sind, wird in Art. 5 lit. c DSG in abschliessender Weise geregelt. Es handelt sich dabei um

- Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten,
- Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie,
- genetische Daten,
- biometrische Daten, die eine natürliche Person eindeutig identifizieren,
- Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen,
- Massnahmen der sozialen Hilfe.

Daten über die Einkommens- und Vermögensverhältnisse gehören nicht zu den besonders schützenswerten Daten nach Datenschutzgesetz. Der Profiling-Begriff im neuen DSG ersetzt den bisherigen Begriff des Persönlichkeitsprofils. Das «Profiling mit hohem Risiko» nach Art. 5 lit. g DSG kommt dem alten Begriff des Persönlichkeitsprofils jedoch sehr nahe. Während das alte Persönlichkeitsprofil einen statischen Zustand beschreibt, bezieht sich der neue Begriff des Profilings auf den Bewertungsvorgang als solchen.⁶ Das Profiling mit hohem Risiko verlangt zudem eine Datenverknüpfung, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt. Entscheidend ist somit, ob sich die verknüpften Informationen zu einem umfassenden Bild der betroffenen Person verdichten.⁷

Einzelne Datenfelder lassen erkennen, dass unter Umständen auch besonders schützenswerte Personendaten bearbeitet werden. So können beispielsweise aufgrund der Angaben zu Konfession oder Taggeldverarbeitung Aussagen über die Religion oder die Gesundheit der betroffenen Arbeitnehmer gemacht werden. Bereits die Angabe über die Konfession gilt als besonders schützenswertes Personendatum im Sinne von Art. 5 lit. c DSG⁸. Als Angaben über die Gesundheit gelten alle Informationen, die direkt oder indirekt Rückschlüsse über den physischen oder psychischen Gesundheitszustand einer Person zulassen⁹.

Je nach Datenschutzverständnis oder Interessenslage wird verlangt, dass für eine Klassifizierung von Personendaten nicht bloss auf die abstrakte gesetzliche Aufzählung gemäss Art. 5 lit. c DSG abgestellt wird. Massgebend soll vielmehr auch die Frage nach der tatsächlichen Schutzwürdigkeit konkreter Daten sein. So muss im Zusammenhang mit dem Lohnmeldeverfahren die Frage gestellt werden, ob die blosser Konfessionsangabe oder die blosser Angabe, jemand beziehe IV- oder UVG-Taggelder, schon als besonders schützenswert zu klassifizieren ist. Diese Frage kann nur in Berücksichtigung des jeweiligen Kontextes (generelle Aussagekraft der Daten, konkreter Informationsgehalt für den jeweiligen Datenempfänger, Möglichkeit der Verknüpfung mit anderen Daten, mögliche weitere Datenbearbeitung und -empfänger) beantwortet werden.

⁶ Matthias Glatthaar/Annika Schröder, Kommentierung zu Art. 5 lit. f und g DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz – Version: 19.08.2023, Rz. 3, 17: <https://onlinekommentar.ch/de/kommentare/dsg5fundg> (besucht am 14. Mai 2024).

⁷ Matthias Glatthaar/Annika Schröder, Kommentierung zu Art. 5 lit. f und g DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz – Version: 19.08.2023, Rz. 23: <https://onlinekommentar.ch/de/kommentare/dsg5fundg> (besucht am 14. Mai 2024).

⁸ vgl. Yvonne Jöhri, Handkommentar DSG, Zürich 2008, Art. 3 Bst. c, N 47.

⁹ Yvonne Jöhri, Handkommentar DSG, Zürich 2008, Art. 3 Bst. c, N 48.

Hingegen darf davon ausgegangen werden, dass kein Profiling durchgeführt wird, da mit den Lohn-
daten keine Beurteilung wesentlicher Aspekte der Persönlichkeit der betroffenen Personen gemacht wer-
den können.

5.4.3 Fazit

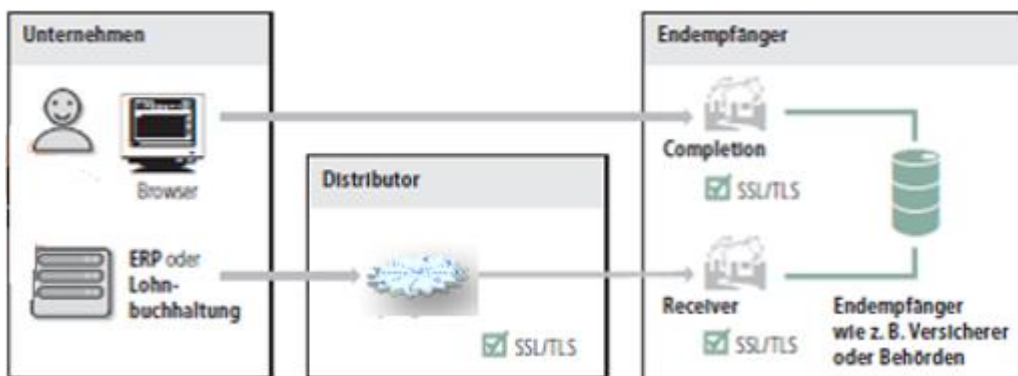
Bei der Übermittlung von Lohndaten gemäss der obenstehenden Deklaration handelt es sich um eine
datenschutzrechtlich relevante Bearbeitung von Personendaten.

Auf Grund der Menge der übermittelten Daten ist grundsätzlich von einem grossen Potenzial von Per-
sönlichkeitsverletzungen auszugehen. Die Sicherheitsmassnahmen zum Schutz der Daten sind ent-
sprechend sorgfältig zu wählen.

