Freie und Hansestadt Hamburg
Finanzbehörde
Amt für Haushalt und Aufgabenplanung

07.09.2016
Karsten Mante
Tel: 42823-2181

Verfahrensbeschreibung nach §9 Hamburgisches Datenschutzgesetz (HmbDSG) für das IT-Verfahren SAP Fraud Management (SAP-FM)

Inhalt

1 Name und Anschrift der datenverarbeitende Stelle

Freie und Hansestadt Hamburg
Finanzbehörde
Kasse.Hamburg
Kassenprozesse, Schnittstellen und Fachverfahren (K21)
Bahrenfelder Straße 254 - 260
22765 Hamburg

2 Bezeichnung des Verfahrens und Zweckbestimmung

2.1 Bezeichnung des Verfahren

Die Bezeichnung des IT-Verfahrens, welches im Rahmen des Internen Kontrollsystems (IKS) verwendet und realisiert werden soll, lautet „SAP Fraud Management“, abgekürzt SAP-FM.

2.2 Zweckbestimmung für die Datenerhebung, -verarbeitung und -nutzung

In der Kernverwaltung der FHH wird folgende SAP-Modullandschaft eingesetzt:

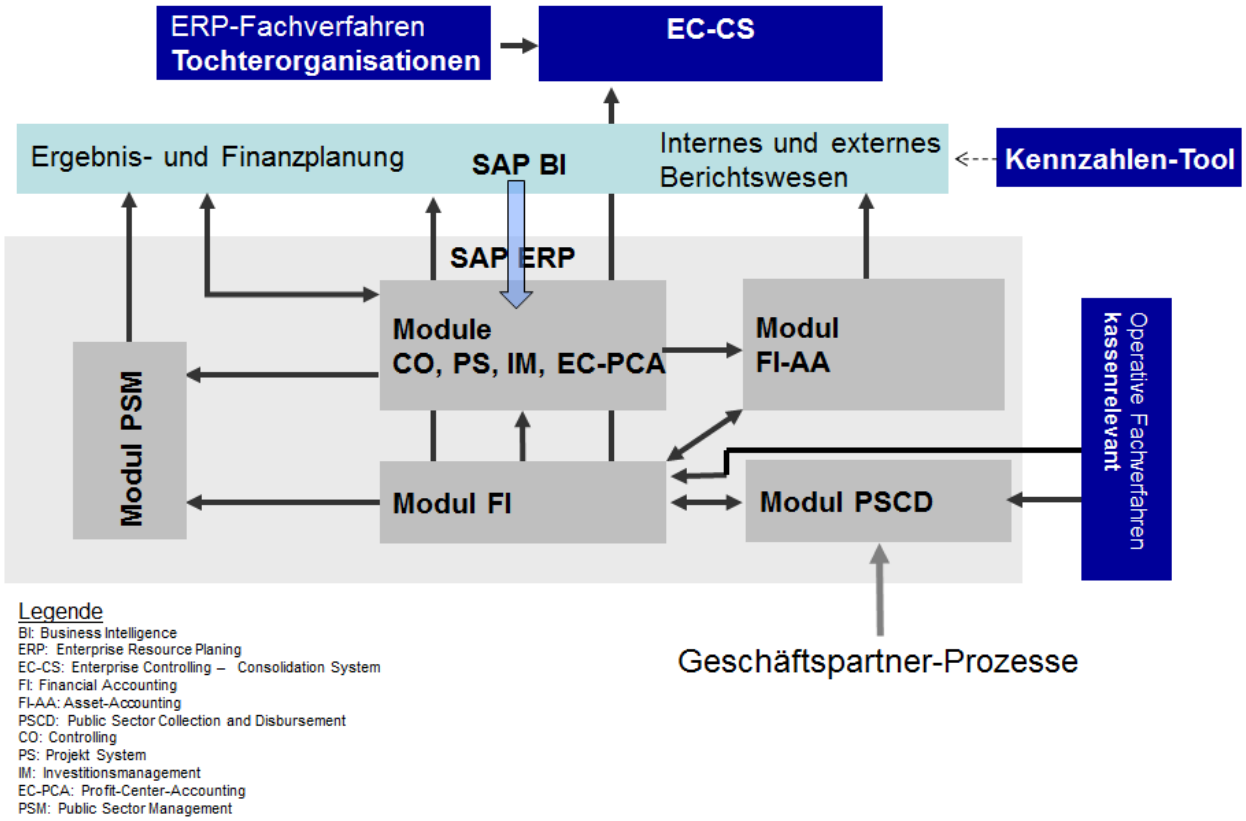

Abbildung 1: SAP-Modullandschaft der FHH

Insbesondere integrierte und mächtige ERP-Systeme wie z. B. SAP-RVP bergen diverse Fehlermöglichkeiten. Mit SAP-FM werden die möglichen Fehler- und Betrugsanfälligkeiten minimiert.
Verzahnte Prozesse (z.B. die Leistung von Ausgaben mittels Kreditorenrechnungen zu einem Geschäftspartner) finden in unterschiedlichsten Modulen statt. Es sind zahlreiche qualitätssichernde Maßnahmen im Umfeld des ERP-Systems erforderlich. Sie sollen mittels SAP-FM effizienter durchgeführt werden.

Mit der Produktivsetzung in 2016 soll das Fraud Management zunächst mit einem überschaubaren Portfolio an Regeln bezogen auf Bewirtschaftungs- und Kassenprozesse in SAP-RVP starten. Diese Prozesse sind detailliert in den Fachkonzepten Kasse und Bewirtschaftung beschrieben.
Anhand der Regeln gibt SAP-FM sogenannte Alarmmeldungen aus, die taggleich gemäß Abbildung 2 (Fraud Prozess) abgearbeitet werden. Die Anwenderinnen und Anwender greifen zur Recherche des vollständigen Sachverhalts auf das Quellsystem (Stufe 1 SAP-RVP) zu. Wie konkret mit den Alarmmeldungen umgegangen werden muss, ist je Regel vorgegeben.
Die Gesamtheit der Alarmmeldungen wird in einem kontinuierlichen Prozess zur Verfeinerung der Regeln genutzt.

