

Beschreibung der Stadt Fiktivia für das Betriebsmittel

Telefonsystem (TKS)

[Dokument-ID: BM202110111620]

BayLfD-Stand: 01.05.2022

Inhalt

| | |
|---|---|
| 1. Beteiligte Personen und Status | 2 |
| 2. Anlagen bzw. Verweise zum Betriebsmittel | 2 |
| 3. Änderungshistorie | 2 |
| 4. Zeitpunkt der nächsten routinemäßigen Überprüfung | 2 |
| 5. Allgemeine Angaben | 3 |
| 6. Eigenschaften des Betriebsmittels | 3 |
| 7. Freigabe von nutzenden Verarbeitungen | 4 |
| 8. Kategorien der personenbezogenen Daten | 4 |
| 9. Kategorien der betroffenen Personen | 4 |
| 10. Kategorien der Empfänger | 4 |
| 11. Übermittlungen von personenbezogenen Daten | 4 |
| 12. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien | 5 |
| 13. Ausgangsrisiko | 5 |
| 14. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen | 5 |
| 15. Restrisiko | 5 |
| 16. Genutzte unmittelbare Betriebsmittel | 6 |
| 17. Federführende fachliche Organisationseinheit | 6 |
| 18. Stellungnahme des behördlichen Datenschutzbeauftragten | 6 |

1. Beteiligte Personen und Status

| | | |
|--|--|--|
| 1.1 An Beschreibung beteiligte Person(en) und ihre Rolle(n) Musterfrau, Klara [Federführung, Fachbereich] Mustertech, Eva [Beratung, IT] Muster, Hans [Beratung, bDSB] | 1.2 Status <input checked="" type="checkbox"/> in Bearbeitung <input type="checkbox"/> Aktiviert <input type="checkbox"/> Deaktiviert <input type="checkbox"/> Sonstig: <bitte Status angeben> | 1.3 Anmerkung zum Status --- |
|--|--|--|

2. Anlagen bzw. Verweise zum Betriebsmittel

| Nr. | Bezeichnung der Anlage bzw. des Verweises | Quelle und Anmerkung |
|-----|--|---|
| A1 | Beschreibung Betriebsmittelgruppe „Bildschirmarbeitsplatz“ | Dok-ID BM202110070840 |
| A2 | Betriebshandbuch „TK-System“ inkl. Berechtigungskonzept und Informationen sowie Anleitungen für die relevanten TKS-Benutzer. | Dok-ID 201206091000 |
| A3 | Spezifikation „Telefonanlage“ inkl. Lösch- und Protokollierungskonfiguration sowie Testkonzept | Dok-ID 200702181010 |
| A4 | Städtische Dienstanweisung für IT und Telekommunikation | Dok-ID 200309091000 |
| A5 | BSI-Baustein „NET.4.1:TK-Anlagen“ | https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompodium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html |
| A6 | BSI-Baustein „NET.4.2: VoIP“ | |
| A7 | (…) | (…) |

3. Änderungshistorie

| Wann? | Wer? | Was? |
|------------|-------------------|-----------------|
| 11.10.2021 | Musterfrau, Klara | Initialisierung |
| (…) | (…) | (…) |

4. Zeitpunkt der nächsten routinemäßigen Überprüfung

Klicken Sie hier, um ein Datum einzugeben.

5. Allgemeine Angaben

| | | |
|--|---------------------------------|--|
| 5.1 Bezeichnung des Betriebsmittels Telefonsystem der Stadt (TKS) | 5.2 Aktenzeichen 0471 | 5.3 Stand siehe 3. Änderungshistorie |
| 5.4 Verantwortlicher (Bezeichnung, Anschrift, Telefonnummer und E-Mail-Adresse der Institution) Stadt Fiktivia, Musterstraße 1, 85346 Musterhausen, Tel.: 0867532468-0, poststelle@fiktivia.de | | |
| 5.5 Datenschutzbeauftragter des Verantwortlichen (Name, dienstliche Anschrift, Telefonnummer und E-Mail-Adresse) Herr Hans Muster, Rechtsabteilung, Musterstraße 1, 85346 Musterhausen, Tel.: 0867532468-30, datenschutz@fiktivia.de | | |
| 5.6 Betreiber (Bezeichnung, Anschrift, Telefonnummer und E-Mail-Adresse der Institution) Betreiber ist der Verantwortliche, siehe Punkt 5.4 | | |
| 5.7 Datenschutzbeauftragter des Betreibers (Name, dienstliche Anschrift, Telefonnummer und E-Mail-Adresse) Siehe Punkt 5.5 | | |