5.5 Datenfluss Lohnstandard-CH (ELM)

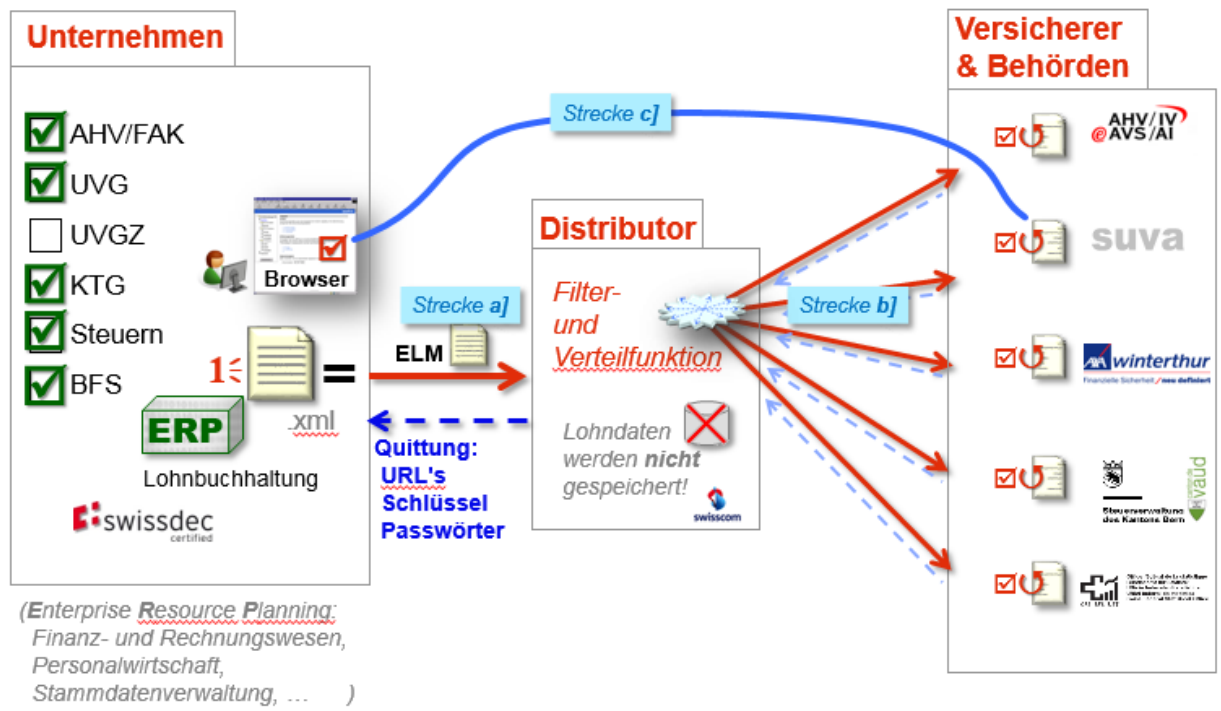
Der Datenfluss kann der folgenden, vereinfachten Darstellung entnommen werden:

Swissdec Datenfluss



Die Unternehmen übermitteln die Daten an den Distributor, welcher diese in Empfang nimmt, nach Empfänger filtert und verteilt. Der Verein Swissdec selbst stellt nur die Infrastruktur zur Verfügung, greift aber nicht auf die übermittelten Daten selbst zu. Die Daten werden im flüchtigen Hauptspeicher des Distributors bis zur erfolgreichen Übermittlung zwischengespeichert und anschliessend gelöscht (Ausführliche Erklärungen zur Speicherung von Informationen und Daten auf dem Distributor sind in den AGB des Vereins Swissdec auf der Website zu finden). **Es werden keine Personendaten gespeichert.**

Skizze zur Kommunikation



Ablaufbeschreibung Schritte 1) bis 3)

- 1) Die **Übermittlung** geschieht in **Echtzeit**
(*Signature + Encryption; Web Services Security (WSS)*)
 - i. Die Buchhaltung extrahiert die notwendigen Nutzdaten und übermittelt diese an den Distributor (Strecke a]).
 - ii. Der Distributor prüft, filtert und verteilt die Nutzdaten an die adressierten Endempfänger-Institutionen (Strecke b]).
 - iii. Die Endempfänger prüfen die Nutzdaten und quittieren deren Empfang beim Distributor (Strecke b]).
 - iv. Der Distributor sammelt alle Quittungen und quittiert damit seinerseits bei der Buchhaltung (Strecke a]).
- 2) Die **Freigabe** der Meldung erfolgt mittels Browser (Strecke c])
- 3) Danach werden eventuell weitere Daten beim Endempfänger abgeholt (Strecke a] und b]) und direkt in die Buchhaltung integriert.

5.6 Datenfluss Leistungsstandard-CH (KLE)

Sobald eine Ereignismeldung bei einem Versicherer erfolgreich registriert werden konnte, stellt der Versicherer dem Betrieb Informationen und Daten zur Verfügung.

Die folgende Grafik zeigt auf, um welche Informationen / Daten es sich handeln kann:



5.7 Rechtmässigkeit der Datenbearbeitung

5.7.1 Allgemeines

Organe des Bundes oder der Kantone dürfen Personendaten bearbeiten, wenn dafür eine **gesetzliche Grundlage** besteht (Art. 34 Abs. 1 DSG; analoge Bestimmungen in den kantonalen Datenschutzgesetzen). Für die Bearbeitung von besonders schützenswerten Personendaten oder bei Profiling bedarf es formeller Gesetze (Art. 34 Abs. 2 DSG sowie kantonale Datenschutzgesetze). Man spricht in diesem Zusammenhang vom **Legitizitätsprinzip**.

Privatpersonen (Versicherungsanstalten des privaten Rechts) dürfen Personendaten bearbeiten, jedoch hat die Bearbeitung rechtmässig zu sein und darf die Persönlichkeit der betroffenen Person nicht widerrechtlich verletzen (Art. 6 Abs. 1 i.V.m. Art. 30 DSGVO¹⁰).

5.7.2 Lohnstandard-CH (ELM)

Die beteiligten Behörden des Bundes und der Kantone dürfen, wie bereits erwähnt, die Lohndaten nur dann bearbeiten, wenn dafür eine gesetzliche Grundlage vorhanden ist. Das Legalitätsprinzip gilt auch für die Versicherungsanstalten des privaten Rechts, wenn sie öffentlich-rechtliche Aufgaben ausüben. Dies ist z.B. im Rahmen der obligatorischen Unfallversicherung oder der obligatorischen Krankenpflegeversicherung oder im obligatorischen Bereich des BVG der Fall. Im Bereich der Zusatzversicherung kommen für diese Unternehmen hingegen die privatrechtlichen Vorschriften zur Anwendung. Hier müssen sie dafür Sorge tragen, dass sie auf Grund ihrer vertraglichen Vereinbarungen mit den Versicherungsnehmern berechtigt sind, die erforderlichen Daten zu bearbeiten.

Das Vorhandensein der **Rechtsgrundlagen für die Datenbearbeitung** ist somit für den Lohnstandard-CH (ELM) von grundlegender Bedeutung.

