Datenschutzrechtliche Risikoanalyse

zum Betriebsmittel

IT-Personalwirtschaftssystem HCM-Fiktivia (HCM)

bei der Stadt Fiktivia

(Dok-ID: RA202202111020)

BayLfD-Stand: 01.05.2022

1. Inhalt:

2. Status und beteiligte Personen:

Status	beteiligte Personen	Anmerkungen
Bearbeitung	Musterfrau, Klara (Federführung, Fachbereich) Mustertech, Eva (Beratung, IT) Muster, Hans (Beratung, bDSB)	

3. Zeitpunkt der nächsten routinemäßigen Überprüfung:

Zeitpunkt	Anmerkungen
01.01.24	

4. Anlagen und Verweise:

ID	Bezeichnung	Anmerkungen
1	Beschreibung Bildschirmarbeitsplatz (BAP)	Datenschutzrechtliche Beschreibung des Betriebtsmittels "Bildschirmarbeitsplatz (BAP)", Verweis: Dok-ID: BM202110070840.
2	usw.	usw.
(…)	(…)	(…)

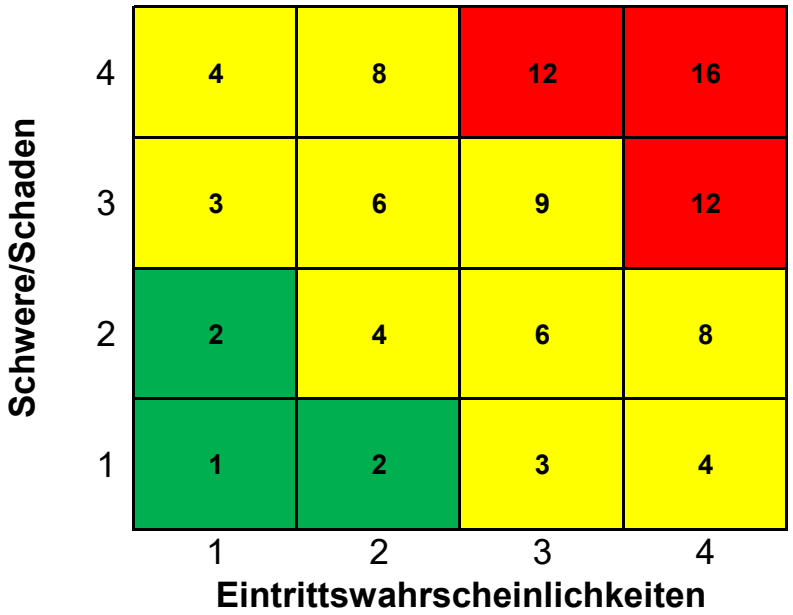
Änderungshistorie

Wann?	Wer?	Was?	Anmerkung
03.01.21	Musterfrau	Initialisierung Risikoanalyse	

Legende

1. Risikomanagement

1.1 Risikomatrix für die Indexierung der Risiken



Index	Bezeichnung Risikoindex
	hohes Risiko
	(normales) Risiko
	geringes Risiko

1.2 Eintrittswahrscheinlichkeit

Grad	Bezeichnung des Grads	Eintrittswahrscheinlichkeit	
		Beschreibung	Beispiel
1	geringfügig	Schaden kann nach derzeitigem Erwartungshorizont nicht eintreten.	Befall durch Schadsoftware bei einem Stand-Alone Rechner, der an keinem Netzwerk angeschlossen ist und an dem keine weiteren Medien angeschlossen werden können.
2	überschaubar	Schaden kann zwar eintreten, aus bislang gemachten Erfahrungen bzw. aufgrund der gegebenen Umstände scheint der Eintritt aber unwahrscheinlich zu sein.	Befall durch Schadsoftware bei einem Rechner, der aktuell gehalten, mit aktueller Antivirensoftware ausgestattet und nur mit einem BSI zertifizierten Firmennetzwerk verbunden ist.
3	substanziell	Schadenseintritt scheint auf Basis bislang gemachter Erfahrungen bzw. aufgrund der gegebenen Umstände zwar möglich, aber nicht sehr wahrscheinlich zu sein.	Befall durch Schadsoftware bei einem Rechner, der aktuell gehalten, mit aktueller Antivirensoftware ausgestattet und direkt mit dem Internet verbunden ist.
4	groß	Schadenseintritt scheint auf Basis bislang gemachter Erfahrungen bzw. aufgrund der gegebenen Umstände möglich und sehr wahrscheinlich zu sein.	Befall durch Schadsoftware bei einem veralteten Windows-XP Rechner ohne Antivirensoftware, der direkt mit dem Internet verbunden ist.

