Formular „Technische und organisatorische Maßnahmen“ – TOM
gemäß Punkt V.4 der Datenschutzvereinbarung

**Technische und organisatorische Maßnahmen zur Umsetzung der in der AMS-Datenschutzvereinbarung festgelegten Datensicherheitsanforderungen**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Versions-Nr.[[1]](#footnote-1)** | **Datum** | **Ersteller\_in** | **Unternehmen****& Unternehmenssitz** | **Funktion im Unternehmen** |
| Drop-Down | Text hier eingeben. | Text hier eingeben. | Text hier eingeben. | Text hier eingeben. |
| Drop-Down | Text hier eingeben. | Text hier eingeben. | Text hier eingeben. | Text hier eingeben. |
| Drop-Down | Text hier eingeben. | Text hier eingeben. | Text hier eingeben. | Text hier eingeben. |
| Drop-Down | Text hier eingeben. | Text hier eingeben. | Text hier eingeben. | Text hier eingeben. |

In Umsetzung des **Artikels 32 der DSGVO** setzen wir **für vom AMS erteilte Datenverarbeitungsaufträge** Maßnahmen, die ein dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenes Schutzniveau gewährleisten.

Die technischen und organisatorischen Maßnahmen (TOM) sind nachfolgend angeführt. Wir überprüfen, bewerten und evaluieren (Art. 32 Abs 1 lit. d DSGVO) diese Maßnahmen **alle drei Jahre** auf ihre Wirksamkeit und passen sie erforderlichenfalls an. Eine Anpassung der TOM wird auch dann vorgenommen, wenn sich die Risikoeinschätzung (zB durch die Einführung einer neuen Datenanwendung) verändert oder von Seiten des AMS eine Anpassung als erforderlich erachtet wird.

Wir bestätigen, dass folgendes Formular vollständig ausgefüllt, alle geforderten Inhalte vorgelegt sowie eine Risikoanalyse gemäß Punkt 2 erstellt wurde.

|  |  |
| --- | --- |
| Ort, Datum eintragen.Ort, Datum | Name und Funktion eintragen.Name und Funktion |
|  | Unterschrift |

**Inhaltsverzeichnis**

[1. Einführung 3](#_Toc147237474)

[2. Risikoanalyse 4](#_Toc147237475)

[3. Datenschutzrechtliche Schulungen 5](#_Toc147237476)

[4. Zutrittsbeschränkungen 6](#_Toc147237477)

[5. Zugangs-, Zugriffs- und Betriebsbeschränkungen 7](#_Toc147237478)

[6. Verfügbarkeit, Belastbarkeit und Löschung 10](#_Toc147237479)

[7. Überprüfungsmöglichkeiten der rechtmäßigen Datenverarbeitung 12](#_Toc147237480)

# **Einführung**

Das Arbeitsmarktservice (AMS) nimmt die Verantwortung für die personenbezogenen Daten seiner Kund\_innen ernst. Diese Verantwortung erstreckt sich auch auf Sie als Partnerinstitution. Zur Erbringung der mit dem AMS vereinbarten Leistung verarbeiten Sie Daten der AMS-Kund\_innen. Ihre Organisation gilt daher datenschutzrechtlich als Auftragsverarbeiter\_in des AMS.

Gemäß DSGVO darf das AMS jedoch nur solche Auftragsverarbeiter\_innen heranziehen, welche (insbesondere im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen) hinreichende Garantien dafür bieten, dass technische und organisatorische Maßnahmen getroffen werden, die den Anforderungen der DSGVO genügen.

Damit das AMS erkennen kann, dass entsprechende Maßnahmen durch Sie gesetzt werden, ersuchen wir Sie, die nachfolgenden Fragen zu beantworten und die grundsätzlichen Vorgangsweisen Ihrer Organisation prägnant und nachvollziehbar darzustellen. Sollten einzelne Standorte von diesen grundsätzlichen Vorgehensweisen wesentlich abweichen, sind die Abweichungen standortspezifisch zu erläutern.

In diesen TOM ist es nicht erforderlich, Ihre Sicherheitsarchitektur im Detail preiszugeben bzw. detailliertere Nachweise beizulegen. Bei Überprüfungen, etwa im Zuge von Vor-Ort-Kontrollen, ist das AMS jedoch berechtigt, Nachweise zu den getroffenen Maßnahmen, wie zB ein mit den Aufgaben der Mitarbeiter\_innen korrespondierendes Berechtigungssystem, einzufordern.

