**DATENSCHUTZVEREINBARUNG**

**gemäß Art. 28 Datenschutz-Grundverordnung[[1]](#footnote-2) (DSGVO)**

abgeschlossen zwischen

dem Arbeitsmarktservice, vertreten durch Teilorganisation, Adresse,

**als Verantwortlicher (VA) im Sinne des Art. 4 Z 7 DSGVO einerseits**

und

Unternehmen, Adresse

**als Auftragsverarbeiter (A) im Sinne des Art 4 Z 8 DSGVO** **andererseits.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Verantwortliche Personen beim Auftragsverarbeiter** | | | |
|  | **Funktion** | **Name** | **Kontaktadresse inkl.**  **Telefonnummer und E-Mail Adresse** |
| 1 | Geschäftsführung |  |  |
| 2 | *falls erforderlich bzw. freiwillig eingerichtet*: Datenschutzbeauftragte/r im Sinne der DSGVO |  |  |
| 3 | *falls kein/e Datenschutzbeauftragte/r vorhanden:* Ansprechperson für datenschutzrechtliche Fragestellungen[[2]](#footnote-3) |  |  |
| 4 | Verantwortliche/r für Datensicherheit  *(falls vorhanden)* |  |  |

Über Änderungen wird der VA unverzüglich informiert.

**I. Präambel**

1. Der VA schließt im Namen und auf Rechnung des Bundes mit dem A Verträge über den Maßnahmentyp <XX> gemäß der jeweils gültigen BRL XX ab.

In diesen Verträgen sind Gegenstand und Dauer der Verarbeitung der personenbezogenen Daten, Art und Zweck der Verarbeitung dieser Daten und die Kategorien der betroffenen Personen festgelegt.

2. Die vorliegende Vereinbarung regelt in Ergänzung zu diesen Verträgen die zulässigen personenbezogenen Datenarten, die Dauer der Aufbewahrung sowie die datenschutzrechtlichen Verpflichtungen bezüglich **jener personenbezogenen Daten** (nachfolgend nur Daten), **die für die Erbringung der Hauptleistung (teilnehmerInnenbezogene Leistung)** dieser Verträge erforderlich sind.

3. Datenschutzrechtliche Verpflichtungen im Zusammenhang mit der Verwendung von **Daten für die Prüfung der widmungsmäßen Verwendung bzw. Abnahme und Abrechnung der Leistung sowie für die damit zusammenhängenden Kontrollzwecke** sind in den unter Punkt I.1 angeführten Verträgen geregelt und sind **nicht Gegenstand** dieser Vereinbarung.

4. Mit Unterfertigung der Vereinbarung verpflichtet sich der A zur Einhaltung nachfolgender Bestimmungen und bestätigt im Sinne des Art. 28 DSGVO, dass geeignete technische oder organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung der Daten auftragskonform und im Einklang mit den Anforderungen der DSGVO und des Datenschutzgesetzes (DSG) erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet ist.

Die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Art. 42 kann als Faktor herangezogen werden, um hinreichende Garantien nachzuweisen (Art. 28 Abs. 5 DSGVO).

**II. Zulässige Datenarten  
(Art. 28 Abs. 3 DSGVO)**

Zur Erfüllung der unter Pkt. I.1 genannten Verträge dürfen ausschließlich nachfolgende Datenarten verarbeitet werden und dies auch nur, soweit sie für die Erbringung der vom VA dem A vertraglich überbundenen Tätigkeiten im Einzelfall eine wesentliche Voraussetzung bilden:

***[Es sind durch die LGS jene Daten zu löschen, die für den gegenständlichen Vertrag nicht erforderlich sind]***

**1. Stammdaten der Arbeitsuchenden:**

a) Namen (Vornamen, Familiennamen),

b) Sozialversicherungsnummer und Geburtsdatum,

c) Geschlecht,

d) Staatsangehörigkeit, Aufenthalts- und Arbeitsberechtigungen,

e) Adresse des Wohnsitzes oder Aufenthaltsortes,

f) Telefonnummer,

g) E-Mail-Adresse,

h) Bankverbindung und Kontonummer.

**2. Daten über Beruf und Ausbildung:**

a) Berufs- und Beschäftigungswünsche,

b) Ausbildungen und Ausbildungswünsche,

c) bisherige berufliche Tätigkeiten,

d) beruflich verwertbare Fähigkeiten und Fertigkeiten,

e) sonstige persönliche Umstände, die die berufliche Verwendung berühren.

