DSFA-Bericht

Bericht der Stadt Fiktivia
zur Datenschutz-Folgenabschätzung (DSFA)
für den Verarbeitungsvorgang

Personal verwalten

[Dokument-ID: 222222]

Inhalt

1. Information zur DSFA

1.1 Beteiligte Personen und Status

1.1.1 An DSFA beteiligte Person(en) und ihre Rolle(n)	1.1.2 Status der DSFA	1.1.3 Anmerkung zum Status
Bossen, Karin [Auftraggeberin] Bauer, Berta [Federführung DSFA-Erstellung] Hofer, Birgit [Vertretung Verantwortlicher] Müller, Bernhard [Vertretung IT-Bereich] Muster, Hans, bDSB [Beratung] Schulz, Peter [Review]	☒ in Bearbeitung ☐ Aktiviert ☐ Deaktiviert ☐ Sonstig: <bitte Status angeben>	Initialer Entwurf wurde nach Methode und Mustern des BayLfD erstellt.
1.1.4 Kontaktdaten Datenschutzbeauftragte/r Siehe =>(4) Punkt 5.6 aus der Beschreibung der Verarbeitungstätigkeit „Personal verwalten“.		

1.2 Anlagen bzw. Verweise zum DSFA-Bericht

Nr.	Bezeichnung der Anlage bzw. des Verweises	Quelle und Anmerkung
1	Risikoanalyse Datensicherheitsziele	Anlage (Dok-ID 353535)
2	Risikoanalyse Schutzbedarfsziele	Anlage (Dok-ID 363636)
3	Stellungnahme DSB	Anlage, noch offen
4	Beschreibung der Verarbeitungstätigkeit „Personal verwalten“	Verweis (Dok-ID: 111111)
5	Löschkonzept „Personal verwalten“	Verweis (Dok-ID: 121654)
6	Auskunftskonzept „Personal verwalten“	Verweis (Dok-ID: 121610)
7	Datenkategorien und ihre Dateneingabefelder	Verweis (Dok-ID 121034)
8	Standardmaßnahmen IT-Infrastruktur	Verweis (Dok-ID 515151)
9	Spezifikation Druckstraßen DRS-1 und DRS-2	Verweis (Dok-ID 515531)
10	Spezifikation Intranet	Verweis (Dok-ID 867151)
11	Spezifikation HCM-Formularserver FormServ-HCM	Verweis (Dok-ID 513291)
12	Spezifikation IT-Personalwirtschaftssystem HCM-Fiktivia	Verweis (Dok-ID 173455)
13	Prozesslandkarte „Personal verwalten“ inkl. Geschäftsprozesse (GP)	Verweis (Dok-ID 394208)
14	Prozesslandkarte „Ausübung eines DSGVO-Betroffenheitsrechts managen“ inkl. GP	Verweis (Dok-ID 121690)
15	Prozesslandkarte „Geschäftsprozesse managen“ inkl. GP	Verweis (Dok-ID 121300)

1.3 Änderungshistorie

Wann?	Wer?	Was?
15.03.19	Bauer, Berta	Initialer Entwurf des DSFA-Berichts

1.4 Zeitpunkt der nächsten routinemäßigen Überprüfung

Klicken Sie hier, um ein Datum einzugeben.

2. Kontext

2.1 Überblick

2.1.1 ■ Welche Verarbeitung ist geplant? ■

Unter die Verarbeitungstätigkeit fallen:

a) HR-Kernfunktionen: In diesem Bereich werden die Personalstammdaten verarbeitet, also z.B. relevante Kontaktdaten, Finanzdaten, Arbeitsverträge usw.
b) HR-Gehaltsabrechnung: Zusammensetzung des Arbeitsentgelts (Grundgehalt, Zuschläge, Abschläge, Zulagen usw.) wird monatlich je Personalfall ermittelt.
c) Zeit- und Anwesenheitsmanagement: Verarbeitung der Arbeitszeiten, Urlaube, Dienstbefreiungen usw.
d) Personalplanung und -analyse: Simulation der Personalkosten und Personalbedarfe für die Zukunft.
e) Organisationsmanagement: Verwaltung aller Dienststellen/Ämter und ihrer Hierarchiestrukturen sowie Zuordnung der Beschäftigten über das Stellenmanagement zu den einzelnen Organisationseinheiten.

