Der Bayerische Landesbeauftragte
für den Datenschutz

# Einführung zu den DSFA-Werkzeugen in Modulform

## (DSFA-Modulhinweise)

**Stand:** 1. Mai 2022

Der Bayerische Landesbeauftragte für den Datenschutz stellt als Hilfsmittel für die Durchführung einer **Datenschutz-Folgenabschätzung** (DSFA) und einer **allgemeinen datenschutzrechtlichen Risikoanalyse** auf seiner Internetpräsenz

**https://www.datenschutz-bayern.de**

in der Rubrik „DSFA" die im Folgenden näher beschriebenen Module bereit. Je **Modul** werden – jeweils in Word- oder Excel- und als PDF-Version – **unausgefüllte Formulare** (Blankovorlagen) sowie diese **Formulare** ausgefüllt **mit fiktiven Anwendungsbeispielen** angeboten.

## Neuerungen im Vergleich zu den Vorversionen der Module

Die Module wurden im Vergleich zu den Vorversionen

- **erweitert**. – Neu hinzugekommen sind etwa die Beschreibungen und Risikoanalysen für die Betriebsmittel Videokonferenzsystem, Bildschirmarbeitsplatz und Telefonsystem.
- **ergänzt**. – In der Beschreibung der Verarbeitungstätigkeit (Modul 1) wurde der Punkt „13. Genutzte unmittelbare Betriebsmittel" als unverzichtbarer Brückenschlag zu den Betriebsmitteln neu eingefügt. Zudem wird nun zu allen Eingabefeldern am Ende ein Ausfüllhinweis gegeben. Die Beschreibung zum Betriebsmittel IT-Personalwirtschaftssystem wurde ebenfalls ergänzt.
- **optimiert**. – Wesentliche Überlegungen und Optimierungspotenziale aus der Praxis, wie sie in der Orientierungshilfe „Risikoanalyse und Datenschutz-Folgenabschätzung – Systematik, Anforderungen, Beispiele" dargestellt werden, finden nunmehr auch in den Modulen als „Good-Practice-Ansätze" Berücksichtigung. Hierzu gehören insbesondere die Unterscheidung zwischen Verarbeitungstätigkeiten und diese unterstützende Betriebsmittel sowie die Skalierbarkeit von datenschutzrechtlichen Risikoanalysen durch die Ausbaustufen „Small", „Medium" und „Large". Die Ausbaustufe „Large" wurde optimiert, indem in einer Tabellenkalkulationsdatei nicht mehr für jedes Gewährleistungsziel ein einzelnes Tabellenblatt, sondern ein separates Tabellenblatt nur noch für jede der beiden angewendeten Methoden (Risikomanagement und Zielerfüllungsmanagement) verwendet wird. Sollte eine Stelle, wie zuvor dargestellt, auch weiterhin je Gewährleistungsziel die relevanten Szenarien darstellen, so berührt dies nur die Form der Darstellung und ist inhaltlich ohne Relevanz.

**Der Bayerische Landesbeauftragte für den Datenschutz**
**80538 München | Wagmüllerstraße 18 | Telefon: +49 89 21 26 72-0**
**poststelle@datenschutz-bayern.de | https://www.datenschutz-bayern.de**

## Fiktives Beispiel als Anschauungsobjekt

Als fiktives Anwendungsbeispiel dient die bayerische Stadt „Fiktivia“. Die frei erfundene Großstadt hat ein Personalamt, das für den städtischen Kernprozess „Personal verwalten“ verantwortlich ist. In der Stadt – und somit auch im Personalamt – ist Geschäftsprozessmanagement durchgehend umgesetzt, das heißt, es gibt unter anderem eine Prozesslandkarte „Personal verwalten“, die alle dazugehörenden Geschäftsprozess unter sich vereint. Von dieser Prozesslandkarte umfasst sind die Geschäftsprozesse „Personal einstellen“, „Arbeitszeit und Anwesenheit managen“, „Entgelt abrechnen“, „Beschäftigungsverhältnis beenden“, „Versorgung managen“ und „Stellen managen“. Nicht umfasst sind hingegen insbesondere die Prozesse „Bewerbungen managen“, „Betriebliches Gesundheitsmanagement durchführen“, „Aus- und Fortbildung managen“, „Disziplinarverfahren durchführen“ und „Beihilfe managen“.

