**Technische und organisatorische Maßnahmen (TOM)** **zur**

**Umsetzung der in der AMS-Datenschutzvereinbarung festgelegten**

**Datensicherheitsanforderungen**

**der**

**[*Firma, Unternehmenssitz bitte ergänzen!*]**

|  |  |  |  |
| --- | --- | --- | --- |
| Versions-Nr.[[1]](#footnote-2) | Datum | Erstellerin/Ersteller | Funktion im Unternehmen |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

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.

Ort, Datum Unterschrift

(rechtsgültige Fertigung)

(Der Name und die Funktion ist in Blockbuchstaben hinzuzufügen.)

Inhaltsverzeichnis

[1. Einführung 16](file:///\\s0010004\alle_x\AMF\ALL\_Richtlinie\Entwürfe\2018%20-%20allgemein\Versandunterlagen\ohne%20Korrekturen\Entwurf_Formular%20TOM_V6_11052018.docx#_Toc503529239)

[2. Risikoanalyse 17](file:///\\s0010004\alle_x\AMF\ALL\_Richtlinie\Entwürfe\2018%20-%20allgemein\Versandunterlagen\ohne%20Korrekturen\Entwurf_Formular%20TOM_V6_11052018.docx#_Toc503529240)

[3. Datenschutzrechtliche Schulungen 18](file:///\\s0010004\alle_x\AMF\ALL\_Richtlinie\Entwürfe\2018%20-%20allgemein\Versandunterlagen\ohne%20Korrekturen\Entwurf_Formular%20TOM_V6_11052018.docx#_Toc503529264)

[4. Zutrittsbeschränkungen 19](file:///\\s0010004\alle_x\AMF\ALL\_Richtlinie\Entwürfe\2018%20-%20allgemein\Versandunterlagen\ohne%20Korrekturen\Entwurf_Formular%20TOM_V6_11052018.docx#_Toc503529265)

[5. Zugangs-, Zugriffs- und Betriebsbeschränkungen 20](file:///\\s0010004\alle_x\AMF\ALL\_Richtlinie\Entwürfe\2018%20-%20allgemein\Versandunterlagen\ohne%20Korrekturen\Entwurf_Formular%20TOM_V6_11052018.docx#_Toc503529266)

[6. Verfügbarkeit, Belastbarkeit und Löschung 22](file:///\\s0010004\alle_x\AMF\ALL\_Richtlinie\Entwürfe\2018%20-%20allgemein\Versandunterlagen\ohne%20Korrekturen\Entwurf_Formular%20TOM_V6_11052018.docx#_Toc503529267)

[7. Überprüfungsmöglichkeiten der rechtmäßigen Datenverarbeitung 24](file:///\\s0010004\alle_x\AMF\ALL\_Richtlinie\Entwürfe\2018%20-%20allgemein\Versandunterlagen\ohne%20Korrekturen\Entwurf_Formular%20TOM_V6_11052018.docx#_Toc503529268)

1. **Einführung**

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

Gemäß DSGVO darf das AMS jedoch nur solche Auftragsverarbeiter 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 MitarbeiterInnen 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 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 einzufordern.

1. **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 beizulegen.

1. **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 Mitarbeiterinnen und Mitarbeiter ab. Dabei sollen im Wesentlichen folgende Ziele im Vordergrund stehen:

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

**Verpflichtende Maßnahmen:**

* Die betroffenen Mitarbeiterinnen und Mitarbeiter sind (ein)zuschulen und es sind zumindest alle drei Jahre Auffrischungsschulungen durchzuführen.
* Zusätzlich sind den Mitarbeiterinnen und Mitarbeitern schriftliche Informationen zum Datenschutz und zur Datensicherheit zur Verfügung zu stellen, zB Informationen im Intranet, regelmäßige Datenschutz-Newsletter, Verteilung des IT-Sicherheitshandbuch für Mitarbeiterinnen und Mitarbeiter ([www.it-safe.at](http://www.it-safe.at)).

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

1. **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 Kundinnen und Kunden befinden, angemessen vor unberechtigtem Zutritt geschützt werden (zB Sicherheitsschlösser, Schließsysteme, Alarmanlage, etc).

Führen Sie bitte aus, durch welche **organisatorischen Maßnahmen** die Räume, in denen sich personenbezogene Daten von AMS Kundinnen und Kunden befinden, angemessen vor unberechtigtem Zutritt geschützt werden (zB Schließregelung für die Räumlichkeiten, Schlüsselbuch/Schlüsselregelung, Ausweisregelung, sorgfältige Auswahl von Sicherheitspersonal/Reinigungspersonal/IT-Personal bzw. –Firmen, etc.).