Details siehe =>(13) Prozesslandkarte „Personal verwalten“ zusammen mit allen dazugehörenden und beschriebenen Geschäftsprozessen.

2.1.2 ■ Welche Zwecke hat die Verarbeitung? ■

Siehe =>(4) Punkt 6.1 aus der Beschreibung der Verarbeitungstätigkeit „Personal verwalten“.

2.1.3 ■ Welche Rechtsgrundlagen/Befugnisse für die Verarbeitung gibt es? ■

Siehe =>(4) Punkt 6.2 aus der Beschreibung der Verarbeitungstätigkeit „Personal verwalten“.

2.1.4 ■ Wenn anwendbar, wie wird die Einwilligung der betroffenen Personen eingeholt? ■

Es werden in vorliegendem Zusammenhang keine personenbezogenen Daten auf Grundlage einer Einwilligung verarbeitet (vgl. =>(4) Punkt 6.2 aus der Beschreibung der Verarbeitungstätigkeit „Personal verwalten“).

2.1.5 ■ Welche weiteren Normen, Standards und Zertifizierungen gibt es, die für die Verarbeitung relevant sind? ■

Die bei der Verarbeitung umgesetzten Geschäftsprozesse halten die bestehenden normativen personalwirtschaftlichen Vorgaben ein und berücksichtigen Empfehlungen sachkundiger Dritter. Zudem wird ein weit verbreitetes IT-System mit diversen Zertifizierungen verwendet, von dessen Standards die Stadt nicht nennenswert abweicht. Da dieses HCM-System umfassend die Verarbeitungstätigkeit unterstützt, wird die Verarbeitung von den umgesetzten Standards der HCM-Fachapplikation maßgeblich mit geprägt.

2.1.6 ■ Welche Zuständigkeiten bestehen für die Verarbeitung? ■

Siehe =>(4) Punkt 5 und 13 aus der Beschreibung der Verarbeitungstätigkeit „Personal verwalten“.

2.1.7 ■ Wie sind die Verpflichtungen der Auftragsverarbeiter klar definiert und vertraglich geregelt? ■

Es werden keine Auftragsverarbeiter eingesetzt.

2.1.8 ■ Wurde der Standpunkt der betroffenen Personen eingeholt? ■

2.1.8.1 Wurde der Standpunkt der betroffenen Personen oder ihrer Vertreter eingeholt?

☐ Ja ☒ Nein

2.1.8.2 Anmerkung

Die Stadt hat der bei ihr bestehenden Personalvertretung Gelegenheit zur Stellungnahme gegeben (vgl. Art. 35 Abs. 9 DSGVO). Insbesondere vor dem Hintergrund, dass die betrachtete Verarbeitungstätigkeit schon lange ohne nennenswerte Änderungen betrieben wird, hat die Personalvertretung auf die Abgabe einer Stellungnahme verzichtet.

2.2 Daten, Prozesse und Unterstützung

2.2.1 ■ Welche Kategorien personenbezogener Daten werden verarbeitetet? ■

Nr.	Bezeichnung der Datenkategorie	Anmerkung
---	Siehe =>(4) Punkt 7 aus der Beschreibung der Verarbeitungstätigkeit „Personal verwalten“	---

2.2.2 ■ Welche Kategorien von Personen sind von der Verarbeitung betroffen? ■

Nr.	Bezeichnung der Kategorie betroffener Personen	Anmerkung
---	Siehe =>(4) Punkt 8 aus der Beschreibung der Verarbeitungstätigkeit „Personal verwalten“	---

2.2.3 ■ Welche Empfänger, denen die personenbezogenen Daten offengelegt werden, einschließlich Empfänger in Drittländern oder internationale Organisationen gibt es? ■

Nr.	Empfänger	Anlass der Offenlegung	Anmerkung
---	Siehe =>(4) Punkte 9 und 10 aus der Beschreibung der Verarbeitungstätigkeit „Personal verwalten“	---	---

2.2.4 ■ Wie verläuft der Lebenszyklus von Daten und Prozessen? ■

Lebenszyklus Daten:

Der Lebenszyklus der Daten richtet sich nach den =>(12) Geschäftsprozessen des Kernprozesses „Personal verwalten“, die die Daten erstellen, pflegen und löschen. Zum Löschen siehe =>(5) Löschkonzept „Personal verwalten“.