Bei der Festlegung ihrer technischen und organisatorischen Maßnahmen sollten Sie die mit der DSGVO verbundenen hohen Bußgelder als auch das Recht auf Schadenersatz der Betroffenen nicht außer Acht lassen. Werden durch Ihre Organisation beispielsweise andere als mit dem AMS vereinbarte Daten ermittelt, vorhandene Daten für andere Zwecke verwendet, die Daten nicht vereinbarungsgemäß gelöscht oder geraten die personenbezogenen Daten der AMS-Kundinnen und -Kunden in unbefugte Hände, haften Sie als Auftragsverarbeiter\_in direkt bzw. werden selbst zum Verantwortlichen im Sinne der DSGVO.

Anregungen zum Thema „Datensicherheit“ finden Sie unter anderem unter:

* <https://www.wko.at/site/it-safe/sicherheitshandbuch.html>
* <https://www.wko.at/service/innovation-technologie-digitalisierung/it-sicherheit-datensicherheit.html>
* <https://www.cnil.fr/en/new-guide-regarding-security-personal-data>
* ISO/IEC-27000 Normenreihe
* Österreichische Informationssicherheitshandbuch (www.sicherheitshandbuch.gv.at)
* IT-Grundschutz des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) [www.bsi.bund.de](http://www.bsi.bund.de)

Hinweis: Das AMS übernimmt keine Gewähr und Haftung, dass die nachfolgende Vorlage und die darin erwähnten Maßnahmen den Anforderungen der DSGVO entsprechen. Ihre Ausführungen dienen lediglich dem AMS als interne Überprüfungsgrundlage. Das AMS behält sich vor, diese Erklärung an neue Entwicklungen und Erkenntnisse anzupassen und die entsprechende Umsetzung durch die Auftragsverarbeiter\_in einzufordern.

**Achtung: Die folgenden, unter den Punkten 4 bis 7 beschriebenen Maßnahmen stellen jeweils lediglich Beispiele dar und müssen nicht gänzlich vorliegen bzw. erfüllt sein. Sie haben die Möglichkeit ihre konkreten Maßnahmen in den Feldern „Anmerkungen, andere Maßnahmen“ zu ergänzen.**

# **Risikoanalyse**

Rechtsgrundlage: Art. 32 Abs. 2 DSGVO

Die technischen und organisatorischen Maßnahmen sind unter Berücksichtigung

* des Standes der Technik,
* der Implementierungskosten,
* der Art, des Umfanges, der Umstände und der Zwecke der Verarbeitung,
* der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

*Aus den Erwägungsgründen 75 und 76 der DSGVO:*

Die Risiken für die Rechte und Freiheiten natürlicher Personen können zu einem physischen, materiellen oder immateriellen Schaden führen, insbesondere wenn

* die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von den, dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann,
* die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren,
* personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffende Daten verarbeitet werden,
* persönliche Aspekte bewertet werden, insbesondere, wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen,
* personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.

Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person sollten in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden. Das Risiko sollte anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt.

**Verpflichtende Maßnahmen:**

✓ Es ist eine Risikoanalyse zur Datenverarbeitung für die, vom AMS beauftragte Dienstleistungen durchzuführen. Falls im Einzelfall erforderlich, ist eine Datenschutzfolgenabschätzung gemäß Art.35 durchzuführen.

✓ Diese Risikoanalyse ist regelmäßig zu überprüfen und anzupassen.

✓ Die technischen und organisatorischen Maßnahmen sind gemäß den Ergebnissen der Risikoanalyse zu treffen.

**Die Risikoanalyse ist den TOM‘s beizulegen.**

# **Datenschutzrechtliche Schulungen**

Rechtsgrundlage: insb. Art. 28 Abs. 3 lit. b, 29 und 39 Abs. 1 lit. a und b DSGVO

Die Einhaltung von datenschutzrechtlichen Bestimmungen hängt in hohem Maße von einer ausreichenden Sensibilisierung und Datenschutzschulung der Mitarbeiter\_innen ab. Dabei sollen im Wesentlichen folgende Ziele im Vordergrund stehen:

* Bewusstsein für datenschutzrechtliche Probleme schaffen
* Erläuterung der datenschutzrechtlichen Aufgaben und Verpflichtungen der Mitarbeiter\_innen
* Mitarbeiter\_innen zu datenschutzkonformem Verhalten befähigen
* Bereitschaft zu datenschutzkonformem Verhalten fördern

**Verpflichtende Maßnahmen:**

✓ Die betroffenen Mitarbeiter\_innen sind (ein)zuschulen und es sind zumindest alle drei Jahre Auffrischungsschulungen durchzuführen.