6. Eigenschaften des Betriebsmittels

| | |
|---|---|
| 6.1 Kurzdarstellung Die Stadt verwendet ein selbst betriebenes Telefonsystem (TKS) für die Sprachtelefonie. Dieses besteht insbesondere aus der zentralen Telefonanlage und den daran angeschlossenen Endgeräten. | |
| 6.2 Abgrenzung Von dieser Beschreibung werden Endgeräte für die Sprachtelefonie, die nicht an das TKS angebunden sind, nicht mit umfasst (z.B. Handy mit eigenem Mobilfunkvertrag). Ebenfalls nicht mit umfasst sind andere Telekommunikationsdienste, wie etwa Fax-Systeme. (...) | |
| 6.3 Ausführliche Eigenschaftsdarstellung Mit dem städtischen zentralen Telefonsystem, kurz TKS, werden die Telefon-Endgeräte intern verbunden und sind extern an das öffentliche Telefonnetz angeschlossen. Die genutzte Systemtechnik ist IP-basiert (Voice over IP - VoIP). Neben drahtgebundenen werden auch mobile Endgeräte verwendet. (...) | |
| 6.4 Komplexität <input type="checkbox"/> hoch <input checked="" type="checkbox"/> niedrig | 6.5 Anmerkung zur Komplexität Die Komplexität der TKS-Verarbeitung wird als überschaubar und nicht als hoch komplex angesehen. (...) |
| 6.6 Notwendigkeit und Verhältnismäßigkeit Die Sprachtelefonie ist als Kommunikationsmittel unverzichtbar. (...) | |
| 6.7 Aggregation <input type="checkbox"/> Einzelbetriebsmittel <input type="checkbox"/> Betriebsmittelgruppe <input checked="" type="checkbox"/> Unterbetriebsmittel <input type="checkbox"/> Sonstig: <bitte Aggregation angeben> | 6.8 Anmerkung zur Aggregation Das TKS wird als Unterbetriebsmittel der übergeordneten Betriebsmittelgruppe „Bildschirmarbeitsplatz“ (siehe Anlage A1) modelliert. |

7. Freigabe von nutzenden Verarbeitungen

| |
|---|
| 7.1 Nicht freigegebene Verarbeitungen In jedem Organisationsbereich ist nach einer Prüfung festgelegt, welche organisationsspezifischen Daten nicht mündlich und somit auch nicht telefonisch verarbeitet werden dürfen (siehe Anlage A4). (...) |
| 7.2 Verarbeitungen mit Freigabe nach Einzelfallentscheidung --- |
| 7.3 Freigegebene Verarbeitungen Die Nutzung des TKS ist in den Bereichen möglich, in denen die Nutzung nicht ausdrücklich ausgeschlossen (siehe Punkt 7.1) oder bei sorgfältiger Betrachtung nicht angeraten ist. |

8. Kategorien der personenbezogenen Daten

| Nr. | Bezeichnung der Daten |
|-----|--|
| D1 | Das TKS unterstützt zahlreiche Verarbeitungstätigkeiten. Dementsprechend umfangreich ist die Bandbreite der verarbeiteten möglichen Inhaltsdaten . |
| D2 | Metadaten, die bei der Sprachtelefonie verarbeitet werden (Rahmendaten), wie etwa Rufnummern. |
| D3 | Daten, die durch die Administration des TKS verarbeitet werden. Darunter fallen: <ul style="list-style-type: none">• Benutzerkontodaten,• Systemprotokollierung von Systemzugriffen,• (...) |
| D4 | (...) |