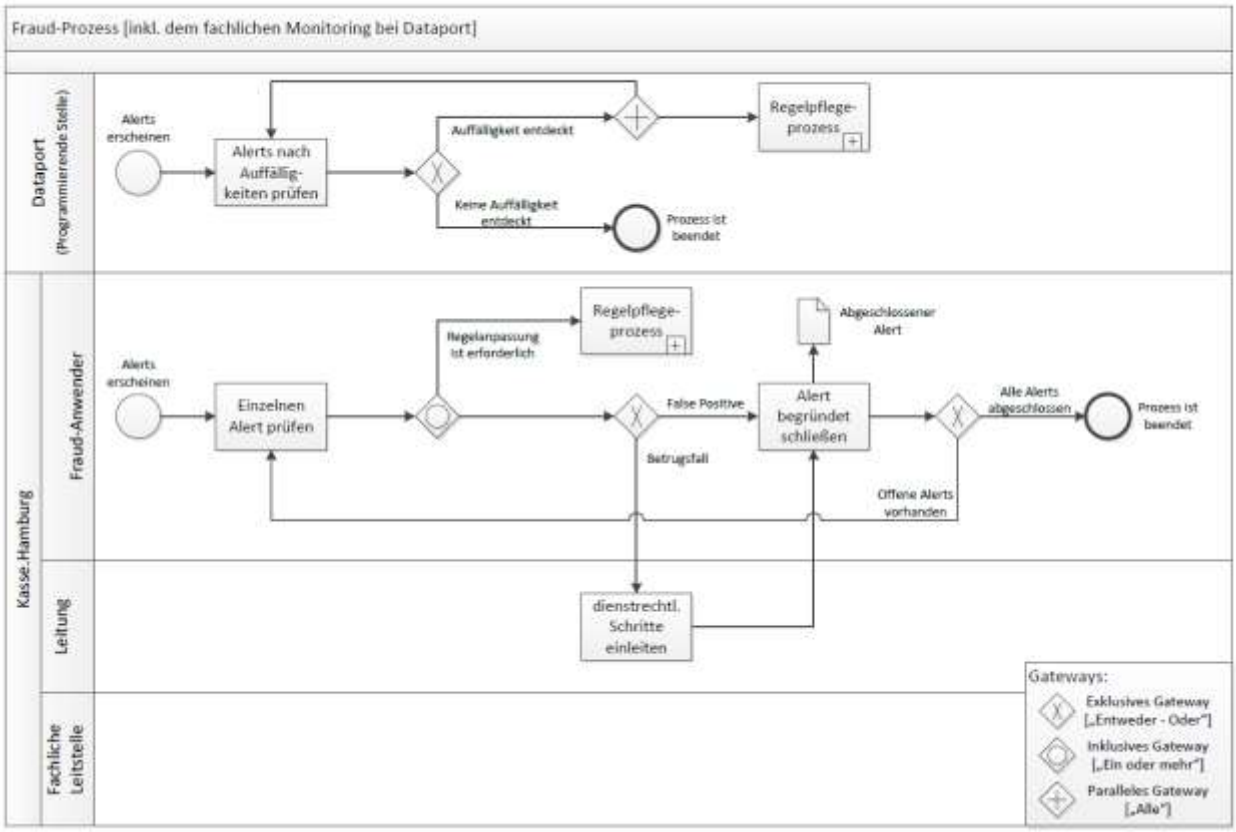

Abbildung 2: Fraud-Prozess

Mit der Verarbeitung der Daten (siehe 3.1) werden folgende Ziele verfolgt:

- Ordnungsgemäße Bereitstellung und Abbildung der Daten aus den Quellsystemen (Stufe 1 SAP-RVP)
- Erzeugung der Alarmmeldungen anhand der Daten aus den Quellsystemen gemäß der Zielsetzung der definierten Regeln im IT-System SAP-FM
- Revisionssicherheit der manuellen Prüfungen, die SAP-FM in der Anwendenden Stelle auslöst
- Überwachung und Qualitätssicherung der Buchungen in HKR-Verfahren (Stufe 1 SAP-RVP) zwecks Vermeidung finanzieller Schäden, Betrug etc.

3 Art der verarbeiteten Daten, Rechtsgrundlage

3.1 Art der verarbeiteten Daten

Folgende personenbezogene Daten werden zu den unter Nr. 4 aufgeführten Betroffenen aus den Quellsystemen (zum Produktivstart lediglich SAP-RVP) in die Datenbank des SAP-FM importiert:

- Geschäftspartnerdaten (Anrede, Vorname, Nachname)
- Postalische Anschrift (Straße, Hausnummer, PLZ, Ort, Land, Region)
- Organisationsinformation (Firma, Abteilung)
- Lieferanten- bzw. Kundendaten (Bankverbindung, Zahlungsbedingungen)
