Datenschutzrechtliche Risikoanalyse

Risikoanalyse der Stadt Fiktivia für das Betriebsmittel

Videokonferenzsystem „VK-Fiktivia“ (VKS)

[Dokument-ID: RA202202111000]

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
Musterfrau, Klara [Federführung, Fachbereich] Muster, Eva [Beratung, IT] Mustermann, Hans [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	Beschreibung für das Betriebsmittel „VK-Fiktivia“	Dok-ID BM202201250900
A2	Mindeststandard des BSI für Videokonferenzdienste (Version 1.0 vom 07.10.21)	https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Videokonferenzdienste/Videokonferenzdienste_node.html
A3	(…)	(…)

1.3 Änderungshistorie

Wann?	Wer?	Was?
11.02.22	Musterfrau, Klara	Initialisierung
(…)	(…)	(…)

1.4 Zeitpunkt der nächsten routinemäßigen Überprüfung

Klicken Sie hier, um ein Datum einzugeben.

2. Zielverarbeitung

2.1 ■ Beschreibung ■

Siehe Anlage A1.

2.2 ■ Anmerkungen ■

---

3. Risikobewertung relevanter Szenarien

3.1 ■ Vertraulichkeit (VT) ■

3.1.1 Beschreibung relevanter Szenarien und deren möglichen Folgen/Auswirkungen

Folgende Szenarien wurden betrachtet:

- Unbefugte Teilnahme
  Unbefugte melden sich unbemerkt als Teilnehmende an und haben Zugriff insbesondere auf die Inhaltsdaten der Videokonferenz.

- Unzureichende Konferenztrennung
  Aufgrund von VKS-Fehlern werden unterschiedliche, aber zeitgleich laufende Videokonferenzen nicht hinreichend technisch getrennt, so dass Teilnehmende von der einen auch unbefugt an anderen Konferenzen teilnehmen können.

- Datenverarbeitung von nicht teilnehmenden Personen
  Bild und/oder Ton von Personen aus dem Umfeld der teilnehmenden Personen werden von dem VKS mitverarbeitet (z.B. eine Person aus dem Haushalt des Konferenzteilnehmers läuft durch das Bild oder spricht im Hintergrund).

- Unbefugte Aufzeichnung
  Teilnehmer erstellen unbefugt eine Aufzeichnung der Videokonferenz und verarbeiten diese weiter.

- Unbefugter Systemzugriff
  Unbefugte verschaffen sich einen Zugriff zum VKS und verarbeiten personenbezogenen VKS-Daten.

- Abhörung
  Der elektronische Datenfluss der Videokonferenz wird unbefugt „abgehört“ und weiter verarbeitet.

- (…)

Obwohl sensible personenbezogene Daten nicht mit dem VKS verarbeitet werden dürfen (vgl. Punkt 7.1 in der VKS-Beschreibung (Anlage A1)), können substanzielle Folgen für betroffene Personen bei einem Vertraulichkeitsbruch nicht ausgeschlossen werden. (…)

3.1.2 Risiko ohne TOM (Ausgangsrisiko)	3.1.3 Risiko mit TOM (Restrisiko)	3.1.4 Anmerkung zur Risikobewertung
☒ hoch….	☐ hoch….	Beim VKS ist die Anforderung der Vertraulichkeit ein Risikoschwerpunkt. Aktuelle Empfehlungen zum Stand der Technik (z.B. Anlage A2) wurden daher besonders sorgfältig, umfassend analysiert und wirksam umgesetzt.
☐ normal	☒ normal	
☐ niedrig	☐ niedrig	

3.2 ■ Verfügbarkeit (VB) ■

3.2.1 Beschreibung relevanter Szenarien und deren möglichen Folgen/Auswirkungen		
Folgende Szenarien wurden betrachtet: • Ausfall VKS Durch einen IT-Fehler oder eine sonstige Ressourcenstörung kann eine angesetzte Videokonferenz nicht durchgeführt werden. • (…) Aus den bislang gemachten Erfahrungen mit Videokonferenzen konnten bei vereinzelten Verfügungsproblemen allenfalls überschaubare Folgen für betroffene Personen identifiziert werden. (…)		
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** Insbesondere das mögliche Ausweichen auf eine Telefonkonferenz lässt das Restrisiko niedrig erscheinen.

