Bearbeitungsreglement für die Datensammlung nach KVG der Stiftung der Taggeldkasse bildende KünstlerInnen

1. Allgemeine Bestimmungen

1.1 Rechtliche Grundlage

Gestützt auf Art. 21 der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) in Verbindung mit Art. 84 des Bundesgesetzes über die Krankenversicherung (KVG) hat die Stiftung der Taggeldkasse bildende KünstlerInnen für die automatisierte Datensammlung das vorliegende Bearbeitungsreglement erstellt.

1.2 Ziel des Bearbeitungsreglements

Das Bearbeitungsreglement umschreibt insbesondere die Datenbearbeitungs- und Kontrollverfahren und den Betrieb der elektronischen Datenbearbeitung. Es enthält Angaben über das für den Datenschutz und die Datensicherheit verantwortliche Organ, über die Herkunft der Daten und die Zwecke, für welche sie regelmässig bekannt gegeben werden und beschreibt das Verfahren für die Erteilung der Zugriffsberechtigungen auf die Produkte der elektronischen Informationssysteme.

1.3 Zweck der Datenbearbeitung

Der Zweck der Datensammlung ist primär im Bundesgesetz über die Krankenversicherung (KVG) geregelt, gemäss Art. 84 KVG gilt:

> *„Die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung dieses Gesetzes betrauten Organe sind befugt, die Personendaten, einschliesslich besonders schützenswerter Daten und Persönlichkeitsprofile, zu bearbeiten oder bearbeiten zu lassen, die sie benötigen, um die ihnen nach diesem Gesetz übertragenen Aufgaben zu erfüllen, namentlich um:*
>
> *a) für die Einhaltung der Versicherungspflicht zu sorgen;*
>
> *c) Leistungsansprüche zu beurteilen sowie Leistungen zu berechnen, zu gewähren und mit Leistungen anderer Sozialversicherungen zu koordinieren;*
>
> *e) ein Rückgriffsrecht gegenüber einem haftpflichtigen Dritten geltend zu machen;*
>
> *f) die Aufsicht über die Durchführung dieses Gesetzes auszuüben;*

g) Statistiken zu führen;

h) die Versichertennummer der AHV zuzuweisen oder zu verifizieren;

Der Zweck der Stiftung ist der Betrieb einer Taggeldversicherung zugunsten bildender KünstlerInnen nach Massgabe des Bundesgesetzes über die Krankenversicherung (KVG). Die Stiftung strebt kein Gewinn an, etwaige Gewinne werden reinvestiert und das Vermögen darf nur zu Zwecken der Taggeldversicherung sowie gegebenenfalls der Unfallversicherung nach Massgabe der Reglemente verwendet werden.

Die Datensammlung der Stiftung dient somit diesem Zweck.

1.4 Verantwortliche Stelle

Die Stiftung der Taggeldkasse bildende KünstlerInnen ist eine reine Taggeldversicherung gemäss Art. 1a Ziffer 1 i.V.m. Art. 67 f. KVG. Die Stiftung, resp. deren Organe, sind die verantwortlichen Personen betreffend der Bearbeitung und Verwaltung von Daten (Einhaltung von Datenschutz und Datensicherheit). Inhaberin, resp. Owner der Datensammlung und Informatiksysteme ist die Stiftung. Mit den beschriebenen Massnahmen sorgt die Stiftung für die Einhaltung der relevanten Vorschriften.

Die Stiftung, resp. deren Organe, ist auch diejenige Stelle, welche für den Datenschutz und die Datensicherheit verantwortlich ist.

1.5 Schweigepflicht nach Art. 33 ATSG

Sämtliche Mitarbeitenden der Stiftung oder beteiligter Dritter unterstehen der Schweigepflicht nach Art. 33 ATSG.

Bei der Verletzungen der Schweigepflicht unterstehen sie spezialgesetzlich den Strafbestimmungen des Art. 92 KVG. Zusammen mit dem Arbeitsvertrag unterzeichnen die Mitarbeitenden die Geheimhaltungs- und Schweigepflicht.

1.6 Auslagerung von Dienstleistungen

Die gesamte Geschäfts- und Rechnungsführung der Stiftung ist an die Swiss Life AG ausgegliedert. Die in diesem Reglement definierten Massnahmen gelten für diese in gleicher Weise.

