Datenschutzfolgenabschätzung (DSFA)

Strukturiert & einfach nach dem Standard-Datenschutzmodell

am Beispiel eines Bewerberportals

Deckblatt – grundlegende Daten (Stammdaten)

VERARBEITUNG: Art. 4 Nr. 2 DSGVO *(allgemeine Beschreibung)*	Annahme von Bewerbungen via Online-Bewerberportal zu vakanten Stellen in einer Behörde. Sichtung, Auswertung und Durchführung des Bewerbungsverfahrens
Verantwortlicher: Art. 4 Nr. 7 DSGVO	Firma / Behörde Musterdorf Anschrift E-Mail Telefon
Datenschutz-beauftragte* r:	Vorname, Name Anschrift E-Mail
Grundregeln: Art. 5 DSGVO	**<u>Prinzipielle und grundsätzliche Anforderungen an die personenbezogene Datenverarbeitung, die durchgängig zu beachten sind:</u>** **Rechtmäßigkeit** *(Verbot der rechtswidrigen Verarbeitung)* **Verarbeitung nach Treu und Glauben** *(eine auf Zuverlässigkeit, Aufrichtigkeit und Rücksichtnahme beruhende innere und äußere Haltung gegenüber einem Anderen, verkürzt: Fairness)* **Transparenz** *(alle Informationen und Mitteilungen zur Verarbeitung personenbezogener Daten leicht zugänglich und in klarer und einfacher Sprache)* **Zweckbindung** *(Zwecke sollen eindeutig und rechtmäßig zum Zeitpunkt der Erhebung feststehen)* **Datenminimierung** *(Beschränkung auf das notwendige Maß)* **Richtigkeit** *Art. 5 Abs. 1 lit. d DSGVO enthält drei Grundpflichten:* *- Verbot der unrichtigen Erhebung oder Speicherung von Daten (HS1 Var. 1)* *- Gebot der Aktualisierung unrichtig gewordener Daten (HS1 Var. 2)* *- Gebot der Löschung oder Berichtigung unrichtig gespeicherter Daten (HS2)* **Speicherbegrenzung** *(Löschfristen festlegen und überprüfen)* **Integrität und Vertraulichkeit** *(verboten ist eine Verarbeitung ohne angemessene technische oder organisatorische Schutzmaßnahmen - TOM)* **Rechenschaftspflicht** *(Nachweis führen, dass die Grundpflichten nach Art. 5 Abs. 1 DSGVO erfüllt werden)*
Rechtsgrundlage: Art. 6 Abs. 1 DSGVO listet die Bedingungen auf. Die jeweilige Rechtsnorm (Spezialgesetz) ist die Ermächtigungsgrundlage und ist hier zu nennen.	§ 85 Abs. 1 Landesbeamtengesetz (LBG) i.V.m. § 15 Landesdatenschutzgesetz (LDSG): gilt für **<u>alle</u>** Beschäftigten

Die in Art. 35 DSGVO normierte Datenschutzfolgen-abschätzung (DSFA) adressiert die Verantwortlichen und deren Verarbeitungsverfahren. Dabei ist die Verarbeitung so zu beschreiben, dass ein objektiver Beobachter sofort erkennen kann, um welches Verfahren es sich hier handelt.

Neben den vollständigen Daten des Verantwortlichen werden der Vollständigkeit halber auch die Daten des/der Datenschutzbeauftragten erfasst. Immerhin nimmt diese Funktion beratend und überwachend an der Erstellung der DSFA teil (Artt. 35 Abs. 2, 39 Abs. 1 c) DSGVO).

Der Hinweis auf die prägenden Grundsätze in Art. 5 DSGVO mit kurzen einfachen Erläuterungen gibt auch die in Art. 8 Abs. 2 der Charta der Grundrechte der Europäischen Union (GRCh) garantierten Konditionen wieder.

Das Verbotsprinzip mit Erlaubnisvorbehalt erfordert ausnahmslos eine Ermächtigungsgrundlage. Art. 6 Abs. 1 DSGVO listet die Bedingungen für eine rechtmäßige Verarbeitung auf. Daraus folgt, dass einer der Erlaubnistatbestände erfüllt sein muss und exakt dieser jeweilige Erlaubnistatbestand ist zu erfassen.

Schwellwertanalyse

Prüfung, ob eine Datenschutzfolgenabschätzung durchzuführen ist (Frage: Besteht ein **hohes** Risiko für die Rechte und Freiheiten natürlicher Personen?)

	Kategorien von personenbezogenen I Kategorie des personenbezogenen Datums (Betroffenenkategorie)	genaue Bezeichnung des personenbezogenen Datums (Datenkategorie)	Erforderlichkeit Wert	Erforderlichkeit Begründung	Verhältnismäßigkeit	Beteiligte Verant-wortlicher	Beteiligte Dritte (z.B. Auftrags-verarbeiter)	Daten-übermittlung (welche Daten an wen?)	Löschfrist	Art der Verarbeitung
1	Beschäftigte Bewerberdaten	Kontaktdaten Fotos Qualifikationsinformationen bisherige Tätigkeiten Schwerbehinderten-eigenschaft	ja	ohne Bewerberdaten kein Bewerbungs-verfahren resp. anschl. keine Begründung eines Arbeits-verhältnisses	Praxis ist es, Bewerbungen elektronisch zu versenden. Bewerbern werden dadurch Transfer und Druckkosten erspart. Bewerbungen in Papierform sind weiterhin zugelassen.	Fachdienst Personal	RZ Musterdorf	entfällt	6 Monate nach Beendigung des Bewerbungs-verfahrens	Der / Die Bewerber* in gibt die Bewerberdaten im Bewerberportal selbst ein. Nach Abschluss der Eingaben erfolgt der Versand an den zuständigen Fachdienst Personal, der die tägliche Sichtung und das administrative Verfahren organisiert hat. Die Daten werden ausschließlich auf dem Server des Empfängers gespeichert. Der Zugriff erfolgt nur durch autorisierte Beschäftigte nach einem Rollen-und Rechtekonzept. Die Offenlegung der Daten findet dem Zweck entsprechend gegenüber dem Auswahlgremium statt. Die Daten werden nach Zweckerfüllung unter Beachtung der gesetzlichen Fristen gelöscht.

Umfang der Verarbeitung:	im Verhältnis zur Beschäftigtenzahl eher gering
Umstände der Verarbeitung:	Alternative zu Bewerbungen in Papierform;
Zweck der Verarbeitung:	Begründung eines Beschäftigungsverhältnisses
Schnittstellen	Die Daten werden vom Bewerberportal automatisiert per Mail an die empfangende Behörde verschickt.
Schutzklasse	hoch