9. Kategorien der betroffenen Personen

| Nr. | Betroffene Personen |
|-----|--|
| P1 | Personen, deren Daten als Inhaltsdaten verarbeitet werden (Verarbeitung der Datenkategorien D1). |
| P2 | Personen, die an der Sprachtelefonie des TKS teilnehmen (Verarbeitung der Datenkategorie D2). |
| P3 | Personen, die das TKS administrieren (Verarbeitung der Datenkategorie D3). |
| P4 | (...) |

10. Kategorien der Empfänger

| Nr. | Empfänger | Anlass der Offenlegung |
|-----|-----------|------------------------|
| --- | --- | --- |

11. Übermittlungen von personenbezogenen Daten

| Nr. | Drittland oder internationale Organisation | Geeignete Garantien im Falle einer Übermittlung nach Art. 49 Abs. 1 Unterabsatz 2 DSGVO |
|-----|--|---|
| -- | --- | --- |

12. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien

| Nr. | Löschungsfrist |
|-----|---|
| F1 | Siehe Löschkonfiguration des TKS (Anlage A3). |

13. Ausgangsrisiko

| 13.1 Risiko ohne TOM | 13.2 Begründung und Anmerkung zur Risikobewertung |
|---|--|
| <input checked="" type="checkbox"/> hoch.... <input type="checkbox"/> normal <input type="checkbox"/> niedrig | Einen besonderen Risikoschwerpunkt weist die Sprachtelefonie im Bereich der Vertraulichkeit auf. Je nach Verarbeitungstätigkeiten, die das TKS nutzt, kann das Risiko insbesondere im Hinblick auf die möglichen Folgen einer Vertraulichkeitsverletzung für betroffene Personen hoch sein. (...). |

14. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

Folgende Maßnahmen wurden hinsichtlich des TKS wirksam umgesetzt:

a) Spezielle Maßnahmen

- **M15.1 Netztrennung**
Das VoIP-Netz ist in geeigneter Weise vom städtischen Datennetz getrennt (vgl. Anlage A3).
- **M15.2 Headset**
Das Nutzen von Headsets beim Telefonieren ist in bestimmten Konstellationen vorgeschrieben (vgl. Anlage A4).
- (...)

b) Adaptive Maßnahmen

- **M15.4 Konfiguration**
Nicht benötigte oder wegen ihres Risikopotenzials als kritisch eingestufte Leistungsmerkmale sind dauerhaft deaktiviert und können nur durch speziell berechtigte Administratoren geändert werden (vgl. Anlage A3).
- **M15.5 Testkonzept**
Bei Neueinrichtung oder bei einer relevanten Änderung einer TKS-Komponente wird ein Test nach dem zuvor initial erstellten TKS-Testkonzept (vgl. Anlage A3) durchgeführt und dokumentiert.
- **M15.6 Berechtigung**
Ein TKS-Berechtigungskonzept besteht (vgl. Anlage A2).
- **M15.7 Sensibilisierung**
Anlassbezogen werden die städtischen Beschäftigten bzgl. der Risiken beim Telefonieren sensibilisiert (vgl. Anlage A4).
- (...)

c) Übergreifende Maßnahmen

- **M15.10 Firewall**
Die bestehende Firewall ist für den Einsatz von VoIP angepasst (vgl. Anlage A3).
- (...)

15. Restrisiko

| 15.1 Risiko mit TOM | 15.2 Anmerkung zur Risikobewertung |
|---|---|
| <input type="checkbox"/> hoch.... <input checked="" type="checkbox"/> normal <input type="checkbox"/> niedrig | Nach wirksamer Umsetzung aller unter Punkt 14 genannten Maßnahmen zeigt die Erfahrung, dass ein angemessenes Schutzniveau erreicht wird. (...). |

16. Genutzte unmittelbare Betriebsmittel

| Bezeichnung | Verweisung |
|-------------|------------|
| --- | --- |

17. Federführende fachliche Organisationseinheit

Dienststelle / Referat / Organisationseinheit

Städtisches Referat für IT – IT-Referat

18. Stellungnahme des behördlichen Datenschutzbeauftragten

18.1 Liegt eine Stellungnahme des behördlichen Datenschutzbeauftragten vor?

Ja Nein

18.2 Ggf. nähere Erläuterung

Der behördliche Datenschutzbeauftragte war bei Erstellung dieser Beschreibung beratend mit beteiligt.