Im Zusammenhang mit dem Nachweis der Rechtmässigkeit der Datenbearbeitung bei der Übermittlung der Lohndaten über den Distributor gelten die folgenden **Grundsätze**:

- Grundsätzlich verfügen alle Datenempfänger über die entsprechenden Rechtsgrundlagen, die sie dazu ermächtigen, den Datensendern die Art und Weise, wie diese ihnen die Daten übermitteln müssen, vorzugeben¹¹. Diese Rechtsgrundlagen ermächtigen die Datenempfänger aber nur, die Unternehmen zu verpflichten, die Löhne zu melden und dabei Vorgaben über die Art und Weise der Lohnmeldung zu beachten. Keinesfalls erhalten die Datenempfänger damit das Recht, die Übermittlung von Daten zu verlangen, für welche keine oder keine ausreichende Rechtsgrundlage vorhanden ist.
- Der Verein Swissdec stellt die Infrastruktur für die Datenübermittlung inklusive Filterung der Daten zur Verfügung. Der Verein Swissdec ist dabei ein Outsourcing Partner der Datenempfänger gemäss Art. 9 DSGVO (siehe dazu die Ausführungen unter Ziffer 5.8).
- Jeder Empfänger bleibt daher auch weiterhin dafür verantwortlich, dass er nur die Daten erhält, die er laut Gesetz bearbeiten darf. Er hat unter anderem sicherzustellen, dass er oder seine Interessensvertretung im Verein Swissdec eine sogenannte «Datenschutzerklärung» unterzeichnet hat. Darin bestätigt er oder seine Interessensvertretung, dass er das Vorliegen einer genügenden gesetzlichen oder vertraglichen Grundlage für Datenempfang und Bearbeitung geprüft hat und hierfür die Verantwortung trägt.
- Nur wer direkt oder indirekt eine «**Datenschutzerklärung**» unterzeichnet hat, kann Datenempfänger werden. Die Liste der Datenempfänger ist auf der Website des Vereins Swissdec zu finden (siehe www.swissdec.ch/elm Datenfelder pro Domäne 20200220_20200602).
- Da der Lohnstandard-CH (ELM) steuert, welches Datenfeld durch den Distributor welchem Datenempfänger zugestellt wird, muss bei der Erstellung und Weiterentwicklung des Lohnstandard-CH (ELM) die entsprechende Rechtsgrundlage nachgewiesen werden. Jeder Empfänger erhält regelmässig die Liste mit den Datenfeldern, für welche er als Empfänger vorgesehen ist. Er ist verpflichtet, die Liste zu prüfen und die Rechtsgrundlage anzugeben bzw. zu bestätigen, dass er über ausreichende Rechtsgrundlagen für die Bearbeitung der Datenfelder verfügt.
- Diese Liste bildet die **transparente und nachvollziehbare Grundlage** für die Steuerung der Filterfunktion des Distributors.

¹⁰ Handkommentar zum Datenschutzgesetz, Rosenthal, N 3 zu Art. 4.

¹¹ Beispiele: Art. 143 Abs. 1 AHVV, Art. 116 Abs. 1 UVV.

- Die **Transparenz** bleibt auch für die **Datenlieferanten** weiterhin bestehen: Jedem Unternehmen steht es frei, im Einzelfall zu entscheiden, dass die Lohndaten nur an einen oder nur an bestimmte Empfänger gesandt werden. Es wird direkt eine Institution (Versicherer & Behörde) adressiert, z.B. «S999» für die Suva (explizit) oder es wird in der Verteilung des Lohnausweise (LA) keine direkte kantonale Steuerverwaltung angegeben, sondern der Distributor filtert und verteilt die LA an die zuständigen Kantone (gekoppelte Kantone) (implizit). Der Lohnstandard-CH (ELM) und der Distributor machen hierzu keine Einschränkungen. Zudem kann es sich nach erfolgter Übermittlung über einen Link direkt ins System des Empfängers einloggen und die angekommenen Daten überprüfen und/oder ergänzen (mit Ausnahme des Systems der Steuerverwaltung). Anschliessend erfolgt die Freigabe direkt im System des Empfängers.
- Von Seiten des Vereins Swissdec werden damit die Grundlagen geschaffen, um Art und Inhalt der übermittelten Daten für alle Beteiligten **transparent und nachvollziehbar** zu machen.

5.7.3 Leistungsstandard-CH (KLE)

Im Leistungsstandard-CH (KLE) geht es um die automatisierte Abwicklung von Ereignissen (basierend auf einem Unfall oder einer Krankheit) zwischen dem Unternehmen und der betreffenden Versicherung ausgehend von einem Swissdec-zertifizierten ERP-Programm. Gesetzliche Grundlagen bilden das UVG und das ATSG (bei der Unfallversicherung) sowie das VVG (bei Unfallzusatzversicherung sowie der Krankentaggeldversicherung). Für alle beteiligten Versicherer (Suva und Privatversicherer) ist das Bundesgesetz über den Datenschutz (DSG) anwendbar. Im Bereich UVG handeln die Versicherer aber als Bundesorgane, im Bereich UVGZ und KTG als private Versicherungsgesellschaften.

Die Datenbearbeitung basiert daher

- im Bereich der Unfallversicherung auf dem UVG sowie dem ATSG (Legalitätsprinzip)
- und in den Bereichen UVGZ und KTG auf einer vertraglichen Vereinbarung zwischen dem Versicherer und dem Unternehmen basierend auf dem VVG
- sowie auf dem Bundesgesetz über den Datenschutz (DSG).

5.8 Outsourcing der Datenbearbeitung

5.8.1 Allgemein

Bundesorgane sind gemäss DSG berechtigt, bei der Bearbeitung von Personendaten Dritte beizuziehen, wenn der Datenschutz gewährleistet ist (Art. 16 DSG, Art. 22 VDSG).

Massgebende Rechtsgrundlage für die Auslagerung von Datenbearbeitung an einen Dritten ist Art. 9 DSG. Gemäss Art. 9 DSG kann das Bearbeiten von Personendaten durch Vereinbarung oder Gesetz Dritten übertragen werden, wenn

- a. die Daten nur so bearbeitet werden, wie der Auftraggeber selbst es tun dürfte (d.h. unter Beachtung der für ihn geltenden datenschutzrechtlichen Bedingungen); und
- b. keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet; und
- c. der Auftraggeber sich vergewissert, dass der Dritte die Datensicherheit gewährleistet.

5.8.2 Outsourcing des Datenempfangs an den Verein Swissdec

Die Datenempfänger möchten, aufgrund der oben erwähnten Vorteile (Einhaltung des Datenschutzes, einfache Umsetzung von Gesetzesänderungen, etc.) die Daten via Distributor entgegennehmen. Die Datenempfänger haben hierfür den Verein Swissdec gegründet (oder sind später beigetreten) und mit dem Betrieb des Distributors bzw. dem Empfang und der Bearbeitung der Daten beauftragt. Der Distributor, welcher eine entscheidende Rolle bei der Filterung und Zustellung der Daten spielt, wird gesteuert durch den Lohnstandard-CH (ELM) bzw. den Leistungsstandard-CH (KLE), an dessen Erstellung und Weiterentwicklung wiederum die Datenempfänger mitwirken. Es handelt sich um ein **Outsourcing der Datenbearbeitung** gemäss Art. 9 DSG.