Im Auslagerungsvertrag mit der Swiss Life ist klar geregelt, dass diese die Daten nur so bearbeiten darf, wie dies die Stiftung tun dürfte. Die Zweckbindung ist somit garantiert. Die Einhaltung der Regeln der Stiftung ist damit vertraglich fixiert.

Die Stiftung überprüft durch ihre Organe regelmässig mittels angemessener Kontrollen, ob die Bedingungen des Datenschutzes eingehalten werden.

Die Übermittlung der Daten zwischen der Stiftung und Swiss Life ist geregelt.

2. Datensammlung

2.1 Struktur der Datensammlung

Die Datensammlung der Stiftung besteht aus folgenden Systemen und Inhalten:

- KUBIK, Erfassungssystem der Stiftung Taggeldkasse. Dieses System wird nur für die Stiftung Taggeldkasse eingesetzt. Im Erfassungssystem werden für die Versicherten folgende Daten erfasst:

- Name, Adresse, Versichertennummer, Geburtsdatum, Geschlecht, Eintrittsdatum, Rentenalter (m/w), Sektion Kunstverband, Zahlstelle sowie ob ein Vorbehalt bei Aufnahme besteht

- Schadenfall, Erfassungsdatum, Krankheitsgrad, -dauer, Leistungsanspruch sowie Zahlungsdatum

- Verbuchungsinformation zuhanden des Buchhaltungssystem SAP (Kontierungsinformationen)

2.2 Schnittstellen

Die Stiftung erhält sämtliche persönlichen Daten ausschliesslich vom Versicherungsnehmern, bzw. direkt von dessen Vertrauensarzt. Die Prüfung, ob der Versicherungsnehmer Mitglied der Kunstverbandes "visarte", "SGBK" oder "SKV" ist, erfolgt zwischen ausschliesslich zwischen Stiftung Taggeldkasse und den Kunstverbänden.

Mittels starker Identifikation und Authentifikation, Verschlüsselungs- und modernsten Übertragungstechnologien werden der Datenschutz und die entsprechende Datensicherheit gewährleistet.

3. Beteiligte Stellen

3.1 Stiftung

Die Stiftung der Taggeldkasse bildende KünstlerInnen ist Ownerin der Datensammlung und der Daten.

3.2 Swiss Life

Die gesamte Geschäfts- und Rechnungsführung der Stiftung ist an die Swiss Life AG ausgegliedert. Swiss Life bearbeitet somit die Daten der Stiftung zweckgebunden und vertraulich.

3.3 Weitere beteiligte Stellen

Keine weiteren beteiligten Personen.

3.4 Applikationsowner

Die definierten Informations Owner, zusammen mit den Applikationsowner Business und IT, sorgen für die Datensammlungen bei der Stiftung und Swiss Life, für die Einhaltung der Bestimmungen der relevanten Weisungen zum Datenschutz und der Datensicherheit.

4. Benutzer und Datenzugriff

4.1 Benutzer

Zugriffsberechtigt auf die Datensammlung und Daten der Stiftung sind nur namentlich bezeichnete Personen, welche diese Daten für die tägliche Arbeit benötigen (für die Ausrichtung oder Überprüfung der Taggelder).

Zudem erhalten Systemadministratoren oder Applikationsverantwortliche zweckgebunden Zugriff auf diese Daten.

Sonstige Mitarbeitende von externen Dienstleistungsunternehmen haben keinen Zugriff.

4.2 Benutzerverwaltung

Für sämtliche Produkte, Applikationen und Datensammlungen bestehen dokumentierte Prozesse und Abläufe zur Verwaltung der Benutzer, Berechtigungen und Rollen, sowie deren spezifische Zugriffsberechtigungen. Zuständig für die Abwicklung des Berechtigungsverfahren ist der zuständige Berechtigungsprofilverantwortliche (BPV), in Absprache mit den Stiftungsverantwortlichen. Der jeweilige Antrag für eine Berechtigungsanfrage wird von diesen Personen geprüft und vom Service Help Desk umgesetzt.