**3. Daten über wirtschaftliche und soziale Rahmenbedingungen:**

a) Familienstand (einschließlich Lebensgemeinschaft),

b) unterhaltsberechtigte Kinder,

c) Art und Umfang von Sorgepflichten, die die Verfügbarkeit am Arbeitsmarkt berühren,

d) sonstige Umstände, die die Verfügbarkeit am Arbeitsmarkt berühren,

e) ausgeübte (geringfügige) Erwerbstätigkeiten,

f) Einkommen (eigenes Einkommen, Partnereinkommen),

g) außerordentliche Aufwendungen,

h) Versicherungszeiten,

i) Bemessungsgrundlagen,

j) Höhe von Leistungen und Beihilfen,

k) Bezugszeiten von Leistungen und Beihilfen,

l) Zeiten der Arbeitsuche.

**4. Gesundheitsdaten:**

a) gesundheitliche Einschränkungen, die die Arbeitsfähigkeit oder die Verfügbarkeit in Frage stellen oder die berufliche Verwendung berühren,

b) gesundheitliche Einschränkungen der Arbeitsuchenden und ihrer Angehörigen (einschließlich LebensgefährtInnen), die einen finanziellen Mehraufwand erfordern.

c) Daten über Erkrankungen zur Abwicklung des § 36 AMSG bzw. § 42 AlVG

d) Daten zur Unfallmeldung gemäß § 40a AlvG

**5. Daten über Beschäftigungsverläufe, Arbeitsuche und Betreuungsverläufe:**

a) bisherige Beschäftigungen,

b) Umstände der Auflösung von Arbeitsverhältnissen,

c) Pläne und Ergebnisse der Arbeitsuche und Betreuung,

d) Umstände des Nichtzustandekommens von Arbeitsverhältnissen,

e) Dauer und Höhe gewährter Beihilfen,

f) Sanktionen wegen Fehlverhaltens,

g) Betroffenheit von Streik oder Aussperrung.

**6. Stammdaten der Arbeitgeber:**

a) Firmennamen und Betriebsnamen,

b) Firmensitz und Betriebssitz,

c) Struktur des Betriebes (zB Konzern-, Stamm-, Filialbetrieb),

d) Betriebsgröße,

e) Betriebsgegenstand,

f) Branchenzugehörigkeit,

g) Zahl und Struktur der Beschäftigten,

h) Betriebsinhaber und verantwortliche Mitglieder der Geschäftsführung,

i) Ansprechpartner,

j) Dienstgeberkontonummer und Unternehmenskennzahl,

k) Telefonnummer,

l) E-Mail-Adresse,

m) sonstige Kontaktmöglichkeiten,

n) Bankverbindung und Kontonummer.

**7. Daten über offene Stellen:**

a) Beruf und Tätigkeiten,

b) erforderliche und erwünschte Ausbildungen,

c) erforderliche und erwünschte Praxis,

d) erforderliche und erwünschte Kenntnisse, Fähigkeiten und Voraussetzungen,

e) besondere gesundheitliche Anforderungen der Arbeitsplätze,

f) Arbeitsorte,

g) Arbeitszeit (Lage und Ausmaß),

h) Entlohnung,

i) besondere Arbeitsbedingungen.

**8. Daten über das Beschäftigungs- und Personalsuchverhalten der Arbeitgeber:**

a) Umstände der (geplanten oder erfolgten) Auflösung von Arbeitsverhältnissen,

b) Umstände des Zustandekommens und des Nichtzustandekommens von Arbeitsverhältnissen,

c) Sanktionen wegen Fehlverhaltens,

d) Betroffenheit von Streik oder Aussperrung.

**III. Umfang und Mittel der Datenverarbeitung   
(Art. 25 und 28 Abs. 3 lit a sowie letzter Absatz DSGVO und § 6 Abs. 1 DSG)**

1. Der A verarbeitet die Daten ausschließlich zur Erbringung der im unter Punkt I.1 angeführten Verträge vorgesehenen Aufgaben sowie zur Erfüllung von darüber hinausgehenden vertragsbezogenen und dokumentierten Weisungen des VA.

Der A hat den VA unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des VA verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

2. Bei der Entwicklung, Gestaltung, Auswahl und Nutzung von Datenanwendungen ist das Recht auf Datenschutz unter gebührender Berücksichtigung des Standes der Technik sicherzustellen (Datenschutz durch Technik – „data protection by design“, Datenschutz durch datenschutzfreundliche Voreinstellungen – „data protection by default“).

3. Alle im Zusammenhang mit der Erfüllung der Verträge verarbeiteten Daten sind vom A dem VA zu überlassen, falls diese vom VA angefordert werden.