A	Bewertungskriterien	Wert	Erläuterung
1	Bewerten oder Einstufen (*Erstellen von Profilen und Prognosen; Nutzung von Datenbeständen mittels Algorithmen*)	**nein**	
2	Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung (*hier trifft die Maschine die Entscheidung*)	**nein**	
3	Systematische Überwachung *(weiträumige Überwachung öffentlich zugänglicher Bereiche, die planmäßig und umfangreich erfolgt, z.B. automatisierte Kennzeichenerfassung)*	**nein**	
4	Vertrauliche oder höchst persönliche (sensible) Daten (*siehe Art. 9: z.B. biometrische Daten oder Gesundheitsdaten* *und 10 DSGVO: personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten*)	**ja**	Es wird die Schwerbehinderteneigenschaft - und damit ein Gesundheitsdatum- abgefragt. Gemäß AGG besteht ein Recht auf Teilnahme an Vorstellungsgesprächen für schwerbehinderte Bewerber/innen
5	Datenverarbeitung in großem Umfang	**nein**	
6	Abgleichen oder Zusammenführen von Datensätzen (*Daten aus unterschiedlichen Zwecken oder Verantwortlichen*)	**nein**	
7	Daten zu schutzbedürftigen Betroffenen (*es besteht ein Machtungleichgewicht; d.h. die betroffenen Personen sind auf die Verarbeitung angewiesen, z.B. Kinder, Arbeitnehmern, Patienten etc.*)	**ja**	Im Verhältnis Arbeitgeber / Arbeitnehmer besteht ein Machungleichgewicht. Das trifft auch auf Bewerber/innen zu.
8	Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen (*z.B. Fingerprint, Gesichtserkennung*)	**nein**	
9	Fälle, in denen die Verarbeitung an sich „die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrages hindert“ *(Beispiel: Bank nutzt Daten der Kreditauskunftei zur Kreditentscheidung).*	**nein**	
10	Aufsichtsbehördliche Positiv-Liste gemäß Art. 35 Abs. 4 DSGVO = Liste der Verarbeitungstätigkeiten, für die eine DFSA durchzuführen ist (Pflichtliste).	**nein**	Begleittext

B. Ergebnis:

Aufgrund der vorstehend festgestellten Kriterien ist von einem hohen Risiko auszugehen. Es ist eine Datenschutzfolgenabschätzung durchzuführen.

Vertraulichkeit		**Nichtverkettung**
Die Offenbarung von personenbezogenen Daten an Unbefugte ist zu vermeiden. Das gilt ebenso für die Technik als auch für andere Organisationseinheiten.		Personenbezogene Daten dürfen nicht zusammengeführt / verkettet werden, es sei denn, die Verarbeitung erfolgt innerhalb des Zweckes für die sie erhoben wurden.
Maßnahmen der Zutritts-, Zugangs- und Zugriffskontrolle sind hierfür geeignet. Ebenso die Pseudonymisierung, sofern der „Schlüssel“ nur besonders Befugten zugänglich ist.		**Baustein:** 50 Trennung
Die Trennungskontrolle ist ebenso dem Gewährleistungsziel Nichtverkettung zuzuordnen.		
Bausteine:		
11 Aufbewahrung		
50 Trennung		
Integrität		**Transparenz**
Prozesse und Systeme müssen innerhalb der jeweiligen Vorgaben verlaufen. Des Weiteren müssen die personenbezogenen Daten unversehrt, vollständig und aktuell bleiben.		Sowohl Betroffene als auch Verantwortliche und Prüfinstanzen müssen erkennen können, welche Daten für welchen Zweck bei einer Verarbeitungstätigkeit verarbeitet werden, welche Systeme und Prozesse verwendet werden, wohin die Daten fließen und wer die rechtliche Verantwortung in den jeweiligen Phasen trägt.
Weitergabe- und Eingabekontrolle werden dem gerecht.		**Bausteine:**
Bausteine:		11 Aufbewahrung
11 Aufbewahrung		41 Planung & Spezifikation
50 Trennung		42 Dokumentation
		43 Protokollierung
Verfügbarkeit		**Intervenierbarkeit**
Personenbezogene Daten müssen zur Verfügung stehen und ordnungsgemäß im vorgesehenen Prozess verwendet werden können.		Sicherstellung, dass die Betroffenen die Ihnen garantierten Rechte jederzeit wirksam wahrnehmen können. Das erfordert die Möglichkeit des jederzeitigen Eingriffs in die Datenverarbeitung.
Die Maßnahmen zur Verfügbarkeit und Belastbarkeit sowie die rasche Wiederherstellbarkeit sind hierfür geeignet.		**Baustein:** 11 Aufbewahrung

Die TOM "Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit.d DSGVO; Art. 25 Abs. 1 DSGVO)" und Rechenschaftspflicht, genehmigte Verhaltensregeln, Zertifizierung (Art. 32 Abs. 3 DSGVO) sind übergreifend und gehen im SDM auf, so z.B.

- Datenschutzmanagement: Hausregeln, Organisation von Prozessen (**Baustein:** 80 Datenschutzmanagement)
- Datenschutzfreundliche Voreinstellung: Adressat ist der Verantwortliche, der seine Technik auf dem neuesten Stand halten muss.
- Auftragskontrolle: klare Weisungen an den Auftragsverarbeiter, der in der Regel die Technik stellt.
- Die DSFA resp. das Protokoll dazu dient der Rechenschaftspflicht.

Risikoermittlung

Schutzziel	Komponente Die Kommentarfelder geben Anhaltspunkte	Risiko-quellen	Risiken / mögliche Schäden Wodurch wird das Schutzziel gefährdet?	Ereignisse (die zu einer Verwirklichung des Schadens führen können)	Eintrittswahrscheinlichkeit		Schwere des möglichen	
					Einstufung	Begründung	Einstufung	Erläuterung
Datenminierung	Oberziel							
Verfügbarkeit	Daten							
	Systeme							
	Prozesse							
Integrität	Daten			belegt mit Auswahlfeldern				
	Systeme							
	Prozesse							
Vertraulichkeit	Daten							
	Systeme							
	Prozesse							
Transparenz	Daten							
	Systeme							
	Prozesse							
Nichtverkettbarkeit	Daten							
	Systeme							
	Prozesse							
Intervenierbarkeit	Daten							
	Systeme							
	Prozesse							

