Datenschutzrechtliche Risikoanalyse

Risikoanalyse der <Stelle> für das Betriebsmittel

<Bezeichnung Betriebsmittel>

[Dokument-ID: <Dokumenten-ID>]

BayLfD-Stand: 01.05.2022

Inhalt

1. Information zur Risikoanalyse (RA)

1.1 Beteiligte Personen und Status

1.1.1 An RA beteiligte Person(en) und ihre Rolle(n)	1.1.2 Status der RA	1.1.3 Anmerkung zum Status
<Name>, <Vorname> [Federführung, Fachbereich] <Name>, <Vorname> [Beratung, IT] <Name>, <Vorname> [Beratung, bDSB]	☒ in Bearbeitung ☐ Aktiviert ☐ Deaktiviert ☐ Sonstig: <ggf. Status angeben>	

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. Zielverarbeitung

2.1 Beschreibung

2.2 Anmerkungen

3. Risikobewertung relevanter Szenarien

3.1 Vertraulichkeit (VT)

3.1.1 Beschreibung relevanter Szenarien und deren möglichen Folgen/Auswirkungen		
3.1.2 Risiko ohne TOM (Ausgangsrisiko) ☐ hoch…. ☐ normal ☐ niedrig	**3.1.3 Risiko mit TOM (Restrisiko)** ☐ hoch…. ☐ normal ☐ niedrig	**3.1.4 Anmerkung zur Risikobewertung**

3.2 Verfügbarkeit (VB)

3.2.1 Beschreibung relevanter Szenarien und deren möglichen Folgen/Auswirkungen		
3.2.2 Risiko ohne TOM (Ausgangsrisiko) ☐ hoch…. ☐ normal ☐ niedrig	**3.2.3 Risiko mit TOM (Restrisiko)** ☐ hoch…. ☐ normal ☐ niedrig	**3.2.4 Anmerkung zur Risikobewertung**

3.3 Datenintegrität (DI)

3.3.1 Beschreibung relevanter Szenarien und deren möglichen Folgen/Auswirkungen		
3.3.2 Risiko ohne TOM (Ausgangsrisiko) ☐ hoch…. ☐ normal ☐ niedrig	**3.3.3 Risiko mit TOM (Restrisiko)** ☐ hoch…. ☐ normal ☐ niedrig	**3.3.4 Anmerkung zur Risikobewertung**

3.4 Richtigkeit und Konzeptionseinhaltung (RI)

3.4.1 Beschreibung relevanter Szenarien und deren möglichen Folgen/Auswirkungen

3.4.2 Risiko ohne TOM (Ausgangsrisiko)	3.4.3 Risiko mit TOM (Restrisiko)	3.4.4 Anmerkung zur Risikobewertung
☐ hoch…. ☐ normal ☐ niedrig	☐ hoch…. ☐ normal ☐ niedrig	

3.5 ■ Datenminimierung (DM) ■

3.5.1 Beschreibung relevanter Szenarien und deren möglichen Folgen/Auswirkungen		
3.5.2 Risiko ohne TOM (Ausgangsrisiko)	**3.5.3 Risiko mit TOM (Restrisiko)**	**3.5.4 Anmerkung zur Risikobewertung**
☐ hoch…. ☐ normal ☐ niedrig	☐ hoch…. ☐ normal ☐ niedrig	

3.6 ■ Nichtverkettung (NV) ■

3.6.1 Beschreibung relevanter Szenarien und deren möglichen Folgen/Auswirkungen		
3.6.2 Risiko ohne TOM (Ausgangsrisiko)	**3.6.3 Risiko mit TOM (Restrisiko)**	**3.6.4 Anmerkung zur Risikobewertung**
☐ hoch…. ☐ normal ☐ niedrig	☐ hoch…. ☐ normal ☐ niedrig	