Davon unberührt sind absolute gesetzliche Verschwiegenheitsverpflichtungen (zB § 37 Psychologengesetz 2013 unter Berücksichtigung von § 36 Abs. 3 Psychologengesetz 2013), welchen der A bei der Erfüllung seiner ihm vom VA überbundenen Leistungen allenfalls unterliegt.

4. Die Verarbeitung dieser Daten für andere, als mit dem VA vereinbarte Zwecke („Verwendung für eigene Zwecke“) ist – nach vorheriger Rücksprache mit dem VA[[3]](#footnote-4) – dem A nur gestattet, als es dafür eine Grundlage im Unionsrecht oder in nationalen Rechtsvorschriften gibt und der A die betroffene Person nachweislich darüber informiert, dass diese Verarbeitung nicht der Erfüllung des mit dem VA geschlossenen Vertrages dient.

Besteht eine solche Grundlage nicht, bedarf die Verarbeitung der Daten für eigene Zwecke einer DSGVO-konformen Einwilligung (Art. 4 Z 11 DSGVO) der betroffenen Person unter inhaltsgetreuer Verwendung der als Pflichtinhalt markierten Passage des im Anhang befindlichen Einwilligungsmusters.

5. Der A wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art. 30 Abs. 2 DSGVO zu errichten hat.

Des Weiteren unterstützt der A den VA bei Erstellung und Fortschreibung seines Verarbeitungsverzeichnisses im Zusammenhang mit der beauftragten Verarbeitung. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem VA auf Anforderung unverzüglich zuzuleiten.

**IV. Vertraulichkeitsverpflichtung   
(Art. 28 Abs. 3 lit b und 29 DSGVO sowie § 6 DSG)**

1. Der A darf zur Erfüllung der Verträge und der damit zusammenhängenden Aufträge nur solche Mitarbeiterinnen und Mitarbeiter heranziehen, die sich ihm gegenüber zur Wahrung des Datengeheimnisses verpflichtet haben und über die einschlägigen – insbesondere datenschutzrechtlichen und strafrechtlichen – Bestimmungen nachweislich informiert wurden.

2. Darüber hinaus hat sich der A von seinen Mitarbeiterinnen und Mitarbeitern vertraglich ausdrücklich zusichern zu lassen, dass sie Daten nur aufgrund von ausdrücklichen schriftlichen Anordnungen des A übermitteln und das Datengeheimnis auch nach Beendigung ihres Vertragsverhältnisses zum A einhalten werden (siehe Musterbeispiel in der Beilage). Der A ist für die Vollständigkeit und die Zulässigkeit der Anordnungen verantwortlich sowie darüber hinaus auch dafür, dass die Mitarbeiterinnen und Mitarbeiter über die für sie geltenden Anordnungen ausreichend informiert sind (§ 6 Abs. 2 und 3 DSG).

3. Die unterfertigte Verpflichtungserklärung hat der A – nach Aufforderung – unverzüglich dem VA in Kopie oder elektronisch zur Verfügung zu stellen.

Mitarbeiterinnen und Mitarbeiter, die keine oder keine ausreichende Verpflichtungserklärung abgegeben haben, dürfen vom A für die Erbringung der Leistungen aus den Verträgen nicht herangezogen werden. Derartigen Untersagungserklärungen des VA hat der A unverzüglich zu entsprechen.

**V. Sicherheit der Verarbeitung   
(Art. 28 Abs. 3 lit c iVm Art. 32 DSGVO)**

1. Der A hat für vom VA erteilte Datenverarbeitungsaufträge alle gemäß Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zu ergreifen.

2. Es sind dabei folgende AMS-spezifische Anforderungen mit zu berücksichtigen:

*Datenschutzschulungen*

Die betroffenen Mitarbeiterinnen und Mitarbeiter sind (ein)zuschulen und es sind zumindest alle drei Jahre Auffrischungsschulungen durchzuführen. Zusätzlich sind schriftliche Informationen den Mitarbeiterinnen und Mitarbeitern zum Datenschutz und zur Datensicherheit zur Verfügung zu stellen.

*eAMS-Konto*

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.

*Zugriffsbeschränkungen bei EDV-Geräten, die von unterschiedlichen Teilnehmerinnen und Teilnehmern verwendet werden*

Es sind Vorkehrungen zu treffen, dass personenbezogene Daten auf EDV-Geräten, die von unterschiedlichen Teilnehmerinnen und Teilnehmern benutzt werden, vor unberechtigtem Zugriff geschützt sind.