1. **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 (zB durch Einstieg mittels Benutzer/Passwort, automatische Sperrmechanismen, Einsatz von Anti-Viren-Software, Firewalls, VPN Technologien, Sperren von externen Schnittstellen, E-Mail Verschlüsselung, Verschlüsselung von Datenträger, frühestmögliche Pseudonymisierung der Daten etc.) und wie die manuell geführten personenbezogenen Daten („Papierakt“) vor unberechtigtem Zugriff geschützt werden (zB Ablage in versperrten Schränken).

**Verpflichtende AMS-spezifische Maßnahmen:**

* Die vertraglich vorgeschriebenen eServices des eAMS-Kontos sind für die elektronische Kommunikation mit dem AMS zu verwenden. Die betroffenen Mitarbeiterinnen und Mitarbeiter 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 Teilnehmerinnen und Teilnehmern 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 (zB durch ein laufend gewartetes Berechtigungskonzept, Standardprozess für Berechtigungsvergabe, Passwort-Richtlinie, Telearbeit-Richtlinie, Nutzungsverbot von nichtbetrieblicher Soft- und Hardware, Installationsberechtigung von Programmen ausschließlich durch IT-AdministratorInnen, laufende Softwareaktualisierung, insbesondere von sicherheitsrelevanter Software [Antiviren-Programme, Browser etc.], Datenträgerverwaltung, Mobile Device Management, Regelungen beim Ausscheiden von MitarbeiterInnen etc.) und die manuell geführten personenbezogenen Daten („Papierakt“) vor unberechtigtem Zugriff geschützt werden.

1. **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

Führen Sie bitte aus, durch welche **technischen Maßnahmen Sie die Verfügbarkeit der Daten und die Belastbarkeit der EDV-Systeme** gewährleisten (zB ausreichende EDV-Kapazität, Klimatisierung der Serverräume, unterbrechungsfreie Stromversorgung (USV) der Server, Maßnahmen gegen Feuer, Wasser, starke elektromagnetische Felder etc.).

Führen Sie bitte aus, durch welche **organisatorischen Maßnahmen Sie die Verfügbarkeit der Daten und die Belastbarkeit der EDV-Systeme** gewährleisten (zB durch ein getestetes Backup- und Recoverykonzept, Aufbewahrung der Datensicherung an einem externen sicheren Ort, Vorliegen eines Notfallplans etc.).

Führen Sie bitte aus, durch welche Maßnahmen Sie die **ordnungsgemäße Löschung bzw. Vernichtung der Daten** gewährleisten (zB durch eine automatisierte Löschungsroutine, manuelle Löschung, verlässliche und effektive Vernichtung von nicht mehr benötigten Datenträgern [Papier, CD, DVD, USB-Stick, Festplatte etc.], Einsatz von geeigneten Löschprogrammen, die Daten auf Datenträgern, die wiederverwendet werden sollen, irreversibel löschen etc.).

1. **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 (zB durch Protokollierung auf Ebene der individuellen Benutzernamen, stichprobenartige Auswertung durch befugte Personen, Dokumentation der Datenübermittlungen, Dokumentenmanagement etc.), um die rechtmäßige Verarbeitung zu überprüfen.

Sehr geehrte Teilnehmerin, sehr geehrter Teilnehmer,

wir, XX, wurden vom Arbeitsmarktservice (AMS) betraut, Sie bei der Integration in den Arbeitsmarkt zu unterstützen. Das erfolgt insb. durch folgende Leistungen:

XXXX

Zu diesem Zweck verarbeiten wir für das AMS nachfolgende Daten von Ihnen:

- XX (personenbezogene Daten gemäß der mit dem AMS abgeschlossenen Datenschutzvereinbarung anführen – es ist ausreichend, dass die Hauptdatenkategorien, wie zB Stammdaten, Daten über Beruf und Ausbildung etc. allenfalls mit Erläuterungen angeführt werden.)

Diese Daten benötigen wir, um Sie bestmöglich bei der Erreichung des mit dem AMS festgelegten Zieles (zB Abklärung des Berufswunsches) unterstützen zu können.

Dem AMS geben wir insbesondere bekannt:

- Ihre Abwesenheitszeiten und den jeweiligen Grund;

- Datum und Grund der Beendigung Ihrer Teilnahme,

- einen individuellen Bericht, der dem AMS zur weiteren Betreuung dient

- individuelle Ausbildungsinhalte/den Lern- und Prüfungserfolg

- den von Ihnen erstellten Lebenslauf.

