DSFA-Bericht

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

Personal verwalten

[Dokument-ID: 222222]

BayLfD-Stand: 01.05.2022

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 Punkt 5.6 aus der Beschreibung der Verarbeitungstätigkeit „Personal verwalten“ (Anlage A1).		

1.2 Anlagen bzw. Verweise

Nr.	Bezeichnung der Anlage bzw. des Verweises	Quelle und Anmerkung
A1	Beschreibung der Verarbeitungstätigkeit „Personal verwalten“	Dok-ID: 111111
A2	Risikoanalyse zur DSFA „Personal verwalten“	Dok-ID RA353535
A3	Stellungnahme DSB	Dok-ID 458742
A4	Datenkategorien und ihre Dateneingabefelder für „HCM“	Dok-ID 121034
A5	Prozesslandkarte „Personal verwalten“ inkl. Geschäftsprozesse	Dok-ID 394208
A6	Fachliches Löschkonzept „Personal verwalten“	Dok-ID 133967
A7	Fachliches Auskunftskonzept „Personal verwalten“	Dok-ID 133966
A8	Prozesslandkarte „Ausübung eines DSGVO-Betroffenheitsrechts managen“ inkl. Geschäftsprozesse	Dok-ID 412346
A9	Prozesslandkarte „Geschäftsprozesse managen“ inkl. Geschäftsprozesse	Dok-ID 404040
A10	(…)	(..)

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 Prozesslandkarte „Personal verwalten“ zusammen mit allen dazugehörenden und beschriebenen Geschäftsprozessen (Anlage A5).

2.1.2 ■ Welche Zwecke hat die Verarbeitung? ■

Siehe Punkt 6.1 aus der Beschreibung der Verarbeitungstätigkeit „Personal verwalten“ (Anlage A1).

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

Siehe Punkt 6.2 aus der Beschreibung der Verarbeitungstätigkeit „Personal verwalten“ (Anlage A1).

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. Punkt 6.2 aus der Beschreibung der Verarbeitungstätigkeit „Personal verwalten“, Anlage A1).

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 (siehe Punkt 13 aus der Beschreibung der Verarbeitungstätigkeit „Personal verwalten“,

Anlage A1). 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 Punkt 5 und 14 aus der Beschreibung der Verarbeitungstätigkeit „Personal verwalten“ (Anlage A1).

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
D1	Siehe Punkt 7 – D1 bis D9 aus der Beschreibung der Verarbeitungstätigkeit „Personal verwalten“ (Anlage A1)	---

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

Nr.	Bezeichnung der Kategorie betroffener Personen	Anmerkung
P1	Siehe Punkt 8 – P1 aus der Beschreibung der Verarbeitungstätigkeit „Personal verwalten“ (Anlage A1)	---

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 Punkte 9 und 10 aus der Beschreibung der Verarbeitungstätigkeit „Personal verwalten“ (Anlage A1)	---	---

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

Lebenszyklus Daten:

Der Lebenszyklus der Daten richtet sich nach den Geschäftsprozessen des Kernprozesses „Personal verwalten“ (Anlage A5), die die Daten erheben, bereithalten, verwenden und löschen. Zum Löschen siehe fachliches Löschkonzept „Personal verwalten“ (Anlage A6).

Lebenszyklus Prozesse:
Das Geschäftsprozessmanagement, insbesondere die Geschäftsprozesse „Neuen Prozess etablieren“ und „Etablierten Prozess ändern“ bestimmen den Lebenszyklus der betroffenen Prozesse, siehe Prozesslandkarte „Geschäftsprozesse managen“ zusammen mit allen dazugehörigen und beschriebenen Geschäftsprozessen (Anlage A9).

2.2.5 ■ Mit Hilfe welcher Betriebsmittel erfolgt die Datenverarbeitung? ■

Alle genutzten unmittelbaren Betriebsmittel sind unter dem Punkt 13 und alle genutzten mittelbaren Betriebsmittel sind unter dem Punkt 12 der Beschreibung der Verarbeitungstätigkeit „Personal verwalten“ (Anlage A1) festgehalten.

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.

3.1.2 ■ Warum sind die Daten erforderlich? ■

Ausschließlich erforderliche Daten zu verarbeiten und insbesondere keinen Datenüberhang zu erzeugen, ist in der Personalverwaltung von sehr großer Bedeutung. Daher wird bei allen genutzten Betriebsmitteln konsequent darauf geachtet, die Einhaltung der Erforderlichkeit konsequent umzusetzen und geeignet nachzuweisen (siehe z.B. Anlage A4 „Datenkategorien und ihre Dateneingabefelder für ‚HCM'" (HCM)).

