

Datenschutzrechtliche Risikoanalyse zur Datenschutz-Folgenabschätzung (DSFA)

<Bezeichnung DSFA>

bei der <Stelle>

(Dok-ID: <Dokument-ID>)

BayLfD-Stand: 01.05.2022

1. Inhalt:

Blatt	Bezeichnung	Hinweis zum Inhalt
1	Inhaltsverzeichnis & Status & Beteiligte & Termin Routineprüfung & Anlagen und Verweise	Übersicht der unterschiedlichen Tabellenblätter, Status der Risikoanalyse, an der Risikoanalyse beteiligte Personen, geplantes Review und Anlagen und Verweisungen
2	Fassung	Übersicht der Änderungen, die an der Risikoanalyse durchgeführt wurden
3	Legende	Verwendete Risikoanalysemethoden (Risiko- und Zielerfüllungsmanagement)
4	Risikomanagement	Risikomanagement für alle SDM-Datensicherheitsziele
5	Zielerfüllungsmanagement	Zielerfüllungsmanagement für alle SDM-Schutzbedarfssziele
6	Maßnahmen	Liste aller geplanten oder bereits umgesetzten technischen und organisatorischen Schutzmaßnahmen (TOMs)

2. Status und beteiligte Personen:

Status	beteiligte Personen	Anmerkungen
Bearbeitung		

3. Zeitpunkt der nächsten routinemäßigen Überprüfung:

Zeitpunkt	Anmerkungen
01.01.24	

4. Anlagen und Verweise:

ID	Bezeichnung	Anmerkungen
1		
2	(...)	(...)

Änderungshistorie

[illegible]

Legende

1. Risikomanagement

1.1 Risikomatrix für die Indexierung der Risiken

Schwere/Schaden	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
		1	2	3	4
		Eintrittswahrscheinlichkeiten			