Neben den personalwirtschaftlichen Prozessen gibt es auch Prozesse, die dem Geschäftsprozessmanagement selbst oder dem stadtweiten Datenschutzmanagement dienen.

Dem Geschäftsprozessmanagement dient etwa der übergreifende Geschäftsprozess „Prozess ändern“, der die dauerhafte Übereinstimmung zwischen der konzeptionellen Prozessmodellierung (Soll) und der aktuell gelebten Prozessumsetzung (Ist) gewährleistet.

Dem Datenschutzmanagement dient insbesondere der städtische Geschäftsprozess „Ausübung eines DSGVO-Betroffenheitsrechts managen“. Bei der Stadt koordiniert und stellt eine zentrale Stelle sicher, dass Datenschutz-Anfragen betroffener Personen gegebenenfalls zur Beantwortung an die relevanten Dienststellen weitergegeben und die qualitätsgesicherten Antworten der Dienststellen an die betroffene Person fristgerecht weitergeleitet werden.

Bei der Stadt wird der Kernprozess „Personal verwalten“ schon sehr lange und umfangreich durch das IT-System „HCM-Fiktivia“ (auf dem Markt angebotenes und weit verbreitetes Standardprodukt) unterstützt, das von der Stadt selbst betrieben wird (sog. On-Premises-Systemlösung).

Zudem betreibt die Stadt ein Maßnahmen-Managementsystem. Dieses zentrale IT-System unterstützt neben der Umsetzung der Datenschutz-Schutzmaßnahmen auch die nachhaltige und wirksame Umsetzung von Maßnahmen anderer Bereiche (z. B. Maßnahmen aus den Bereichen Betriebliches Gesundheitsmanagement, Arbeitssicherheit, Informationssicherheit und Antikorruption).

Die Stadt Fiktivia hat als öffentliche Stelle ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Datenschutz-Grundverordnung (DSGVO) erstellt, das auf einer Vorlage des Bayerischen Staatsministeriums des Innern, für Sport und Integration beruht und auch die Beschreibung der Verarbeitungstätigkeit „Personal verwalten“ mit umfasst.

Die für die Stadt Fiktivia zuständige Datenschutz-Aufsichtsbehörde führt in ihrer DSFA-Blacklist nach Art. 35 Abs. 4 DSGVO unter anderem die Fallgruppe „Personalverwaltung“, für die unter bestimmten Voraussetzungen eine DSFA erforderlich ist. Diese Fallgruppe ist definiert als umfangreiche Verarbeitung von Personalaktendaten, die auch vertrauliche oder höchstpersönliche Daten betrifft. Die Verarbeitungstätigkeit „Personal verwalten“ der Stadt

Fiktivia unterfällt dieser Fallgruppe, so dass eine Datenschutz-Folgenabschätzung nach Art. 35 Abs. 4 DSGVO erforderlich ist.

Folgende Module stellen auszugsweise und skizzenhaft Möglichkeiten dar, wie der Nachweis für eine DSFA, für eine allgemeine datenschutzrechtliche Risikoanalyse und für die Erfüllung weiterer damit im Zusammenhang stehender datenschutzrechtlicher Anforderungen grundsätzlich erbracht werden kann. Der Zweck dieser Module ist die Veranschaulichung und eine Methodenkonkretisierung im Rahmen eines Good-Practice-Ansatzes. Der damit verbundene Empfehlungscharakter bezieht sich ausschließlich auf den Aufbau- und die Vernetzungsstruktur der Modulunterlagen, nicht jedoch auf die einzelnen inhaltlichen Ausfüllbeispiele, die regelmäßig nicht vollständig dargestellt sind und nur zur Anschauung dienen. Zudem sind die Modulunterlagen immer zusammen mit den einschlägigen, auf der Homepage des Bayerischen Landesbeauftragten für den Datenschutz veröffentlichten und im Folgenden auch zitierten Orientierungshilfen oder sonstigen Arbeitshilfen zu verstehen und anzuwenden.