Das Verfahren für die Zugriffsberechtigung wird somit über die Verantwortlichen der Stiftung gesteuert, wobei Berechtigte nur solange zugriffsberechtigt bleiben, wie dies für Ihre tägliche Arbeit notwendig ist. Bei einem Austritt oder einem Stellenwechsel werden die Berechtigungen automatisch entzogen.

4.3 Ausbildung der Benutzer

Betreffend Datenschutz und Datensicherheit werden die Benutzer regelmässig geschult und weitergebildet. Dies betrifft auch den spezifischen Bereich der Bearbeitung der Daten der Stiftung.

5. Bearbeitung der Daten / Datenkategorien

5.1 Datenbeschaffung

Die Daten stammen hauptsächlich von den Versicherungsnehmern der Taggeldkasse selbst, sowie von deren Vertretungen.

5.2 Datenkategorien

Im Anhang 1 sind die vorhandenen Datenkategorien der Stiftung aufgeführt.

5.3 Datenklassifikation

Die Daten sind als vertraulich klassifiziert. Sämtliche Massnahmen sind dem erhöhten Schutzniveau angepasst. Die Bearbeitungsregeln sind in einer Weisung geregelt und die Mitarbeitenden werden dabei regelmässig geschult.

5.4 Datenweitergabe

Betreffend die Datenbekanntgabe gilt gemäss Art. 85 KVG folgendes:

> *„Sofern kein überwiegendes Privatinteresse entgegensteht, dürfen Organe, die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung dieses Gesetzes betraut sind, Daten in Abweichung von Artikel 33 ATSG bekannt geben:*

a) anderen mit der Durchführung sowie der Kontrolle oder der Beaufsichtigung der Durchführung dieses Gesetzes betrauten Organen, wenn die Daten für die Erfüllung der ihnen nach diesem Gesetz übertragenen Aufgaben erforderlich sind;

b) Organen einer anderen Sozialversicherung, wenn sich in Abweichung von Artikel 32 Absatz 2 ATSG eine Pflicht zur Bekanntgabe aus einem Bundesgesetz ergibt;

bbis) Organen einer anderen Sozialversicherung für die Zuweisung oder Verifizierung der Versichertennummer der AHV;

c) den für die Quellensteuer zuständigen Behörden, nach den Artikeln 88 und 100 des Bundesgesetzes vom 14. Dezember 1990 über die direkte Bundessteuer sowie den entsprechenden kantonalen Bestimmungen;

d) den Organen der Bundesstatistik, nach dem Bundesstatistikgesetz vom 9. Oktober 1992;

e) Stellen, die mit der Führung von Statistiken zur Durchführung dieses Gesetzes betraut sind, wenn die Daten für die Erfüllung dieser Aufgabe erforderlich sind und die Anonymität der Versicherten gewahrt bleibt;

f) den zuständigen kantonalen Behörden, wenn es sich um Daten nach Artikel 22a handelt und diese für die Planung der Spitäler und Pflegeheime sowie für die Beurteilung der Tarife erforderlich sind;

g) den Strafuntersuchungsbehörden, wenn die Anzeige oder die Abwendung eines Verbrechens die Datenbekanntgabe erfordert;

…

5 In den übrigen Fällen dürfen Daten in Abweichung von Artikel 33 ATSG an Dritte wie folgt bekannt gegeben werden:

a) nicht personenbezogene Daten, sofern die Bekanntgabe einem überwiegenden Interesse entspricht;

b) Personendaten, sofern die betroffene Person im Einzelfall schriftlich eingewilligt hat oder, wenn das Einholen der Einwilligung nicht möglich ist, diese nach den Umständen als im Interesse der versicherten Person vorausgesetzt werden darf.“

Die Daten werden bekannt gegeben für die:

- Beurteilung von Leistungsansprüchen
- Verwaltung der vertraglichen Beziehung
- Rechnungswesen
- Koordination mit anderen Sozialversicherungen gemäss Prüfung der Anträge

Unter die Datenempfänger fallen:

- Versicherte und von Ihnen bevollmächtigte Personen
- Behörden (z.B. IV-Stelle)
- Swiss Life

- Vertrauensärzte

Die weitere Datenbekanntgabe ist im KVG geregelt.