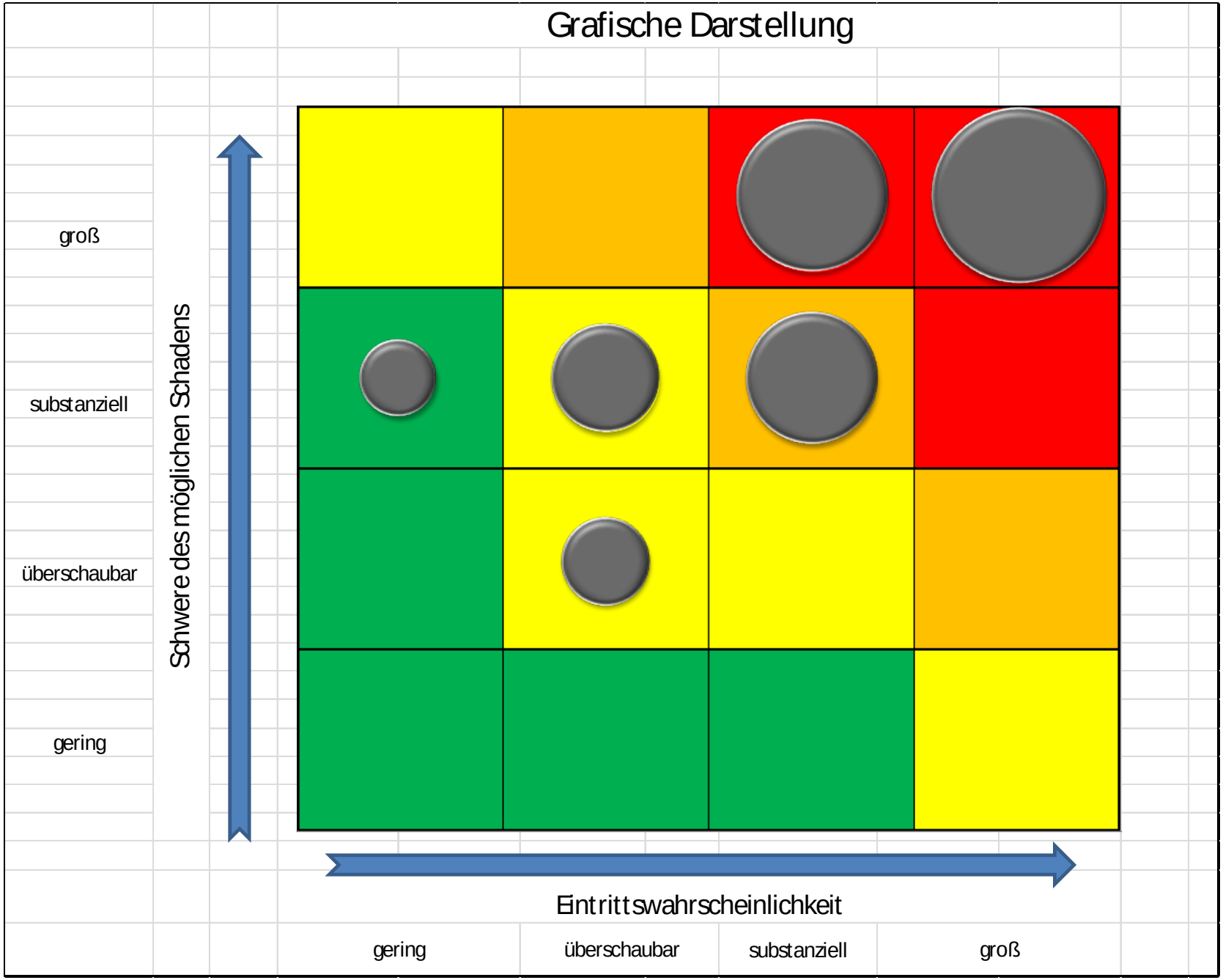
Maßnahmen_Soll-Bestimmung

	Datenübernahme aus Risikoermittlung									
Schutzziel	Risikoquellen	Risiken / mögliche Schäden Wodurch wird das Schutzziel gefährdet?	Ereignisse (die zu einer Verwirklichung des Schadens führen können)	Komponente Die Kommentarfelder geben Anhaltspunkte	Maßnahmen zur Eindämmung des Risikos *(? =Beispiele im Kommentarfeld aus SDM)* Die Bausteine zum Standard-Datenschutzmodell finden Sie hier: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/	Eintrittswahrscheinlichkeit		Schwere des möglichen Schadens		Restrisiko = Produktwert
						Einstufung	Begründung	Einstufung	Erläuterung	
					?					

Risikoermittlung (Status quo ohne Maßnahmen)

Schutzziel	Komponente Die Kommentarfelder geben Anhaltspunkte	Risikoquellen	Risiken / mögliche Schäden Wodurch wird das Schutzziel gefährdet?	Ereignisse (die zu einer Verwirklichung des Schadens führen können)	Eintrittswahrscheinlichkeit		Schwere des möglichen Schadens	
					Einstufung	Begründung	Einstufung	Erläuterung
Datenminierung	**Oberziel**	Verantwortlicher	Verarbeitung nicht vorhergesehener Daten	Der/Die Bewerber/in übermittelt mehr Daten als erforderlich und es erfolgt weder Rückgabe noch Löschung	**überschaubar**	Der/Die Bewerber/in möchte sich besonders gut präsentieren und reichert die Bewerbung mit Zusatzdaten an.	**überschaubar**	Nicht erforderliche Daten könnten mit einbezogen werden und ggf. zu einem anderen Ergebnis führen.
Verfügbarkeit	Daten	Verantwortlicher	wirtschaftliche oder gesellschaftliche Nachteile	Bewerbung kommt nicht oder nicht fristgerecht an	**überschaubar**	Datenverluste sind eher selten	**substanziell**	Die Nichtteilnahme am Bewerbungsverfahren nimmt die Chance auf Einstellung
	Systeme	Auftragsverarbeiter	wirtschaftliche oder gesellschaftliche Nachteile	Ausfall der Systeme	**überschaubar**	Im Regelbetrieb sind Ausfälle eher selten	**substanziell**	
	Prozesse	Verantwortlicher	wirtschaftliche oder gesellschaftliche Nachteile	Bewerbungsunterlagen kommen nicht rechtzeitig beim Verantwortlichen an, weil Zuständigkeiten ungeklärt sind	**geringfügig**	bereits über die Aufgabenzuweisung sind Zuständigkeiten erkennbar	**substanziell**	
Integrität	Daten	Verantwortlicher	wirtschaftliche oder gesellschaftliche Nachteile	Löschung oder Beschädigung der eingegangenen Bewerbungsunterlagen; fehlerhafte Weiterleitung	**substanziell**	menschliches Fehlverhalten bei hoher Arbeitsbelastung	**substanziell**	Die Nichtteilnahme am Bewerbungsverfahren nimmt die Chance auf Einstellung
	Systeme	Auftragsverarbeiter	wirtschaftliche oder gesellschaftliche Nachteile	unsicherer Versand	**groß**	fehlender Schutz resp. Verschlüsselung	**groß**	
	Prozesse	Verantwortlicher	wirtschaftliche oder gesellschaftliche Nachteile	Umgang mit E-Mails nicht oder nicht ausreichend geregelt	**überschaubar**	Der Umgang mit Posteingängen ist fehlerträchtig	**substanziell**	
Vertraulichkeit	Daten	Verantwortlicher	Unbefugte Offenlegung von und Zugang zu Daten	Offenbarung der Bewerbungsbemühungen kann das Verfahren resp. bestehende Arbeitsverhältnis beeinflussen.	**überschaubar**	mangelhafte Verschwiegenheit	**substanziell**	Kein faires Verfahren und/oder Nachteile im bestehenden Arbeitsverhältnis
	Systeme	Auftragsverarbeiter	Unbefugte Offenlegung von und Zugang zu Daten	fehlende Kontrollmechanismen; mangelhafte Mandantentrennung	**groß**	Der Zugang zum Netz hat weitreichende Folgen	**groß**	
	Prozesse	Verantwortlicher	Unbefugte Offenlegung von und Zugang zu Daten	Belehrung zur Verschwiegenheit und Vertraulichkeit zur Datenverarbeitung sind unterblieben	**überschaubar**	gesunder Menschenverstand lässt auch ohne Belehrung erwarten, dass ein vertraulicher Umgang erfolgt	**substanziell**	
Transparenz	Daten	Verantwortlicher	Für den Betroffenen intransparente Verarbeitung	Umfang der Datenverarbeitung sowie Betroffenenrechte sind nicht erkennbar	**geringfügig**	Die Anforderungen an den/die Bewerber/in sind regelmäßig in der Ausschreibung beschrieben: Betroffenenrechte sind gesetzlich verankert.	**substanziell**	Etwaige Benachteiligungen werden nicht bekannt, folglich keine bzw. erschwerte Abwehr möglich.
	Systeme	Auftragsverarbeiter	Für den Betroffenen intransparente Verarbeitung	keine ausreichende Protokollierung	**überschaubar**	Überprüfung ist nur mit hohem Aufwand möglich	**substanziell**	
	Prozesse	Verantwortlicher	Für den Betroffenen intransparente Verarbeitung	Protokollierung und Betroffenenrechte sind nicht ausreichend geregelt	**überschaubar**	Eine Zuordnung zum jeweilig HandelInden ist erschwert, so dass ggf. Aktionen nicht nachvollzogen werden können.	**substanziell**	
Nichtverkettbarkeit	Daten	Verantwortlicher	Unbefugte oder unrechtmäßige Verarbeitung	Die Bewerbungsunterlagen werden auch zu anderen Zwecken verwendet	**substanziell**	fehlende Kenntnis zum Zweck und Fahrlässigkeit	**groß**	unrechtmäßige Datenverarbeitung, folglich Grundrechtsverletzung
	Systeme	Auftragsverarbeiter	Unbefugte oder unrechtmäßige Verarbeitung	keine Trennung von Datenbeständen; ungeordnete Schnittstellen	**substanziell**	nicht ausreichende Kenntnis der datenschutzrechtlichen Notwendigkeiten	**groß**	
	Prozesse	Verantwortlicher	Unbefugte oder unrechtmäßige Verarbeitung	keine hinreichende Bestimmung des Verwendungszwecks	**substanziell**	Schnelligkeit vor Sorgfalt	**groß**	
Intervenierbarkeit	Daten	Verantwortlicher	Verweigerung der Betroffenenrechte	ungeordnete Datenablage	**substanziell**	Bearbeitung durch verschiedene Sachbearbeiter kann zu unterschiedlicher Ablage führen	**groß**	werden Daten nicht aufgefunden, können Betroffenenrechte nicht oder nicht vollständig wahrgenommen werden
	Systeme	Auftragsverarbeiter	Verweigerung der Betroffenenrechte	fehlende Funktionalitäten	**substanziell**	unterschiedliche Daten / Datenformate werden nicht geordnet resp. unübersichtlich abgelegt	**substanziell**	die Wahrnehmung der Betroffenenrechte wird erheblich erschwert
	Prozesse	Verantwortlicher	Verweigerung der Betroffenenrechte	fehlende Anweisungen zu Ordnerstrukturen	**substanziell**	fehlendes resp. unvollständiges Datenschutzmanagement	**groß**	siehe zu Daten