Voraussetzung für das Outsourcing ist in jedem Fall, dass der **Schutz** und die **Sicherheit der Daten** gewahrt bleibt. Zu diesem Zweck schliesst der Verein Swissdec einen Vertrag mit dem Betreiber des Distributors, in welchem er sich zur auftragsgemässen und weisungsgebundenen Datenbearbeitung verpflichtet. Die Verantwortung für die datenschutzkonforme Datenbearbeitung bleibt bei den einzelnen Datenempfängern, welche ihre Verantwortung im Rahmen ihrer Mitbestimmungsrechte im Verein Swissdec wahrnehmen müssen.

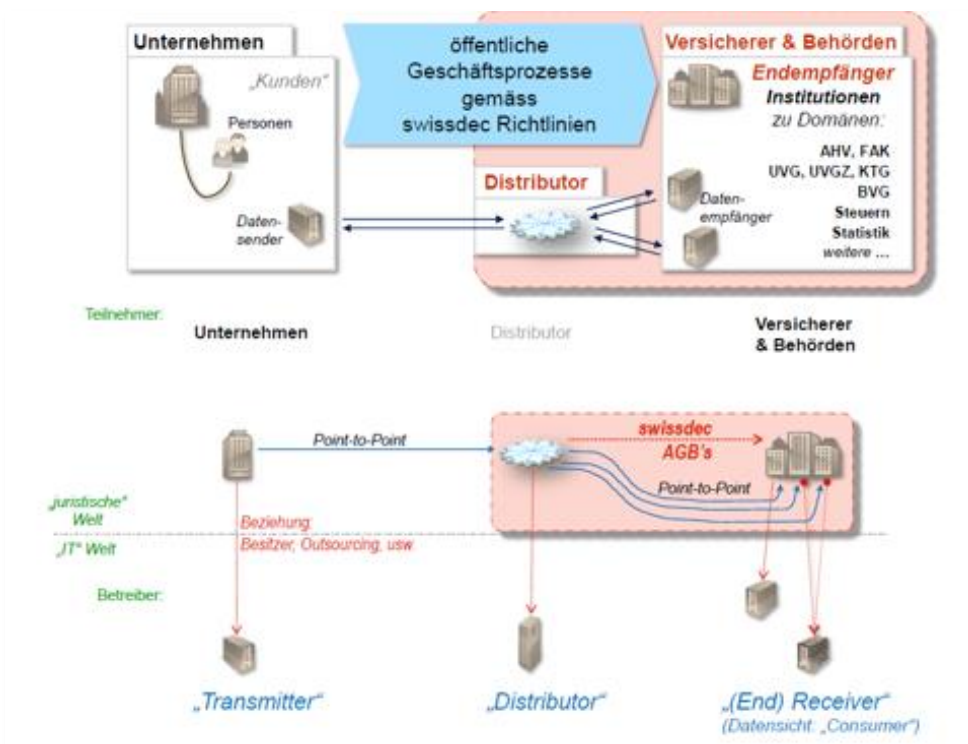
Um den Datenschutz und die Datensicherheit zu verbessern, können gemäss Art. 13 DSGVO Hersteller von Datenbearbeitungssystemen oder –programmen sowie Unternehmen oder Bundesorgane, die Personendaten bearbeiten, ihre Systeme, Verfahren und ihre Organisation einer **Bewertung durch anerkannte unabhängige Zertifizierungsstellen** unterziehen. Der Verein Swissdec hat das Datenschutzlabel GoodPriv@cy erworben und ist gemäss der Verordnung über die Datenschutzzertifizierung (VDSZ) zertifiziert.

5.8.3 Outsourcing des Vereins Swissdec an Dritte

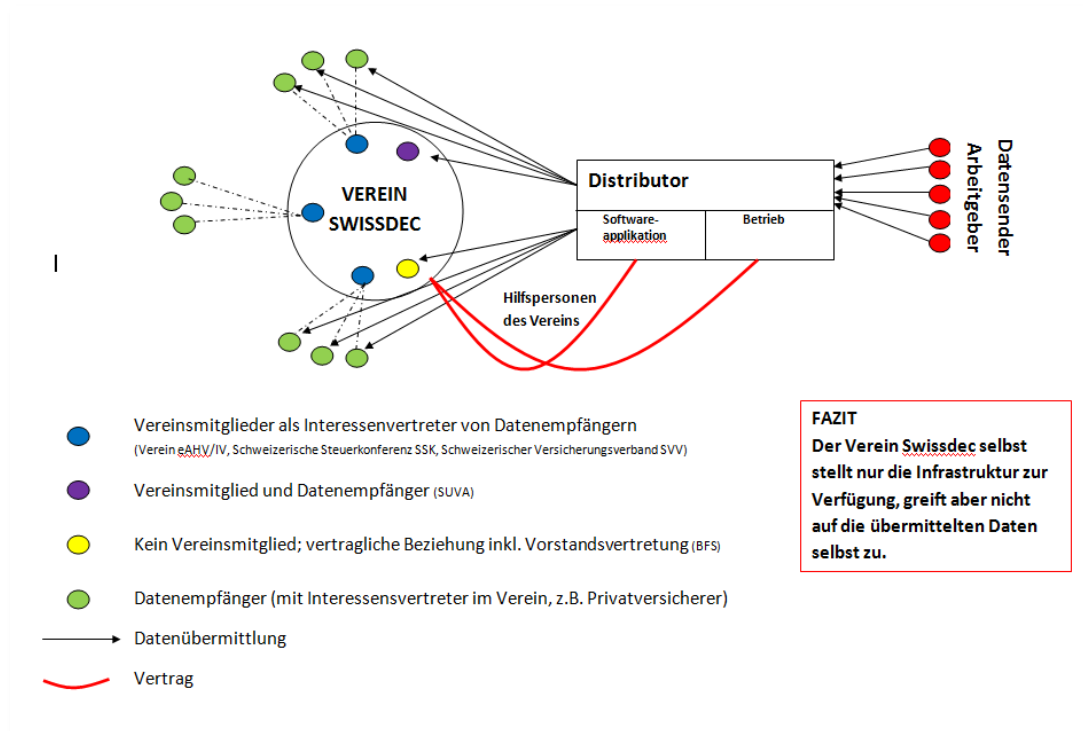
Der Distributor wird im Auftrag des Vereins Swissdec im Rechenzentrum des Betreibers¹² betrieben sowie von einem spezialisierten Dienstleister gewartet und weiterentwickelt. Mit beiden Unternehmen bestehen Verträge, die diese zur Einhaltung des Datenschutzes, insbesondere zur Gewährleistung der Datensicherheit, verpflichten. Aus datenschutzrechtlicher Sicht handelt es sich dabei wiederum um eine Datenbearbeitung durch Dritte gemäss Art. 9 DSGVO. Beide Unternehmen sind dabei Hilfspersonen des Vereins Swissdec.