6. Aufbewahrungsdauer und Löschung der Daten

Sowohl die Stiftung als auch die Swiss Life erfüllen die gesetzlichen Vorgaben betreffend der Archivierung. Die Dauer der Archivierung nach Geschäftsabschluss richtet sich somit ebenfalls nach den gesetzlichen Vorgaben. Danach werden die Daten gelöscht und vernichtet.

7. Technische und organisatorische Massnahmen

7.1 Zugangskontrolle

Der Zugang ist gesichert und geregelt: Sämtliche Räumlichkeiten der Stiftung und beteiligter Dritter, in denen Personendaten bearbeitet werden, sind entweder elektronisch oder manuell vor dem Zugang unbefugter Personen gesichert (das Hauptbüro ist ausserhalb der Arbeitszeiten abgeschlossen). Von aussen ist eine Kontrolle mittels Badge und Zugangskontrolle angebracht. Zugänge werden protokolliert.

Zutritt in die Räume, bei denen Daten der Stiftung bearbeitet werden, haben nur die jeweils spezifisch mit dieser Arbeit betrauten Personen (need to know / least privileage).

Schutzzonen bestimmen die Sicherheitsvorkehrungen: Die Arbeitsplätze sind vor dem Zutritt unbefugter Dritter geschützt. Ein Alarmsystem ist in allen Räumen installiert.

Spezialräume und Räume wie Rechenzentrum und Data-Ware-House sind wie folgt geschützt:

- Das Rechenzentrum und sämtliche Data-Ware-Houses / Data-Center / Data-Server sind gemäss Ihrer Schutzklasse mit erhöhten Sicherheitsanforderungen gesichert und bieten nur Zugang für ausschliesslich für den Betrieb spezifisch berechtigte Personen.

- Der Zutritt wird protokolliert.

- Ein Alarmsystem ist der erhöhten Schutzklasse ausgerichtet.

- Die Server befinden sich in Kellerräumen, welche sich in speziell dafür eingerichteten Schutzräumen befinden.

7.2 Personendatenträgerkontrolle

Durch informationstechnische Vorkehrungen ist es ausschliesslich berechtigten Personen möglich, Daten auf den elektronischen Datenträgern zu bearbeiten. Nur berechtigte Personen erhalten Zugriff auf Datensammlungen und Informatiksysteme der Stiftung oder Swiss Life. Zudem sind alle Daten durch Verschluss zu sichern und werden fachgerecht entsorgt. Damit wird verhindert, dass unbefugte Personen Datenträger mit Personendaten der Stiftung lesen, kopieren, ändern oder entfernen können.

Die interne Organisation der Stiftung oder beteiligter Dritter legt für alle Mitarbeitenden die entsprechenden Zugangsprofile und Rechte fest. Diese werden regelmässig kontrolliert.

Der Mitarbeitende hat sich beim Anschalten des Systems / Notebooks zu identifizieren und authentifizieren. Dies wird jeweils protokolliert.

7.3 Benutzerkontrolle / Identifizierung und Authentifizierung

Rollenabhängige Zugriffsrechte, Authentifikation und Identifikation, Firewalls und ein klar geregelter Fernzugriff stellen sicher, dass nur befugte Personen Zugriff auf die Daten der Stiftung ausüben können.

Die Identifizierung einer Person und die dazugehörige Authentifizierung werden mit folgenden Massnahmen sichergestellt:

- Der Zugriff auf die Systeme der Stiftung oder Swiss Life ist durch die User-ID kombiniert mit einem zeitlich befristeten, individuellen, angemessen starken Passwort geschützt. Der Zugriff auf einige Systeme ist nur mittels Verwendung eines zusätzlichen Passwortes freigegeben.

- Der Umgang mit Passwörtern ist zudem in einer spezifischen Weisung geregelt und wird regelmässig kontrolliert.

- Sämtliche Benutzerkonten, welche eine Authentifizierung erlauben, sind individuell. Auf ein Benutzerkonto kommt nur eine Person.

- Sämtliche Harddisks der Mitarbeitenden sind zusätzlich mit Passwort geschützt.

- Passwörtern müssen stark sein und sind regelmässig (alle 3 Monate) zu wechseln.

7.4 Bekanntgabekontrolle

Datenempfänger, denen Personendaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden, werden über die Schnittstellen identifiziert und angemessen authentifiziert. Zudem werden Daten in der Regel nur an die gemäss Ziffer 5.4 definierten Stellen, meist brieflich versandt.