3.3 ■ Datenintegrität (DI) ■

3.3.1 Beschreibung relevanter Szenarien und deren möglichen Folgen/Auswirkungen		
Relevante Szenarien, die die Datenintegrität neben einer unbefugten Teilnahme (vgl. Punkt 3.1) im Kontext einer Videokonferenz betreffen, sind der Stadt (noch) nicht bekannt.		
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		
Folgende Szenarien wurden betrachtet: • Aktualität von Konzepten/Vorgaben Wichtige Aktualisierungen beim organisatorischen und/oder technischen Ablauf einer VKS-Konferenz werden nicht in die relevanten Konzepte eingearbeitet, wodurch eine künftige Beachtung nicht sichergestellt ist. • (…) Bei nicht aktuellen Vorgaben und Konzepten könnten personenbezogene Daten durch das VKS nicht rechtskonform und damit mit substanziellen Folgen für betroffene Personen verarbeitet werden,		
3.4.2 Risiko ohne TOM (Ausgangsrisiko) ☐ hoch…. ☒ normal ☐ niedrig	**3.4.3 Risiko mit TOM (Restrisiko)** ☐ hoch…. ☐ normal ☒ niedrig	**3.4.4 Anmerkung zur Risikobewertung** Das Änderungsmanagement ist bei Stadt zuverlässig etabliert.

3.5 ■ Datenminimierung (DM) ■

3.5.1 Beschreibung relevanter Szenarien und deren möglichen Folgen/Auswirkungen
Folgende Szenarien wurden betrachtet:

- Unbefugte Aufzeichnung (siehe Punkt 3.1.1)
- Sonstiger Datenüberhang
  Es werden Inhaltsdaten über das VKS verarbeitet, deren Verarbeitung von Vornherein nicht erforderlich ist.
- Löschung
  Protokolldaten für administrative Zugriffe werden nicht gelöscht.
- (…)

Die Folgen für betroffene Personen werden als überschaubare angesehen.

3.5.2 Risiko ohne TOM (Ausgangsrisiko)	3.5.3 Risiko mit TOM (Restrisiko)	3.5.4 Anmerkung zur Risikobewertung
☐ hoch….	☐ hoch….	Bei mündlichen Kommunikationen besteht trotz Vorgaben und Sensibilisierung die Gefahr, dass nicht erforderliche personenbezogene Daten ausgetauscht werden.
☒ normal	☒ normal	
☐ niedrig	☐ niedrig	

3.6 Nichtverkettung (NV)

3.6.1 Beschreibung relevanter Szenarien und deren möglichen Folgen/Auswirkungen

Folgende Szenarien wurden betrachtet:

- Unzureichende Konferenztrennung (siehe Punkt 3.1.1)
- (…)

Die Folgen sind überschaubar für betroffene Personen.

3.6.2 Risiko ohne TOM (Ausgangsrisiko)	3.6.3 Risiko mit TOM (Restrisiko)	3.6.4 Anmerkung zur Risikobewertung
☐ hoch….	☐ hoch….	Die in diesem Bereich wirkenden Schutzmaßnahmen führen zu einem angemessenen Schutzniveau.
☒ normal	☒ normal	
☐ niedrig	☐ niedrig	

3.7 Transparenz (TP)

3.7.1 Beschreibung relevanter Szenarien und deren möglichen Folgen/Auswirkungen

Folgende Szenarien wurden betrachtet:

- Informationspflicht
  Die Informationspflichten nach Art. 13 DSGVO werden nicht (vollständig) erfüllt.
- (…)

Die Folgen für betroffene Personen werden als überschaubar eingeschätzt.