3. Die technischen und organisatorischen Maßnahmen sind spätestens alle drei Jahre auf ihre Wirksamkeit zu überprüfen, zu bewerten und zu evaluieren (Art. 32 Abs. 1 lit. d DSGVO) sowie erforderlichenfalls anzupassen. Eine zwischenzeitliche Anpassung ist auch dann vorzunehmen, wenn sich die Risikoeinschätzung (zB durch die Einführung einer neuen Datenanwendung) verändert oder von Seiten des VA eine Anpassung als erforderlich erachtet wird. Wird das Schutzniveau reduziert, stellt das eine Vertragsänderung dar und ist nur mit Zustimmung des VA zulässig.

4. Der Nachweis über diese Maßnahmen kann entweder durch

* die Anwendung von genehmigten Verhaltensregeln gemäß Art. 40 DSGVO oder
* eine Zertifizierung gemäß Art. 42 DSGVO oder
* das im Anhang befindliche Formular „Technische und organisatorische Maßnahmen – TOM“

erfolgen.

5. Liegt ein aktueller Nachweis der Landesgeschäftsstelle des Arbeitsmarktservice bereits vor, ist eine erneute Vorlage nicht erforderlich.

**VI. Sub-Auftragsverarbeiter   
(Art. 28 Abs. 3 lit d iVm Art. 28 Abs. 2 und Abs. 4 sowie Art. 44 ff DSGVO)**

1. Sub-Auftragsverarbeiter sind ausschließlich solche Unternehmen, deren Leistungen einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen und die zur Leistungserbringung personenbezogene Daten der TeilnehmerInnen verarbeiten müssen.

2. Der VA erteilt dem A die Genehmigung Sub-Auftragsverarbeiter zur Erfüllung der unter Punkt I.1 anführten Verträge in Anspruch zu nehmen bzw. bestehende zu ersetzen, wenn

* der A eine solche Inanspruchnahme dem VA eine angemessene Zeit (2 Wochen) vorab unter Angabe des Einsatzzeitpunktes schriftlich mitteilt und
* der VA nicht bis zum Zeitpunkt des Einsatzes schriftlich Einspruch erhebt und
* der A eine Vereinbarung im Sinne des Art. 28 Abs. 4 DSGVO mit dem Sub- Auftragsverarbeiter abschließt. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem A auf Grund dieser Vereinbarung obliegen.

Die Vereinbarung hat der A – nach Aufforderung - unverzüglich dem VA vorzulegen.

Eine solche Vereinbarung mit dem Sub-Auftragsverarbeiter ist nicht erforderlich, wenn der Sub-Auftragsverarbeiter und dessen Mitarbeiterinnen und Mitarbeiter einer gesetzlichen Verschwiegenheitspflicht unterliegen.

3. Einzelpersonen, die auf Basis eines freien Dienstvertrages oder eines Werkvertrages als TrainerIn/BeraterIn arbeiten und die über keine für Träger typische betriebliche Struktur verfügen, gelten nicht als Sub-Auftragsverarbeiter. Diese sind datenschutzrechtlich als MitarbeiterInnen des Trägers zu behandeln. Es gilt Pkt. IV dieser Datenschutzvereinbarung.

4. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der A gegenüber dem VA für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

**VII. Datenübermittlung an ein Drittland  
(Art. 44 – 50 DSGVO)**

Die Übermittlung von Daten an ein Land innerhalb des EWR und der Schweiz (auch an Sub-Auftragsverarbeiter zB bei Cloud-Lösungen) ist zulässig. Übermittlungen an andere Länder sind nur zulässig, sofern die Übermittlung, im Rahmen von genehmigten Verhaltensregeln (Art. 40 DSGVO) oder Zertifizierungen (Art. 42 DSGVO) als zulässig erachtet wurden.

**VIII. Gewährleistung der Betroffenenrechte  
(Art. 28 Abs. 3 lit e iVm Kapitel III der DSGVO)**

1. Der A hat unter sinngemäßer Verwendung des im Anhang befindlichen Musters „Muster zur Erfüllung der Informationspflicht der AMS-Teilnehmerinnen und –Teilnehmer gemäß Art. 13 DSGVO“ die AMS-Teilnehmerinnen und –Teilnehmer zu Beginn der Maßnahme über die Datenverarbeitung zu informieren. Dabei ist zwischen der Datenverarbeitung als Auftragsverarbeiter des AMS und der Datenverarbeitung als Verantwortlicher zu differenzieren. Im Sinne der Rechenschaftspflicht ist die Erfüllung der Informationspflicht entsprechend zu dokumentieren.

2. Der A hat mit geeigneten technischen und organisatorischen Maßnahmen den VA zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Person nachzukommen. Dazu zählen insbesondere das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Widerspruch (siehe Kapitel III der DSGVO).

3. Wird ein Antrag auf Auskunft an einen A gerichtet, hat der A eine DSGVO-konforme Auskunft auch über die, für den VA verarbeiteten Daten vorzunehmen. Der VA ist zeitgleich über diese Auskunft zu informieren.