1.3 Schwere/Schaden

Grad	Bezeichnung des Grads	Schwere der Folgen / möglicher Schaden	
		Beschreibung	Beispiel

1	geringfügig	Betroffene erleiden eventuell Unannehmlichkeiten, die sie aber mit einigen Problemen überwinden können.	**immateriell:** leichte Verärgerung **materiell:** Zeitverlust **physisch:** vorübergehende Kopfschmerzen
2	überschaubar	Betroffene erleiden eventuell signifkante Unannehmlichkeiten, die sie aber mit einigen Schwierigkeiten überwinden können.	**immateriell:** geringe, aber objektiv nachweisbare psychische Beschwerden **materiell:** deutlich spürbarer Verlust an privatem Komfort **physisch:** minderschwere körperliche Schäden (z. B. leichte Krankheit)
3	substanziell	Betroffene erleiden eventuell signifkante Konsequenzen, die sie nur mit ernsthaften Schwierigkeiten überwinden können.	**immateriell:** schwere psychische Beschwerden **materiell:** finanzielle Schwierigkeiten **physisch:** schwere körperliche Beschwerden
4	groß	Betroffene erleiden eventuell signifkante oder sogar unumkehrbare Konsequenzen, die sie nicht überwinden können.	**immateriell:** dauerhafte, schwere psychische Beschwerden **materiell:** erhebliche Schulden **physisch:** dauerhafte, schwere körperliche Beschwerden

2. Zielerfüllungsmanagement

Ergebnis der Gefährdungsbewertung

Index	Bezeichnung Gefährdungsindex
	Keine Gefährdung, d.h. prognostizierte Vollerfüllung des betrachteten Ziels
	Es kann von einer kontinuierlichen Vollerfüllung des Ziels vertretbar ausgegangen werden. Gleichwohl kann eine Gefährdung des Ziels nicht ganz ausgeschlossen werden.
	Unzureichendes Schutzniveau für das betrachtete Ziel

Risikomanagement

Gewährleistungsziele	Summarische Risikobetrachtung	Index
DI - Datenintegrität VB - Verfügbarkeit VT- Vertraulichkeit	**Ermittlung des Risikoindexes über alle Einzelrisiken (unten stehendes Risikoprofil) nach der Maximum-Methode, d.h. der vorkommende höchste Risikoindex wird dem SDM-Datensicherheitsziel zugeordnet.**	ge