3.7.2 Risiko ohne TOM (Ausgangsrisiko)	3.7.3 Risiko mit TOM (Restrisiko)	3.7.4 Anmerkung zur Risikobewertung
☐ hoch….	☐ hoch….	Die umgesetzte Automatisierung des Informationsprozesses lässt keine nennenswerte Gefährdung erwarten.
☒ normal	☐ normal	
☐ niedrig	☒ niedrig	

3.8 Intervenierbarkeit (IV)

3.8.1 Beschreibung relevanter Szenarien und deren möglichen Folgen/Auswirkungen

Folgende Szenarien wurden betrachtet:

- Auskunftsersuchen
  Die Stadt kann ein rechtmäßiges Auskunftsersuchen einer betroffenen Person nicht rechtskonform beantworten.
- Löschersuchen
  Die Stadt kann einem rechtmäßigen Löschersuchen einer betroffenen Person nicht rechtskonform nachkommen.
- (…)

Die Folgen für betroffene Personen werden als überschaubar eingeschätzt.

3.8.2 Risiko ohne TOM (Ausgangsrisiko)	3.8.3 Risiko mit TOM (Restrisiko)	3.8.4 Anmerkung zur Risikobewertung
☐ **hoch….** ☒ **normal** ☐ **niedrig**	☐ **hoch….** ☐ **normal** ☒ **niedrig**	Die in diesem Bereich wirkenden Schutzmaßnahmen führen zu einem angemessenen Schutzniveau.

3.9 ■ Gesamtbewertung ■

3.9.1 Gesamtbewertung Restrisiko

Nach dem Maximalprinzip besteht insgesamt ein „**normales**“ Restrisiko bzw. eine vertretbare Restgefährdung (vgl. VT, DM und NV), das von der Stadt als angemessen angesehen wird. Nach den Regelungen im Datenschutz-Management werden auch die Risiken bei der Verarbeitung durch das VKS laufend überwacht, so dass eine Änderung des Risikoprofils rasch erkannt und geeignet behandelt werden kann.

4. Schutzmaßnahmen (TOM)

4.1 ■ Spezielle TOM ■

Nr.	TOM – Bezeichnung und Beschreibung	Wirkung	Verweise
4.1.1	**Kamera- und Mikrofonaktivität:** Alle genutzten Endgeräte (z.B. PC, Tablet, Smartphone) der teilnehmenden Personen stellen auf der IT-Anwendungsebene – soweit nutzbar – auffällig und eindeutig mittels eines Kamera- und Mikrofonsymbols optisch dar, wenn die Kamera und/oder das Mikrofon in der Videokonferenz aktiviert sind. Zusätzlich zu diesen optischen Darstellungen ist auch ein entsprechendes akustische Ansage für die Kamera- und Mikrofonaktivität initial konfiguriert (Barrierefreiheit). Vor dem Beitritt und während der Videokonferenz können teilnehmende Personen ihre Kamera und ihr Mikrofon jederzeit deaktivieren.	VT, DM, NV	//Spezifikation „VK-Fiktivia“ (Dok-ID 201907020945).
4.1.2	**Teilnehmerliste:** Alle Teilnehmenden haben die Möglichkeit, sich jederzeit während der Konferenz eine Liste der in der Videokonferenz befindlichen Teilnehmenden anzeigen zu lassen. Das Beitreten sowie das Verlassen von Teilnehmenden wird akustisch über einen Ton allen anderen Teilnehmenden signalisiert.	VT, NV	//Spezifikation „VK-Fiktivia“ (Dok-ID 201907020945).
4.1.3	**Chat:** Gesendete Chat-Nachrichten werden nicht archiviert und werden spätestens beim Beenden einer Konferenz automatisch gelöscht. Durch die Moderierenden einer Konferenz kann die Chat-Funktion vollständig deaktiviert werden.	VT, NV	//Spezifikation „VK-Fiktivia“ (Dok-ID 201907020945).
4.1.4	**Teilen von Bildschirminhalten:** Die Funktionen zum Teilen von Bildschirminhalten ermöglicht eine zuverlässige aktive Auswahl der zu teilenden Inhalte (z. B. gesamter Desktop oder nur bestimmte Fenster, Programme oder Dateien). Die Teilenden können jederzeit die Funktion zum Teilen wieder deaktivieren.	VT, DM, NV	//Spezifikation „VK-Fiktivia“ (Dok-ID 201907020945).
4.1.5	**Virtueller Hintergrund:** Vor dem Beitritt und während der Videokonferenz können von den teilnehmenden Personen Funktionen zur Hintergrundauswahl (virtueller oder verwischter Hintergrund) genutzt werden.	VT, DM, NV	//Spezifikation „VK-Fiktivia“ (Dok-ID 201907020945).
4.1.6	**Moderation:** Nur Personen mit einer Moderatorenrolle können	VT, NV	//Spezifikation „VK-Fiktivia“ (Dok-ID 201907020945).