7.5 Speicherkontrolle

Die unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Daten ist mittels rollenbasierten Zugriffsrechten sowie der Trennung von Test, Entwicklung und Produktion sichergestellt. Der Schutz von Malware und unberechtigtem externen Zugriff ist mit Antivirus und Firewalls sichergestellt.

Daten werden revisionsgerecht archiviert.

7.6 Technische Anforderungen an Endgeräte

Es sind keine Endgeräte im Einsatz, welche Daten der Benutzer verarbeiten.

7.7 Zugriffskontrolle

Es ist sichergestellt, dass nur Personen auf Daten der Stiftung zugreifen können, welche diese Daten für die tägliche Arbeit und die Ausübung des Zweckes der Stiftung erfordern.

7.8 Eingabekontrolle / Protokollierung

Alle Systeme verfügen über eine protokollierte Bearbeitung, inkl. deren Zugriff auf Daten. Dies dient sowohl als Integritätsschutz, als auch zur Überprüfung der Zweckbindung der Daten. Die Protokollierung wird damit in Anwendung von Art. 10 VDSG durchgeführt. Die Protokolle werden für eine bestimmte Zeitspanne fachgerecht aufbewahrt, wobei sie ausschliesslich Personen zugänglich sind, denen die Überwachung und die Kontrolle der Datenschutzvorschriften obliegen und sind ebenfalls zweckgebunden.

7.9 Programmentwicklung

Es wird eine Trennung zwischen Entwicklung, Test und Produktion eingehalten.

7.10 Aufsicht und Verantwortung

Die Informations Owner, zusammen mit den Applikationsverantwortlichen, beaufsichtigen, dass sich die Personen an die Weisungen, das vorliegende Bearbeitungsreglement und Anordnungen halten.

7.11 Besucher im Gebäude der Stiftung oder beteiligter Dritter

Bei Besuchern wird der Zugang so geregelt, dass sie sich nicht alleine im Gebäude aufhalten können, sondern nur in Begleitung und vorgängiger Anmeldung. Bei der Anmeldung werden die Personalien mittels Ausweis geprüft, welcher während dem Aufenthalt im Depot aufbewahrt wird.

7.12 Sicherheit des Arbeitsplatzes

Die Sicherheit des Arbeitsplatzes der Mitarbeitenden ist mit folgenden Massnahmen geschützt:

- Die Arbeitsplätze sind so eingerichtet, dass die Bildschirme nicht von der Tür aus eingesehen werden können.
- Die Mitarbeitenden sind angewiesen und werden regelmässig geschult, dass gedruckte Dokumente nicht unbeaufsichtigt beim Drucker liegenbleiben.
- Es gilt in allen Arbeitsplätzen eine klare „Clean-Desk-Policy“. Sämtliche Dokumente sind wegzuschliessen.
- Notebooks sind in allen Arbeitsplätzen angekettet und abgeschlossen.
- Sämtliche Notebooks sind mit Firewalls und Antivirenprogrammen geschützt, welche regelmässig aktualisiert werden und „state-of-the-art“ sind.

7.13 Zugang ausserhalb der Organisation

Auf die Daten der Stiftung wird nur innerhalb der Organisation oder beteiligter Dritter zugegriffen. Auch externe Datenträger sind nicht im Einsatz bei der Bearbeitung von Daten der Stiftung.

7.14 Langfristiger Schutz der Daten

Die definierten Sicherheitsmassnahmen müssen während dem gesamten Lebenszyklus gewährleistet werden, wozu folgende Massnahmen dienen:

- Die Daten werden nur von dazu ausgebildeten und berechtigten Personen erfasst.

- In einem Test werden nach Möglichkeit nur fiktive oder anonymisierte Daten verwendet.

- Die Erfassung, Änderung, Vernichtung und der Zugriff auf die Daten wird protokolliert. Diese ist klar umschrieben und dient nur definierten Sicherungszwecken, so dass die Protokollierung klaren Kriterien folgt. Die Zugriffsrechte auf die Protokolle sind klar geregelt (need to know) und zweckgebunden. Protokolle erhalten die gleichen Schutzmechanismen wie Daten (Schutz vor unberechtigtem Zugriff und Veränderungen).