ID	Schwachstelle	Risikoquelle	Risiko-Szenario	Eintrittswahrscheinlichkeit		Schwere/Schaden		Index	Maßnahme-Bezeichnung	Risikoeinschätzung mit Maßnahmen	
Ziel				Erläuterung	Grad	Erläuterung	Grad			Erläuterung	Index
1 VB	**Datenverlust** Beim Einsatz von IT-Systemen können elektronische Daten verloren gehen.	# IT-Fehlfunktion	Hard- und/oder Software-Fehlfunktion führen dazu, dass erforderliche elektronische Daten unwiederbringlich verloren gehen.	Aufgrund der Komplexität des HCM-Systems (zahlreiche, zusammenwirkende Komponenten, häufige Updates usw.) ist ein Datenverlust durch IT-Fehlfunktionen sehr wahrscheinlich.	4	Wesentliche Daten sind in Papierform vorhanden, so dass der Schaden bei einem Verlust der digitalen Daten im Rahmen bleibt .	2	8	M.1 Basis Backup-Struktur nutzen M.2 Dienstleistungsangebot HCM-Hersteller nutzen	Datenverluste bei von der Stadt betriebenen Systemen, die mit dem HCM-System vergleichbar sind, gehen gegen Null.	gr
2 VB DI		# IT-User (intern)	User-Interaktionen mit dem HCM-System führen dazu, dass erforderliche Daten unwiederbringlich verloren gehen oder unberechtigt geändert werden.	Aufgrund der angespannten Personalsituation werden teilweise auch noch sehr unerfahrene HCM-Sachbearbeiter eingesetzt.	2		2	4	M.1 Basis Backup-Struktur nutzen M.3 Löschberechtigung restriktiv vergeben M.4 HCM-Benutzer schulen M.5 4-Augen-Prinzip für tragende Personaldateneingaben umsetzen M.6 Keine Bearbeitung der eigenen Personaldaten zulassen M.7 Wiederholte Falscheingaben sammeln und auswerten	Die Maßnahmen zusammen führen zu einer deutlich reduzierten Eintrittswahrscheinlichkeit.	gr
3 VB DI		# IT-User (extern)	Interaktionen externer User (z.B. Finanzprüfer, Auditoren) mit dem HCM-System führen dazu, dass erforderliche Daten unwiederbringlich verloren gehen oder unberechtigt geändert werden.	Zugriffe externer User auf das produktive HCM-System finden nur selten statt.	2		2	4	M.8 Lesenden Zugriff für befugte Externe konfigurieren	Fehlbedienungen von externen Benutzern, die zu einem Datenverlust führen, sind nicht vorstellbar, da solche Benutzer stets nur mit Leserechten ausgestattet sind (bewährtes Standardbenutzerprofil).	gr
4 VB DI		# Administrator	Interaktionen eines User mit weitreichenden Administratorenrechten im HCM-System führen dazu, dass erforderliche Daten unwiederbringlich verloren gehen oder unberechtigt geändert werden.	Da es das Alltagsgeschäft von Administratoren ist, mit produktiven IT-Systemen richtig umzugehen, ist der Eintritt unwahrscheinlich.	2		2	4	M.1 Basis Backup-Struktur nutzen M.5 4-Augen-Prinzip für tragende Personaldatenänderungen umsetzen M.9 HCM-Administratoren zertifizieren	Blickt man auf die schon lange aktive Administrationstätigkeit mit Umsetzung der Maßnahmen zurück, so erscheint der Eintritt als sehr unwahrscheinlich.	gr
5 VB	**Ressourcen** Notwendige Ressourcen stehen nicht zur Verfügung.	# Personal	Fehlendes, nicht mittelfristig ersetzbares Personal als unverzichtbare HCM-User bringt monatliche Personalabrechnung zum Stehen.	Altersstruktur des betroffenen Personals und relativ hohe Fluktation von Experten im HCM-Umfeld verschärfen die Situation.	3	Falls die Entgeltabrechnung nicht ordnungsgemäß läuft, kann dies zu ernsthaften finanziellen Schwierigkeiten der Beschäftigten führen.	3	9	M.10 Prozess für manuelle Abschlagszahlung vorhalten M.11 Kopfmonopole mittels Teambildung reduzieren M.12 Dienstleistung Dritter nutzen	Vor dem Hintergrund von Personalsparmaßnahmen ist nur ein normales Risiko erreichbar.	ge
6 VB		# IT-Fehlfunktion	HCM funktioniert aufgrund einer Störung bzw. eines Fehlers nicht ordnungsgemäß.	Die Komplexität zusammen mit der dynamischen Aktualisierung hat in der Vergangenheit zu solchen Störungen von HCM geführt.	4		3	12	M.13 Patch Management HCM durchführen M.14 Systematisch HCM-Tests durchführen M.2 Dienstleistungsangebot HCM-Hersteller nutzen	---	ge
									M.15 Rollen- und Berechtigungskonzept für HCM implementieren		