Nr.	TOM – Bezeichnung und Beschreibung	Wirkung	Verweise
	• Teilnehmende nach erfolgreicher Identifizierung im Warteraum an einer Konferenz teilnehmen lassen, • unberechtigte Teilnehmende aus der Videokonferenz ausschließen, • den Vortragsmodus aktivieren und deaktivieren (alle Kameras und Mikrofone deaktiviert mit Ausnahme der Vortragenden) und • eine Videokonferenz beenden.		
4.1.7	**Bedarfsgerechte personelle Zusatzausstattung:** Bei Bedarf werden nutzende Beschäftigte geeignet ausgestattet (z. B. mit Headset und Sichtschutzfolie), um insbesondere auch im Home-Office eine sichere Teilnahme an Videokonferenzen zu gewährleisten.	VT, NV	//Konzept Betriebskonzept „VK-Fiktivia“ (Dok-ID 202001160900).
4.1.8	**Bedarfsgerechte räumliche Zusatzausstattung:** Bei Räume mit einer fest installierten Videokonferenzmöglichkeit (z. B. Raumsysteme) wird der Raum entsprechend sicher ausgewählt und gegebenenfalls geeignet eingerichtet.	VT, NV	//Konzept Betriebskonzept „VK-Fiktivia“ (Dok-ID 202001160900).
4.1.9	**Ausgeschlossene Funktionen:** Im Rahmen einer Videokonferenz sind weder eine Aufzeichnung der Konferenz noch eine Dateiablage mittels des VKS möglich.	VT, DM, NV	//Spezifikation „VK-Fiktivia“ (Dok-ID 201907020945).
4.1.10	**Telefonkonferenz als Alternative:** Bei Nichtverfügbarkeit oder Störung des VKS kann bei Bedarf auf eine Telefonkonferenz ausgewichen werden.	VB, DM	//Spezifikation „Telefonanlage“ (Dok-ID 20702181010).
4.1.11	(…)	(…)	(…)

4.2 ■ Adaptive TOM ■

Nr.	TOM – Bezeichnung und Beschreibung	Wirkung	Verweise
4.2.1	**Authentifizierung:** Die Einwahl in eine Videokonferenz erfolgt mittels einer eindeutige Raumnummer und einer PIN, die auf einem sichern Weg den Teilnehmenden übermittelt werden.	VT, RI, NV	//Spezifikation „VK-Fiktivia“ (Dok-ID 201907020945).
4.2.2	**Berechtigung:** Für die Anwender sowie die Administratoren des VKS besteht ein Rollen- und Berechtigungskonzept, das den Rollen nach dem „Need-to-know“-Prinzip nur die minimal notwendigen Berechtigungen zuweist. Davon mit umfasst sind insbesondere auch die Berechtigung für die User-Metadaten (z.B. Protokolldaten) sowie die Berechtigung für die Änderung von kritischen Konfigurationen und Leistungsmerkmalen.	VT, DI, NV	//Konzept Berechtigungsmanagement „VK-Fiktivia“ (Dok-ID 201908021030).
4.2.3	**Verschlüsselung:** Eine angemessene Transportverschlüsselung der Inhaltsdaten wie auch der Rahmendaten ist wirksam umgesetzt.	VT, DI, NV	//Spezifikation „VK-Fiktivia“ (Dok-ID 201907020945).
4.2.4	**Patch Management:** Das VKS wird durch regelmäßige und vorab geprüfte (Funktions-/Sicherheits-)Updates aktuell gehalten. Dabei kommt ein Testkonzept zur Anwendung, das alle technischen und fachlichen Anforderungen umfasst.	VT, DI, VB, NV	//Konzept Betriebskonzept „VK-Fiktivia“ (Dok-ID 202001160900) und //Konzept Testkonzept "VK-Fi„tivia" (Dok-ID 202001101000).
4.2.5	**Sensibilisierung:** Eine Einweisung und Information für VKS-Benutzende wird in geeigneter Form durchgeführt.	VT, RI, DM, TP, NV	//Konzept Einweisungsprozess „VK-Fiktivia“ (Dok-ID 201909120850) inkl. //Doku Anleitung „VK-Fiktivia“ (Dok-ID 201909151300) und //Konzept Information „VK-Fiktivia“ (Dok-ID 20190916090).
4.2.6	**Protokollierung:** Durch eine automatisierte Protokollierung (Log-Dateien) werden Videokonferenzen, die in der Vergangenheit stattfanden, prüfbar gemacht.	VB, TP	//Konzept Betriebskonzept „VK-Fiktivia“ (Dok-ID 202001160900).
4.2.7	**Löschen:**	VT,DM, NV, IV	//Konzept Betriebskonzept „VK-Fiktivia“ (Dok-ID 202001160900).

