DSFA-Bericht

Bericht der <Stelle>
zur Datenschutz-Folgenabschätzung (DSFA)
für den Verarbeitungsvorgang

<Bezeichnung VT>

[Dokument-ID: <Dokument-ID>]

BayLfD-Stand: 01.05.2022

Inhalt

1. INFORMATION ZUR DSFA 3

1.1 BETEILIGTE PERSONEN UND STATUS 3
1.2 ANLAGEN BZW. VERWEISE 3
1.3 ÄNDERUNGSHISTORIE 3
1.4 ZEITPUNKT DER NÄCHSTEN ROUTINEMÄßIGEN ÜBERPRÜFUNG 3

2. KONTEXT 4

2.1 ÜBERBLICK 4
2.1.1 ■Welche Verarbeitung ist geplant?■ 4
2.1.2 ■Welche Zwecke hat die Verarbeitung?■ 4
2.1.3 ■Welche Rechtsgrundlagen/Befugnisse für die Verarbeitung gibt es?■ 4
2.1.4 ■Wenn anwendbar, wie wird die Einwilligung der betroffenen Personen eingeholt?■ 4
2.1.5 ■Welche weiteren Normen, Standards und Zertifizierungen gibt es, die für die Verarbeitung relevant sind?■ 4
2.1.6 ■Welche Zuständigkeiten bestehen für die Verarbeitung?■ 4
2.1.7 ■Wie sind die Verpflichtungen der Auftragsverarbeiter klar definiert und vertraglich geregelt?■ 4
2.1.8 ■Wurde der Standpunkt der betroffenen Personen eingeholt?■ 4
2.2 DATEN, PROZESSE UND UNTERSTÜTZUNG 4
2.2.1 ■Welche Kategorien personenbezogener Daten werden verarbeitetet?■ 4
2.2.2 ■Welche Kategorien von Personen sind von der Verarbeitung betroffen?■ 5
2.2.3 ■Welche Empfänger, denen die personenbezogenen Daten offengelegt werden, einschließlich Empfänger in Drittländern oder internationale Organisationen gibt es?■ 5
2.2.4 ■Wie verläuft der Lebenszyklus von Daten und Prozessen?■ 5
2.2.5 ■Mit Hilfe welcher Betriebsmittel erfolgt die Datenverarbeitung?■ 5

3. GRUNDLEGENDE PRINZIPIEN 6

3.1 VERHÄLTNISMÄßIGKEIT UND NOTWENDIGKEIT 6
3.1.1 ■Warum ist die Verarbeitung zwingend erforderlich und ein verhältnismäßiges Mittel, den angestrebten Zweck zu erreichen? ■ 6
3.1.2 ■Warum sind die Daten erforderlich? ■ 6
3.1.3 ■Wie werden die Daten korrekt und auf dem neuesten Stand gehalten? ■ 6
3.1.4 ■Welche Speicherdauer haben die Daten? ■ 6
3.2 UMSETZUNG DER BETROFFENENRECHTE 6
3.2.1 ■Wie werden die betroffenen Personen über die Verarbeitung informiert? ■ 6
3.2.2 ■Wie können Betroffene ihr Recht auf Auskunft ausüben? ■ 6
3.2.3 ■Wie können betroffene Personen ihr Recht auf Löschung ausüben? ■ 6
3.2.4 ■Wie können betroffene Personen ihr Recht auf Berichtigung ausüben? ■ 6
3.2.5 ■Wie können betroffene Personen ihr Recht auf Einschränkung oder Widerspruch der Verarbeitung ausüben? ■ 6
3.2.6 ■Wie können betroffene Personen ihr Recht auf Datenübertragbarkeit ausüben? ■ 6
4. RISIKEN 7
4.1 RISIKOANALYSE 7
4.1.1 ■Wie wird die Erfüllung der SDM-Datensicherheitsziele gewährleistet? ■ 7
4.1.2 ■Wie wird die Erfüllung der SDM-Schutzbedarfsziele gewährleistet? ■ 7
4.1.3 ■Risikogesamtbewertung: Wie wird die Einhaltung der DSGVO gewährleistet? ■ 7
4.1.4 ■Abstimmung mit der zuständigen Aufsichtsbehörde? ■ 7

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
<Name>, <Vorname> [Auftraggeber] <Name>, <Vorname> [Federführung Erstellung] <Name>, <Vorname> [Vertretung Verantwortlicher] <Name>, <Vorname> [Vertretung IT-Bereich] <Name>, <Vorname> [Review] <Name>, <Vorname>, bDSB [Beratung]	☒ in Bearbeitung ☐ Aktiviert ☐ Deaktiviert ☐ Sonstig: <bitte Status angeben>	
1.1.4 Kontaktdaten Datenschutzbeauftragte/r		

1.2 Anlagen bzw. Verweise

Nr.	Bezeichnung der Anlage bzw. des Verweises	Quelle und Anmerkung
A1		
A2	(…)	(…)

1.3 Änderungshistorie

Wann?	Wer?	Was?

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? ■

2.1.2 ■ Welche Zwecke hat die Verarbeitung? ■

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

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

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

2.1.6 ■ Welche Zuständigkeiten bestehen für die Verarbeitung? ■

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

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

2.2 Daten, Prozesse und Unterstützung

2.2.1 ■ Welche Kategorien personenbezogener Daten werden verarbeitetet? ■

Nr.	Bezeichnung der Datenkategorie	Anmerkung
D1		
D2	(…)	(…)

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

Nr.	Bezeichnung der Kategorie betroffener Personen	Anmerkung
P1		
P2	(…)	(…)

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
E1			
E2	(…)	(…)	(…)

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

2.2.5 ■ Mit Hilfe welcher Betriebsmittel erfolgt die Datenverarbeitung? ■

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?** ■

3.1.2 ■ **Warum sind die Daten erforderlich?** ■

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

3.1.4 ■ **Welche Speicherdauer haben die Daten?** ■

3.2 Umsetzung der Betroffenenrechte

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

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

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

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

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

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

4. Risiken

4.1 Risikoanalyse

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

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

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

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

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.