ID / Ziel	Schwachstelle	Risikoquelle	Risiko-Szenario	Eintrittswahrscheinlichkeit – Erläuterung	Eintrittswahrscheinlichkeit – Grad	Schwere/Schaden – Erläuterung	Schwere/Schaden – Grad	Index	Maßnahme-Bezeichnung	Risikoeinschätzung mit Maßnahmen – Erläuterung	Risikoeinschätzung mit Maßnahmen – Index
7 VT	**Unbefugte Verarbeitung** HCM-Daten können unbefugt verarbeitet werden.	# Personal # IT-User # IT-Fehlfunktion	Bei der Nutzung von HCM durch einen IT-User kann dieser unbefugt Daten verarbeiten.	Das Zugriffsmanagement von HCM ist technisch sehr komplex und damit fehleranfällig sowie angewiesen auf aktuelle Benutzerdaten (prozessuale Schnittstelle insbesondere zur Stellenbesetzung).	3	Eine unbefugte Verarbeitung von Daten aus der Personalverwaltung kann mit einem hohen Risiko für betroffene Personen verbunden sein.	4	12	M.14 Systematisch HCM-Tests durchführen M.16 Identity Management (IdM) implementieren M.17 Verschwiegenheit Personalsachbearbeitung gewährleisten	Bei der Komplexität der Berechtigungs-verwaltung im HCM muss dieses Einzelrisiko stets im Fokus bleiben.	ge
8 VT		# Personal # IT-User # IT-Fehlfunktion	Bei der Datenübetragung mittels automatisierter Schnittstelle werden HCM-Daten unbefugt verarbeitet.	HCM hat zahlreiche automatisierte Schnittstellen zu unterschiedlichen Stellen	2		4	8	M.18 Schnittstellenkonzept HCM implementieren	---	gr
9 VT		# Personal # IT-User # IT-Fehlfunktion	Nach einem Export von Daten aus HCM können diese unbefugt verarbeitet werden.	HCM bietet zahlreiche Möglichkeiten an, Daten elektronisch zu exportieren oder auszudrucken.	3		4	12	M.19 Export elektronischer HCM-Daten technisch beschränken und regeln M.20 Ausdruck von HCM-Daten regeln	Die "manuelle" Auslagerung von HCM-Daten ist ein Dauerthema.	ge
10 VT VB DI		# Straftäter	Mit Hilfe einer beliebig ausgestalteten Schadsoftware werden erforderliche Daten unbefugt verarbeitet, unberechtigt geändert oder gehen unwiederbringlich verloren.	Cyberkriminelle Angriffe nehmen ständig zu, so dass der Eintritt als sehr wahrscheinlich einzustufen ist.	4		4	16	M.21 Basis Schadsoftware-/ Hackerabwehrsystem nutzen M.1 Basis Backup-Struktur nutzen	Dieses Restrisiko wird bei anderen betriebenen IT-Systemen, die mit dem HCM-System vergleichbar sind, entsprechend eingestuft. Bzgl. HCM-System sind keine Besonderheiten erkennbar.	ge
(…)	**usw.**	usw.	usw.	usw.	4	usw.	4	16	usw. (…)		ge

Zielerfüllungsmanagement

Gewährleistungsziel	Summarische Gefährdungsbetrachtung	Index
DM - Datenminimierung **IV - Intervenierbarkeit** **KE - Konzepteinhaltung** **NV - Nichtverkettung** **RI - Richtigkeit** **TP - Transparenz**	**Ermittlung des Gefährdungsindexes über alle Einzelgefährdungen (unten stehendes Gefährdungsprofil) nach der Maximum-Methode, d.h. die vorkommende höchste Gefährdungsstufe wird dem SDM-Schutzbedarfsziel zugeordnet.**	ge