3.7 ■ Transparenz (TP) ■

3.7.1 Beschreibung relevanter Szenarien und deren möglichen Folgen/Auswirkungen		
3.7.2 Risiko ohne TOM (Ausgangsrisiko)	**3.7.3 Risiko mit TOM (Restrisiko)**	**3.7.4 Anmerkung zur Risikobewertung**
☐ hoch…. ☐ normal ☐ niedrig	☐ hoch…. ☐ normal ☐ niedrig	

3.8 ■ Intervenierbarkeit (IV) ■

3.8.1 Beschreibung relevanter Szenarien und deren möglichen Folgen/Auswirkungen		
3.8.2 Risiko ohne TOM (Ausgangsrisiko)	**3.8.3 Risiko mit TOM (Restrisiko)**	**3.8.4 Anmerkung zur Risikobewertung**
☐ hoch…. ☐ normal	☐ hoch…. ☐ normal	

☐ **niedrig**	☐ **niedrig**	

3.9 ■ Gesamtbewertung ■

3.9.1 Gesamtbewertung Restrisiko

4. Schutzmaßnahmen (TOM)

4.1 ■ Spezielle TOM ■

Nr.	TOM – Bezeichnung und Beschreibung	Wirkung	Verweise
4.1.1			
4.1.2	(…)	(…)	(…)

4.2 ■ Adaptive TOM ■

Nr.	TOM – Bezeichnung und Beschreibung	Wirkung	Verweise
4.2.1			
4.2.2	(…)	(…)	(…)

4.3 ■ Übergreifende TOM ■

Nr.	TOM – Bezeichnung und Beschreibung	Wirkung	Verweise
4.3.1			
4.3.2	(…)		

Ausfüllhinweise zum Formular

A) Zielsetzung der Risikoanalyse

Eine allgemeine Risikoanalyse stellt im Vergleich zur DSFA ein vereinfachtes Verfahren dar. Aber auch wenn keine Hochrisikoverarbeitungen nach Art. 35 DSGVO vorliegt, trifft den Verantwortlichen nach Art. 24, 25 und 32 DSGVO die Pflicht, geeignete technische und organisatorische Maßnahmen wirksam umzusetzen, um sicherzustellen, dass die Art und Weise einer Verarbeitung mit den Vorgaben der DSGVO in Einklang steht. Die Einhaltung dieser Pflicht muss grundsätzlich bei Fehlen eines alternativen Nachweisinstruments durch den Verantwortlichen angemessen mittels einer Risikoanalyse dokumentiert werden.
Dieses Formular orientiert sich an der Methode für eine allgemeine datenschutzrechtliche Risikoanalyse, die der Bayerische Landesbeauftragte für den Datenschutz auf seiner Homepage (vgl. https://www.datenschutz-bayern.de) in dem Bereich „DSFA“ für bayerische öffentliche Stellen veröffentlicht hat.