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 Punkt 11 aus der Beschreibung der Verarbeitungstätigkeit „Personal verwalten" (Anlage A1) sowie das fachliches Löschkonzept „Personal verwalten" (Anlage A6).

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 Prozesslandkarte „Ausübung eines DSGVO-Betroffenheitsrechts managen“ inklusive der dazugehörenden Geschäftsprozesse (Anlage A8)).

Auskunft:

Die Datenzusammenstellung zur Beantwortung eines Auskunftsersuchens einer betroffenen Person wird auch durch spezielle Standard-Abfragen, welche in den genutzten Betriebsmitteln technisch implementiert sind, unterstützt. Die Möglichkeiten für eine im Einzelfall bedarfsgerechte Datenzusammenstellung ergeben sich aus dem fachlichen Auskunftskonzept „Personal verwalten“ (vgl. Anlage A7).

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:

Im fachlichen Löschkonzept „Personal verwalten“ wird dargestellt (vgl. Anlage A6), wie rechtskonforme Löschanforderungen 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 Berichtigungsansprüche werden u.a. durch Änderungsfunktionen in den genutzten Betriebsmitteln 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.

Einschränkung:

Rechtskonforme Einschränkungsansprüche werden u.a. durch das Zugriffsmanagement der relevanten genutzten Betriebsmittel technisch umgesetzt.

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 „Verfügbarkeit“, „Vertraulichkeit“ und den Teilaspekt „Datenintegrität“ des SDM-Gewährleistungsziels „Integrität“ wurde eine Risikoanalyse mittels einer klassischen Risikomanagement-Methode durchgeführt. Die genaue Durchführung und Ergebnisse sind aus der Anlage A2 „Risikoanalyse zur DSFA ‚Personal verwalten‘“ 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 eine Risikoanalyse anhand der Zielerfüllungsmanagement-Methode durchgeführt, deren Inhalte und Ergebnisse sich aus der Anlage A2 „Risikoanalyse zur DSFA ‚Personal verwalten‘“ 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 das Restrisiko im Bereich der SDM-Gewährleistungsziele zu folgendem Ergebnis:

1. normales Risiko für Verfügbarkeit, Vertraulichkeit und Datenintegrität
2. vertretbare Gefährdung für Datenminimierung, Intervenierbarkeit, Transparenz, Nichtverkettung, Konzeptionseinhaltung und Richtigkeit

Insgesamt ergeben somit die beiden durchgeführten Risikoanalysen für die SDM-Datensicherheitsziele und für die SDM-Schutzbedarfsziele, 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.)

Ausfüllhinweise zum Formular

A) Allgemeines

- Der Begriff „**Daten**“ steht in diesem Formular für „personenbezogene Daten“.
- Der Begriff „**DSFA**“ wird in diesem Formular für „DSFA-Bericht“ verwendet
- Parameter des Einzelfalls werden in **spitzen Klammern** angegeben, z.B. „<Name>“