ID / Ziel	Schwachstelle	Gefährdungsquelle	Gefährdungszenario	Gefährdungsbewertung Erläuterung	Gefährdungsbewertung Index	Maßnahme-Bezeichnung	Gefährdungsbewertung Erläuterung	Gefährdungsbewertung Index
1 DM NV	**Datenüberhang** Es können Daten verarbeitet werden, deren Verarbeitung noch nie erforderlich war.	# IT-User	**Eingabefelder** in HCM werden für die Speicherung und sonstige Verarbeitung nicht erforderlicher Daten bzw. zu nicht abgedeckten Verarbeitungszwecken genutzt.	In HCM existieren etwa frei befüllbare Bemerkungsfelder.	ro	M.30 Datenkategorien und ihre Dateneingabefelder für „HCM“ implementieren M.31 Risikoorientiert HCM-Freitextfelder auswerten M.4 HCM-Benutzer schulen	Eine lückenlose Kontrolle ist organisatorisch und technisch nicht möglich.	ge
		# Personal # IT-Fehlfunktion	**Schnittstellen:** Nicht erforderliche bzw. zweckfremde Daten fließen über eine technische Schnittstelle in HCM und werden dort verarbeitet und/oder fließen aus HCM heraus für eine Weiterverarbeitung durch Externe.	HCM hat zahlreiche automatisierte Schnittstellen.Die Beschreibung technischer Schnittstellen und deren rechtskonforme und zuverlässige Ausgestaltung ist eine sehr komplexe, fehlerträchtige Aufgabe.	ro	M.18 Schnittstellenkonzept HCM implementieren	Durch konsequente Inventarisierung und Management dieser Schnittstellen ist die Rechtstreue gewährleistet.	gr
		(…)	(…)	(…)	ro	(…)	(…)	ge
2 DM	**Datenlöschung** Es können Daten verarbeitet werden, die insbesondere seit dem schon erfolgten Wegfall bzw. der Erreichung des Verarbeitungszwecks bereits gelöscht sein müssten.	# Personal # IT-User # IT-Fehlfunktion	Nicht mehr erforderliche Daten werden weiterhin durch HCM verarbeitet.	In HCM müssen ganze Altfälle (Löschen von Personalfällen) und auch teilweise Daten aus aktiven Personalfällen (punktuelles Löschen) durchgeführt werden. Aufgrund von stark vernetzten Daten, einer großen Datenbandbreite, Anforderungen an eine Rückrechnung usw. kann ein Löschvorgang sowohl technisch als auch organisatorisch äußerst komplex sein.	ro	M.32 Fachliches Löschkonzept implementieren M.33 Löschkonzept "HCM" implementieren (…)		ge
3 DM	**Automatisierte Entscheidung** Betroffene Personen können ihr Recht auf Abwehr automatisierter Entscheidungen im Einzelfall nicht wahrnehmen (Art. 22 DSGVO).	# Personal	Ein ordnungsgemäß geltend gemachter Anspruch auf Abwehr automatisierter Entscheidungen wird nicht erfüllt.	Im städtischen Personalwesen gibt es keine automatisierten Entscheidungen, wie diese vorausgesetzt werden.	---	---	---	---
	Auskunft Betroffene Personen können ihr Recht auf Auskunft nicht wahrnehmen (Art.15 DSGVO).					Siehe Maßnahmen zu ID ZM-2 M.34 Auskunftskonzept "HCM" implementieren M.35 HCM-Hersteller Muster liefern lassen M.36 An HCM-Kundenaustauschtreffen bedarfsgerecht teilnehmen (..)		
	Berichtigung Betroffene Personen können ihr Recht auf Berichtigung nicht wahrnehmen (Art.16 DSGVO).							