Auf direkte Anfrage des AMS können wir auch noch weitere Informationen an dieses weiterleiten.

Sofern wir vom AMS damit beauftragt sind, übermitteln wir vermittlungsrelevante Daten auch an potentielle Arbeitgeber oder Arbeitserprobungs- und Arbeitstrainingsstellen.

[Falls weitere Übermittlungen im Auftrag des AMS an weitere Dritte vorzunehmen sind, sind diese ebenfalls durch den Träger anzuführen.]

Ihre Daten speichern wir für das AMS noch 6 Monate nach Ende unseres Vertrages mit dem AMS. Danach werden alle Daten gelöscht, die wir nicht für die Abrechnung unserer Leistung benötigen. Sollen wir Daten für Sie noch weiter aufbewahren (zB zur Ausstellung einer Kopie der Teilnahmebestätigung), brauchen wir dafür von Ihnen einen gesonderten Auftrag. Bitte wenden Sie sich dazu an XX.

Neben der Datenverarbeitung für das AMS müssen wir [beispielweise] zur Erfüllung unserer gesetzlichen Verpflichtungen als Arbeitgeber zum Zwecke XX nachfolgende Daten XX von Ihnen verwenden.

Wir geben Ihnen gerne Einsicht in die Daten, die wir über Sie verarbeiten. Bitte wenden Sie sich an XX.

Wollen Sie Ihre Rechte gemäß der Datenschutz-Grundverordnung (DSGVO), wie Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung geltend machen, wenden Sie sich bitte an: xx

Sollten Sie die Datenverarbeitung als rechtswidrig erachten, haben Sie ein Beschwerderecht bei der Österreichischen Datenschutzbehörde, Barichgasse 40-42, 1030 Wien.

*! Bitte die ausgefüllte[[2]](#footnote-3) Meldung des Vorfalles umgehend an* [*ams.datenschutz@ams.at*](mailto:ams.datenschutz@ams.at) *übermitteln !*

|  |  |
| --- | --- |
| Name der ausfüllenden Person: |  |
| Telefonnummer: |  |
| Email-Adresse: |  |

# Allgemeines

|  |
| --- |
| * 1. Name und Anschrift des Auftragsverarbeiters |
| * 1. Wurde der Vorfall bereits der Datenschutzbehörde gemeldet? Wenn ja, wann? (Bitte die übermittelte Meldung beilegen!) |
| * 1. Kategorie des Vorfalls  |  |  | | --- | --- | |  | Fehlversendung personenbezogener Daten | |  | Hacking personenbezogener Daten | |  | Diebstahl personenbezogener Daten | |  | Softwarefehler | |  | Verlust personenbezogener Daten | |  | Fehlentsorgung personenbezogener Daten | |  | Schadcode | |  | Sonstiges |   Sonstiges: |

# Beschreibung

|  |
| --- |
| * 1. Ursache des Vorfalls |
| * 1. Bitte um Angabe des Zeitraums/Zeitpunkts[[3]](#footnote-4) (möglichst exakte Zeitangabe): |
| * 1. Zeitpunkt der Feststellung des Vorfalls (möglichst exakte Zeitangabe): |
| * 1. Beschreibung des Datenschutzvorfalls |
| * 1. Art der Verletzung  |  |  | | --- | --- | |  | Verlust personenbezogener Daten | |  | Veränderung personenbezogener Daten | |  | Vernichtung personenbezogener Daten | |  | unbefugter Zugang zu personenbezogener Daten | |  | unbefugte Weitergabe personenbezogener Daten | |  | unbefugte Veränderung personenbezogener Daten | |  | unberechtigter Weitergabe/unberechtigter Zugriff Dritter | |  | Datenverlust durch verloren gegangenes Medium | |  | Datenverlust durch Hacking | |  | Datenverlust durch Ausspähen wie Skimming oder Phishing | |  | Datenverlust durch Diebstahl | |  | Datenverlust durch sonstige Umstände | |  |  |   Anderes: |
| * 1. Geben Sie bitte die betroffenen Personengruppen an?   Anmerkungen: |
| * 1. Wie viele Personen (Anzahl der Betroffenen) sind betroffen? |
| * 1. Geben Sie bitte die betroffenen Datenkategorien an: |
| * 1. Welche besonderen Datenkategorien[[4]](#footnote-5) sind betroffen? |