Lebenszyklus Prozesse:
Das Geschäftsprozessmanagement, insbesondere die Geschäftsprozesse „Neuen Prozess etablieren“ und „Etablierten Prozess ändern“ bestimmen den Lebenszyklus der betroffenen Prozesse, siehe =>(15) Prozesslandkarte „Geschäftsprozesse managen“ zusammen mit allen dazugehörigen und beschriebenen Geschäftsprozessen.

2.2.5 ■ Mit Hilfe welcher Betriebsmittel erfolgt die Datenverarbeitung? ■

Betriebsmittel sind das =>(12) IT-Personalwirtschaftssystem HCM-Fiktivia, =>(9) die Druckstraßen DRS-1 und DRS-2 im Druckzentrum des städtischen Hauptrechenzentrums, =>(10) das städtische Intranet und =>(11) der HCM-Formularserver FormServ-HCM.
Details ergeben sich aus der jeweiligen Spezifikation der genutzten Betriebsmittel.

3. Grundlegende Prinzipien

3.1 Verhältnismäßigkeit und Notwendigkeit

3.1.1 ■ Warum ist die Verarbeitung zwingend erforderlich und ein verhältnismäßiges Mittel, den angestrebten Zweck zu erreichen? ■

Organisatorische, personelle und soziale Maßnahmen, insbesondere zur Personalverwaltung und Personalwirtschaft, müssen im Rahmen von Arbeits- und Dienstverhältnissen nach unterschiedlichen normativen und weiteren Vorgaben durchgeführt werden.
Bei der in der Stadt Fiktivia vorliegenden sehr hohen Komplexität der Personalverwaltung, die zudem insbesondere durch stetig neue normative Vorgaben eine relativ hohe Dynamik aufweist, ist die konzipierte und durch das IT-Personalwirtschaftssystem HCM-Fiktivia IT-unterstützte Verarbeitung unter Beachtung der normativen Vorgaben verhältnismäßig. Es sind keine alternativen Vorgehensweisen bekannt, die in die Rechte und Freiheiten betroffener Personen weniger stark eingreifen.

3.1.2 ■ Warum sind die Daten erforderlich? ■

Siehe =>(7) Anlage „Datenkategorien und ihre Dateneingabefelder“ zur Beschreibung der Verarbeitungstätigkeit „Personal verwalten“; in dieser Anlage ist zu jedem Eingabedatum bzw. Eingabebereich die Erforderlichkeit dokumentiert.

3.1.3 ■ Wie werden die Daten korrekt und auf dem neuesten Stand gehalten? ■

Wie aus den relevanten Geschäftsprozessen hervorgeht, lösen denkbare Datenänderungen immer Ereignisse (z.B. Änderungsmitteilung) aus, die zeitnah für die erforderlichen Änderungen in den führenden Informationssystemen sorgen.

3.1.4 ■ Welche Speicherdauer haben die Daten? ■

Siehe =>(4) Punkt 11 aus der Beschreibung der Verarbeitungstätigkeit „Personal verwalten“ sowie =>(5) das Löschkonzept „Personal verwalten“.

3.2 Umsetzung der Betroffenenrechte

3.2.1 ■ Wie werden die betroffenen Personen über die Verarbeitung informiert? ■

Die Information betroffener Personen erfolgt zweistufig:
(a) Information im Umfang von Art. 13 f. DSGVO werden den betroffenen Personen zum jeweils gesetzlich vorgesehen Zeitpunkt erteilt. Für Bewerberinnen und Bewerber werden Informationen auf speziellen Internetseiten der Stadt vorgehalten. Neu eingestellten Beschäftigten wird mit Einstellung ein entsprechendes Informationsdokument übergeben. Beschäftigte in bereits bestehenden Beschäftigungsverhältnissen wurden am 25.05.2018 durch Übersendung des vorgenannten Informationsdokuments informiert.

(b) Bei zusätzlichem Auskunftsbedarf sind zu den einzelnen Verarbeitungsbereichen Kontaktmöglichkeiten angegeben, über die spezifische Detailinformationen von betroffenen Personen bezogen werden können.