✓ Zusätzlich sind schriftliche Informationen den Mitarbeiter\_innen zum Datenschutz und zur Datensicherheit zur Verfügung zu stellen, zB Informationen im Intranet, regelmäßige Datenschutz-Newsletter, Verteilung des IT-Sicherheitshandbuch für Mitarbeiter\_innen ([www.it-safe.at](http://www.it-safe.at)).

Die Aktivitäten sind nachvollziehbar, insbesondere in Form von Teilnahmezertifikate/Besuchsbestätigungen der Mitarbeiter\_innen mit Punktation der Inhalte, Ort, Datum und Dauer der Schulungen zu dokumentieren und **auf Aufforderung vorzulegen**.

# **Zutrittsbeschränkungen**

Rechtsgrundlage: insb. Art. 5 Abs. 1 lit. f sowie Art. 28 Abs. 3 lit. c und 32 Abs. 1 lit. b DSGVO

Führen Sie bitte aus, durch welche **technischen Maßnahmen** die Räume, in denen sich personenbezogene Daten von AMS Kund\_innen befinden, angemessen vor unberechtigtem Zutritt geschützt werden.

|  |  |  |
| --- | --- | --- |
| **Sicherheitsschlösser** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Schließsysteme** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Alarmanlage** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |
| --- |
| **Anmerkungen, andere Maßnahmen (optional):** |
|       |

Führen Sie bitte aus, durch welche **organisatorischen Maßnahmen** die Räume, in denen sich personenbezogene Daten von AMS Kund\_innen befinden, angemessen vor unberechtigtem Zutritt geschützt werden.

|  |  |  |
| --- | --- | --- |
| **Schließregelung für die Räumlichkeiten** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Schlüsselbuch/Schlüsselregelung** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Ausweisregelung** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Sorgfältige Auswahl von Sicherheits-/Reinigungs-/IT-Personal bzw. -Firmen** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |
| --- |
| **Anmerkungen, andere Maßnahmen (optional):** |
|       |

# **Zugangs-, Zugriffs- und Betriebsbeschränkungen**

Rechtsgrundlage: insb. Art. 5 Abs. 1 lit. f sowie Art. 28 Abs. 3 lit. c und 32 Abs. 1 lit. b DSGVO

Führen Sie bitte aus, durch welche **technischen Maßnahmen** personenbezogene Daten in Ihren EDV-Systemen vor unberechtigtem Zugang und Zugriff als auch unbefugter Inbetriebnahme geschützt werden und wie die manuell geführten personenbezogenen Daten („Papierakt“) vor unberechtigtem Zugriff geschützt werden.

|  |  |  |
| --- | --- | --- |
| **Einstieg mittels Benutzer/Passwort** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Automatische Sperrmechanismen** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Einsatz von Anti-Viren Software** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Firewall** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **VPN Technologien** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Sperre von externen Schnittstellen (z.B. USB-Zugänge für externe Geräte)** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **eMail Verschlüsselungen** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Verschlüsselung von Datenträgern** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Frühestmögliche Pseudonymisierung der Daten** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Ablage von Papierakten in versperrten Schränken** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |
| --- |
| **Anmerkungen, andere Maßnahmen (optional):** |
|       |

**Verpflichtende AMS-spezifische Maßnahmen:**

✓ Die vertraglich vorgeschriebenen eServices des eAMS-Kontos sind für die elektronische Kommunikation mit dem AMS zu verwenden. Die betroffenen Mitarbeiter\_innen sind darüber schriftlich zu informieren.

✓ Das eService „Projekt/Veranstaltungszuordnung“ des eAMS-Kontos ist zwingend zu verwenden und laufend zu warten. Als Grundlage ist ein Berechtigungskonzept zu erstellen.

✓ Es sind Vorkehrungen zu treffen, dass personenbezogene Daten auf EDV-Geräten, die von unterschiedlichen Teilnehmer\_innen benutzt werden, vor unberechtigtem Zugriff geschützt sind.

Die Aktivitäten sind zu dokumentieren und **auf Aufforderung vorzulegen**.