- Sämtliche Bewegungsdaten des Rechnungswesens für die Geschäftsbeziehungen, die ein Geschäftspartner zur FHH unterhält (z.B. Leistungen der Jugendmusikschule, Tatbestände aus Verkehrsordnungswidrigkeiten etc.)

Die vorgenannten Daten für Geschäftspartner werden für natürliche Personen geführt, aber auch für juristische Personen, die allerdings vom Geltungsbereich des HmbDSG nicht erfasst sind. Auf speziell berechtigungstechnisch abgegrenzten Mitarbeitergeschäftspartnern werden Zahlungsvorgänge wie Reisekosten, Beihilfe, Abschlagzahlungen und Vorschüsse gebucht. Monatliche Entgelt- und Bezügezahlungen werden im SAP RVP nicht gebucht.

Folgende personenbezogene Daten werden von den Beschäftigten der FHH, die als Anwender in SAP-System berechtigt sind, im Quellsystem gespeichert und ebenfalls in das SAP-FM importiert:

- Personendaten (Vorname, Nachname)

3.2 Rechtsgrundlagen

Rechtsgrundlage für die Datenverarbeitung ist allgemein die Verordnung über die gemeinsame Personenkontendatei des ressourcensteuernden Verfahrens („Einheitspersonenkontenverordnung“) vom 7. Oktober 2003 in Verbindung mit §§ 5, 11a, 12 HmbDSG sowie in Verbindung mit §70ff. LHO.
Für die Beschäftigten der FHH gelten §89 (2) HmbBG sowie diese Vereinbarung nach §28 (1) HmbDSG.