3.2.2 ■ Wie können Betroffene ihr Recht auf Auskunft ausüben? ■

Bei der Stadt koordiniert und stellt eine zentrale Stelle sicher, dass Datenschutz-Anfragen betroffener Personen ggf. zur Beantwortung bzw. Umsetzung an die relevanten Dienststellen weitergeleitet und die qualitätsgesicherten Antworten der Dienststellen an die betroffene Person fristgerecht weitergegeben werden (Details siehe **=>(14)** Prozesslandkarte „Ausübung eines DSGVO-Betroffenheitsrechts managen“ inklusive der dazugehörenden Geschäftsprozesse).

Auskunft:

Die Datenzusammenstellung zur Beantwortung eines Auskunftsersuchens einer betroffenen Person, die mit HCM-Fiktivia verarbeitet wird, wird durch einen speziellen Standard-Report technisch unterstützt. Die genaue Vorgehensweise ergibt sich aus dem **=>(6)** Auskunftskonzept „Personal verwalten“.

3.2.3 ■ Wie können betroffene Personen ihr Recht auf Löschung ausüben? ■

Zum Kernprozess „Ausübung eines DSGVO-Betroffenheitsrechts managen“ siehe Punkt 3.2.2.

Löschung:

Rechtskonforme Löschanforderungen können in HCM-Fiktivia durch punktuelle (Löschung von „Einzeldaten“ in einem Personalfall) und personalfallbezogene (Löschung gesamter Personalfall) Löschfunktionen umgesetzt werden.

3.2.4 ■ Wie können betroffene Personen ihr Recht auf Berichtigung ausüben? ■

Zum Kernprozess „Ausübung eines DSGVO-Betroffenheitsrechts managen“ siehe Punkt 3.2.2.

Berichtigung:

Rechtskonforme Berichtigungen werden u.a. durch Änderungsfunktionen von HCM-Fiktivia technisch umgesetzt.

3.2.5 ■ Wie können betroffene Personen ihr Recht auf Einschränkung oder Widerspruch der Verarbeitung ausüben? ■

Zum Kernprozess „Ausübung eines DSGVO-Betroffenheitsrechts managen“ siehe Punkt 3.2.2.

3.2.6 ■ Wie können betroffene Personen ihr Recht auf Datenübertragbarkeit ausüben? ■

Eine Recht auf Datenübertragbarkeit besteht vorliegend nicht: Die gesetzlichen Voraussetzungen von Art. 20 Abs. 1 DSGVO sind nicht gegeben; zudem greift der Ausschlusstatbestand des Art. 20 Abs. 3 Satz 2 DSGVO.

4. Risiken

4.1 Risikoanalyse

4.1.1 ■ Wie wird die Erfüllung der SDM-Datensicherheitsziele gewährleistet? ■

Für die SDM-Gewährleistungsziele der klassischen Informationssicherheit „Verfügbarkeit“, „Vertraulichkeit“ und den Teilaspekt „Datenintegrität“ des SDM-Gewährleistungsziels „Integrität“ wurde die Risikoanalyse mittels einer klassischen Risikomanagementmethode ermittelt. Die genaue Durchführung und Ergebnisse sind =>(1) aus der Anlage 1 „Risikoanalyse Datensicherheitsziele“ ersichtlich.

4.1.2 ■ Wie wird die Erfüllung der SDM-Schutzbedarfsziele gewährleistet? ■

Für die SDM-Gewährleistungsziele „Datenminimierung“, „Intervenierbarkeit“, „Transparenz“ und „Nichtverkettung“ sowie der Teilaspekte „Konzepteinhaltung“ und „Richtigkeit“ des SDM-Gewährleistungsziels „Integrität“ wurde die Risikoanalyse anhand eines Zielerfüllungsmanagements durchgeführt, dessen Inhalte und Ergebnisse sich =>(2) aus der Anlage 2 „Risikoanalyse Schutzbedarfsziele“ ergeben.