ID / Ziel	Schwachstelle	Gefährdungsquelle	Gefährdungszenario	Gefährdungsbewertung		Maßnahme-Bezeichnung	Gefährdungsbewertung	
				Erläuterung	Index		Erläuterung	Index
4 IV TP NV	**Löschung** Betroffene Personen können ihr Recht auf Löschung nicht wahrnehmen (Art. 17 Abs. 1 DSGVO).	# IT-User # Personal # IT-Fehlfunktion	Ein ordnungsgemäß geltend gemachtes Betroffenenrecht wird nicht oder nicht rechtzeitig erfüllt.	Betroffenenrechte können grundsätzlich mittels der mächtigen Anwendungsplattform HCM ohne allzu große Herausforderungen erfüllt werden.	ge		Nach den bislang gemachten Erfahren können die Betroffenenrechte wirksam im HCM-Kontext ausgeübt werden.	gr
	Einschränkung Betroffene Personen können ihr Recht auf Einschränkung der Verarbeitung nicht wahrnehmen (Art. 18 DSGVO).							
	Datenübertragbarkeit Betroffene Personen können ihr Recht auf Datenübertragbarkeit nicht wahrnehmen (Art. 20 DSGVO).							
	Widerspruch Betroffene Personen können ihr Recht auf Widerspruch nicht wahrnehmen (Art. 21 Abs. 1 Satz 1 DSGVO).							
5 TP	**Information** Die Informationspflichten nach Art. 13, 14 DSGVO werden nicht (vollständig) erfüllt.	# Personal	Die normativen Mindestinhalte der erforderlichen Information zu HCM werden betroffenen Personen nicht bereitgestellt.	Die rechtskonforme Ermittlung der inhaltlichen Informationsaspekte ist bzgl. HCM komplex und damit fehleranfällig.	ge	M.35 HCM-Hersteller Muster liefern lassen	Muster des HCM-Hersteller wird zuverlässig und fortlaufend aktualisiert.	gr
6 NV	**Zweckentfremdung** Die pbDaten können rechtswidrig für einen anderen Zweck verarbeitet werden.	# Personal # IT-Fehlfunktion	Durch hochintegrative Systeme (z.B. EIN System für Personal- und Finanzwirtschaft) werden Daten verschiedener Fachbereiche zusammengeführt und können rechtswidrig verarbeitet werden (z.B. wegen Lücke in Berechtigungskonzept oder technischer Fehler bei Berechtigungssteuerung).	Hinsichtlich der bestehenden Komplexität integrativer IT-Systeme sind unbeabsichtigte Konfigurationslücken und technische Fehler bei der Berechtigungssteuerung als Gefährdung für die Erfüllung der Nichtverkettung einzuschätzen.	ge	M.37 Separates HCM-System verwenden (…)	Aufgrund technischer Systemtrennung ist die Nichtverkettung angemessen gewährleistet.	gr
7 KE	**Aktualität Konzepte** Die relevanten Vorgaben für die Prozesse und sie unterstützende Systeme, die an der Verarbeitung der Daten beteiligt sind, können veraltern und damit nicht mehr gültig sein.	# Personal	Der Nachweis einer ordnungsgemäßen Verarbeitung kann nicht erbracht werden.	Die Synchronisation der dokumentierten Konzeption und der tatsächlichen Umsetzung ist nicht immer gegeben	ge	M.38 Selbstdokumentation-Funktionen von HCM nutzen (…)	Veränderungsmanagement ist bereits gut etabliert.	gr
8	**Richtigkeit** Daten können entgegen den sachlichen Anforderungen falsch oder unvollständig verarbeitet werden, notwendige Änderungen von	# Personal	Beschäftigte bzw. die Personalsachbearbeitung versäumen es, veraltete Daten zu aktualisieren	Zahlreiche Aktualisierung basieren auf manuell	ge	M.39 HCM-Eingabehilfen anbieten M.40 Automatisierte Plausibiliätschecks umsetzen	In HCM sind die Daten erfahrungsgemäß insbesondere aufgrund der hohen Vernetzung und	ge

ID / Ziel	Schwachstelle	Gefährdungsquelle	Gefährdungszenario	Gefährdungsbewertung – Erläuterung	Gefährdungsbewertung – Index	Maßnahme-Bezeichnung	Gefährdungsbewertung – Erläuterung	Gefährdungsbewertung – Index
RI	verarbeitet werden, notwendige Änderungen von Daten können unberücksichtigt bleiben und falsche Metadaten können zu einer falschen Verarbeitung führen.	# IT-User	oder Daten ihren sachlichen Anforderungen entsprechend zu verarbeiten.	angestoßenen Prozessen.	ge	M.41 Regelmäßige Datenstandsberichte an Beschäftigte geben (…)	insbesondere aufgrund der hohen Vernetzung und der intensiven Verwendung aktuell.	ge
(…)	usw.	usw.	usw.	usw.	ro	usw.	usw.	ge

Schutzmaßnahmen (TOMs)