Die vertraglichen Beziehungen bei der Übermittlung der Daten unter Verwendung des Distributors können wie folgt dargestellt werden:

Swissdec Verantwortlichkeit (AGBs)



¹² Die Swisscom AG betreibt den Distributor im Auftrag des Vereins Swissdec in ihrem Rechenzentrum.



5.8.4 Gesetzliche oder vertragliche Geheimhaltungspflichten

Wie bereits erwähnt, ist die Bearbeitung von Personendaten durch einen Dritten nur zulässig, wenn keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet (Art. 9 Abs. 1 lit. b DSGVO).

Geheimhaltungspflichten bestehen jedoch z.B. für die Steuerbehörden mit dem Steuergeheimnis (z.B. 110 DBG, § 120 StG ZH) und für die Träger der Sozialversicherungen mit der Schweigepflicht nach Art. 33 ATSG. Diese sieht vor, dass Personen, welche an der Durchführung sowie der Kontrolle oder der Beaufsichtigung der Durchführung der Sozialversicherungsgesetze beteiligt sind, gegenüber Dritten Verschwiegenheit zu bewahren haben.

Es stellt sich nun die Frage, ob diese Geheimhaltungspflichten auch so weit gehen, dass sie ein Outsourcing im Sinne von Art. 9 DSGVO verbieten.

Nicht jede gesetzliche oder vertragliche Geheimhaltungspflicht verbietet ein Outsourcing. Eine Geheimhaltungsverpflichtung müsste so weit reichen, dass sie die konkret ins Auge gefasste Übertragung der Datenbearbeitung (im Sinne von Art. 9 DSGVO) ausschliesst. Dies muss unter Berücksichtigung aller Umstände durch die Auslegung der betreffenden Geheimhaltungsklausel ermittelt werden¹³.

Bei der konkret angesprochenen Datenbearbeitung fungiert der Verein Swissdec als Outsourcing Partner, d. h. als «verlängerter Arm» oder ausgelagerte Abteilung der weiterhin verantwortlichen Stellen (Bundesamt für Statistik etc.), welche als Herrin der Daten die volle Verfügungsgewalt behält und damit auch allein über Erhebung, Verarbeitung und Nutzung ihrer Personendaten bestimmt (Vgl. S. 17¹⁴). Weder das Steuergeheimnis noch die Schweigepflicht für die Träger der Sozialversicherungen gehen so weit, dass sie ein solches Outsourcing ausschliessen.

Fazit

- Die einzelnen Datenempfänger schliessen mit dem Verein Swissdec einen Vertrag über die Nutzung des Distributors zur Übermittlung und dem Empfang von Daten, indem sie bei der Kopplung an den

¹³ David Rosenthal, Handkommentar zum Datenschutzgesetz, Zürich 2008, Art. 10a Abs. 1 Bst. b, N102.

¹⁴ Gola/Somerus, Bundesdatenschutzgesetz, 8. Auflage, München 2005.

Distributor die Allgemeinen Geschäftsbedingungen des Vereins Swissdec akzeptieren. Sie stellen den Distributor wiederum ihren Kunden für die Datenübermittlung zur Verfügung.

- Der Verein Swissdec handelt als Outsourcing Partner im Sinne von Art. 9 DSG und ist unter Einhaltung der datenschutzrechtlichen Vorgaben der Datenempfänger zur Datenbearbeitung berechtigt.
- Die Datenempfänger bleiben dafür verantwortlich, dass die Daten nur so bearbeitet werden, wie sie es selbst tun dürften. Sie überprüfen die gesetzlichen Grundlagen (Rechtmässigkeit der Datenbearbeitung) regelmässig. Zurzeit schliessen keine gesetzlichen oder vertraglichen Geheimhaltungspflichten die Datenbearbeitung aus.

5.9 Verhältnismässigkeitsgrundsatz

5.9.1 Allgemein

Jede Bearbeitung von Personendaten muss verhältnismässig sein (Art. 6 Abs. 2 DSG). Aus diesem allgemein geltenden Verhältnismässigkeitsgrundsatz lässt sich für die Datenbearbeitung ableiten, dass ein Datenbearbeiter nur diejenigen Daten bearbeiten darf, die er für einen bestimmten Zweck objektiv tatsächlich benötigt¹⁵. Der Verhältnismässigkeitsgrundsatz verlangt also, dass eine Datenbearbeitung mit Blick auf die zu erfüllende Aufgabe auf das tatsächlich Erforderliche und Notwendige beschränkt wird.

5.9.2 Lohnstandard-CH (ELM)

Die Frage der Verhältnismässigkeit ist sowohl im Hinblick auf die vorgesehene Deklaration der Lohndaten (Richtlinie für Lohndatenverarbeitung RL-LDV) als auch für die Übermittlung der Lohndaten (Richtlinie für Lohndatenübermittlung RL-LDÜ) zu beurteilen.

Die Richtlinie für Lohndatenverarbeitung (RL-LDV) enthält alle Daten, welche die Empfänger zur Erfüllung ihrer gesetzlichen oder vertraglichen Pflichten benötigen. Die benötigten Daten lassen sich dabei aus den anwendbaren gesetzlichen Grundlagen ableiten.

So sind z. B. die UVG-Versicherer berechtigt, alle Daten zu bearbeiten, welche sie benötigen, um Prämien zu berechnen, zu kontrollieren und zu erheben, Leistungsansprüche zu beurteilen sowie Leistungen zu berechnen, zu gewähren und mit Leistungen anderer Sozialversicherungen zu koordinieren, etc. (Art. 96 UVG). Soweit die in der RL-LDV enthaltenen Daten erforderlich sind, um diese Aufgaben ausüben zu können und nicht weitere, zur Aufgabenerfüllung nicht benötigte Daten erhoben werden, erfüllt die RL-LDV die datenschutzrechtlichen Anforderungen gemäss dem Verhältnismässigkeitsgrundsatz. Der Nachweis, dass die Daten zur Erfüllung des gesetzlichen oder vertraglichen Auftrages benötigt werden, erfolgt durch die Liste gemäss Ziffer 5.7.2.