4.1.3 ■ Risikogesamtbewertung: Wie wird die Einhaltung der DSGVO gewährleistet? ■

Ergebnis Zielgesamtbewertung:
Die beiden durchgeführten Risikoanalysen (siehe Punkte 4.1.1 und 4.1.2) führten im Hinblick auf die SDM-Gewährleistungszeile zu folgendem Ergebnis:

1.	Verfügbarkeit:	ge
2.	Vertraulichkeit:	ge
3.	Datenintegrität:	ge
4.	Datenminimierung:	ge
5.	Intervenierbarkeit:	ge
6.	Transparenz:	gr
7.	Nichtverkettung:	ge
8.	Konzeptionseinhaltung:	ge
9.	Richtigkeit:	ge

Insgesamt ergeben somit die beiden durchgeführten Risikoanalysen für die SDM-Datensicherheitsziele und für die SDM-Schutzbedarfsziele im Ergebnis, dass die SDM-Gewährleistungsziele als erfüllt angesehen werden können. Die betrachtete Verarbeitungstätigkeit „Personal verwalten“ steht nach wirksamer Umsetzung der in der DSFA festgelegten Datenschutzmaßnahmen im Einklang mit der Datenschutz-Grundverordnung.

4.1.4 ■ Abstimmung mit der zuständigen Aufsichtsbehörde? ■

4.1.4.1 Wurde die zuständige Aufsichtsbehörde konsultiert bzw. ist eine Konsultation geplant?

☐ Ja ☒ Nein

4.1.4.2 Begründung

Keine hohen Restrisiken identifiziert.

4.1.4.3 Beschreibung der Abstimmung (zeitlicher Verlauf, Status, Verweis auf Schriftverkehr, Ergebnisse usw.)

4.2 Geplante oder bereits umgesetzte Datenschutzmaßnahmen

ID	Bezeichnung	Beschreibung und Anmerkung
M.1	Basis Backup-Struktur nutzen	Die Stadt stellt für ihre IT-Infrastruktur zahlreiche Basiskomponenten für die Datensicherung (z.B. redundantes Rechenzentrum, zentrale Backup-Server) inkl. der für die Betreuung erforderlichen Organisation zur Verfügung. Das HCM muss nachweisbar (Spezifikation und Umsetzungsnachweis) in diese Basis-Infrastruktur für die Datensicherung integriert werden. =>(8) SM.200603281115 aus dem Papier „Standardmaßnahmen IT-Infrastruktur“
M.2	Dienstleistungsangebot HCM-Hersteller nutzen	Der Hersteller von HCM-Fiktivia bietet von der Stadt zu nutzende Unterstützungsleistungen beim Systembetrieb an, die über den städtischen Pflegevertrag (siehe Dok-ID 452356) abgerufen werden können. Zudem besteht zwischen der Stadt und dem Hersteller ein Dienstleistungsrahmenvertrag über 150 Personentage pro Jahr (siehe Dok-ID 985432), die im Rahmen des HCM-System flexibel eingesetzt werden können. Da dieser Vertrag am 31.12.2019 enden wird, ist ein neuer Rahmenvertrag in Höhe von 150 Personentagen pro Jahr ab 01.01.2020 auszuschreiben. Darin müssen insbesondere ausreichend Dienstleistungskapazität für die Themen „Beratung Daten HCM-System wiederherstellen“, „Datenfehleingaben vermeiden und erkennen“ und „Workflow (z.B. 4-Augen-Prinzip)“ gesichert werden. Da keine Fernwartung existiert und der Hersteller von HCM-Fiktivia keine Möglichkeit hat, auf personenbezogene Daten der Stadt zuzugreifen, besteht keine Auftragsverarbeitung.
M.3	Löschberechtigung restriktiv vergeben	Systembenutzer haben grundsätzlich keine Löschberechtigung, d.h. nur in begründeten und dokumentierten Ausnahmefällen kann eine Löschberechtigung zugewiesen werden.
M.4	HCM-Benutzer schulen	Alle HCM-Benutzer, die im System personenbezogene Daten neu eingeben, ändern und/oder löschen können (Berechtigungskonzept), dürfen dies erst nach dem erfolgreichen Besuch der dafür vorgesehenen HCM-Schulung und einem regelmäßig erbrachten Kompetenznachweis.
M.5	Lesenden Zugriff für berechtigte Dritte konfigurieren	Für berechtigte Dritte (z.B. Finanzprüfer, Auditoren) ist im Rollen- und Berechtigungskonzept eine Rolle vorhanden, die nur einen lesenden Zugriff auf die relevanten Daten gestattet. Die durchgängige Verwendung dieser Rolle in den einschlägigen Fällen ist gewährleistet.
M.6	HCM-Administratoren zertifizieren	Alle HCM-Administratoren müssen ein geeignetes Zertifikat „HCM-Administrator“ des HCM-Herstellers besitzen.
M.7	Basis Schadsoftware-/ Hackerabwehrsystem nutzen	Die Stadt stellt für ihre IT-Infrastruktur zahlreiche Basiskomponenten für die Abwehr von Computerkriminalität (z.B. Antiviren-Software, Firewalls) inkl. der für die Betreuung erforderlichen Organisation zur Verfügung. Fachanwendungen der Stadt sind im Betrieb automatisiert von diesem Schutz, der für den betrachteten Verarbeitungsvorgang ausreicht, mit umfasst. =>(8) SM.200905281744 aus dem Papier „Standardmaßnahmen IT-Infrastruktur“
M.8	Kopfmonopole mittels Teambildung reduzieren	Die Kernaufgaben der Personalabrechnung müssen jederzeit durch mindestens zwei Beschäftigte durchführbar sein.
M.9	Dienstleistung Dritter nutzen	Voraussetzungen sind geschaffen (z.B. Rahmenverträge), dass bei unvorhersehbaren Personalausfall für die personalwirtschaftlichen Kernaufgaben geeignete Dritte die dringlichen Aufgaben übernehmen können.