B) Hinweise zu den Einzelpunkten

Punkt	Ausfüllhinweis
1.1.1	Angabe der **an der Risikoanalyse 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 Risikoanalyse insgesamt zuständig ist und diese insbesondere auch aktiviert) • Federführung (falls man die Durchführung der Risikoanalyse als (Klein-)Projekt versteht, entspricht das Aufgabenprofil der Federführung dem einer Projektleitung) • Vertretung Auftraggeber/in (naheliegend ist, dass ein Vertreter der Fachlichkeit, die die Zielverarbeitung gestaltet und beschreibt, diese Rolle wahrnimmt) • Vertretung IT-Bereich (bei einer Risikoanalyse werden zumeist auch die klassischen IT-Sicherheitsziele und die Risikolage der betroffenen IT-Komponenten 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 Risikoanalyse-Erstellung selbst nicht beteiligt war, die Risikoanalyse insbesondere im Hinblick auf Logik, Plausibilität, Verständlichkeit und Vollständigkeit überprüfen zu lassen)
1.1.2	Der mögliche **Status der Risikoanalyse** umfasst auch eine Aktivierung und Deaktivierung. Vor dem Hintergrund der Skalierbarkeit einer Risikoanalyse wurde der neutrale Begriff „Aktivierung“ gewählt, nicht stärker formalisierte Begriffe, wie z.B. „Freigabe“. Eine Deaktivierung kommt etwa in Betracht, wenn die Risikoanalyse durch eine andere Risikoanalyse ersetzt wird, bei der die weitere Fortsetzung der Risikoanalyse-Versionierung nicht sinnvoll erscheint (z.B. neue Risikoanalyse betrachtet einen anderen Zuschnitt der Zielverarbeitung).
1.1.3	Optionale **Anmerkungen zum festgelegten Status**.
1.2	Der Unterschied zwischen einer **Anlage und einem Verweis** zur Risikoanalyse ist, dass die Anlage fest und ausschließlich zur Risikoanalyse gehört, während die verwiesenen Dokumente auch in anderen Zusammenhängen verwendet werden (Mehrfachverwendung).
1.3	In der **Änderungshistorie** werden die wesentlichen Änderungen der Risikoanalyse nachvollziehbar festgehalten.
1.4	Da die Risikoanalyse regelmäßig hinsichtlich eines inzwischen eingetretenen Änderungsbedarfs überprüft werden sollte, kann hier ein **routinemäßiges Überprüfungsdatum** eingetragen werden.

Punkt	Ausfüllhinweis
2.1	Beschreibung und Abgrenzung der Verarbeitung, die Gegenstand der Risikoanalyse ist (**Zielverarbeitung**).
2.2	**Anmerkungen** zur **Zielverarbeitung**.
3.1.1	Beschreibung relevanter **Szenarien** und daraus ergebender **Folgen** für betroffene Personen im Bereich der **Vertraulichkeit**.
3.1.2	**Maximales Ausgangsrisko** im Hinblick auf die unter 3.1.1 genannten Szenarien.
3.1.3	**Maximales Restrisko** im Hinblick auf die unter 3.1.1 genannten Szenarien.
3.1.4	**Anmerkungen** zur Bewertung des Ausgangs- und Rest**risikos**.
3.2.1	Beschreibung relevanter **Szenarien** und daraus ergebender **Folgen** für betroffene Personen im Bereich der **Verfügbarkeit**.
3.2.2	**Maximales Ausgangsrisko** im Hinblick auf die unter 3.2.1 genannten Szenarien.
3.2.3	**Maximales Restrisko** im Hinblick auf die unter 3.2.1 genannten Szenarien.
3.2.4	**Anmerkungen** zur Bewertung des Ausgangs- und Rest**risikos.**
3.3.1	Beschreibung relevanter **Szenarien** und daraus ergebender **Folgen** für betroffene Personen im Bereich der **Datenintegrität**.
3.3.2	**Maximales Ausgangsrisko** im Hinblick auf die unter 3.3.1 genannten Szenarien.
3.3.3	**Maximales Restrisko** im Hinblick auf die unter 3.3.1 genannten Szenarien.
3.3.4	**Anmerkungen** zur Bewertung des Ausgangs- und Rest**risikos.**
3.4.1	Beschreibung relevanter **Szenarien** und daraus ergebender **Folgen** für betroffene Personen im Bereich der **Richtigkeit und Konzepteinhaltung**.
3.4.2	**Maximales Ausgangsrisko** im Hinblick auf die unter 3.4.1 genannten Szenarien.
3.4.3	**Maximales Restrisko** im Hinblick auf die unter 3.4.1 genannten Szenarien.
3.4.4	**Anmerkungen** zur Bewertung des Ausgangs- und Rest**risikos.**
3.5.1	Beschreibung relevanter **Szenarien** und daraus ergebender **Folgen** für betroffene Personen im Bereich der **Datenminimierung**.
3.5.2	**Maximales Ausgangsrisko** im Hinblick auf die unter 3.5.1 genannten Szenarien.
3.5.3	**Maximales Restrisko** im Hinblick auf die unter 3.5.1 genannten Szenarien.
3.5.4	**Anmerkungen** zur Bewertung des Ausgangs- und Rest**risikos.**
3.6.1	Beschreibung relevanter **Szenarien** und daraus ergebender **Folgen** für betroffene Personen im Bereich der **Nichtverkettung**.
3.6.2	**Maximales Ausgangsrisko** im Hinblick auf die unter 3.6.1 genannten Szenarien.
3.6.3	**Maximales Restrisko** im Hinblick auf die unter 3.6.1 genannten Szenarien.