Lässt der Antrag auf Auskunft erkennen, dass auch Daten beauskunftet werden sollen, die direkt durch das AMS verarbeitet werden, hat der A den Antrag unverzüglich an den VA weiterzuleiten und dies dem Antragsteller mitzuteilen.

4. Der A wird zusätzlich ermächtigt, einer betroffenen Person, die ihre Identität aktenkundig nachgewiesen hat, Einsicht über die von ihm zu dieser Person verarbeiteten Daten zu geben.

5. Wird ein Antrag auf Berichtigung, Löschung, Einschränkung der Verarbeitung und Widerspruch eingebracht, dann ist dieser in Bezug auf die Daten, die für den VA verarbeitet werden, an den VA unverzüglich weiterzuleiten und dies dem Antragsteller mitzuteilen.

**IX. Unterstützungsverpflichtungen des Auftragsverarbeiters  
(Art. 28 Abs. 3 lit f iVm Art. 32 – 36 DSGVO)**

1. Der A ist verpflichtet, den VA unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten (Sicherheit der Verarbeitung, Meldung von Verletzungen des Schutzes personenbezogener Daten, Datenschutz-Folgenabschätzung und damit verbundene Konsultationen) zu unterstützen.

2. Wenn dem A eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem VA unverzüglich (Art. 33 Abs. 2 DSGVO).

3. Das im Anhang zu Punkt IX. enthaltene Formular betreffend die Meldung eines Datenschutzvorfalles für AMS Auftragsverarbeiter ist bei Datenschutzvorfällen verpflichtend zu verwenden.

**X. Datenaufbewahrung / Datenvernichtung  
(Art. 5 Abs. 1 lit e und Art. 28 Abs. 3 lit g DSGVO)**

1. Der A hat die vom VA übermittelten bzw. bereitgestellten Daten, die zur Erfüllung der Verträge selbst erhobenen Daten sowie die Verarbeitungsergebnisse für **genau 6 Monate nach jeweiligem Vertragsende** weiter aufzubewahren.

Als Zeitpunkt des Vertragsendes gilt im Falle von Rahmenverträgen das Ende des jeweiligen Einzelvertrages. In jenen Fällen in denen die Teilnehmerin/der Teilnehmer in Folgeverträge übertritt, gilt als fristauslösendes Ereignis das Ende jenes Vertrages, aus dem die Person ausgeschieden ist.

[ANMERKUNG FÜR LGS: Nur in begründeten Ausnahmefällen und sofern zweckmäßig, kann alternativ als fristauslösendes Ereignis an Stelle des Vertragsendes auch die Beendigung der Teilnahme der Person gewählt werden.]

Der A hat während der Aufbewahrungsfrist die Daten unter strikter Einhaltung des Art. 32 DSGVO vor unbefugter Einsicht gesichert aufzubewahren.

2. **Nach Ablauf** der Aufbewahrungsfrist sind die Daten **unverzüglich zu löschen bzw. zu vernichten**. Diese Verpflichtung erfasst automationsunterstützt und manuell verarbeitete Daten gleichermaßen. Der VA ist über die erfolgte Löschung bzw. Vernichtung der Daten unter Verwendung der Bestätigungsfunktion im eAMS-Konto zu informieren.

3. Hat der A Daten rechtmäßig im Auftrag eines anderen Kostenträgers oder aufgrund zulässiger Verwendung für eigene Zwecke (III.4. dieser Vereinbarung) weiter zu verarbeiten, bedeutet die Bestätigung der erfolgten Datenvernichtung/-löschung, dass die Daten keinesfalls mehr für das Arbeitsmarktservice verarbeitet werden. Ist nur ein Teil der Daten im Auftrag des anderen Kostenträgers weiter zu verarbeiten, so ist der verbleibende Rest zu löschen bzw. zu vernichten.

4. Sofern gesetzliche Regelungen (zB arbeits-, sozial-, steuerrechtliche Bestimmungen, Ärztegesetz) eine längere Aufbewahrungsfrist festlegen, wird die Pflicht zur Vernichtung der davon erfassten Daten mit Ablauf dieser gesetzlichen Fristen schlagend.

**XI. Kontrolle durch den VA  
(Art. 28 Abs. 3 lit h DSGVO)**

Der A verpflichtet sich, dem VA alle erforderlichen Informationen zum Nachweis der Einhaltung der im Art. 28 DSGVO niedergelegten Pflichten zur Verfügung zu stellen und Überprüfungen, einschließlich Inspektionen, die vom VA oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, zu ermöglichen und dazu beizutragen.