¹⁵ Basler Kommentar, N 12 zu Art. 4.

Bei der Verhältnismässigkeit der Datenbearbeitung im Zusammenhang mit der Übermittlung der Lohn-
daten ist die **Richtlinie für Lohndatenübermittlung (RL-LDÜ)** zu beurteilen. Ein Unternehmen, das
eine Swissdec-zertifizierte ERP-Software nutzt, hat die Möglichkeit, die Lohnmeldungen allen Daten-
empfängern gleichzeitig mit einem «Klick» zu übermitteln.

Durch Einsatz des sogenannten Distributors, einer Software-Applikation, welche die Daten nach Emp-
fängern filtert, wird sicherstellt, dass die Empfänger ausschliesslich diejenigen Daten erhalten, zu deren
Bearbeitung sie berechtigt sind.

Folgende Vorteile bildet der Einsatz eines zentralen Distributors (Share Economy-Ansatz):

- Einfachere Entwicklung, Testen und Produktion (statt sehr viele «n:m» nur «n:1:m» Verbindungen).
- Anonymisieren der Daten z.B. Teil-Anonymisierung für die Statistiken des BFS.
- Da die Filterfunktion im Distributor automatisiert wird, wird der Mensch als «Fehlerquelle» ausge-
schlossen.
- Der Distributor übernimmt das Mapping der Versionen vom Sender zu den Empfängern bei unter-
schiedlichen Versionen (V 2.2 → V4.0, V4.0 → V2.2).
- Der Distributor ermöglicht eine Standardisierung von Datensicherheitsmassnahmen, wie z.B. TLS-
verschlüsselte Übermittlungswege (doppelte Verschlüsselung), Verwendung von elektronischen Sig-
naturverfahren, Einsatz einer speziellen «Application Firewall», etc.
- Korrekturen, welche auf Grund von Gesetzesänderungen erforderlich sind, können an einem einzi-
gen Punkt vorgenommen werden.
- Für die Unternehmen ist diese Übermittlungsart mit weniger Zeitaufwand verbunden, da sie nicht für
jeden Empfänger eine separate Übermittlung durchführen müssen.
- Die Lohndaten werden im Rahmen der Übermittlung auf Plausibilität und Validität kontrolliert.
- Jedem Unternehmen steht es frei, im Einzelfall zu entscheiden, dass die Lohndaten nur an einen
oder nur an bestimmte Empfänger gesandt werden. Diese Funktionalität ist in jeder zertifizierten
Lohnbuchhaltung enthalten. Der Lohnstandard-CH (ELM) und der Distributor machen hierzu keine
Einschränkungen.

Ferner ist an dieser Stelle nochmals darauf hinzuweisen, dass beim Einsatz des Distributors keine Per-
sonendaten gespeichert werden. Eine eigentliche Vermischung der Daten mit anderen Daten findet
nicht statt.

Da keine Personendaten gespeichert werden, erfolgt zum Beispiel auch kein Profiling. Die Daten kom-
men in den Distributor, werden «aufgespalten» und «verschwinden» dann wieder aus dem Distributor.

Werden die übermittelten Daten im Rahmen des «Completion-Prozesses» durch den Datensender «ge-
löscht», werden diese beim Datenempfänger in der Regel nicht unmittelbar tatsächlich gelöscht, son-
dern zunächst einmal als «gelöscht» gekennzeichnet.

Der Grund für dieses Vorgehen liegt einerseits in den technischen Voraussetzungen bei den Daten-
empfängern – eine unmittelbare Löschung der Daten ist häufig technisch gar nicht möglich, da es sich
um einen sehr komplexen Vorgang handelt. Zudem hat es sich gezeigt, dass die Datensender in sol-
chen Fällen sehr häufig Rückfragen haben, die der Datenempfänger nicht mehr beantworten kann,
wenn die Daten nicht mehr vorhanden sind. Daher haben sich einige der Datenempfänger entschieden,
einen Löschmodus vorzusehen, der sicherstellt, dass die Daten nicht mehr verwendet werden können
(ausser bei Rückfragen) und diese innerhalb einer bestimmten Frist manuell gelöscht werden.

Da die übermittelten Daten in einer geschützten Umgebung gespeichert werden und zu keinem ande-
ren als den ursprünglich vereinbarten Zweck verwendet sowie innerhalb einer bestimmten Frist tatsäch-
lich kontrolliert gelöscht werden, führt dieses Vorgehen aus der Sicht des Vereins Swissdec zu keinem
erhöhten Risiko für Persönlichkeitsverletzungen der betroffenen Personen.

Zusammenfassend wird der Verhältnismässigkeitsgrundsatz in den beiden Richtlinien für Lohndatenverarbeitung und für Lohndatenübermittlung wie folgt berücksichtigt:

- Der **Distributor** filtert die Daten bei der Übermittlung und leitet sie an die jeweils berechtigten Stellen weiter.
- Der Lohnstandard-CH (ELM) ist so konzipiert, dass sämtliche Empfänger nur die Lohndaten erhalten, welche sie zur **Erfüllung ihres gesetzlichen Auftrages benötigen**.
- Für jeden Empfänger besteht eine Liste mit allen Daten, welche dieser über den Distributor empfangen wird. Für jede Liste pro Domäne ist in der Datenschutzerklärung angegeben, für welche Aufgabenerfüllung der jeweilige Empfänger das Datum benötigt (Zweck) und auf welcher Rechtsgrundlage die Datenbearbeitung basiert. Diese Listen dienen auch als Organisationsinstrument für den Distributor. Sie bilden die Basis für die Steuerung der Filterfunktion des Distributors und dienen als Nachweis der Rechtsgrundlagen der Datenbearbeitung. Bei einer Änderung der gesetzlichen Grundlagen kann die jeweilige Liste angepasst werden.
- Die definitive Löschung von Daten im Rahmen der «Completion-Funktion» erfolgt je nach Datenempfänger erst nach einer definierten Zeit, da sie noch für Rückfragen benötigt werden. Dabei ist sichergestellt, dass die Daten geschützt gespeichert und nur zweckgebunden verwendet werden.

5.9.3 Leistungsstandard-CH (KLE)

Es werden lediglich jene personenbezogenen Daten der versicherten Person an den Distributor bzw. Versicherer und Behörden übermittelt, die zur Identifikation der betroffenen Person und zur Erhebung, Überprüfung und Zuordnung der beantragten Taggelderleistungen an den betroffenen Personen erforderlich sind.