Grafische Darstellung

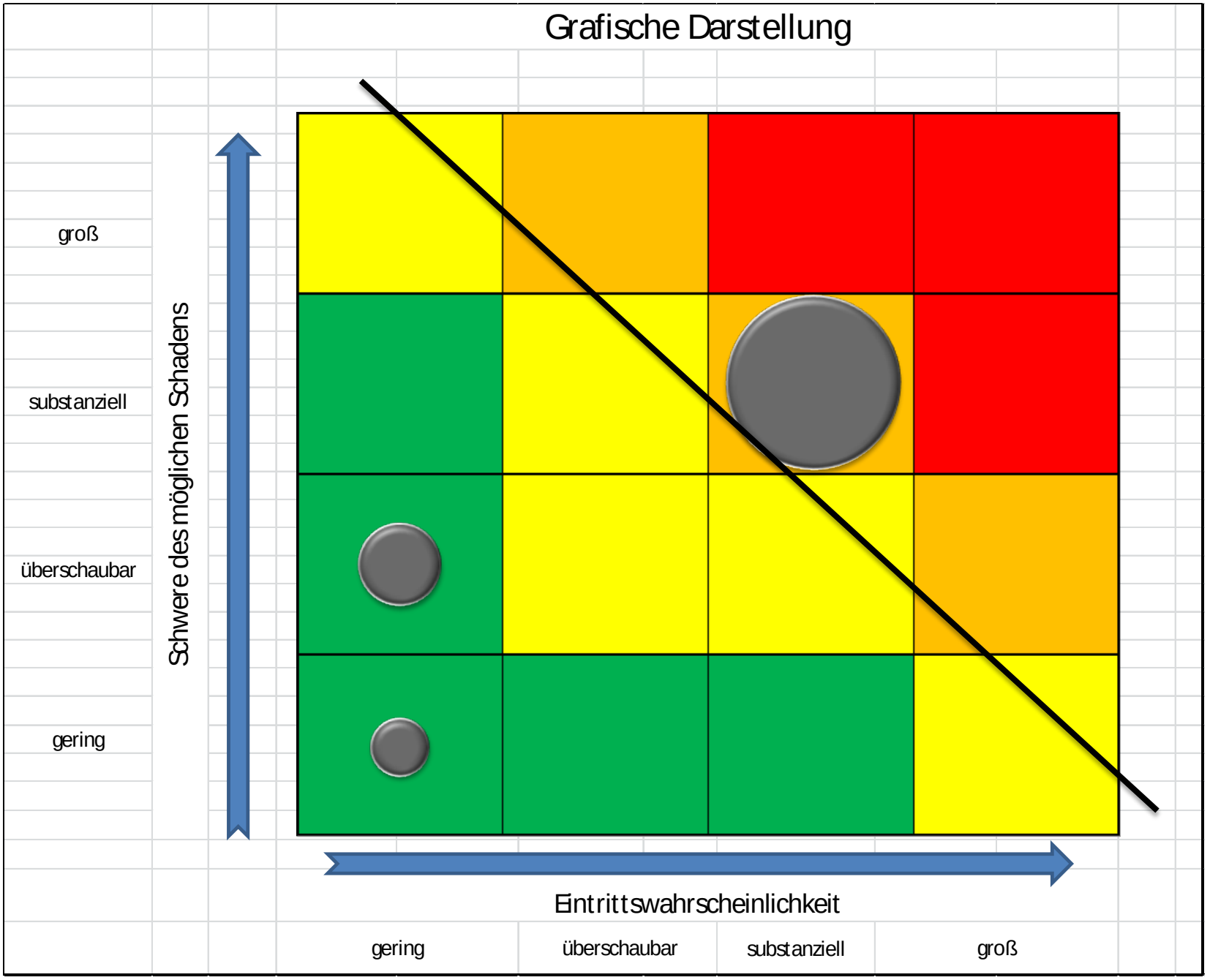


Maßnahmen_Soll-Bestimmung

Datenübernahme aus Risikoermittlung

Schutzziel	Risikoquellen	Risiken / mögliche Schäden Wodurch wird das Schutzziel gefährdet?	Ereignisse (die zu einer Verwirklichung des Schadens führen können)	Komponente Die Kommentarfelder geben Anhaltspunkte	Maßnahmen zur Eindämmung des Risikos *(? =Beispiele im Kommentarfeld aus SDM)* Die Bausteine zum Standard-Datenschutzmodell finden Sie hier: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/_		Eintrittswahrscheinlichkeit		Schwere des möglichen Schadens		Restrisiko = Produktwert
							Einstufung	Begründung	Einstufung	Erläuterung	
Datenminierung	Verantwortlicher	wirtschaftliche oder gesellschaftliche Nachteile	Bewerbung kommt nicht oder nicht fristgerecht an	Oberziel	Der Bewerberfragenkatalog ist so aufgestellt, dass ausschließlich zur Aufgabenerfüllung erforderliche Daten erhoben werden. Ohne diese Daten ist eine Aufgabenerledigung nicht möglich. Eine Löschroutine ist installiert (6 Monate nach Ende Bewerbungsverfahren)	?	geringfügig	Abweichungen vom Fragenkatalog können nicht gänzlich ausgeschlossen werden, sind aber insgesamt eher selten.	geringfügig	Sollte der/die Bewerberin mehr Daten als gefordert liefert, so geschieht das selbstbestimmt.	1
Verfügbarkeit	Verantwortlicher	wirtschaftliche oder gesellschaftliche Nachteile	Bewerbung kommt nicht oder nicht fristgerecht an	Daten	Das Bewerberportal wird durch RZ Musterdorf zur Verfügung gestellt. Dort gehen die Bewerbungen ein. Im Portal wird darauf hingewiesen, dass nach Erhalt der Bewerbung eine Bestätigungsmail gesendet wird, so dass das Nichtankommen erkennbar wird.		geringfügig	Bewerber hat eine Gegenkontrolle und kann ggf. reagieren.	geringfügig	Auch Bewerbungen im Papierform können alternativ gewählt werden.	1
	Auftragsverarbeiter	wirtschaftliche oder gesellschaftliche Nachteile	Ausfall der Systeme	Systeme	Der Vertrag zur Auftragsverarbeiter verpflichtet das Rechenzentrum, eine hohe Verfügbarkeit sicherzustellen und ausreichende Redundanzen zu gewährleisten. Desweiteren sind Schutzmaßnahmen zu treffen, die auf dem aktuellen Stand sein müssen.	?	geringfügig	Der laufende Betrieb zeigt die Umsetzung der diesbezüglichen Weisungen	überschaubar	Sollte es in Einzelfällen zu einer Nichtteilnahme wegen einer durch den Auftragsverarbeiters zu vertretenen unterbliebenen Übermittlung der Bewerbungsunterlagen kommen, besteht ein Entschädigungsanspruch.	2
	Verantwortlicher	wirtschaftliche oder gesellschaftliche Nachteile	Bewerbungsunterlagen kommen nicht rechtzeitig beim Verantwortlichen an, weil Zuständigkeiten ungeklärt sind	Prozesse	Der Anbieter gewährleistet eine Rückmeldung über das Eingehen der Bewerbung. Dem Rechenzentrum wurden die technischen und organisatorischen Maßnahmen vorgegeben.		geringfügig	Die vorgesehenen technischen und organisatorischen Maßnahmen entsprechend dem Stand der Technik.	überschaubar	Etwaige Behinderungen für den/die Bewerber/in sind durch die getroffenen eingedämmt.	2
Integrität	Verantwortlicher	wirtschaftliche oder gesellschaftliche Nachteile	Löschung oder Beschädigung der eingegangenen Bewerbungsunterlagen; fehlerhafte Weiterleitung	Daten	Über das Rollen- und Rechtekonzept ist der Eingang der Bewerbungen auf den berechtigten Personenkreis im Fachdienst Personal beschränkt.		geringfügig	Der Kreis der Zugriffsberechtigten ist beschränkt.	überschaubar	Sollte es in Einzelfällen zu einer Nichtteilnahme wegen eines durch den Verantwortlichen zu vertretenen Verlustes der Bewerbungsunterlagen kommen, besteht ein Entschädigungsanspruch.	2
	Auftragsverarbeiter	wirtschaftliche oder gesellschaftliche Nachteile	unsicherer Versand	Systeme	An den Anbieter "Mustermann" ist die Forderung gestellt, eine Ende-zu-Ende-Verschlüsselung zu gewährleisten. Das wurde auch zugesagt. Die Umsetzung ist noch offen.	?	substanziell	Die Umsetzung der Maßnahme ist offen, was die Eintrittswahrscheinlichkeit erhöht.	substanziell	Die Nichtteilnahme am Bewerbungsverfahren bzw. die Manipulation von Bewerberdaten führt zu einer Benachteiligung.	9
	Verantwortlicher	wirtschaftliche oder gesellschaftliche Nachteile	Umgang mit E-Mails nicht oder nicht ausreichend geregelt	Prozesse	Der Umgang mit dem elektronischen Posteingang ist allen an der Verarbeitung Beteiligten bekannt und wird eingehalten.		geringfügig	Die Nichtbeachtung von organisatorischen Vorgaben stellt ein Dienstvergehen dar.	geringfügig	Eine Pflichtverletzung löst einen Entschädigungsanspruch aus.	1
Vertraulichkeit	Verantwortlicher	Unbefugte Offenlegung von und Zugang zu Daten	Offenbarung der Bewerbungsbemühungen kann das Verfahren resp.	Daten	Es bestehen Diskretionsvorgaben, die im Rahmen der Vertraulichkeitsverpflichtung jedem Beschäftigten bekannt sind.		geringfügig	Die Nichtbeachtung von organisatorischen Vorgaben stellt ein Dienstvergehen dar.	überschaubar	Die Offenbarung von Bewerbungsbemühungen muss nicht zwingend zu einer Benachteiligung führen.	2