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 signifikante 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 signifikante 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 signifikante 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 Risikoidexes über alle Einzelrisiken (unten stehendes Risikoprofil) nach der Maximum-Methode, d.h. der vorkommende höchste Risikoidex 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 VT		Ungenügende Sicherheit des Browsers	# Browser	Auf das Analysetool wird über Internetbrowser zugegriffen. Schwachstellen in der Browser-Sicherheit können zu Datenabfluss führen.	Aufgrund der Funktionsweise des Zugriffs kann ein Browserdefizit nicht vollends ausgeschlossen werden. Die Browser-Sicherheit wird von Herstellern kontinuierlich überprüft und verbessert	2	Es handelt sich gegenüber unbefugten Dritten um sensible Personendaten.	3	6	Hinweis an Nutzer des Tools, aktuelle Browserversionen zu verwenden CSP und SRI als zusätzliche Schutzebenen Architektur der Software minimiert Angriffspunkte auf Daten (Client-Side Only)	Eine Browser-Schwachstelle kann mit den Maßnahmen eingedämmt werden. Die Eintrittswahrscheinlichkeit wird durch die Maßnahmen reduziert.	ge
1 VB		Mangelndes Bewusstsein der Anwender über den richtigen und vertraulichen Umgang mit (Roh)daten	# Anwender	Rohdaten werden durch den Anwender unverschlüsselt oder unsachgemäß abgespeichert / abgelegt / übertragen / weitergegeben, dadurch können Unbefugte Zugang zu den Rohdaten erhalten.	Bei einem breiten Anwenderkreis sind Fehler im Umgang mit Daten möglich.	4	Es handelt sich gegenüber unbefugten Dritten um sensible Personendaten.	3	12	Schulung der Nutzer Dokumentation der Verantwortlichkeiten Weitergabekontrolle, d.h. keine Datenübertragung an Server oder Dritte, kein E-Mail-Versand oder Exportfunktion im Tool, CSP (Content Security Policy) verhindert Datenabfluss	Durch Kombination der Maßnahmen wird das Risiko auf ein Minimum reduziert.	ge
			# Anwender	Dritte können den Arbeitsplatz / Bildschirm des Anwender einsehen und so die Rohdaten sehen.	Aufgrund der Vielzahl der Anwender ist nicht auszuschließen, dass die jeweiligen Arbeitsmittel konsequent gesperrt werden	4	Es handelt sich gegenüber unbefugten Dritten um sensible Personendaten.	3	12	Deutlicher Hinweis im Analysetool Schulung der Nutzer Dokumentation der Verantwortlichkeiten	Durch Kombination der Maßnahmen wird das Risiko auf ein Minimum reduziert.	ge
3 VT VB		Fehlerhaftigkeit bzw. Veränderlichkeit des Codes	# Hosting	Durch Kompromittierung des Hosting-Servers (Code-Manipulation) kann die Software so verändert werden, dass die softwareinhärenten Funktionen zum Datenschutz außer Kraft gesetzt werden.	Eine zielgerichtete Manipulation ist im Einsatzbereich der Software und bei Einsatz sicherer Hosting-Infrastruktur unwahrscheinlich.	2	Es handelt sich gegenüber unbefugten Dritten um sensible Personendaten.	3	6	Deployment auf vertrauenswürdiger Infrastruktur (deutscher / bayerischer Server) Regelmäßige Integritäts- und Sicherheitsprüfungen	Durch besondere Prüfungen und Kontrollen wird das Risiko der Manipulation auf ein Minimum reduziert.	ge
			# Software	Durch fehlerhaften Code oder Sicherheitslücken im Browser, bei der Webanwendung oder beim Hostinganbieter können personenbezogene Daten in die Hände unbefugter Personen gelangen	Software- bzw. Hostingfehler sind aufgrund der Architektur unwahrscheinlich, können aber nicht ausgeschlossen werden.	2	Es handelt sich gegenüber unbefugten Dritten um sensible Personendaten.	3	6	Versionskontrolle Deployment auf vertrauenswürdiger Infrastruktur (deutscher / bayerischer Server); regelmäßige Integritätsprüfungen, weitere Sicherheitsmaßnahmen , Versionskontrolle	Durch besondere Prüfungen und Kontrollen wird das Risiko der Manipulation auf ein Minimum reduziert.	ge
4 VT		Das Tool ist über einen Weblink ohne Anmeldung verfügbar und wird von vielen Personen parallel genutzt	# Fehlendes Anwendermanagement / Zugriffskontrolle # Multiple Anwender	Dritte oder andere Anwender gelangen über das Tool unbefugt an fremde Daten bzw. Daten aus anderen Sessions	Durch die Architektur der Software wird das Risiko für einen unbefugten Zugriff auf fremde Daten erheblich verringert.	1	Es handelt sich gegenüber unbefugten Dritten um sensible Personendaten.	3	3	Zugangskontrolle: Same Origin Policy Zugriffskontrolle: Client Side Only Verarbeitung, keine persistente Speicherung Trennungskontrolle: Automatische Isolation durch Browser-Architektur, keine Vermischung mit anderen Datenbeständen möglich, Sessions sind vollständig voneinander getrennt.	Durch besondere Kontrollen wird das Risiko des unauthorisierten Zugriffs auf ein Minimum reduziert.	ge
5 VB		Tool / WebApp ist nicht verfügbar	# Hosting # Software	Vielzahl an parallelen Usern führt zu Unerreichbarkeit der Seite	Da kein Backendserver genutzt wird, gibt es kein Problem einer begrenzten Sessionanzahl. Das Tool muss lediglich einmal vom Server geladen werden.	1	Die Folge ist regelmäßig lediglich die Nichterreichbarkeit des Tools für die Anwender. Die Handlung ist nachholbar, sodass kein größerer Schaden entsteht	1	1	Verfügbarkeitskontrolle: HTTPS-only Deployment, Hosting auf zuverlässiger Infrastruktur, regelmäßige Verfügbarkeitsprüfung Rasche Wiederherstellbarkeit: schnelles re-deployment möglich, Versionskontrolle für schnelle Rollbacks, keine Datenbanken / persistenten Systeme, die wieder hergestellt werden müssen	Durch die Maßnahmen wird die Ausfallzeit auf ein Minimum reduziert.	gr
6 VT VB DI		Nutzung externer Ressourcen	# Software	Durch Einbindung externer Ressourcen wie APIs, Bibliotheken etc. besteht die Gefahr der Kompromittierung von Daten	Der Einsatz externer Ressourcen ist minimiert bzw. wird durch technische Sicherheitsmaßnahmen entsprechend der geltenden Standards überwacht	2	Die Schwere ist abhängig von dem Ausmaß der Kompromittierung sowie von dem Zugriff erlangenden Personenkreis	3	6	Transportverschlüsselung Content Security Policy Subresource Policy Keine Nutzung externer Abhängigkeiten	Verschlüsselung und die Einhaltung der geltenden Sicherheitsstandards für sicherheitskritische Konfigurationen.	ge