Bei der Erstellung der Module wurde darauf geachtet, durch Bausteinbildung und anschließender Vernetzung der Bausteine beispielhaft zu zeigen, wie ein denkbarer effizienter Nachweis implementiert werden kann. Die nachstehende Abbildung zeigt die folgenden fünf Betrachtungsgegenstände:

- **Verarbeitungstätigkeit „Personal verwalten“**, kurz VT „Personal verwalten“, einschließlich DSFA,
- **Betriebsmittel IT-Personalwirtschaftssystem „HCM-Fiktivia“**, kurz BM „HCM“, einschließlich Risikoanalyse,
- **Betriebsmittel Videokonferenzsystem „VK-Fiktivia“**, kurz BM „VKS“, einschließlich Risikoanalyse,
- **Betriebsmittel Bildschirmarbeitsplatz „BAP-Fiktivia“**, kurz BM „BAP“, einschließlich Risikoanalyse und
- **Unterbetriebsmittel Telefonsystem „TKS-Fiktivia“**, kurz BM „TKS“, einschließlich Risikoanalyse

sowie die sechs Module (kurz M1, M2 usw.), welche die fünf Betrachtungsgegenstände behandeln (in blauen Rechtecken).

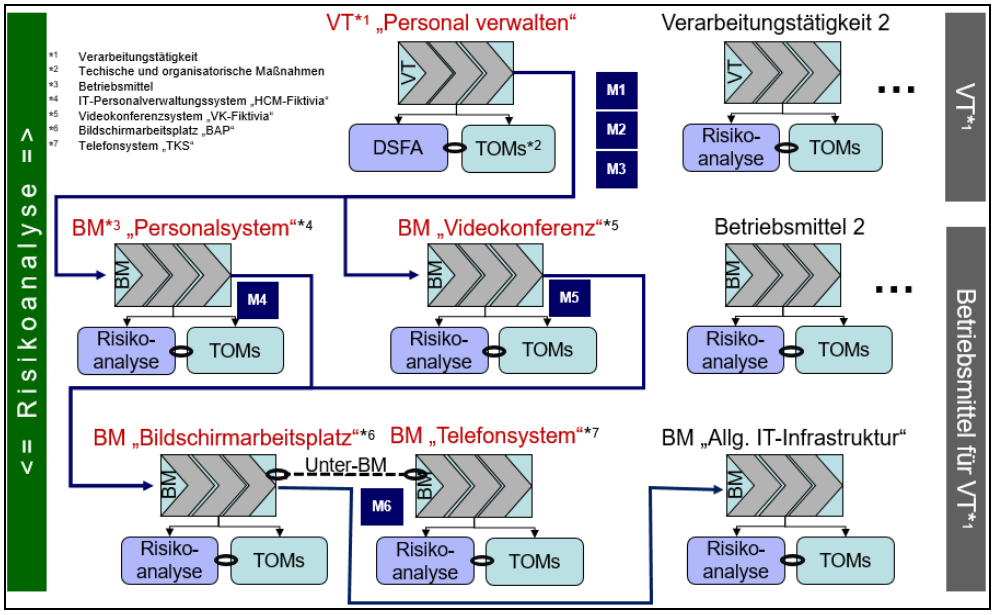


Abbildung: Übersicht der Bausteine und der Module, die diese behandeln

Insgesamt werden somit die folgenden sechs Module als Arbeitshilfen zur Verfügung gestellt. Die dabei genannten Ausbaustufen der Risikoanalysen („Small“, „Medium“ und „Large“) wurden in der einschlägigen Orientierungshilfe bereits dargestellt und definiert.[1]

### Modul 1: Beschreibung einer Verarbeitungstätigkeit[2]

Die Beschreibung orientiert sich an dem veröffentlichten Muster des Bayerischen Staatsministeriums des Innern, für Sport und Integration (StMI), das schon seit Längerem unter

**https://www.stmi.bayern.de/sus/datensicherheit/datenschutz/reform_arbeitshilfen/index.php**

abrufbar ist. Ergänzt wurde das Muster des StMI insbesondere um eine erste Seite, in der wesentliche Metadaten zur Beschreibung festgehalten werden.