ID	Bezeichnung	Beschreibung und Anmerkung
M.10	Manuelle Abschlagzahlung	Prozess ist festgelegt und verifiziert, der manuelle Abschlagzahlungen an die städtischen Beschäftigten bei einem Ausfall des IT-Personalwirtschaftssystem HCM-Fiktivia ermöglicht.
M.11	Berechtigungskonfiguration testen	Insbesondere mit Regressionstests und umfassenden Testfällen ist die fehlerfreie Umsetzung des Rollen-und Berechtigungskonzepts regelmäßig zu testen.
M.12	Identity Management (IdM) umsetzen	Projekt zum IdM aufsetzen und durchführen. Solange das IdM nicht größtenteils automatisiert Berechtigungswechsel initiiert, muss bei den bisherigen entsprechenden Prozessen auf die rasche Berechtigungsanpassung bei Beschäftigtenwechsel geachtet werden.
M.13	Städtischen Beschäftigten durch Dienstanweisung sensibilisieren	Das von einem Beschäftigten erwartete Verhalten für die Reduzierung des Einzelrisikos wird über eine entsprechende Dienstanweisung kommuniziert und die Einhaltung gewährleistet.
M.14	IT-Arbeitsplatz wird automatisiert gesperrt	Bei Inaktivität wird der Arbeitsplatz automatisch gesperrt.
M.15	Dienstanweisung für die Übermittlung personenbezogener Daten umsetzen	In dieser Dienstanweisung wird das erwartete Verhalten der städtischen Beschäftigten bei der Übermittlung personenbezogener Daten (Prüfung Befugnis, geeignetes Medium, Pseudonymisierung/Anonymisierung, Erforderlichkeit der Verarbeitung usw.) beschrieben.
M.16	Internen Meldeprozess für Datenschutz-Verstöße implementieren	Im Rahmen des Datenschutz-Managements werden neue Prozesse aufgesetzt. Ein wichtiger neuer Prozess ist die zeitnahe Meldung von datenschutzrechtlich relevanten Schwachstellen und Verstößen an eine zentrale Stelle (städtischer DSB).
M.17	Nur verschlüsselte Datenträger verwenden	Mobile Datenträger in beliebiger Form (z.B. Laptop, USB-Stick) werden vor der Speicherung von Daten so verschlüsselt, dass bei einem Verlust eine unbefugte Entschlüsselung nach dem Stand der Technik unwahrscheinlich ist.
M.18	Datenexport auf das Notwendige beschränken	Datenexportmöglichkeiten vom IT-Personalwirtschaftssystem HCM-Fiktivia technisch auf das Notwendige beschränken.
M.19	Beteiligungen am Posteinlauf und Postauslauf auf das Notwendige beschränken	Die Zeichnungskette nach einem Posteingang oder vor einem Postausgang wird auf das absolut Notwendige beschränkt.
M.20	Beschäftige bzgl. der Anfertigung von Kopien sensibilisieren	Die Vorgabe, dass Kopien von Personaldaten nur in den festgelegten Ausnahmefällen gemacht werden dürfen, ist den Beschäftigten von Ihren Führungskräften in regelmäßigen Abständen zu kommunizieren.
M.21	Thema "Führung von Nebenakten" in die Fortbildung für Führungskräfte mit aufnehmen	Hinweis „Nebenakten sind zu vermeiden und nur auf die gesetzlich festgelegten Ausnahmefälle beschränkt“ regelmäßig an die Führungskräfte im Rahmen relevanter Fortbildungen kommunizieren.
M.22	Vier-Augen-Prinzip für tragende Personaldateneingaben umsetzen	Alle kritischen Dateneingabeprozesse sind zu identifizieren und zu dokumentieren. Alle identifizierten Eingaben sind – falls noch nicht geschehen – mit dem Vier-Augen-Prinzip zumindest organisatorisch abzusichern.
M.23	Wiederholte Falscheingaben sammeln und auswerten	Falscheingaben, die sich wiederholen, werden im Personalamt zentral gesammelt und im Rahmen einer regelmäßigen Auswertung Aktionen für die künftige Vermeidung festgelegt (z.B. Fehler in Schulung aufnehmen, „Brandbrief“)
M.24	Keine Selbstbearbeitung zulassen	Systemuser können technisch über das Rollen- und Berechtigungskonzept abgesichert nicht ihre eigenen Personaldaten bearbeiten.
M.25	HCM-Vorlagewesen standardisieren	Im Rahmen der geplanten Digitalisierung (HCM-Portal) auch die HCM-Vorlagen quantitativ reduzieren, auf das Notwendige inhaltlich reduzieren, vereinheitlichen und inventarisieren.