Risikoa

DSFA "Personal verwalten"

4 RM

ID	Schwachstelle	Risikoquelle	Risiko-Szenario	Eintrittswahrscheinlichkeit		Schwere/Schaden		Index	Maßnahme-Bezeichnung	Risikoeinschätzung mit Maßnahmen	
Ziel				Erläuterung	Grad	Erläuterung	Grad			Erläuterung	Index
7 VT VB DI	Weiterentwicklung der Software	# Software	Fehlende Kontrollen oder lockerere Sicherheitsstandards bei Updates führen zu Sicherheitslücken	Es bestehen Verfahren zur Überprüfung, Bewertung und Evaluierung von Änderungen entsprechend der geltenden Standards, sodass ein geringes Restrisiko verbleibt	2	Die Schwere ist abhängig von der Art einer potenziellen Sicherheitslücke, bzw. Softwarefehler und deren Ausnutzung . Schlimmstenfalls gelangen personenbezogene Daten an Unbefugte.	3	6	Datenschutz-Management Datenschutzfreundliche Voreinstellungen Patch- und Updatemanagement Kontinuierliche Sicherheitschecks Incident-Response: Direkte Meldung von Vorfällen durch Entwicklungsfirma an betroffene Behörden und Aufarbeitung des Vorfalls.	Durch Kombination der Maßnahmen wird das Risiko auf ein Minimum reduziert.	ge

Zielerfüllungsmanagement

Gewährleistungsziel		Summarische Gefährdungsbetrachtung							Index
DM - Datenminimierung IV - Interventionsbarkeit KE - Konzeptinhaltung NV - Nichtverfälschung RI - Richtigkeit TP - Transparenz		Ermittlung des Gefährdungsindex 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	Gefährdungsszenario	Gefährdungsbewertung		Maßnahme-Bezeichnung	Gefährdungsbewertung	
					Erläuterung	Index		Erläuterung	Index
4	Unzureichende Datenminimierung	#Anwender		In der Datenvorbereitung werden vom Anwender mehr Daten erhoben / aus den Personalsystemen gezogen, als für die Erstellung der Gleichstellungskonzepte notwendig ist. Diese werden in das Tool eingespielt und dort in den Berichten verarbeitet.		ge	Eindeutige Dokumentation des Datenbedarfs über Handbuch, folgt dem Prinzip der Datensparsamkeit	Geschulte Mitarbeiter des Personalreferats verwenden nur die nötigen Daten.	gr
							Initial-Schulung der Nutzer, fortlaufende Unterweisung		
							Dokumentation der Verantwortlichkeiten		
5	Unzureichende Anonymisierung und Pseudonymisierung	#Anwender		Daten werden in der Datenvorbereitung nicht ausreichend anonymisiert oder pseudonymisiert, wodurch Rückschlüsse auf betroffene Personen möglich sind		gr	Initial-Schulung der Nutzer, fortlaufende Unterweisung	Geschulte Mitarbeiter des Personalreferats verwenden nur pseudonymisierte Daten.	gr
							Dokumentation der Verantwortlichkeiten		
		#Software	Im Bericht werden Daten ausgegeben, die Rückschlüsse auf Einzelpersonen möglich machen.	Tool wertet Namen nicht aus		gr	Die App gibt ausschließlich aggregierte Daten aus		gr
							Funktionalität, die verhindert, dass in den Datenauswertungen Ergebnisse < 5 Personen ausgegeben werden		

Schutzmaßnahmen (TOMs)

						
ID	Bezeichnung	Kurzbeschreibung		Verweise	Anmerkungen	
M.1	Schulung der Nutzer	alle Beschäftigte des StMAS sind verpflichtet, einen BayLearn-Kurs zur IT-Sicherheit zu absolvieren				
M1+n	Es wird auf die Anlage "reportix_Gleichstellung_Bayern-Anlage_TOM.docx" Bezug genommen	(…)		(…)	(…)	