Nr.	TOM – Bezeichnung und Beschreibung	Wirkung	Verweise
	Personenbezogene Daten, die länger als die Durchführungszeit der entsprechenden Videokonferenz verarbeitet werden (z.B. Protokolldaten, Benutzerkonto), werden nach den festgelegten Aufbewahrungsfristen gelöscht. Alle anderen personenbezogenen Daten werden spätestens zusammen mit der Beendigung einer Videokonferenz automatisiert gelöscht.		
4.2.8	**Auskunft:** Ein Muster mit Erstellungshinweisen zeigt auf, wie im Fall eines Auskunftsanspruchs die einschlägigen personenbezogenen Daten aus dem VKS zu einer betroffenen Person zusammengestellt werden können.	IV, TP	//Konzept Betriebskonzept „VK-Fiktivia“ (Dok-ID 202001160900).
4.2.9	**Information:** Für die Nutzung des VKS wurde eine Information nach Art. 13 DSGVO erstellt, die an die betroffenen Personen vorab gegeben wird.	TP	//Information „VK-Fiktivia“ (Dok-ID 20190916090).
4.2.10	**Geschäftsprozess:** Der Geschäftsprozess „Videokonferenz durchführen“ wurde als städtischer Geschäftsprozess modelliert, in die städtische Prozesslandkarte integriert und veröffentlicht.	Alle Ziele	//Geschäftsprozess „Videokonferenz durchführen“ (Dok-ID 202106051500).
4.2.11	(…)	(…)	(…)

4.3 ■ Übergreifende TOM ■

Nr.	TOM – Bezeichnung und Beschreibung	Wirkung	Verweise
4.3.1	**Datenschutz-Managementsystem:** Ein Datenschutz-Managementsystem ist bei der Stadt wirksam eingeführt.	Alle Ziele	//Konzept DS-Management (Dok-ID 201503010900).
4.3.2	**Regelung Datenübermittlung:** Eine Dienstanweisung für die Übermittlung personenbezogener Daten existiert und ist wirksam verankert.	VT, DM, NV, TP	//Anweisung Datenübermittlung (Dok-ID 201804231015).
4.3.3	**Informationssicherheitsmanagementsystem und Sicherheitskonzept:** Die Stadt hat im Rahmen ihres Informationssicherheitsmanagementsystems (ISMS) ein Informationssicherheitskonzept (ISK) nach IT-Grundschutz des BSI wirksam umgesetzt.	VT, VB, DI	//Konzept ISMS (Dok-ID 278169) und //Konzept ISK (Dok-ID 16340).

Nr.	TOM – Bezeichnung und Beschreibung	Wirkung	Verweise
4.3.4	**Veränderungsmanagement:** Technische und organisatorische Änderungen beim Ablauf einer VKS-Videokonferenz werden systematisch erfasst und in die einschlägigen Konzepte eingearbeitet.	RI	//Geschäftsprozess „Änderungen managen (Changemanagement)“ (Dok-ID 201709161400).
4.3.5	(…)		

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.