ID	Bezeichnung	Beschreibung und Anmerkung
M.26	HCM-Vorlagen (papiergebunden und digital) freigeben	Alle Versionen von Vorlagen mit Personaldaten müssen vor ihrer Produktivsetzung durch einen Datenschutz-Experten geprüft und freigegeben werden.
M.27	Schnittstellenkonzepte für HCM-Fiktivia managen	Zu jeder technischen Schnittstelle von HCM-Fiktivia existiert u.a. ein Schnittstellenkonzept, das stets aktuell gehalten und in jeder Produktions-Version datenschutzrechtlich geprüft und freigegeben ist.
M.28	Risikoorientiert auswerten	Durch regelmäßige, risikoorientierte Auswertungen in HCM-Fiktivia (Selbstaudit) wird die Befolgung der Vorgaben überprüft.
M.29	Rollen- und Berechtigungskonzept umsetzen	Ein geeignetes Rollen- und Berechtigungskonzept, das sich so weit es geht an Standards orientiert, ist umzusetzen und ständig aktuell zu halten.
M.30	Informationen zur Personalverwaltung freigeben	Datenschutzrechtliche Informationen müssen vor ihrer Produktivsetzung durch einen Datenschutz-Experten geprüft und freigegeben werden.
M.31	Personalsachbearbeitung schulen und sensibilisieren	Personen, die Personalsachbearbeitung durchführen oder verantworten, werden bei Aufnahme ihrer Tätigkeit und danach regelmäßig zu folgenden Themen geschult: - Datenschutzrechtlicher Informationspflicht nachkommen
M.32	Verständlichkeitsprüfung durchführen	Durch geeignete Personen (Repräsentanten der betroffenen Personen) werden die beabsichtigten Informationen auf allgemeine Verständlichkeit geprüft und diese Prüfung dokumentiert.
M.33	Informationen mittels 3-Stufen-Modell bereitstellen	Die Informationen werden durchgängig in den folgenden 3 Stufen, die im Konkretisierungsgrad stetig zunehmen, bereitgestellt: 1. Stufe: Dezentrale Information (z.B. Hinweis im Arbeitsvertrag) 2. Stufe: Zentrale Information (DS-Portal) 3. Stufe: Experteninformation (für bestimmten Bereich zuständige Ansprechpartner)
M.34	Datenschutz-Managementsystem nutzen	Der Prozess „Personal verwalten“ wird unter die Kontrolle und Steuerung des städtischen Datenschutz-Managements gestellt. Das zentrale Datenschutz-Managementsystem wurde eingerichtet, um über den gesamten Lebenszyklus aller städtischen Verarbeitungstätigkeiten bei der Wahrung der datenschutzrechtlichen Anforderungen zu unterstützen.
M.35	IT-Unterstützung von HCM-Fiktiva nutzen	HCM-Fiktivia stellt Spezialberichte zur Unterstützung des Auskunftsanspruchs standardmäßig zur Verfügung, die auf die Stadt angepasst und dann genutzt werden.
M.36	Löschkonzept Personaldaten umsetzen	Das bestehende Löschkonzept umsetzen und ggf. geänderten Rahmenbedingungen ständig anpassen.
M.37	Separates HCM-System verwenden	HCM-Fiktivia wird als von anderen Fachanwendungen getrenntes System betrieben.
M.38	Separates HCM-Data-warehouse-System verwenden	Für die Zusammenführung und Auswertung von Personaldaten wird ausschließlich ein separates HCM-Datawarehouse-System eingesetzt.
M.39	Enterprise Architecture Management (EAM-Tool)	Für das IT-unterstützte Management von Schnittstellen und weiteren Komponenten der IT-Landkarte wird ein EAM-Tool verwendet.
M.40	Zweckänderungsverfahren implementieren	Um bei einer existierenden Verarbeitung ihren Zweck zu ändern, insbesondere zu erweitern, wird vorab durch ein Zweckänderungsverfahren die Rechtmäßigkeit geprüft und ggf. die erforderlichen Dokumentationen (z.B. Verzeichnis von Verarbeitungstätigkeiten, DSFA) angepasst.
M.41	Personal bereichsspezifisch einsetzen	Personal aus der Personalsachbearbeitung wird nicht zeitgleich/parallel in anderen Fachbereichen außerhalb der Personalverwaltung eingesetzt.