	Auftragsverarbeiter	Unbefugte Offenlegung von und Zugang zu Daten	fehlende Kontrollmechanismen; mangelhafte	Systeme	Mit dem Anbieter ist vereinbart, dass eine Mandantentrennung zwingend erfolgt.	?	geringfügig	Im normalen Betrieb sind keine Abweichungen zu erwarten.	überschaubar	Die Offenbarung von Bewerbungsbemühungen muss nicht zwingend zu einer Benachteiligung führen.	2
	Verantwortlicher	Unbefugte Offenlegung von und Zugang zu Daten	Belehrung zur Verschwiegenheit und Vertraulichkeit zur Datenverarbeitung sind unterblieben	Prozesse	Es ist Einstellungsstandard, jede/n neue/n Beschäftigte/n umfänglich über die Hausregeln zu informieren und zur Vertraulichkeit und Verschwiegenheit zu verpflichten.		geringfügig	Die Nichtbeachtung von organisatorischen Vorgaben stellt ein Dienstvergehen dar.	überschaubar	Die Offenbarung von Bewerbungsbemühungen muss nicht zwingend zu einer Benachteiligung führen.	2
Transparenz	Verantwortlicher	Für den Betroffenen intransparente Verarbeitung	Umfang der Datenverarbeitung sowie Betroffenenrechte sind nicht erkennbar	Daten	Die Hinweise im Bewerberportal befinden sich im Zugangsbereich und auf der Karriereseite der Behörde.		geringfügig	Die Informationslage ist gut.	geringfügig	Es liegt in der Selbstverantwortung der Bewerberin/des Bewerbers die Informationen zu lesen.	1
	Auftragsverarbeiter	Für den Betroffenen intransparente Verarbeitung	keine ausreichende Protokollierung	Systeme	Sowohl mit dem Anbieter als auch mit dem Rechenzentrum sind Protokollierungspflichten vereinbart.	?	geringfügig	Nach dem Stand der Technik ist eine durchgängige Protokollierung zu erwarten.	geringfügig	Backups lassen eine Rekonstruktion zu.	1
	Verantwortlicher	Für den Betroffenen intransparente Verarbeitung	Protokollierung und Betroffenenrechte sind nicht ausreichend geregelt	Prozesse	Sowohl Protokollierung als auch Betroffenenrechte sind technisch und organisatorisch geregelt (Vertrag zur Auftragsverarbeitung sowie Datenschutzmanagement)		geringfügig	Die TOM sind aufgestellt und jedem/jeder Beschäftigten bekannt gemacht.	geringfügig	Die Datenkategorien sind durch eigenen Eingaben bekannt. Die Betroffenenrechte sind gesetzlich geregelt und darüber erkennbar.	1
Nichtverkettbarkeit	Verantwortlicher	Unbefugte oder unrechtmäßige Verarbeitung	Die Bewerbungsunterlagen werden auch zu anderen Zwecken verwendet	Daten	Über das Rollen- und Rechtekonzept erhalten nur beteiligte Fachdienste Kenntnis über die Daten des Bewerbers/der Bewerberin. Die Zweckgebundenheit der Daten ist allen Beteiligten bekannt.		geringfügig	Die Mitarbeitersensibilisierung zur Zweckgebundenheit erfolgt kontinuierlich.	geringfügig	Unbefugte Zweckänderung würde eine Rechtswidrigkeit darstellen und zu einer Nichtverwertbarkeit der Daten führen.	1
	Auftragsverarbeiter	Unbefugte oder unrechtmäßige Verarbeitung	keine Trennung von Datenbeständen; ungeordnete Schnittstellen	Systeme	Mandantentrennung und Schnittstellen sind geregelt.	?	geringfügig	Im normalen Betrieb sind keine Abweichungen zu erwarten.	geringfügig	Unbefugte Zweckänderung würde eine Rechtswidrigkeit darstellen und zu einer Nichtverwertbarkeit der Daten führen.	1
	Verantwortlicher	Unbefugte oder unrechtmäßige Verarbeitung	keine hinreichende Bestimmung des Verwendungszwecks	Prozesse	Die Bewerberprozesse sind strukturiert und für jedem Beteiligten bekannt.		geringfügig	Die Nichtbeachtung von organisatorischen Vorgaben stellt ein Dienstvergehen dar.	geringfügig	Unbefugte Zweckänderung würde eine Rechtswidrigkeit darstellen und zu einer Nichtverwertbarkeit der Daten führen.	1
Intervenierbarkeit	Verantwortlicher	Verweigerung der Betroffenenrechte	ungeordnete Datenablage	Daten	Für jedes Bewerbungsverfahren wird ein eigener Ordner angelegt.		geringfügig	Im Tagesgeschäft ist von einer Beachtung der Vorgaben auszugehen.	geringfügig	Backups lassen eine Rekonstruktion zu.	1
	Auftragsverarbeiter	Verweigerung der Betroffenenrechte	fehlende Funktionalitäten	Systeme	Sperrung, Löschung, Berichtigung und ggf. Darstellungen der Betroffenen sind technisch möglich.	?	geringfügig	Die technischen Maßnahmen sind ausreichend berücksichtigt.	geringfügig	Löschroutine im 6-Monats-Intervall, so dass in der Zwischenzeit genügend Raum für Invervention besteht.	1
	Verantwortlicher	Verweigerung der Betroffenenrechte	fehlende Anweisungen zu Ordnerstrukturen	Prozesse	Der Bewerberprozess ist so gestaltet, dass jederzeit ein Auffinden der Daten sowie die Wahrnehmung der Betroffenenrechte möglich ist.		geringfügig	Der Prozess ist schlüssig vorgegeben.	geringfügig	Backups unterstützen das Auffinden.	1