**XII. Auflagen**

1. Der A hat etwaige ihn ganz oder teilweise betreffende Auflagen der Datenschutzbehörde (DSB) zu erfüllen. Eine Weigerung, den einschlägigen Auflagen der DSB nachzukommen, stellt für den VA einen Grund zur Auflösung der dieser Vereinbarung zu Grunde liegenden Verträge aus wichtigem Grund dar.

2. Die Datenschutzvereinbarung ist bei Änderungen der dieser Vereinbarung zu Grunde liegenden Verträge sowie bei gesetzlichen oder unionsrechtlichen Änderungen entsprechend anzupassen.

**XIII. Haftung und Schadenersatz  
(Art. 82 DSGVO)**

Der VA und der A haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

**XIV. Anzuwendendes Recht**

Diese Vereinbarung ersetzt alle allfälligen früheren Datenschutzvereinbarungen. Sie unterliegt österreichischem Recht unter Ausschluss des UN-Kaufrechtes sowie der Verweisnormen. Für alle Streitigkeiten aus oder im Zusammenhang mit dieser Vereinbarung werden die sachlich zuständigen Gerichte für den Sitz desVA vereinbart*.*

**XV. Salvatorische Klausel**

Sollten Bestimmungen dieser Vereinbarung ungültig sein oder ungültig werden, so berührt dies nicht die Gültigkeit der übrigen Bestimmungen. Die Vertragsparteien werden sich bemühen, die ungültige Regelung durch eine solche zu ersetzen, die dem Zweck der ungültigen Regelung in rechtskonformer Weise am nächsten kommt.

**XVI. Schriftlichkeit**

Diese Vereinbarung sowie auch jede Änderung dieser Vereinbarung bedarf - im Sinne einer eigenhändigen Unterfertigung - der Schriftform. Das Erfordernis der Schriftform gilt auch dann als erfüllt, wenn der A die Vereinbarung per eAMS-Konto übermittelt und seinen Bindungswillen in der eAMS-Nachricht eindeutig, zB wie folgt erklärt: "Hiermit nehme ich XX, in Vertretung des Unternehmens XX, die Datenschutzvereinbarung zum Projekt XX vom XX.XX.XXXX vollinhaltlich an."

(Ort)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, am \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Arbeitsmarktservice, vertreten durch Arbeitsmarktservice XX

(als Verantwortlicher)

(Ort)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, am \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

XXXX

(als Auftragsverarbeiter)

Anhang:

* Muster Einwilligung im Falle der Verwendung der Daten für eigene Zwecke gemäß Punkt III.4 der Datenschutzvereinbarung
* Muster Verpflichtungserklärung zum Datengeheimnis gemäß Punkt IV.2 der Datenschutzvereinbarung
* Formular „Technische und organisatorische Maßnahmen – TOM““ gemäß Punkt V.4 der Datenschutzvereinbarung
* Muster zur Erfüllung der Informationspflicht der AMS-Teilnehmerinnen und -Teilnehmer gemäß Art. 13 der DSGVO“ gemäß Pkt. VIII.1 der Datenschutzvereinbarung
* Muster zur Meldung eines Datenschutzvorfalles für AMS Auftragsverarbeiter gemäß Punkt IX.3. der Datenschutzvereinbarung

**Einwilligung zur Verarbeitung meiner Daten**

**gemäß Art. 4 Z. 11 Datenschutzgrundverordnung (DSGVO)**

An

<Name und Rechtssitz des Verantwortlichen gemäß Art 4. Z. 7 DSGVO (Projektträger)>

*<falls vorhanden: Nennung des Datenschutzbeauftragten>*

Ich, <Name und Anschrift der betroffenen Person>, erteile die ausdrückliche Einwilligung, dass meine Daten für folgende Verarbeitungsvorgänge durch <Rechtsname des Verantwortlichen (nicht das AMS!)> verwendet werden dürfen.

[Sind verschiedene Verarbeitungsvorgänge von personenbezogenen Daten vorgesehen, ist die Einwilligung für jeden einzelnen Verarbeitungsvorgang einzuholen (siehe Erläuterung Nr. 43 der DSGVO)]

Bitte kreuzen Sie die Verarbeitungsvorgänge an, für die Sie die Einwilligung erteilen:

<Verarbeitungsvorgang 1>

1. Daten

[Geben Sie hier die Datenarten ein.]  
*Es sind die geforderten Datenarten exakt anzuführen.*

1. Zweck, für den die Daten verarbeitet werden

[Geben Sie hier den Zweck ein.]  
*Es ist der exakte „Einzel-Zweck“ anzugeben und nicht bloß „allgemeine Verwendungsfloskeln“. Insgesamt muss die Unterrichtung die betroffene Person in die Lage versetzen, zu wissen, dass und in welchem Umfang sie ihre Einwilligung erteilt.*

1. Für den Fall der Weitergabe der Daten an Dritte: Empfänger (Name und Anschrift), an den die Daten weitergegeben werden

[Geben Sie hier Name und Anschrift des Empfängers ein.]  
*Die Dritten, an die die Daten weitergegeben werden sollen/können, sind genau zu bezeichnen.*

1. Speicherdauer der Daten

[Geben Sie hier die Dauer, für die die personenbezogenen Daten gespeichert werden an oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer.]