Hinweise zum Formular

A) Zielsetzung der Beschreibung

Mit dieser Beschreibung wird ein technisches Betriebsmittel umfassend beschrieben. Technische Betriebsmittel können insbesondere unverzichtbar für eine Verarbeitungstätigkeit sein und diese unmittelbar unterstützen (z. B. IT-gestützter Arbeitsplatz, E-Mail-System) oder in der Umsetzung von technischen und organisatorischen Maßnahmen der Verarbeitungstätigkeit mittelbar dienen, indem sie diese als technische und organisatorische Schutzmaßnahmen hinsichtlich bestehender Risiken absichern (z. B. Backup-System, Firewall, Anti-Schadsoftware-System). Einige Betriebsmittel verarbeiten ihrerseits eigene personenbezogene Daten (spezifische Betriebsmitteldaten). Bei der Auswahl eines Betriebsmittels sind unter anderem auch der Zweck und die Rechtsgrundlage der Verarbeitung, die vom Betriebsmittel unterstützt wird, hinsichtlich der Angemessenheit des Betriebsmittels zu berücksichtigen.

B) Ausfüllhinweise zu den Einzelpunkten

| Punkt | Ausfüllhinweis |
|-------|--|
| 1.1 | <p>Angabe der an der Beschreibung beteiligten Personen mit ihrem Namen und ihrer ausgeübten Rolle(n). Die Anzahl der beteiligten Personen kann je nach Komplexität des betrachteten Betriebsmittels erheblich schwanken. Typische Rollen bei der Beschreibung-Erstellung sind:</p> <ul style="list-style-type: none"> • Auftraggeber/in (Person, die für die Beschreibung insgesamt zuständig ist und diese insbesondere auch aktiviert) • Federführung (falls man die Beschreibung-Erstellung als (Klein-)Projekt versteht, entspricht das Aufgabenprofil der Federführung dem einer Projektleitung) • Vertretung Auftraggeber/in (naheliegender ist, dass ein Vertreter der Fachlichkeit, die das betroffene Betriebsmittel gestaltet und beschreibt, diese Rolle wahrnimmt) • Vertretung IT-Bereich bei Betriebsmittel aus der IT • Beratung (naheliegender hierfür ist der Datenschutzbeauftragte) • Review (als Qualitätssicherungsmaßnahme ist es oft sinnvoll, eine in der Materie kompetente Person, die bei der Beschreibung-Erstellung selbst nicht beteiligt war, die Beschreibung insbesondere im Hinblick auf Logik, Plausibilität, Verständlichkeit und Vollständigkeit überprüfen zu lassen) |
| 1.2 | Der mögliche Standard- Status der Beschreibung umfasst auch eine Aktivierung und Deaktivierung. Eine Deaktivierung kommt etwa in Betracht, wenn die Beschreibung durch eine andere Beschreibung ersetzt wird, bei der die weitere Fortsetzung der Beschreibung-Versionierung nicht sinnvoll erscheint. |
| 1.3 | Optionale Anmerkungen zum festgelegten Status . |
| 2 | Der Unterschied zwischen einer Anlage und einem Verweis zur Beschreibung ist, dass die Anlage fest und ausschließlich zur Beschreibung gehört, während die verwiesenen Dokumente auch in anderen Zusammenhängen verwendet werden (Mehrfachverwendung). |
| 3 | In der Änderungshistorie werden die wesentlichen Änderungen der Beschreibung nachvollziehbar festgehalten. |
| 4 | Da die Beschreibung regelmäßig hinsichtlich eines inzwischen eingetretenen Änderungsbedarfs überprüft werden sollte, kann hier ein routinemäßiges Überprüfungsdatum eingetragen werden. |
| 5.1 | Die Bezeichnung des Betriebsmittels soll allgemeinverständlich sein. |
| 5.2 | Angabe des Aktenzeichens , unter dem die Beschreibung abgelegt wird. |
| 5.3 | Bearbeitungsstand der Beschreibung. |