4 Kreis der Betroffenen

Betroffene im Sinne des § 4 Absatz 1 HmbDSG sind alle natürliche Personen, die in einer Geschäftsbeziehung oder in einem Beschäftigungsverhältnis zur FHH stehen
Insbesondere sind die Mitarbeiterinnen und Mitarbeiter der FHH betroffen, die Daten in den überwachten HKR-Verfahren (Stufe 1 SAP-RVP) erfassen, freigeben und ausbuchen.

5 Empfänger/Empfängerinnen von Daten

Im Rahmen der gesetzlichen Bestimmungen werden nur solche Daten aus dem Quellsystemen importiert, die zwingend für die Aufgabenerfüllung benötigt werden. Werden darüber hinaus

Daten benötigt, so können die Anwenderinnen und Anwender diese direkt im Quellsystem über einen Lesezugriff aufrufen.

5.1 Empfangende dritte Stellen

Es werden keine Daten an dritte Stellen weitergegeben.

5.2 Auftragsdatenverarbeiter

Die gesamte Datenverarbeitung wird bei folgendem Auftragnehmer durchgeführt:

Dataport
Altenholzer Straße 10-14
24161 Altenholz

Zur Unterstützung des Produktivstarts erhält ein Mitarbeiter der SAP AG temporär Zugriff auf das System.

SAP Deutschland AG & Co. KG
Hasso-Plattner-Ring 7
D - 69190 Walldorf

5.3 Empfänger/innen innerhalb der Daten verarbeitenden Stelle, die andere Aufgaben wahrnehmen

Keine.

6 Datenübermittlung nach §17 Abs. 2 und 3 HmbDSG (Übermittlung an Drittländer)

Eine Datenübermittlung von Daten an Stellen außerhalb der EU findet nicht statt.

7 Fristen für Sperrung und Löschung der Daten

7.1 Fristen für die Sperrung der Daten

Wird ein Vorgang im SAP-FM abgeschlossen, so ist er nicht mehr änderbar und ist somit für eine weitere Bearbeitung gesperrt.

7.2 Fristen für die Löschung der Daten

Die Aufbewahrungsfristen erfolgen entsprechend den Bestimmungen über die Aufbewahrung von Informationen des Haushalts-, Kassen- und Rechnungswesens (AufBewBest) (Anlage 5 zu Nr. 4.7 der Verwaltungsvorschriften für Zahlungen, Buchführung und Rechnungslegung (§§ 70 bis 72 und 74 bis 80 LHO).

Eine physische Löschung von Vorgängen im SAP-FM findet nicht statt, eine Archivierung ist derzeit konzeptionell noch nicht vorgesehen.

8 Technische und organisatorische Maßnahmen nach §8 HmbDSG

Durch eine Vielzahl von technischen und organisatorischen Maßnahmen wird der datenschutzrechtlich konforme Umgang mit personenbezogenen Daten sichergestellt.

Folgende generelle Regularien der FHH gelten auch für das SAP-FM:

- Rahmensicherheitskonzept (RaSiKo)
- IuK-Grundschutzkonzept
- Richtlinie zur Datensicherheit im IuK-Bereich (DS-Richtlinie)
- Richtlinien zur Verwaltung von Passwörtern (Passwort-RL)
- Richtlinie über die Sicherheit der Datenverarbeitung auf Arbeitsplatzrechnern und sonstigen Endgeräten (PC-RL)
- Freigaberichtlinie (regelt die Voraussetzungen unter denen eine Software produktiv gehen darf)
- Entsorgungsrichtlinie (regelt die Entsorgung von Datenträgern)
- Konzept zum Virenschutz- und Patchmanagement (VPM-Konzept)
- IT-Architektur Richtlinie

Von Dataport wurden BSI-Grundschutz konforme Dokumentationen für das Rechenzentrum (RZ²), die Netze und die Clients erstellt. Hinweise zum BSI-Grundschutz finden sich auf der Webseite des Bundesamtes unter BSI IT-Grundschutz.