<Verarbeitungsvorgang N>

1) Daten

2) Zweck, für den die Daten verarbeitet werden

3) Für den Fall der Weitergabe der Daten an Dritte: Empfänger (Name und Anschrift), an den die Daten weitergegeben werden

4) Speicherdauer der Daten

**PFLICHTINHALT DER VOM AMS GEFORDERT WIRD:**

**Ich wurde darüber informiert, dass diese Verarbeitungen nicht für Zwecke des Arbeitsmarktservice erfolgen und dass das Arbeitsmarktservice diese Verarbeitung nicht beauftragt hat.**

**Die Verweigerung einer Einwilligung führt zu keinen Konsequenzen aus dem Arbeitslosenversicherungsgesetz oder Arbeitsmarktservicegesetz.**

Ich wurde darüber informiert, dass ich das Recht auf Auskunft über die betreffenden Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder auf Widerspruch gegen die Verarbeitung sowie das Recht auf Datenübertragbarkeit gemäß den Bestimmungen der DSGVO habe. Des Weiteren wurde ich darüber aufgeklärt, dass wenn ich der Ansicht bin, dass die Verarbeitung der mich betreffenden personenbezogenen Daten rechtswidrig ist, das Recht auf Beschwerde bei der Datenschutzbehörde ([www.dsb.gv.at](http://www.dsb.gv.at)) habe.

**Ich erteile diese Einwilligung freiwillig.** Ich kann sie jederzeit ohne Angabe von Gründen schriftlich per E-Mail an [xx@xx.x](mailto:xx@xx.x) oder mittels formlosen Briefes an die Adresse XX widerrufen. Im Fall des Widerrufs ist jedes weitere Verarbeiten der bis zu diesem Zeitpunkt erfassten Daten unverzüglich einzustellen.

Ort, Datum Unterschrift

Verpflichtungserklärung zum Datengeheimnis[[4]](#footnote-5)

Ich ………………………………………… verpflichte mich, das Datengeheimnis gemäß § 6 DSG zu wahren und den Datenschutz und die Datensicherheit unabhängig davon, ob es sich um eine gesetzliche Verpflichtung oder um eine betriebliche Anordnung handelt, einzuhalten.

Mir ist bekannt, dass

* + die personenbezogenen Daten natürlicher wie juristischer Personen einem besonderen Schutz unterliegen und die Verwendung solcher Daten nur unter besonderen Voraussetzungen zulässig ist;
  + es untersagt ist, personenbezogene Daten zu einem anderen als dem zum rechtmäßigen Aufgabenvollzug gehörenden Zweck zu verwenden;
  + es untersagt ist, unbefugten Personen oder unzuständigen Stellen innerhalb und außerhalb des Unternehmens personenbezogene Daten mitzuteilen oder offenzulegen;
  + personenbezogene Daten, die mir auf Grund meiner beruflichen Beschäftigung anvertraut oder zugänglich gemacht wurden, nur auf Grund einer ausdrücklichen Anordnung des jeweiligen Vorgesetzten übermittelt werden dürfen;
  + es untersagt ist, sich unbefugt Daten zu beschaffen oder zu verarbeiten;
  + anvertraute Benutzerkennwörter, Passwörter und sonstige Zugangsberechtigungen sorgfältig verwahrt und geheim zu halten sind;
  + allfällige weiterreichende andere Bestimmungen über die Geheimhaltungspflichten ebenfalls zu beachten sind;
  + diese Verpflichtungen auch nach Beendigung meiner Tätigkeit fortbestehen;
  + aus einer Verweigerung der Befolgung einer Anordnung zur unzulässigen Datenübermittlung mir kein Nachteil erwachsen darf;
  + Verstöße gegen die hier genannten Verschwiegenheitsverpflichtungen nicht nur arbeitsrechtliche Folgen, sondern auch (verwaltungs-)strafrechtliche Folgen haben und schadenersatzpflichtig machen.