Grafische Darstellung



DSFA-Bericht

Verarbeitung:
Annahme von Bewerbungen via Online-Bewerberportal zu vakanten Stellen in einer Behörde.
Sichtung, Auswertung und Durchführung des Bewerbungsverfahrens

Verantwortlicher:
Firma / Behörde Musterdorf
Anschrift
E-Mail
Telefon

Datenschutzbeauftrage*r:
Vorname, Name
Anschrift
E-Mail
Telefon

Kategorien von personenbezogenen Daten	genaue Bezeichnung des personenbezogenen Datums (Datenkategorie)	Erforderlichkeit		Verhältnismäßigkeit	Beteiligte		Daten-übermittlung (welche Daten an wen?)	Löschfrist	Art der Verarbeitung
Kategorie des personenbezogenen Datums (Betroffenenkategorie)		Wert	Begründung		Verant-wortlicher	Dritte (z.B. Auftrags-verarbeiter)			
Beschäftigte Bewerberdaten	Kontaktdaten Fotos Qualifikationsinformationen bisherige Tätigkeiten Schwerbehinderten-eigenschaft	ja	ohne Bewerberdaten kein Bewerbungs-verfahren resp. anschl. keine Begründung eines Arbeits-verhältnisses	Praxis ist es, Bewerbungen elektronisch zu versenden. Bewerbern werden dadurch Transfer und Druckkosten erspart. Bewerbungen in Papierform sind weiterhin zugelassen.	Fachdienst Personal	RZ Musterdorf	entfällt	6 Monate nach Beendigung des Bewerbungs-verfahrens	Der / Die Bewerber*in gibt die Bewerberdaten im Bewerberportal selbst ein. Nach Abschluss der Eingaben erfolgt der Versand an den zuständigen Fachdienst Personal, der die tägliche Sichtung und das administrative Verfahren organisiert hat. Die Daten werden ausschließlich auf dem Server des Empfängers gespeichert. Der Zugriff erfolgt nur durch autorisierte Beschäftigte nach einem Rollen-und Rechtekonzept. Die Offenlegung der Daten findet dem Zweck entsprechend gegenüber dem Auswahlgremium statt. Die Daten werden nach Zweckerfüllung unter Beachtung der gesetzlichen Fristen gelöscht.