| Punkt | Ausfüllhinweis |
|-------|---|
| 5.4 | Falls das beschriebene Betriebsmittel personenbezogenen Daten verarbeitet, wird hier die die Behörde oder sonstige öffentliche Stelle, die selbst oder mittels eines Auftragsverarbeiters die Verarbeitung durchführt, angegeben. Bei einer gemeinsamen Verantwortlichkeit sind hier alle relevanten Verantwortlichen einzutragen. Als „Anschrift“ ist jeweils Postleitzahl, Ort, Straße und Hausnummer anzugeben. |
| 5.5 | Angabe des Datenschutzbeauftragten des Verantwortlichen . |
| 5.6 | Angabe der Stelle , die das Betriebsmittel technisch betreibt . |
| 5.7 | Angabe des Datenschutzbeauftragten des Betreibers . |
| 6.1 | Kurze Darstellung der Haupteigenschaft(en) des Betriebsmittels. |
| 6.2 | Klarstellende Abgrenzung , welche anderen Betriebsmittel nicht von diese Beschreibung mit umfasst werden. |
| 6.3 | Ausführliche Darstellung der wesentlichen Eigenschaften des Betriebsmittel. Detaillierungsgrad orientiert sich insbesondere an die Komplexität und das einschlägige maximale Ausgangsrisiko des Betriebsmittels. |
| 6.4 | Angabe des Komplexitätsgrades für die Verarbeitung durch das Betriebsmittel. |
| 6.5 | Anmerkung und Begründung des angegebenen Komplexitätsgrads . |
| 6.6 | Angabe der wesentlichen Aspekte zum notwendigen und verhältnismäßigen Einsatz des Betriebsmittels. |
| 6.5 | Je nach Komplexität und Bedarf kann ein Betriebsmittel mit unterschiedlichen Aggregationsstufen beschrieben werden. Die Aggregation hilft insbesondere, eine technisch vorhandene Komplexität zwar abbilden zu können, die fachliche Sicht jedoch dabei mit dieser technischen Komplexität nicht unnötig zu belasten (indem z.B. fachlich nur die Betriebsmittelgruppe adressiert wird). |
| 6.6 | Anmerkung zur gewählten Aggregationsstufe . |
| 7.1 | Festlegung und hinreichende Beschreibung von Verarbeitungen , die durch das VKS nicht unterstützt werden dürfen. |
| 7.2 | Festlegung und hinreichende Beschreibung von Verarbeitungen , die erst nach einer Einzelfallenscheidung und gegebenenfalls nach einer Implementierung von zusätzlichen Maßnahmen durch das VKS unterstützt werden dürfen. |
| 7.3 | Verarbeitungen , die das VKS nutzen dürfen. |
| 8 | Unter Kategorien sind aussagefähige Oberbegriffe zu verstehen, z.B. „Name und Vorname“, „Anschrift“, „Staatsangehörigkeit“. Angaben rein technischer Art (z.B. Feldnummern, Schlüsselnummern usw.) sind nicht erforderlich. Die Bezugnahme auf beigefügte Beschreibungen von Datensätzen ist zulässig, wenn aus diesen die personenbezogenen Daten eindeutig hervorgehen. |
| 9 | Zu beschreiben sind hier Personengruppen , die von der Verarbeitung betroffen sind. Anzugeben sind auch Personengruppen innerhalb der öffentlichen Stellen, deren Daten verarbeitet werden. |