- Inhalt und Aufbewahrungsdauer der jeweiligen Logfiles stehen in einem Verhältnis zu den Daten und den Bearbeitungsmassnahmen.

- Die langfristige Archivierung der Daten entspricht den Vorgaben des Obligationenrechts und der GeBüV. Die Löschung oder Vernichtung der Daten ist in einer spezifischen Weisung geregelt.

7.15 Transportkontrolle / Übermittlung der Daten

Müssen die Daten übermittelt werden, erfolgt dies mittels TLS oder VPN-Verbindung. In der Regel werden Daten nicht per Mail verschickt, sondern per Brief an die betroffenen Personen.

8. Rechte der Betroffenen

8.1 Auskunftsrecht

Jede Person kann von der Stiftung oder von Swiss Life Auskunft darüber verlangen, ob Daten über sie bearbeitet werden. Das Auskunftsrecht richtet sich dabei nach den Vorgaben des DSG. Die Gesuche sind unter Beilage einer Kopie eines amtlichen Ausweises an die Stiftung oder Swiss Life AG zu richten.

Das Verfahren ist in der Weisung zum Datenschutz SLCH 8.13 geregelt.

8.2 Informationspflicht bei besonders schützenswerten Daten

Gemäss Art. 7a DSG sind die betroffenen Personen zu informieren, wenn besonders schützenswerte Personendaten oder Persönlichkeitsprofile beschafft werden.

Grundsätzlich werden besonders schützenswerte Personendaten nur mit dem Einverständnis der betroffenen Personen beschafft. In allen anderen Fällen gilt die Ausnahmeregelung gemäss Art. 7a Ziffer 4, wonach aufgrund des gesetzlichen Auftrages die Speicherung oder Bekanntgabe der Daten zulässig ist.

8.3 Berichtigungs- und Löschungsrecht

Die Berichtigungs- und Löschungsrechte betroffener Personen richten sich nach Art. 5 Abs. 2 DSG i.V. Art. 25 DSG, wobei die Gesuche an die Stiftung zu richten sind.

9. Abschliessende Bestimmungen

9.1 Anhänge

Die im vorliegenden Bearbeitungsreglement erwähnten Anhänge sind integrierender Bestandteil des Reglements. Das Bearbeitungsreglement wird beim Datenschutzverantwortlichen Swiss Life verwaltet und aufbewahrt.

9.2 Änderungen des Reglements

Das Bearbeitungsreglement wird regelmässig auf deren Aktualität überprüft und gegebenenfalls angepasst. Änderungen bedürfen der Schriftform und der Zustimmung der Stiftung. Verantwortlich für deren Aktualisierung ist die Stiftung.

9.3 Inkrafttreten

Dieses Reglement tritt mit all seinen Anhängen per sofort in Kraft.

Zürich, 29. September 2011

Stiftung Taggeldkasse bildende KünstlerInnen

Der Präsident:

……

Dr. Stephan P. Thaler

Der Quästor:

……..

Adrian Steinmann

Anhang 1: Datenkategorien

Kategorien der bearbeiteten Personendaten in der Datensammlung:

Anrede
Vorname
Nachname
Firma
Versichertennummer (AHV)
Adresse1
Adresse 2
PLZ
Ort
Land
Telefon
Telefax
E-Mail
Geschlecht
Sprache
Partnernummer (Versichertennummer)
Geburtsdatum
Eintrittsdatum
Austrittsdatum
Rentenalter (berechnet)
Verstorben (ja/nein)
Sektion
Stilrichtung
Zahlungsverbindung: Finanzinstitut, Kontonummer
Vorbehalt bei Aufnahme (ja/nein)
Schadennummer (systemgeneriert)
Meldedatum
Zeitraumdatum von – bis
Beschreibung
Typ (Krankheit / Unfall / Mutterschaft)
Fall geschlossen (ja/nein)
Leistungsfall in Zahlung von Datum bis Datum
Karenzfrist
Grad (Prozent)
Taggeldsatz (informativ)
Taggeld in CHF (informativ)
Betrag total in CHF
Taggeld bezahlt am Datum
Sollkonto (Kontierungsinfo für Buchhaltung SAP)
Habenkonto (Kontierungsinfo für Buchhaltung SAP)