Punkt	Ausfüllhinweis
3.6.4	**Anmerkungen** zur Bewertung des Ausgangs- und Rest**risikos.**
3.7.1	Beschreibung relevanter **Szenarien** und daraus ergebender **Folgen** für betroffene Personen im Bereich der **Transparenz**.
3.7.2	**Maximales Ausgangsrisko** im Hinblick auf die unter 3.7.1 genannten Szenarien.
3.7.3	**Maximales Restrisko** im Hinblick auf die unter 3.7.1 genannten Szenarien.
3.7.4	**Anmerkungen** zur Bewertung des Ausgangs- und Rest**risikos.**
3.8.1	Beschreibung relevanter **Szenarien** und daraus ergebender **Folgen** für betroffene Personen im Bereich der **Intervenierbarkeit**.
3.8.2	**Maximales Ausgangsrisko** im Hinblick auf die unter 3.8.1 genannten Szenarien.
3.8.3	**Maximales Restrisko** im Hinblick auf die unter 3.8.1 genannten Szenarien.
3.8.4	**Anmerkungen** zur Bewertung des Ausgangs- und Rest**risikos.**
3.9.1	**Gesamtbewertung** aller **Restrisiken** und Darlegung, warum insgesamt ein dem Risiko angemessenes Schutzniveau durchgängig gewährleistet ist.
4.1	Aufzählung der **speziellen technischen und organisatorischen Maßnahmen (TOM)** inklusive Angabe deren Wirkung auf die zuvor identifizierten acht Risikobereiche sowie gegebenenfalls Verweisung auf Spezifikationen, Konzepte und andere weiterführende relevante Informationen. Spezielle TOM sind Maßnahmen, deren Implementierung (fast) nur bei der betrachteten Zielverarbeitung sinnvoll ist.
4.2	Aufzählung der **adaptive technischen und organisatorischen Maßnahmen (TOM)** inklusive Angabe deren Wirkung auf die zuvor identifizierten acht Risikobereiche sowie gegebenenfalls Verweisung auf Spezifikationen, Konzepte und andere weiterführende relevante Informationen. Unter adaptiven TOM sind Maßnahmen zu verstehen, die für mehrere Zielverarbeitungen nach einer verarbeitungsspezifischen Ausgestaltung geeignet sind, das Risiko angemessen zu reduzieren. Der Nutzen dieser Maßnahmengruppierung ist darin zu sehen, dass bei den adaptiven, also immer wieder erneut anzupassenden und umzusetzenden TOMs eine Standardisierung, beispielsweise durch Erstellung von Mustern mit Vorgabe der Mindestinhalte und einer Basisstruktur, angeraten sein kann.
4.3	Aufzählung der **übergreifenden technischen und organisatorischen Maßnahmen (TOM)** inklusive Angabe deren Wirkung auf die zuvor identifizierten acht Risikobereiche sowie gegebenenfalls Verweisung auf Spezifikationen, Konzepte und andere weiterführende relevante Informationen. Dies sind TOM, die für zahlreiche Zielverarbeitungen ohne nennenswerte Anpassung an die jeweilige Zielverarbeitung geeignet sind, das Risiko angemessen zu reduzieren. In diesem Kontext ist es regelmäßig sinnvoll, diese TOM in separaten Unterlagen zu spezifizieren und nachzuweisen. Die einzelne Risikoanalyse braucht damit nur auf entsprechende Unterlagen zu verweisen.