B) Hinweise zu Einzelpunkten

Punkt	Ausfüllhinweis
1.1.1	Angabe der **an der DSFA beteiligten Personen** mit ihrem Namen und ihrer ausgeübten Rolle(n). Die Anzahl der beteiligten Personen kann je nach Komplexität des betrachteten Verarbeitungsvorgangs erheblich schwanken. Typische Rollen bei der DSFA-Durchführung sind: • Auftraggeber/in (Person, die für die DSFA insgesamt zuständig ist und diese insbesondere auch aktiviert) • Federführung (falls man die DSFA-Durchführung als (Klein-)Projekt versteht, entspricht das Aufgabenprofil der Federführung dem einer Projektleitung) • Vertretung Auftraggeber/in (naheliegend ist, dass ein Vertreter der Fachlichkeit, die den betroffenen Verarbeitungsvorgang gestaltet und beschreibt, diese Rolle wahrnimmt) • Vertretung IT-Bereich (bei einer DSFA werden zumeist auch die klassischen IT-Sicherheitsziele und die Risikolage der betroffenen IT-Infrastruktur als wesentliche Aspekte mit behandelt) • Beratung (naheliegend hierfür ist der Datenschutzbeauftragte) • Review (als Qualitätssicherungsmaßnahme ist es oft sinnvoll, eine in der Materie kompetente Person, die bei der DSFA-Erstellung selbst nicht beteiligt war, die DSFA insbesondere im Hinblick auf Logik, Plausibilität, Verständlichkeit und Vollständigkeit überprüfen zu lassen)
1.1.2	Der mögliche Standard-**Status der DSFA** umfasst auch eine Aktivierung und Deaktivierung. Vor dem Hintergrund der DSFA-Skalierbarkeit wurde der neutrale Begriff „Aktivierung“ gewählt, nicht stärker formalisierte Begriffe wie z.B. „Freigabe“. Eine Deaktivierung kommt etwa in Betracht, wenn die DSFA-Erforderlichkeit wegfällt oder die DSFA durch eine andere DSFA ersetzt wird, bei der die weitere Fortsetzung der DSFA-Versionierung nicht sinnvoll erscheint (z.B. neue DSFA betrachtet ein anderen Zuschnitt des Verarbeitungsvorgangs).
1.1.3	Optionale **Anmerkungen zum festgelegten Status**.
1.1.4	Angabe der **Kontaktdaten** des **Datenschutzbeauftragten** bzw. der Datenschutzbeauftragten: Name, dienstliche Anschrift, E-Mail-Adresse, Telefonnummer
1.2	Der Unterschied zwischen einer **Anlage und einem Verweis** zur DSFA ist, dass die Anlage fest und ausschließlich zur DSFA gehört, während die verwiesenen Dokumente auch in anderen Zusammenhängen verwendet werden (Mehrfachverwendung).
1.3	In der **Änderungshistorie** werden die wesentlichen Änderungen der DSFA nachvollziehbar festgehalten.
1.4	Da die DSFA regelmäßig hinsichtlich eines inzwischen eingetretenen Änderungsbedarfs überprüft werden sollte, kann hier ein **routinemäßiges Überprüfungsdatum** eingetragen werden.
2.1.1	Geben Sie einen kurzen **beschreibenden Überblick über die geplante Verarbeitung**, ihre Art, ihren Umfang, ihren Kontext, ihre Beteiligten u.s.w..
2.1.2	Voraussetzung für eine rechtskonforme Datenverarbeitung ist eine rechtskonforme **Zwecksetzung** (vgl. Art. 5 Abs. 1 Buchst. b DSGVO). Eine sich daraus ergebende Zweckdefinition ist

Punkt	Ausfüllhinweis
	wiederum die Voraussetzung dafür, die erforderlichen Daten und die Angemessenheit der Prozesse einer Verarbeitung bestimmen zu können. Der ausgewiesene Zweck einer Verarbeitung erlaubt eine logische und praktische Abgrenzung bzw. Trennung einer Verarbeitung von anderen Verarbeitungen.
2.1.3	Soweit keine bereichsspezifische gesetzliche Regelung besteht, kommen als **Rechtsgrundlagen** die Tatbestände nach Art. 4 Abs. 1 BayDSG, Art. 6 Abs. 1 DSGVO – bei besonderen Kategorien personenbezogener Daten in Verbindung mit Art. 9 DSGVO und Art. 8 BayDSG - in Betracht.
2.1.4	Beschreiben Sie die Maßnahmen, die sicherstellen sollen, dass die **Einwilligung** der Betroffenen eingeholt wurde.
2.1.5	Listen Sie die für die Verarbeitung neben den Rechtsgrundlagen weiter geltenden **Normen, Standards und Zertifizierungen** auf, die relevant sind oder eingehalten werden müssen, nicht zuletzt die genehmigten Verhaltensregeln (vgl. Art. 40 der DSGVO) und Zertifizierungen zum Datenschutz (vgl. Art. 42 DSGVO).
2.1.6	Nennen und beschreiben Sie die **Zuständigkeiten folgender Beteiligten**: - Verantwortlicher, - mögliche Auftragsverarbeiter, - mögliche gemeinsame Verantwortliche sowie - Datenschutzbeauftragter.
2.1.7	Nennung der einzelnen **Pflichten des Auftragsverarbeiters** gegenüber dem Verantwortlichen bzw. Verweisung auf die bestehende Auftragsverarbeitungsvereinbarung (vgl. Punkt 1.2).
2.1.8	Angabe, ob der Verantwortliche den **Standpunkt der betroffenen Personen** oder ihrer Vertreter zur beabsichtigten Verarbeitung eingeholt hat oder nicht (dann Begründung).
2.2.1	Unter **Kategorien personenbezogener Daten** sind aussagefähige Oberbegriffe zu verstehen, z.B. „Name und Vorname“, „Anschrift“, „Staatsangehörigkeit“. Angaben rein technischer Art (z.B. Feldnummern, Schlüsselnummern usw.) sind nicht erforderlich. Die Bezugnahme auf beigefügte Beschreibungen von Datensätzen ist zulässig, wenn aus diesen die personenbezogenen Daten eindeutig hervorgehen.
2.2.2	Zu beschreiben sind hier **Personengruppen, die von der Verarbeitung betroffen** sind. Beispiel: „Bauantragsteller“ oder „Beihilfeberechtigte und deren Angehörige“. Anzugeben sind auch Personengruppen innerhalb der öffentlichen Stellen, deren Daten verarbeitet werden. Beispiel: „Sachbearbeiter im Bauamt“.
2.2.3	Nach Art. 4 Nr. 9 DSGVO ist **Empfänger** „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht“. Zu den Empfängern gehören daher auch Auftragsverarbeiter sowie Stellen innerhalb der Behörde, denen die Daten weitergegeben werden oder die Zugriff auf die Daten haben. Zu beachten ist ferner die Ausnahmeregelung des Art 4 Nr. 9 Satz 2 DSGVO, wonach Behörden unter bestimmten, in dieser Vorschrift genannten Voraussetzungen nicht als Empfänger gelten.
2.2.4	Präsentieren und beschreiben Sie die Funktionsweise und den Ablauf der Datenverarbeitung (von der Datensammlung bis zur Datenlöschung, sowie die verschiedenen Verarbeitungsschritte, Speicherung, etc.) zum Beispiel mit Hilfe eines Diagramms der **Datenflüsse** (fügen Sie es als Anhang hinzu) und einer detaillierten Beschreibung der **Prozesse**.