Schutzziel	Komponente	**Ereignisse** (die zu einer Verwirklichung des Schadens führen können) = **identifizierte Risiken**	**Maßnahmen zur Eindämmung des Risikos**
Datenminierung	**Oberziel**	Der/Die Bewerber/in übermittelt mehr Daten als erforderlich und es erfolgt weder Rückgabe noch Löschung	Der Bewerberfragenkatalog ist so aufgestellt, dass ausschließlich zur Aufgabenerfüllung erforderliche Daten erhoben werden. Ohne diese Daten ist eine Aufgabenerledigung nicht möglich. Eine Löschroutine ist installiert (6 Monate nach Ende Bewerbungsverfahren)
Verfügbarkeit	Daten	Bewerbung kommt nicht oder nicht fristgerecht an	Das Bewerberportal wird durch RZ Musterdorf zur Verfügung gestellt. Dort gehen die Bewerbungen ein. Im Portal wird darauf hingewiesen, dass nach Erhalt der Bewerbung eine Bestätigungsmail gesendet wird, so dass das Nichtankommen erkennbar wird.
	Systeme	Ausfall der Systeme	Der Vertrag zur Auftragsverarbeiter verpflichtet das Rechenzentrum, eine hohe Verfügbarkeit sicherzustellen und ausreichende Redundanzen zu gewährleisten. Desweiteren sind Schutzmaßnahmen zu treffen, die auf dem aktuellen Stand sein müssen.
	Prozesse	Bewerbungsunterlagen kommen nicht rechtzeitig beim Verantwortlichen an, weil Zuständigkeiten ungeklärt sind	Der Anbieter gewährleistet eine Rückmeldung über das Eingehen der Bewerbung. Dem Rechenzentrum wurden die technischen und organisatorischen Maßnahmen vorgegeben.
Integrität	Daten	Löschung oder Beschädigung der eingegangenen Bewerbungsunterlagen; fehlerhafte Weiterleitung	Über das Rollen- und Rechtekonzept ist der Eingang der Bewerbungen auf den berechtigten Personenkreis im Fachdienst Personal beschränkt.
	Systeme	unsicherer Versand	An den Anbieter "Mustermann" ist die Forderung gestellt, eine Ende-zu-Ende-Verschlüsselung zu gewährleisten. Das wurde auch zugesagt. Die Umsetzung ist noch offen.
	Prozesse	Umgang mit E-Mails nicht oder nicht ausreichend geregelt	Der Umgang mit dem elektronischen Posteingang ist allen an der Verarbeitung Beteiligten bekannt und wird eingehalten.
Vertraulichkeit	Daten	Offenbarung der Bewerbungsbemühungen kann das Verfahren resp. bestehende Arbeitsverhältnis beeinflussen.	Es bestehen Diskretionsvorgaben, die im Rahmen der Vertraulichkeitsverpflichtung jedem Beschäftigten bekannt sind.
	Systeme	fehlende Kontrollmechanismen; mangelhafte Mandantentrennung	Mit dem Anbieter ist vereinbart, dass eine Mandantentrennung zwingend erfolgt.
	Prozesse	Belehrung zur Verschwiegenheit und Vertraulichkeit zur Datenverarbeitung sind unterblieben	Es ist Einstellungsstandard, jede/n neue/n Beschäftigte/n umfänglich über die Hausregeln zu informieren und zur Vertraulichkeit und Verschwiegenheit zu verpflichten.
Transparenz	Daten	Umfang der Datenverarbeitung sowie Betroffenenrechte sind nicht erkennbar	Die Hinweise im Bewerberportal befinden sich im Zugangsbereich und auf der Karriereseite der Behörde.
	Systeme	keine ausreichende Protokollierung	Sowohl mit dem Anbieter als auch mit dem Rechenzentrum sind Protokollierungspflichten vereinbart.
	Prozesse	Protokollierung und Betroffenenrechte sind nicht ausreichend geregelt	Sowohl Protokollierung als auch Betroffenenrechte sind technisch und organisatorisch geregelt (Vertrag zur Auftragsverarbeitung sowie Datenschutzmanagement)
Nichtverkettbarkeit	Daten	Die Bewerbungsunterlagen werden auch zu anderen Zwecken verwendet	Über das Rollen- und Rechtekonzept erhalten nur beteiligte Fachdienste Kenntnis über die Daten des Bewerbers / der Bewerberin. Die Zweckgebundenheit der Daten ist allen Beteiligten bekannt.
	Systeme	keine Trennung von Datenbeständen; ungeordnete Schnittstellen	Mandantentrennung und Schnittstellen sind geregelt.
	Prozesse	keine hinreichende Bestimmung des Verwendungszwecks	Die Bewerberprozesse sind strukturiert und für jedem Beteiligten bekannt.
Intervenierbarkeit	Daten	ungeordnete Datenablage	Für jedes Bewerbungsverfahren wird ein eigener Ordner angelegt.
	Systeme	fehlende Funktionalitäten	Sperrung, Löschung, Berichtigung und ggf. Darstellungen der Betroffenen sind technisch möglich.
	Prozesse	fehlende Anweisungen zu Ordnerstrukturen	Der Bewerberprozess ist so gestaltet, dass jederzeit ein Auffinden der Daten sowie die Wahrnehmung der Betroffenenrechte möglich ist.