Führen Sie bitte aus, durch welche **organisatorischen Maßnahmen** Ihre EDV-Systeme vor unberechtigtem Zugang und Zugriff als auch unbefugte Inbetriebnahme geschützt werden und die manuell geführten personenbezogenen Daten („Papierakt“) vor unberechtigtem Zugriff geschützt werden.

|  |  |  |
| --- | --- | --- |
| **Nutzung eines Berechtigungskonzepts** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Standardprozess für Berechtigungsvorgabe ist beschrieben** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Nutzung einer Passwort-Richtlinie oder Ähnliches** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Nutzung einer Telearbeit-Richtlinie oder Ähnliches** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Nutzungsverbot von nichtbetrieblicher Soft- und Hardware** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Installationsberechtigung von Programmen liegt ausschließlich bei IT-Administrator\_innen** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Laufende Software-Aktualisierungen, insbesondere von sicherheitsrelevanter Software (Antiviren-Programme, Browser etc.)** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Einrichtung einer Datenträgerverwaltung** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Einrichtung eines Mobile Device Managements** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Regelung zum Ausscheiden von Mitarbeiter\_innen** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Regelungen zum Schutz manuell geführter personenbezogener Daten vor unberechtigtem Zugriff** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |
| --- |
| **Anmerkungen, andere Maßnahmen (optional):** |
|       |

# **Verfügbarkeit, Belastbarkeit und Löschung**

Rechtsgrundlage: insb. Art. 5 Abs. 1 lit. e sowie Art. 28 Abs. 3 lit. c und g und 32 Abs. 1 lit. a DSGVO

Führen Sie bitte aus, durch welche **technischen Maßnahmen** Sie die **Verfügbarkeit der Daten und die Belastbarkeit der EDV-Systeme** gewährleisten.

|  |  |  |
| --- | --- | --- |
| **Es wird auf eine ausreichende EDV-Kapazität geachtet** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Klimatisierung der Serverräume** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Unterbrechungsfreie Stromversorgung (USV) der Server** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Es sind Maßnahmen gegen Feuer, Wasser und elektromagnetische Felder vorgesehen, die die Daten auf den Servern beeinträchtigen könnten** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |
| --- |
| **Anmerkungen, andere Maßnahmen (optional):** |
|       |

Führen Sie bitte aus, durch welche **organisatorischen Maßnahmen** Sie die **Verfügbarkeit der Daten und die Belastbarkeit der EDV-Systeme** gewährleisten.

|  |  |  |
| --- | --- | --- |
| **Einsetzung eines (getesteten) Backup- und Recoverykonzepts** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Aufbewahrung von Datensicherungen an einem externen, sicheren Ort** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Einrichtung eines Notfallplanes** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |
| --- |
| **Anmerkungen, andere Maßnahmen (optional):** |
|       |

Führen Sie bitte aus, durch welche Maßnahmen Sie die **ordnungsgemäße Löschung bzw. Vernichtung der Daten** gewährleisten.

|  |  |  |
| --- | --- | --- |
| **Automatisierte Löschungsroutine** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Manuelle Löschung** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Verlässliche und effektive Vernichtung von nicht mehr benötigten Datenträgern (Papier, CD, DVD, USB-Stick, Festplatten etc.)** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Anwendung geeigneter Löschprogramme zur irreversiblen Löschung von Daten auf Datenträgern, die wiederverwendet werden sollen** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |
| --- |
| **Anmerkungen, andere Maßnahmen (optional):** |
|       |

# **Überprüfungsmöglichkeiten der rechtmäßigen Datenverarbeitung**

Rechtsgrundlage: insb. Art. 5 Abs. 1 lit. a und Abs. 2 sowie Art. 28 Abs. 3 lit. c und 32 Abs. 1 DSGVO

Führen Sie bitte aus, durch welche Maßnahmen Sie feststellen, ob und von wem personenbezogene Daten eingegeben, eingesehen, verändert oder entfernt worden sind, um die rechtmäßige Verarbeitung zu überprüfen.

|  |  |  |
| --- | --- | --- |
| **(Automatische) Protokollierung auf Ebene der individuellen Benutzernamen** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Stichprobenartige Auswertung durch befugte Personen** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Dokumentation der Datenübermittlungen** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |  |  |
| --- | --- | --- |
| **Beschreibung eines Dokumentenmanagements** | **Ja** | **Nein** |
| Zutreffendes ankreuzen: |[ ] [ ]

|  |
| --- |
| **Anmerkungen, andere Maßnahmen (optional):** |
|       |

1. Da die TOM‘s alle drei Jahre oder bei Veränderung der Risikoeinschätzung auf ihre Wirksamkeit zu überprüfen, bewerten und evaluieren (Art. 32 Abs. 1 lit. d DSGVO) sind, sind diese Überarbeitungen versionsweise zu dokumentieren. [↑](#footnote-ref-1)