Punkt	Ausfüllhinweis
2.2.5	Listen Sie die entsprechenden IT-Systeme und andere **Betriebsmittel** auf (Betriebssysteme, Server, Fachanwendungen, Datenbankverwaltungssysteme, Office-Suites, Netze, Protokolle, Konfigurationen, Papierakten usw.).
3.1.1	Begründung, warum auf Basis der entsprechenden Rechtsgrundlage die **Verarbeitung** personenbezogener Daten **zwingend erforderlich** ist und ein **verhältnismäßiges Mittel** darstellt, den angestrebten Zweck zu erreichen.
3.1.2	Erläutern Sie, warum alle **Daten für die Verarbeitung benötigt** werden.
3.1.3	Beschreiben Sie, welche Schritte unternommen wurden, um die **Qualität der Daten** sicherzustellen.
3.1.4	Nennen Sie die relevanten **Speicherdauern** und erklären Sie, warum die jeweilige Speicherdauer durch gesetzliche Anforderungen, andere Regelungen und/oder Verarbeitungsbedürfnisse gerechtfertigt ist.
3.2.1	Beschreiben Sie, welche **Informationen den betroffenen Personen** auf welche Art und Weise zur Verfügung gestellt werden.
3.2.2	Beschreiben Sie die Maßnahmen, mit denen betroffene Personen **Auskunft** zu ihren verarbeiteten Daten erhalten können (Identifizierung relevanter Daten, Einsichtnahme, Datenübermittlung u.ä.).
3.2.3	Beschreiben Sie die Regelungen, mit denen betroffene Personen ihre Daten **löschen** können.
3.2.4	Beschreiben Sie die Regelungen, mit denen betroffene Personen ihre Daten **berichtigt** lassen können.
3.2.5	Beschreiben Sie die Regelungen, mit denen betroffene Personen die Verarbeitung ihrer Daten **einschränken** und ihr **widersprechen** können.
3.2.6	Beschreiben Sie die Maßnahmen, mit denen betroffene Personen ihr ggf. bestehendes Recht auf **Datenübertragbarkeit** ausüben können.
4.1.1	Zum Nachweis der **Erfüllung der SDM-Datensicherheitsziele** verweisen Sie auf die ausgefüllte Anlage Risikoanalyse Datensicherheitsziele oder stellen eine entsprechende Risikoanalyse dar.
4.1.2	Zum Nachweis der **Erfüllung der SDM-Schutzbedarfsziele** verweisen Sie auf die ausgefüllte Anlage Risikoanalyse Datensicherheitsziele oder stellen eine entsprechende Risikoanalyse dar.
4.1.3	Stellen Sie summarisch dar, **wie die Anforderungen der DSGVO durch die Verarbeitung eingehalten werden**.
4.1.4	Stellen Sie dar, ob und falls ja, wie die **Abstimmung mit der zuständigen Datenschutzaufsichtsbehörde** mit welchen Ergebnissen erfolgt ist.