Datum Unterschrift des DSFA-Projektleiters

Datum Unterschrift Verantwortlicher

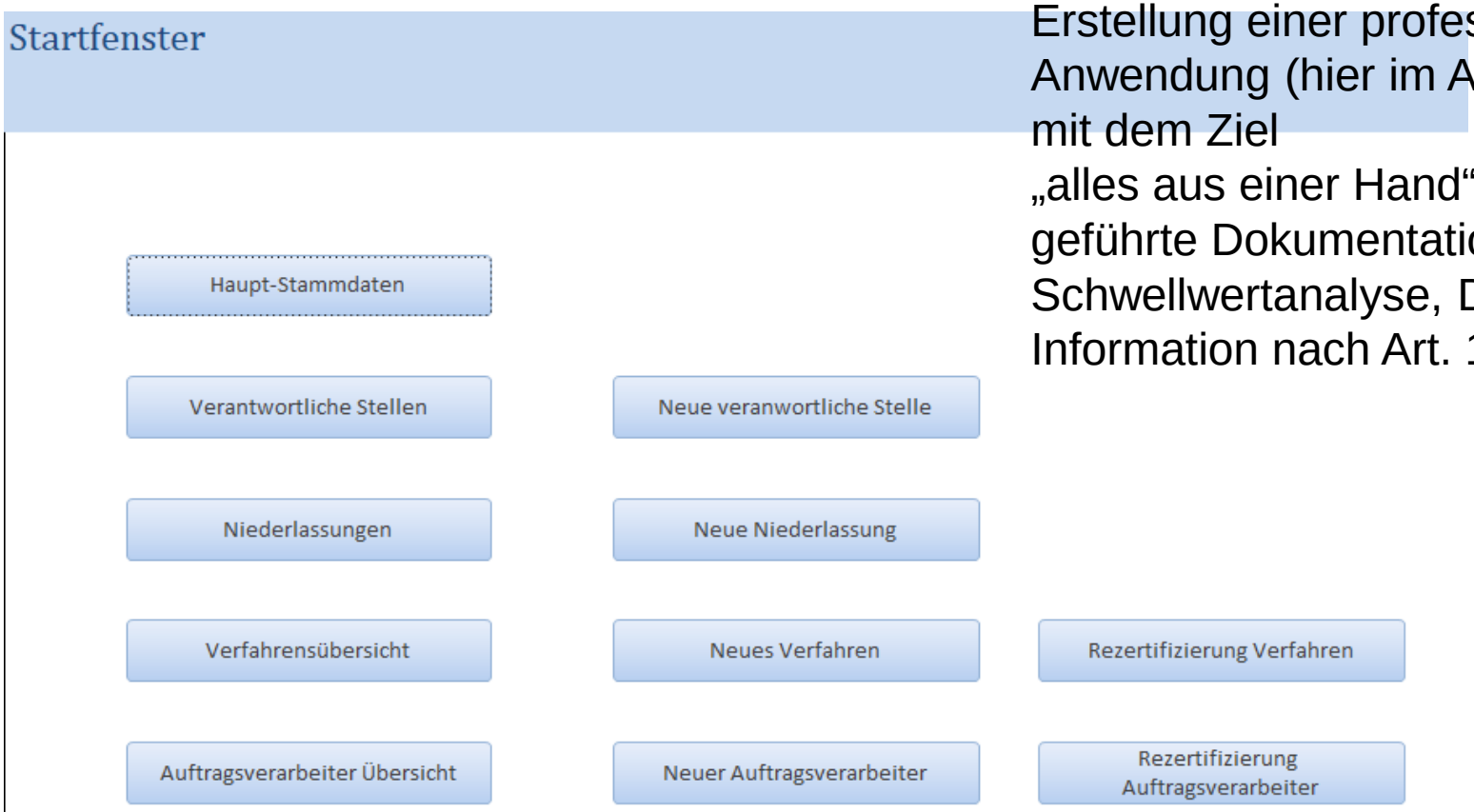
Soll-Ist-Abgleich

Schutzziel	Komponente	Maßnahmen zur Eindämmung des Risikos	vollständige Umsetzung?	wenn nein: Abweichung und Äquivalent beschreiben
Datenminierung	**Oberziel**	Der Bewerberfragenkatalog ist so aufgestellt, dass ausschließlich zur Aufgabenerfüllung erforderliche Daten erhoben werden. Ohne diese Daten ist eine Aufgabenerledigung nicht möglich. Eine Löschroutine ist installiert (6 Monate nach Ende Bewerbungsverfahren)	ja	
Verfügbarkeit	Daten	Das Bewerberportal wird durch RZ Musterdorf zur Verfügung gestellt. Dort gehen die Bewerbungen ein. Im Portal wird darauf hingewiesen, dass nach Erhalt der Bewerbung eine Bestätigungsmail gesendet wird, so dass das Nichtankommen erkennbar wird.	ja	
	Systeme	Der Vertrag zur Auftragsverarbeiter verpflichtet das Rechenzentrum, eine hohe Verfügbarkeit sicherzustellen und ausreichende Redundanzen zu gewährleisten. Desweiteren sind Schutzmaßnahmen zu treffen, die auf dem aktuellen Stand sein müssen.	ja	
	Prozesse	Der Anbieter gewährleistet eine Rückmeldung über das Eingehen der Bewerbung. Dem Rechenzentrum wurden die technischen und organisatorischen Maßnahmen vorgegeben.	ja	
Integrität	Daten	Über das Rollen- und Rechtekonzept ist der Eingang der Bewerbungen auf den berechtigten Personenkreis im Fachdienst Personal beschränkt.	ja	
	Systeme	An den Anbieter "Mustermann" ist die Forderung gestellt, eine Ende-zu-Ende-Verschlüsselung zu gewährleisten. Das wurde auch zugesagt. Die Umsetzung ist noch offen.	nein	kein Äquivalent; Umsetzung ist offen
	Prozesse	Der Umgang mit dem elektronischen Posteingang ist allen an der Verarbeitung Beteiligten bekannt und wird eingehalten.	ja	
Vertraulichkeit	Daten	Es bestehen Diskretionsvorgaben, die im Rahmen der Vertraulichkeitsverpflichtung jedem Beschäftigten bekannt sind.	ja	
	Systeme	Mit dem Anbieter ist vereinbart, dass eine Mandantentrennung zwingend erfolgt.	ja	
	Prozesse	Es ist Einstellungsstandard, jede/n neue/n Beschäftigte/n umfänglich über die Hausregeln zu informieren und zur Vertraulichkeit und Verschwiegenheit zu verpflichten.	ja	
Transparenz	Daten	Die Hinweise im Bewerberportal befinden sich im Zugangsbereich und auf der Karriereseite der Behörde.	ja	
	Systeme	Sowohl mit dem Anbieter als auch mit dem Rechenzentrum sind Protokollierungspflichten vereinbart.	ja	
	Prozesse	Sowohl Protokollierung als auch Betroffenenrechte sind technisch und organisatorisch geregelt (Vertrag zur Auftragsverarbeitung sowie Datenschutzmanagement)	ja	
Nichtverkettbarkeit	Daten	Über das Rollen- und Rechtekonzept erhalten nur beteiligte Fachdienste Kenntnis über die Daten des Bewerbers / der Bewerberin. Die Zweckgebundenheit der Daten ist allen Beteiligten bekannt.	ja	
	Systeme	Mandantentrennung und Schnittstellen sind geregelt.	ja	
	Prozesse	Die Bewerberprozesse sind strukturiert und für jedem Beteiligten bekannt.	ja	
Intervenierbarkeit	Daten	Für jedes Bewerbungsverfahren wird ein eigener Ordner angelegt.	ja	
	Systeme	Sperrung, Löschung, Berichtigung und ggf. Darstellungen der Betroffenen sind technisch möglich.	ja	
	Prozesse	Der Bewerberprozess ist so gestaltet, dass jederzeit ein Auffinden der Daten sowie die Wahrnehmung der Betroffenenrechte möglich ist.	ja	

REVISION

Schutzziel	Komponente Die Kommentar-felder geben Anhaltspunkte	Ist eine Anpassung der Maßnahmen erforderlich?	angepasste Maßnahmen zur Eindämmung des Risikos *(? =Beispiele im Kommentarfeld aus SDM)* Die Bausteine zum Standard-Datenschutzmodell finden Sie hier: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/		Eintrittswahrscheinlichkeit		Schwere des möglichen Schadens		Restrisiko = Produktwert
					Einstufung	Begründung	Einstufung	Erläuterung	
Daten-minierung	Oberziel			?					0
Verfügbarkeit	Daten			?					0
	Systeme								0
	Prozesse								0
Integrität	Daten			?					0
	Systeme								0
	Prozesse								0
Vertraulich-keit	Daten			?					0
	Systeme								0
	Prozesse								0
Transparenz	Daten			?					0
	Systeme								0
	Prozesse								0
Nicht-verkettbarkeit	Daten			?					0
	Systeme								0
	Prozesse								0
Intervenier-barkeit	Daten			?					0
	Systeme								0
	Prozesse								0

Entwicklung



Erstellung einer professionellen Anwendung (hier im Ausschnitt) mit dem Ziel
„alles aus einer Hand“ =
geführte Dokumentation,
Schwellwertanalyse, DSFA,
Information nach Art. 13 DS-GVO

via: Sachverständigenbüro
Bernd Sommerfeldt c/o Rechtsanwaltskanzlei FKF
Bei der Lohmühle 23 , 23554 Lübeck
bernd.sommerfeldt@mediajumper.de
Tel.: 0451 8899124, Mobil: 015140129909

Schwellenanalyse

Schwellenanalyse

Verfahren		Löschfrist	
Kategorie personenbezogen Daten		Art der Verarbeitung (Beschreibung)	
Eindeutige Bezeichnung Personenbezogener Daten		Positiv-Liste Art 35 Abs 4 DS-GVO	https://www.datenschutzzentrum.de/
Für das Verfahren erforderlich	☐	Umfang der Verarbeitung im Verhältnis zur Gesamtverarbeitung	
Begündung der Erforderlichkeit		Umstände der Verarbeitung (auf diesem Weg)	
Verhältnismäßigkeit		Schnittstellen	
Verantwortliche Stelle(n)		Schutzklasse	
Beteiligte Stelle(n)		Kriterium der Entscheidung freier Text	
Verantwortliche*r		Neue technologische oder organisatorische Lösung	☐
Auftragsverarbeiter		Leistung ist abhängig von einer Datennutzung	☐
Datenübermittlung(en) an		Automasiertes Profiling	☐
Datenübermittlungen an Dritte		Automatisierte Entscheidung	☐
		Systematische Überwachung	☐
		Vertrauliche oder höchst persönliche (sensible) Daten	☐
		Datenverarbeitung gehört zur Kerntätigleit	☐
		Datenverarbeitung im großem Umfang	☐
		Abgleichen oder Zusammenführen von Datensätzen	☐
		Daten zu schutzbedürftigen Betroffenen	☐

Die Positivliste soll später bereits in den Verfahrensbeschreibungen integriert werden und bei zutreffendem Verfahren automatisch zur Anwendung kommen.

Conclusion

- Benötigte Ressourcen: Team (Projektleitung, Anwender*innen, Technik, Personalrat, ggf. Anbieter), Räume und Technik (zur Erfassung und Darstellung)
- Aufwand: Je nach Umfang der Verarbeitung kann eine DSFA zwei Arbeitstage umfassen
- Mehrwert:
  - Die Teilnehmer und der Verantwortliche lernen die Verarbeitung kennen, weil sie sich mit der Ressource auseinandersetzen müssen, um Risiken erkennen zu können.
  - Erhöhung der Ressourcenausnutzung
  - Verständnis für das Zusammenwirken
  - Entlastung der Beschäftigten
  - Wirtschaftlichkeit der Anwendung
  - Erkennen von Anpassungsnotwendigkeiten (Art. 25