Die Versicherungen sind dafür verantwortlich, dass nur solche Daten in den Standard integriert werden, die den spezialgesetzlichen und vertraglichen Grundlagen entsprechen. Im Bereich UVG, in dem der Versicherer als Bundesorgan handelt, darf er nur diejenigen Daten bearbeiten, für die er eine gesetzliche Grundlage hat. Im überobligatorischen Bereich beruht die Datenbearbeitung auf Vertrag bzw. auf einer Einwilligung.

5.10 Grundsatz der Zweckbindung

5.10.1 Allgemein

Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist (Art. 6 Abs. 3 DSGVO).

5.10.2 Lohnstandard-CH (ELM) und Leistungsstandard-CH (KLE)

Eine Bearbeitung von Personendaten durch den Verein Swissdec erfolgt nur im Rahmen der Datenübermittlung über den Distributor. Der Grundsatz der Zweckbindung muss dabei berücksichtigt werden.

- Bei der Übermittlung von Daten über den Distributor werden keine Personendaten gespeichert. Die Daten werden zwar kurzfristig zwischengespeichert, sie werden aber unmittelbar nach der erfolgreichen Übermittlung und dem Erhalt der positiven Rückmeldung der Empfänger wieder gelöscht. Das Konzept des Distributors erlaubt somit **keine über die reine Weiterleitung der Daten hinausgehende Datenbearbeitung** durch den Distributor.
- Der **Betreiber des Distributors** wird vertraglich verpflichtet, die Daten nur zur Weiterleitung an die empfangenden Behörden zu verwenden. Eine darüberhinausgehende Bearbeitung der Daten und insbesondere ein Monitoring der Datenbearbeitung ist untersagt.
- Insbesondere ist es dem Betreiber untersagt, zur Erfüllung seiner vertraglichen Pflichten Dritte heranzuziehen, wenn damit eine **Auslagerung der Daten** auf ein **anderes System** oder **ins Ausland** erfolgt.

Die Einhaltung der vertraglichen Pflichten durch den Betreiber des Distributors wird durch regelmässige externe **Audits** kontrolliert.

5.11 Prinzip der Integrität

5.11.1 Allgemein

Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern (Art.6 Abs. 5 DSG). Da die Daten von den betroffenen Personen bzw. deren Arbeitgebern selbst bekannt gegeben werden, dürfen die Datenempfänger von der Richtigkeit der Daten ausgehen, ohne hierfür zusätzliche Integritätskontrollen durchführen zu müssen.

5.11.2 Lohnstandard-CH (ELM) und Leistungsstandard-CH (KLE)

Es liegt im Interesse aller empfangenden Behörden und Versicherungen, die Daten in möglichst guter Qualität zu erhalten, um den Aufwand für die interne Revision sowie für die Arbeitgeberkontrollen möglichst zu reduzieren. Oder bei Ereignissen die Daten in der Qualität zu erhalten um ohne Abklärungen die Verarbeitungsprozesse voranzutreiben.

- Durch die automatisierte und standardisierte Darstellung der Daten mit einer Lohnbuchhaltung, welche den Lohnstandard-CH (ELM) und Leistungsstandard-CH (KLE) unterstützt, werden die Daten bereits in einer guten Qualität im System bearbeitet.
- Jede manuelle Eingabe birgt ein gewisses Fehlerrisiko. Dadurch, dass die Daten für alle erforderlichen Deklarationen nur mehr einmal eingegeben werden müssen, sinkt auch das Risiko von Fehleingaben.
- Bei der Übermittlung der Daten über den Distributor
 - erfolgt eine Überprüfung der **Plausibilität und der Validität** der Daten
 - und beim Lohnstandard-CH (ELM) im Rahmen der sog. **Completion-Funktion** eine Ergänzung von unvollständigen Angaben durch das Unternehmen möglich.

5.12 Datensicherheit

5.12.1 Allgemein

Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden (Art. 8 DSG). Die Art. 1-6 DSV enthalten die näheren Bestimmungen über die Mindestanforderungen an die Datensicherheit.

Eine vorsätzliche Verletzung der Mindestanforderungen an die Datensicherheit (Art. 1-6 DSV) ist seit Inkrafttreten des revidierten DSG strafbar (Art. 61 lit. c DSG).

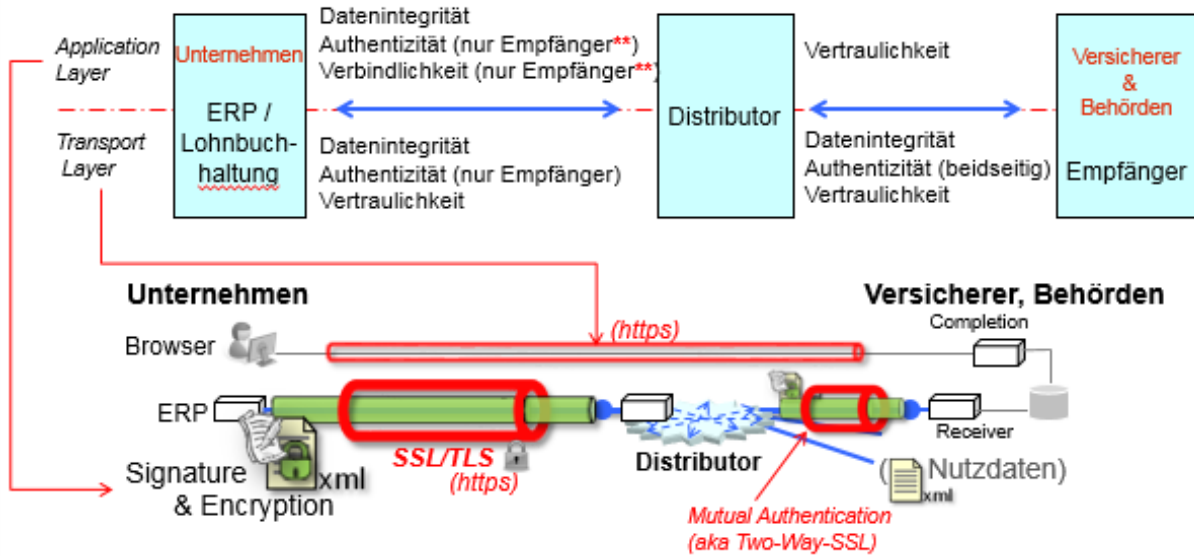
5.12.2 Lohnstandard-CH (ELM)

Wie bereits erwähnt, sind die Anforderungen an die Datensicherheit wegen der Menge der übermittelten Daten und dem damit verbundenen erhöhten Potenzial für Persönlichkeitsverletzungen sehr hoch.