### Modul 2: DSFA-Erforderlichkeitsprüfung[3]

Die Frage, ob ein Verarbeitungsvorgang die Durchführung einer DSFA erfordert, wird insbesondere bei der Einführung neuer als auch bei einer wesentlichen Änderung bestehender Verarbeitungsvorgänge relevant. Der Verantwortliche hat seine Prüfung und die Entscheidung dieser Frage – insbesondere bei der Verneinung einer DSFA-Erforderlichkeit – nachzuweisen. Für die vereinfachte Erbringung dieses datenschutzrechtlichen Nachweises dient dieses Formular.

### Modul 3: DSFA-Bericht für eine Verarbeitungstätigkeit[4]

Der DSFA-Bericht und das durch diesen festgelegte Maßnahmenmanagement sind die beiden Hauptbausteine einer DSFA. In diesem Modul wird allerdings nur der DSFA-Bericht mit der DSFA-Risikoanalyse (Ausbaustufe: Large) als Berichtsanlage dargestellt. Das unverzichtbare Maßnahmenmanagement, das die wirksame Umsetzung aller identifizierten

Schutzmaßnahmen gewährleistet, ist in aller Regel ein übergreifender Prozess, der auch für die Umsetzung anderer Maßnahmen dient. [5]

### Modul 4: Betriebsmittel „IT-Personalwirtschaftssystem HCM-Fiktivia“[1]

In diesem Modul wird gezeigt, wie die Beschreibung für ein Betriebsmittel und eine Risikoanalyse (Ausbaustufe: Large) gestaltet werden können.

### Modul 5: Betriebsmittel „Videokonferenzsystem VK-Fiktivia (VKS)“[1]

In diesem Modul wird gezeigt, wie die Beschreibung für ein Betriebsmittel und eine Risikoanalyse der (Ausbaustufe: Medium) aussehen können.

### Modul 6: Betriebsmittel „Bildschirmarbeitsplatz (BAP)“[1]

In diesem Modul wird gezeigt, wie die Beschreibung für eine komplexe Betriebsmittelgruppe sowie ihre mit Zusatzinformationen versehene Risikoanalyse (Ausbaustufe: Large) und ein zu dieser Gruppe gehörendes Unterbetriebsmittel (Telefonsystem) mit seiner Kombination aus Beschreibung und Risikoanalyse (Ausbaustufe „Small“) ausgestaltet werden können.

Wenn Sie Rückfragen oder Verbesserungsvorschläge haben, nutzen Sie bitte das dafür eingerichtete E-Mail-Postfach

**orientierungshilfen@datenschutz-bayern.de.**

1 Siehe Punkt VI.4 in der Orientierungshilfe „Risikoanalyse und Datenschutz-Folgenabschätzung“, die auf https://www.datenschutz-bayern.de in der Rubrik „DSFA“ abrufbar ist.

2 Siehe Arbeitshilfe „Das Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 Datenschutz-Grundverordnung (DSGVO)“, die auf https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018“ abrufbar ist.

3 Die DSFA-Erforderlichkeitsprüfung wird ausführlich in der Orientierungshilfe „Datenschutz-Folgenabschätzung“, die auf https://www.datenschutz-bayern.de in der Rubrik „DSFA“ abrufbar ist, für die bayerischen öffentlichen Stellen erläutert und konkretisiert.

4 Siehe Fn. 1.

5 Siehe Punkt VII.3.c) in der Orientierungshilfe „Risikoanalyse und Datenschutz-Folgenabschätzung“, Fn. 3.