| Punkt | Ausfüllhinweis |
|-------|---|
| 10 | Kategorien der Empfänger , denen die spezifischen personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen. Nach Art. 4 Nr. 9 DSGVO ist Empfänger „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht“. Zu den Empfängern gehören daher auch Auftragsverarbeiter sowie Stellen innerhalb der Behörde, denen die Daten weitergegeben werden oder die Zugriff auf die Daten haben. Zu beachten ist ferner die Ausnahmeregelung des Art 4 Nr. 9 Satz 2 DSGVO, wonach Behörden unter bestimmten, in dieser Vorschrift genannten Voraussetzungen nicht als Empfänger gelten. |
| 11 | Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation; als Drittländer werden alle Länder außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraumes bezeichnet. Im Falle einer Übermittlung an ein Drittland oder eine internationale Organisation nach Art. 49 Abs. 1 Unterabsatz 2 DSGVO sind die geeigneten Garantien in Bezug auf den Schutz personenbezogener Daten in Spalte 3 festzuhalten. Soweit erforderlich kann dazu auf ergänzende Dokumente verwiesen werden. |
| 12 | Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es für die Zwecke erforderlich ist, für die sie verarbeitet werden (Grundsatz der „Speicherbegrenzung“, Art. 5 Abs. 1 Buchst. e DSGVO). Gespeicherte Daten sind daher unverzüglich zu löschen , sobald sie für die Aufgabenerfüllung der öffentlichen Stelle nicht mehr erforderlich sind (vgl. DSGVO-Erwägungsgrund 39). Der Verantwortliche sollte daher Fristen für die Löschung oder regelmäßige Überprüfung der personenbezogenen Daten vorsehen (vgl. DSGVO-Erwägungsgrund 39). Fachgesetzliche Regelungen sind zu beachten. Über den eigentlichen Speicherungsanlass hinaus kann eine Speicherung auch zur Erfüllung von Dokumentationspflichten erforderlich sein. Anzugeben ist auch der Beginn der Löschungsfrist. Vor einer Löschung von Daten sind die archivrechtlichen Anbietungspflichten zu beachten. |
| 13.1 | Für das Betriebsmittel muss die Höhe des Ausgangsrisikos angegeben werden. |
| 13.2 | Begründung und sonstige Anmerkungen zur generellen Risikoeinstufung des Ausgangsrisikos . |
| 13 | Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DSGVO, ggf. einschließlich der Maßnahmen nach Art. 8 Abs. 2 Satz 2 BayDSG; hier sind die technischen und organisatorischen Maßnahmen nach Art. 32 Abs. 1 DSGVO allgemein zu beschreiben oder darauf – etwa in der Form einer datenschutzrechtlichen Risikoanalyse – zu verweisen. |
| 15.1 | Für das Betriebsmittel muss die Höhe des generellen Restrisikos angegeben werden. |
| 15.2 | Begründung und sonstige Anmerkungen zur Risikoeinstufung des Restrisikos . |
| 16 | Angabe/ Verweis auf Beschreibungen von Betriebsmitteln , die das beschriebene Betriebsmittel unmittelbar nutzt. Von den unmittelbar genutzten Betriebsmitteln zu unterscheiden sind die mittelbar unterstützenden Betriebsmittel, die in Form von Schutzmaßnahmen bestehende Risiken reduzieren (z.B. Backup-System, Firewall-System, Anti-Schadsoftware-System). Die mittelbaren Betriebsmittel finden sich in der Form von Schutzmaßnahmen unter dem Punkt 13. |
| 17 | Hier ist die Dienststelle, das Referat oder die sonstige Organisationseinheit der öffentlichen Stelle anzugeben, die insgesamt für das Betriebsmittel aus fachlicher Sicht federführend ist. |
| 18.1 | Angabe, ob dem Datenschutzbeauftragten des Verantwortlichen vor dem erstmaligen Einsatz oder einer wesentlichen Änderung des Betriebsmittels, mit dem personenbezogene Daten verarbeitet werden, Gelegenheit zur Stellungnahme gegeben wurde. |

| Punkt | Ausfüllhinweis |
|-------|---|
| 18.2 | Erläuterungen zur Stellungnahme des Datenschutzbeauftragten. |