Ferner findet das Betriebshandbuch des Dataport Basisbetriebs in der jeweils aktuellen Fassung Anwendung. Dort sind die wiederkehrenden Standardprozesse die im Betrieb eines SAP-Systems auftreten und die Aufgabenverteilung zwischen Auftragnehmer (Dataport) und Kunden (FHH) beschrieben.

Durch mehrstufige Zugriffsbeschränkungen ist im SAP-FM sichergestellt, dass nur Befugte die personenbezogenen Daten verarbeiten können:

- **Schutz vor generell unberechtigtem Zugriff**
    - durch geregelten Zugriff von wenigen Personen, ausschließlich innerhalb der Kasse.Hamburg. Es gibt ein geregeltes Verfahren zur Neuanlage, Änderung, Passwortvergabe und Löschung von Anwendern. Dieses Verfahren unterliegt dem 4-Augen Prinzip, d.h. es sind immer mindestens zwei Beteiligte erforderlich.
- **Schutz vor spezifisch unberechtigtem Zugriff**
    - durch das Einschränken der ausführbaren Transaktionen und des darin verwalteten Datenbereichs. Grundsätzlich sind nur die für die Aufgabenwahrnehmung benötigten Transaktionen in dem jeweils berechtigten Datenbereich ausführbar.
- **Schutz der personenbezogenen Daten**
    - durch spezifische Einstellungen und Entwicklungen in allen Bereichen. Es dürfen nur die für die Aufgabenwahrnehmung notwendigen personenbezogenen Daten im Zugriff sein.

Datenänderungen werden innerhalb des SAP-Verfahrens protokolliert und können im Rahmen von Prüfungen nachvollzogen werden. Gegenwärtig werden keine Daten gelöscht oder aggregiert. Damit ist die Authentizität und die Revisionsfähigkeit der Daten gewährleistet.

Die Integrität von zusätzlichen Daten wird durch die Validierungsregeln bei der Eingabe der Daten gewährleistet. In diesem Zusammenhang werden folgende Aspekte berücksichtigt.

1. Atomarität:	Transaktionen werden entweder vollständig oder gar nicht ausgeführt.
2. Konsistenz:	Eine Transaktion, die auf einem konsistenten Datenbestand ausgeführt wird, führt wiederum zu einem konsistenten Datenbestand.
3. Isolation:	Es wird gewährleistet, dass sich die einzelnen Transaktionen nicht gegenseitig beeinflussen.
4. Dauerhaftigkeit:	Die Inhalte einer abgeschlossenen Transaktion werden dauerhaft abgespeichert.

Die Verfügbarkeit der Daten ist durch ServiceLevelAgreement (SLA) mit dem Rechenzentrum bzw. eine Dienstvereinbarung mit Dataport sichergestellt.

9 Art der Geräte, Verfahren zur Übermittlung, Sperrung, Lösung, Auskunftserteilung und Benachrichtigung

9.1 Art der Geräte und Stellen, bei denen sie aufgestellt sind

Der Betrieb des SAP-FM-Systems erfolgt in Client/Server-Architektur. Die Clients stellen die nach dem Standard ausgestatteten PCs an den Arbeitsplätzen der Mitarbeiterinnen und Mitarbeitern der Behörden der FHH dar.
Die SAP Server, die SQL-Datenbankserver sowie das Netz werden von Dataport im Rechenzentrum Hamburg (RZ²) betrieben.

9.2 Verfahren zur Übermittlung, Sperrung, Löschung, Auskunftserteilung und Benachrichtigung

Übermittlungen finden wie unter Nr. 5.1 dargestellt nicht statt.

Eine Sperrung von Vorgängen erfolgt automatisiert nach der abschließenden Bearbeitung.

Die Möglichkeit für Betroffene, Auskünfte über die eigenen personenbezogenen Daten gemäß des § 18 HmbDSG zu erhalten ist über die Quellsysteme gegeben und geregelt

Erstellt am: 14.07.2016
Zuletzt aktualisiert am: 21.11.2016

gez. Karsten Mante

Mante/21H-KM

Verfügung:

1. Kopie über die die behördliche Datenschutzbeauftragte -FB 113- an den Hamburgischen Datenschutzbeauftragten -D-

2. Original über Referatsleitung Kassenprozesse, Schnittstellen und Fachverfahren (K21) zum Vorgang Verfahrensbeschreibung