Eine webbasierte Übermittlung von Personendaten bedingt ein erhöhtes Augenmerk auf die Sicherheit der Bearbeitung und Übermittlung der Daten. Die Lohn- und Leistungsdaten werden daher vor der Übermittlung mit einer digitalen Signatur versehen und als Nachricht verschlüsselt. Die Übermittlung erfolgt dann zusätzlich SSL/TLS-verschlüsselt (doppelte Verschlüsselung).

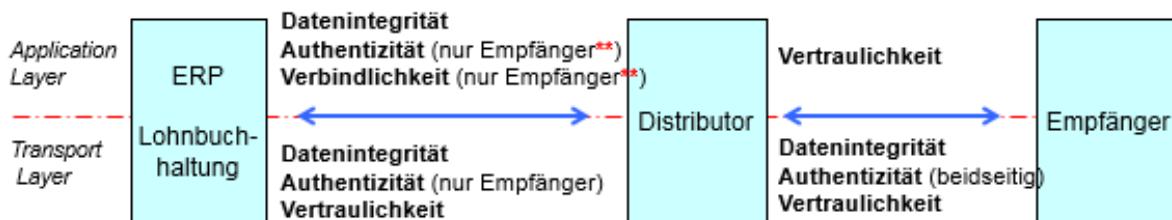
Sicherheit z. B. https und WS Signature & Encryption Web Services Security Standard von Oasis [WSS] – Schutzzielabdeckung:

- In Zukunft** könnte zwischen dem ERP / Lohnbuchhaltung und dem Distributor die Authentizität und Verbindlichkeit **erhöht** werden.



Sicherheit (Schutzzielabdeckung):

- In Zukunft** könnte zwischen dem ERP / Lohnbuchhaltung und dem Distributor die Authentizität^[1] und Verbindlichkeit **erhöht** werden.



- Die Swisscom am SSL/TLS-Endpoint eingesetzte Version war zu **keinem Zeitpunkt durch "Heartbleed" angreifbar**. Zusätzliche Sicherheit gewährleistet die **swissdec Architektur durch die doppelte Verschlüsselung**. Das heisst, dass nebst dem SSL-Tunnel (Transport Ebene) auch die Nutzdaten (Nachrichten Ebene, SOAP WS-Security) verschlüsselt sind. Die beiden Verschlüsselungen werden auf getrennten Systemen dekodiert (Dekodierreihenfolge: zuerst Transport, danach Nutzdaten). Damit wird eine Unabhängigkeit zwischen den beiden Ebenen geschaffen.

^[1] Lösung zurzeit mittels „Fachverfahrensspezifische Selbstauskunft“

Unter einer fachverfahrensspezifischen Selbstauskunft versteht man die Angabe von Informationen (z. B. Kunden- und Vertrags-Nummer, alle Mitarbeiter des Unternehmens, usw. oder letzte Transaktion und Kreditkartenlimit), welche die Zuordnung des Kunden zu einer Akte bzw. einem Datensatz ermöglichen.

(Authentisierung im E-Government; Mechanismen und Anwendungsfelder der Authentisierung https://www.bsi.bund.de/fachthem/egov/download/4_Authen.pdf leider nicht mehr verfügbar)

Nach der erfolgreichen Übermittlung werden die Daten beim Distributor wieder gelöscht, die Aufbewahrung der Daten erfolgt nur bei den Unternehmen und den empfangenden Behörden.

Beim Betrieb des Distributors wird durch die Vereinbarung von Service Level Agreements (SLA) mit dem Betreiber sowie durch regelmässige externe Audits ein besonders hoher Sicherheitsmassstab angelegt.

Weitere Informationen über die Sicherheitsaspekte bei der Übermittlung der Lohndaten unter Verwendung des Lohnstandard-CH (ELM) sind auf der Website enthalten.

5.12.3 Leistungsstandard-CH (KLE)

Da die Versicherer ihren versicherten Unternehmen die Möglichkeit zur Kommunikation via ein Swissdec-zertifiziertes ERP-System geben, sind diese verpflichtet, die **Datensicherheit** zu gewährleisten. Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen **unbefugtes Bearbeiten** geschützt werden (Art. 8 DSG). Da die Kommunikation wechselseitig erfolgt und auch Daten ausgetauscht werden, ist generell ein **hoher Massstab** an die technischen und organisatorischen Massnahmen zur Gewährleistung der Datensicherheit zu stellen.

Das in der Richtlinie beschriebene Authentisierungsverfahren basiert im Wesentlichen auf dem **Vertrag** zwischen dem Unternehmen und dem Versicherer – dort sollten bereits die Ansprechpersonen (inkl. Kontaktdaten) bezeichnet werden und auch das Verfahren bei deren Wechsel definiert werden. Dies betrifft auch einen allfälligen Stellvertreter. Der Versicherer ist verpflichtet, sich im Rahmen des in der Richtlinie beschriebenen Verfahrens ausreichend zu vergewissern, dass die **anrufende Person** tatsächlich vom versicherten Unternehmen stammt und berechtigt ist, diese Informationen zu erhalten. Die Verantwortung dafür, dass im Unternehmen nach der ersten Initialisierung nur eine **berechtigte Person** Zugang zum ERP-System und dem Code gemäss Richtlinie hat, liegt wiederum beim Unternehmen selbst.

5.12.4 Fazit

- Wegen der Menge der übermittelten Daten und des damit verbundenen erhöhten Risikos von Persönlichkeitsverletzungen sind die Sicherheitsanforderungen sehr hoch.
- Die Daten werden signiert und doppelt verschlüsselt übermittelt.
- Die Daten werden beim Distributor nach der erfolgreichen Übermittlung gelöscht.
- Externe Audits beim Betreiber des Distributors stellen sicher, dass die Anforderungen an den Datenschutz eingehalten werden.

6. Haftung

Der Verein Swissdec haftet den Datenempfängern für Schäden, welche er diesen bei der Übermittlung der Daten über den Distributor absichtlich oder grobfahrlässig zufügt, unbeschränkt¹⁶.

Eine weitere Haftung besteht grundsätzlich nicht. Das heisst, der Verein Swissdec haftet insbesondere nicht für Schäden, die aufgrund von Handlungen oder Ereignissen ausserhalb seines Macht- bzw. Verantwortungsbereichs (z. B. aufgrund eines Fehlers beim Datensender) eingetreten sind.

¹⁶ Allgemeine Geschäftsbedingungen für Übermittlung und Empfang von Lohndaten über den Distributor des Vereins Swissdec vom 17. Dezember 2020, abrufbar unter: www.swissdec.ch/document/share/171/6886e4a4-3c39-4810-94ce-692cd206873a