ID	Bezeichnung	Beschreibung und Anmerkung
M.42	Formalisierten Änderungsprozess umsetzen	Vor einer Änderung bei der Verarbeitung muss der formalisierte Änderungsprozess, der zwischen unbedeutenden bis hin zu schwerwiegenden Änderungen unterscheidet, durchlaufen werden.
M.43	Dokumentation regelmäßig auf Änderungen hin überprüfen	Wesentliche Nachweiskomponenten (z.B. Verzeichnis von Verarbeitungstätigkeiten, DSFA-Bericht) nach regelmäßiger Wiedervorlage auf Aktualität hin überprüfen.
M.44	Prinzip führende Datenhaltung anwenden	Informationen, die an mehreren unterschiedlichen Stellen der Dokumentation verwendet werden müssen, werden nur an einer Stelle wegen Konsistenz aufgeführt und gepflegt. Von den weiteren Stellen wird nur auf die zentrale Informations-Darstellungsstelle verwiesen.
M.45	Selbstdokumentation von IT-Komponenten nutzen	Haben die relevanten IT-Komponenten eine Selbstdokumentationsfunktion, so wird diese für die Dokumentation mit genutzt.
M.46	Belegte Personaldaten verarbeiten	Dort, wo Belege die Richtigkeit nachweisen können, sind bei einer Verarbeitung diese Belege zumindest einzusehen und diese Prüfung entsprechend zu dokumentieren.
M.47	Eingabehilfen anbieten	Insbesondere in HCM-Fiktivia werden Eingabehilfen (z.B. Adressregister) und ad hoc Plausibilitätsprüfungen (z.B. Formatprüfung bei E-Mails, Richtigkeit von IBAN) eingesetzt, um typische Fehleingaben zu verhindern.
M.48	Zentrale Datenqualitätsprüfungen durchführen	Regelmäßig wird die Qualität der Personaldaten durch zentrale Qualitätsprüfungen geprüft.
M.49	Datenbankwerkzeuge nur begründet installieren	Datenbankwerkzeuge, wie z.B. MS-Access, werden nur nach einem begründeten Antrag, unter Vorgabe des Nutzungsumfangs und nur befristet auf IT-Arbeitsplätzen installiert.