# Angaben zur Auftragsverarbeitung / gemeinsame Verantwortlicher

|  |
| --- |
| * 1. Werden zur Durchführung der Verarbeitungstätigkeit Auftragsverarbeiter herangezogen bzw. wird die Verarbeitung mit einem gemeinsamen Verantwortlichen durchgeführt? |
| * 1. Name und Anschrift des Auftragsverarbeiters /gemeinsam Verantwortlichen: |
| * 1. Name und Anschrift des Datenschutzbeauftragten des Auftragsverabeiters / gemeinsamen Verantwortlichen |

# Folgen und Auswirkungen

|  |
| --- |
| * 1. Auflistung der möglichen Folgen und Auswirkungen der Datenschutzverletzung für die betroffenen Personen: |
| * 1. Beschreibung der Folgen und Auswirkungen: |

# Maßnahmen

|  |
| --- |
| * 1. Erläuterung der bereits eingeleiteten Sicherheitsmaßnahmen nach dem Datenschutzvorfall, um die betroffenen Personen zu schützen: |
| * 1. Erläuterung, in wie weit die eingeleiteten Maßnahmen zu einer Minderung der nachteiligen Folgen für die betroffenen Personen führen: |
| * 1. Erläuterung der noch geplanten Sicherheitsmaßnahmen |

# Meldung eines Datenschutzvorfalles

(V1.2a)

*Nach Ausfüllen bitte* [*umgehend an das Team des AMS Datenschutzbeauftragten*](mailto:ams.datenschutz@ams.at) *übermitteln*

|  |  |
| --- | --- |
| Informationen zur einmeldenden Person und der Datenverarbeitung | |
| Daten Melder\_in: | *Min. Name, Geschäftsstelle/Unternehmen, Mailadresse.* |
| Verarbeitungszuständige Stelle: | *Organisationseinheit und/oder fachlich für die Verarbeitung zuständige Fachabteilung.* |
| Informationen zum Vorfall | |
| Art: | *Art, der der Vorfall zuzuordnen ist.*  *Stichwortdetails zur Art (z.B. Cyberangriff, Schadsoftware, etc.)* |
| Zeitpunkt und Ort des Vorfalles: | *Zeitpunkt und Ort an dem sich der Vorfall ereignete.* |
| Zeitp. und ggf. Stelle der Kenntnisnahme im AMS: | *Zeitpunkt und Stelle an welchem das AMS die erste Möglichkeit zur Kenntnisnahme vom Vorfalles hatte.* |
| Betroffene persönliche Daten: | *Möglichst genaue Angabe der Betroffenengruppen und sämtlicher beeinträchtigter Datenkategorien; mehrere Einträge mit* ***Komma und******Semikolon*** *trennen (z.B. Mitarbeiter\_innendaten (Name****,*** *Alter)****;*** *Kund\_innendaten (Name****,*** *Sozialversicherungsnummer****,*** *IBAN****,*** *BIC)* |
| Anzahl betroffener Personen und Datensätze | *Anzahl betroffener Personen und die größte Zahl der von der Verletzung beeinträchtigten Datensätze bei derselben Person.* |
| Beschreibung: | *Beschreibung des Vorfalles (z.B. Antrag der Kundin A wurde versehentlich per RSa an Kundin B übermittelt).* |
| Sonstige Informationen zum Vorfall: | *u.a. dann wenn eine dritte Partei am Geschehen beteiligt war (z.B. ein Auftragsverarbeiter des AMS oder ein anderer Verantwortlicher).* |
| Informationen zu erfolgten Maßnahmen | |
| Sofortmaßnahmen: | *Eine Beschreibung jener Maßnahmen, die unmittelbar gesetzt wurden, um negative Folgen aus dem Vorfall für Betroffene zu verhindern oder zumindest zu lindern.* |
| Präventionsmaßnahmen: | *Eine Beschreibung jener Maßnahmen, die gesetzt wurden bzw. vorgesehen sind, um eine Wiederholung gleichartiger Vorfälle zu vermeiden oder zu deren Eintreten bzw. Wirkung zu vermindern.* |

1. Da die TOM 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-2)
2. Soweit möglich; nicht alles muss unbedingt ausgefüllt sein, aber ggf. kann es zu Rückfragen der Datenschutzorganisation kommen [↑](#footnote-ref-3)
3. Wenn nicht bekannt, dann bitte um Angabe des Datums an dem der Vorfall bekannt wurde [↑](#footnote-ref-4)
4. sensiblen Daten (Gesundheitsdaten, Daten zu Straftaten, Religion und Weltanschauung, sexuelle Orientierung, biometrische Daten, Gewerkschaftszugehörigkeit, rassische oder ethnische Herkunft, politische Meinung, Daten zum Sexualleben) [↑](#footnote-ref-5)