ID	Bezeichnung	Kurzbeschreibung	Verweise	Anmerkungen
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. HCM ist nachweisbar in diese Basis-Infrastruktur für die Datensicherung integriert werden.	//Spezifikation Städtisches Backup-System (Dok-ID 200903051300).	
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.	//Vertrag HCM-Pflegevertrag (Dok-ID 452356) und HCM-Rahmenvertrag (Dok-ID 985432).	
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.	//Konzept HCM-Schulungs- und Zertifizierungskonzept (Dok-ID 953428).	
M.5	4-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.	//Konzept Prozesslandkarte „Personal verwalten“ inkl. Geschäftsprozesse (Dok-ID 394208).	
M.6	Keine Bearbeitung der eigenen Personaldaten zulassen	HCM-Benutzer können technisch über das Rollen- und Berechtigungskonzept abgesichert nicht ihre eigenen Personaldaten bearbeiten.	siehe M.16	
M.7	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“).	//Konzept Prozesslandkarte „Personal verwalten“ inkl. Geschäftsprozesse (Dok-ID 394208).	
M.8	Lesenden Zugriff für befugte Externe konfigurieren	Für befugte Externe (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.	siehe M.16	
M.9	HCM-Administratoren zertifizieren	Alle HCM-Administratoren müssen ein geeignetes Zertifikat „HCM-Administrator“ des HCM-Herstellers besitzen.	//Konzept HCM-Schulungs- und Zertifizierungskonzept (Dok-ID 953428).	
M.10	Prozess für manuelle Abschlagszahlung vorhalten	Prozess ist festgelegt und verifiziert, der manuelle Abschlagszahlungen an die städtischen Beschäftigten bei einem HCM-Ausfall ermöglicht.	//Konzept Geschäftsprozess "Manuelle Personalabschlagszahlung" (Dok-ID 847896).	
M.11	Kopfmonopole mittels Teambildung reduzieren	Die Kernaufgaben mit Dringlichkeitsanforderung, bei denen eine HCM-Unterstützung grundsätzlich unverzichtbar ist, sind ordnungsgemäß nach entsprechender Teambildung durchführbar sein.	---	
M.12	Dienstleistung Dritter nutzen	Durch Rahmenverträge werden unerwartete Personallücken durch externe Dienstleister abgedeckt.	//Vertrag Städtischer Rahmenvetrag mit "ExtDL GmbH" (Dok-ID 202107151350)	
M.13	Patch Management HCM durchführen	HCM wird nach Prüfung, Tests und Freigabe durch HCM-Funktions- und HCM-Sicherheitsupdates technisch auf den aktuellen Stand gehalten.	//Konzept Geschäftsprozess "Patch Management für HCM" (Dok-ID 729814).	
M.14	Systematisch HCM-Tests durchführen	Vor Produktivsetzung wesentlicher HCM-Änderungen werden diese systematisch gestestet.	//Konzept Geschäftsprozess "HCM testen" (Dok-ID 729817).	
M.15	Rollen- und Berechtigungskonzept für HCM implementieren	Ein geeignetes Rollen- und Berechtigungskonzept, das sich so weit es geht an Standards orientiert, ist für HCM umzusetzen und ständig aktuell zu halten.	//Konzept Technisches Rollen- und Berechtigungskonzept „HCM“ (Dok-ID 202106080940).	