Mit meiner Unterschrift bestätige ich zugleich den Empfang einer Kopie dieser Verpflichtungserklärung.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ort Datum Verpflichtete(r)

(siehe umseitig § 6 DSG)

**Datengeheimnis gemäß § 6 DSG**

(1) Der Verantwortliche, der Auftragsverarbeiter und ihre Mitarbeiter – das sind Arbeitnehmer (Dienstnehmer) und Personen in einem arbeitnehmerähnlichen (dienstnehmerähnlichen) Verhältnis – haben personenbezogene Daten aus Datenverarbeitungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen personenbezogenen Daten besteht (Datengeheimnis).

(2) Mitarbeiter dürfen personenbezogene Daten nur auf Grund einer ausdrücklichen Anordnung ihres Arbeitgebers (Dienstgebers) übermitteln. Der Verantwortliche und der Auftragsverarbeiter haben, sofern eine solche Verpflichtung ihrer Mitarbeiter nicht schon kraft Gesetzes besteht, diese vertraglich zu verpflichten, personenbezogene Daten aus Datenverarbeitungen nur aufgrund von Anordnungen zu übermitteln und das Datengeheimnis auch nach Beendigung des Arbeitsverhältnisses (Dienstverhältnisses) zum Verantwortlichen oder Auftragsverarbeiter einzuhalten.

(3) Der Verantwortliche und der Auftragsverarbeiter haben die von der Anordnung betroffenen Mitarbeiter über die für sie geltenden Übermittlungsanordnungen und über die Folgen einer Verletzung des Datengeheimnisses zu belehren.

(4) Unbeschadet des verfassungsrechtlichen Weisungsrechts darf einem Mitarbeiter aus der Verweigerung der Befolgung einer Anordnung zur unzulässigen Datenübermittlung kein Nachteil erwachsen.

(5) Ein zugunsten eines Verantwortlichen bestehendes gesetzliches Aussageverweigerungsrecht darf nicht durch die Inanspruchnahme eines für diesen tätigen Auftragsverarbeiters, insbesondere nicht durch die Sicherstellung oder Beschlagnahme von automationsunterstützt verarbeiteten Dokumenten, umgangen werden.

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

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

**Datensicherheitsanforderungen**

**der**

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

|  |  |  |  |
| --- | --- | --- | --- |
| Versions-Nr.[[5]](#footnote-6) | 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, Wickenburggasse 8, 1080 Wien.

*! Bitte die ausgefüllte[[6]](#footnote-7) 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[[7]](#footnote-8) (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[[8]](#footnote-9) 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 |

1. Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) [↑](#footnote-ref-2)
2. Z.B. wenn eine betroffene Person ihre Rechte (insbesondere Auskunfts-, Richtigstellungs- und Löschungsrecht) gegenüber dem AMS geltend macht oder der Schutz von personenbezogenen Daten im Einflussbereich der Partnerinstitution verletzt wurde (Art. 33 Abs. 2 iVm Art. 4 Z 12 DSGVO). [↑](#footnote-ref-3)
3. [↑](#footnote-ref-4)
4. Die vorherige Rücksprache darf unterbleiben, wenn die Verwendung für eigene Zwecke auf einer unmittelbaren Vertragsbeziehung zwischen A und dem Betroffenen (Art. 6 Abs. 1 lit b DSGVO) oder auf berechtigten Interessen des A im unmittelbaren Zusammenhang mit der Leistungserbringung für das AMS   
   (Art. 6 Abs. 1 lit f DSGVO, zB zur Einhaltung der Hausordnung, Wahrung der Informationssicherheit) beruht. Eine unmittelbare Vertragsbeziehung im Sinne dieser Bestimmung besteht nur, sofern ein ausdrücklicher Vertragsabschluss zwischen dem A und dem Betroffenen vorliegt (zB bei Begründung eines Arbeitsverhältnisses des Betroffenen mit dem A bei SÖB/GBP bzw. Ausbildungsverhältnisses im Sinne des § 30 BAG bei Überbetrieblicher Lehrausbildung oder bei Personenzertifizierungen durch den A). Dieses Muster dient ausschließlich der Hilfestellung und ist auf den jeweiligen Einzelfall anzupassen. Das Arbeitsmarktservice übernimmt keine Haftung für die Rechtmäßigkeit. [↑](#footnote-ref-5)
5. 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-6)
6. Soweit möglich; nicht alles muss unbedingt ausgefüllt sein, aber ggf. kann es zu Rückfragen der Datenschutzorganisation kommen [↑](#footnote-ref-7)
7. Wenn nicht bekannt, dann bitte um Angabe des Datums an dem der Vorfall bekannt wurde [↑](#footnote-ref-8)
8. 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-9)