ID	Bezeichnung	Kurzbeschreibung	Verweise	Anmerkungen
M.16	Identity Management (IdM) implementieren	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.	//Projekt IdM bei der Stadt einführen (Dok-ID 202202151000).	
M.17	Verschwiegenheit Personalsachbearbeitung gewährleisten	Die städtischen Beschäftigten sind ab Beginn ihres Dienst- bzw. Arbeitsverhältnisses von Gesetzes wegen verpflichtet, das Datengeheimnis zu beachten. Gemäß Art. 11 Satz 2 BayDSG besteht das Datengeheimnis nach dem Ende der Tätigkeit fort. An diese Verpflichtung werden die Beschäftigte anlassbezogen, regelmäßig aber jährlich erinnert.	//Konzept Regelmäßige Unterweisung städtischer Beschäftigte (Dok-ID 201403041200)	
M.18	Schnittstellenkonzept HCM implementieren	Zu jeder technischen HCM-Schnittstelle existiert u.a. ein Schnittstellenkonzept, das stets aktuell gehalten und in jeder Produktions-Version datenschutzrechtlich geprüft und freigegeben ist.	//Konzept Prozesslandkarte „Personal verwalten“ inkl. Geschäftsprozesse (Dok-ID 394208).	
M.19	Export elektronischer HCM-Daten technisch beschränken und regeln	Elektronische HCM-Exportschnittstellen (z.B. Export in eine Excel-Datei) sind grundsätzlich deaktiviert und werden nur im Bedarfsfall dokumentiert restriktiv freigegeben.	//Konzept Technisches Rollen- und Berechtigungskonzept „HCM“ (Dok-ID 202106080940).	
M.20	Ausdruck von HCM-Daten regeln	Die HCM-Druckfunktion ist grundsätzlich deaktiviert und wird nur im Bedarfsfall restriktiv freigegeben.	//Anweisung Dienstanweisung Datenübermittlung (Dok-ID 201807031600) und //Konzept Technisches Rollen- und Berechtigungskonzept „HCM“ (Dok-ID 202106080940).	
M.21	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. HCM ist nachweisbar in diese Basis-Infrastruktur für die Datensicherung integriert werden.	//Spezifikation Städtisches Anti-Schadsoftware-System (Dok-ID 200903081000).	
(…)	(…)	(…)	(…)	
M.30	Datenkategorien und ihre Dateneingabefelder für „HCM“ implementieren	In einer Feldliste werden alle relevanten HCM-Felder mit ihrem Verarbeitungszweck und der Erforderlichkeitsbegründung aufgezählt.	//Spezifikation Datenkategorien und ihre HCM-Dateneingabefelder (Dok-ID 121034).	
M.31	Risikoorientiert HCM-Freitextfelder auswerten	Relevante HCM-Freitextfelder werden regelmäßig auf rechtskonforme Dateneingabe stichprobenartig überprüft.	//Konzept Geschäftsprozess "Regelmäßiges HCM-Audit durchführen" (Dok-ID 729865).	
M.32	Fachliches Löschkonzept implementieren	Das Löschkonzept für das Personalamt behandelt u.a. Aufbewahrungsfristen, Lösch- und Vernichtungsinstrumente sowie übergreifendes Löschvorgehen.	//Konzept Fachliches Löschkonzept „Personal verwalten“ (Dok-ID 133967)	
M.33	Löschkonzept "HCM" implementieren	Anforderungen des fachlichen Löschkonzepts werden in HCM implementiert.	//Konzept Geschäftsprozess "HCM-Daten löschen" (Dok-ID 847855) und HCM-Löschkonzept (Dok-ID 202106081030).	
M.34	Auskunftskonzept "HCM" implementieren	HCM stellt Spezialberichte zur Unterstützung des Auskunftsanspruchs standardmäßig zur Verfügung, die auf die Stadt angepasst und dann genutzt werden.	//Konzept Datenschutz-Auskunftskonzept „HCM“ (Dok-ID 202106081000).	
M.35	HCM-Hersteller Muster liefern lassen	Der HCM-Hersteller bietet Lösungsansätze inkl. Vorlagen/Muster für die Erfülllung von ausgeübten Betroffenenrechten an, die mit genutzt werden.	---	
M.36	An HCM-Kundenaustauschtreffen bedarfsgerecht teilnehmen	An Kundennetzwerktreffen des HCM-Herstellers bedarfsgerecht teilnehmen, um an Produktentwicklung und Anwendungslösungen teilhaben zu können.	---	
M.37	Separates HCM-System verwenden	HCM wird als von anderen Fachanwendungen getrenntes System betrieben.	// Spezifikation HCM (Dok-ID 254189).	
M.38	Selbstdokumentation-Funktionen von HCM nutzen	Haben die relevanten HCM-Komponenten eine Selbstdokumentationsfunktion, so wird diese für die Dokumentation mit genutzt.	---	
M.39	HCM-Eingabehilfen anbieten	HCM-Eingabefelder werden bedarfsgerecht mit Eingabehilfen ausgestattet (z.B. in der Form von Tooltips).	---	
M.40	Automatisierte Plausibiliätschecks umsetzen	HCM-Eingaben werden automatisiert und bedarfsgerecht auch manuell auf Plausibilität geprüft.	//Konzept Geschäftsprozess "Regelmäßiges HCM-Audit durchführen" (Dok-ID 729865).	
M.41	Regelmäßige Datenstandsberichte an Beschäftigte geben	Wichtige HCM-Daten (z.B. Stammdaten) werden regelmäßig für eine Qualitätssicherung an die Beschäftigten als betroffene Personen gegeben.	//Konzept Prozesslandkarte „Personal verwalten“ inkl. Geschäftsprozesse (Dok-ID 394208).	
M.42	(…)	(..)	(…)	