Verhaltensregeln gemäß Art. 40 Abs. 2 lit. h DSGVO

betreffend Maßnahmen für die Sicherheit der Verarbeitung für Mitglieder der Verbände „Dachverband Berufliche Integration – Austria“ und „arbeit plus - Soziale Unternehmen Österreich“ bei der Leistungserbringung im Rahmen der beruflichen und sozialen Integration

Inhaltsverzeichnis

1. Begriffsbestimmungen ... 3
2. Gegenstand ... 3
3. Zweck ... 5
4. Rechtsgrundlagen und datenschutzrechtliche Rollenverteilung ... 6
4.1. Abgrenzung zur Berufsvereinigung der ArbeitgeberInnen privater Bildungseinrichtungen (BABE) und ihren Verhaltensregeln ... 6
4.2. Datenschutzrechtliche Rollenverteilung ... 8
4.2.1. Unterschiedliche Tätigkeitsbereiche ... 8
4.2.2. Applikationen der FördergeberInnen ... 8
4.2.3. Rolle als Verantwortlicher und Auftragsverarbeiter ... 8
4.2.3.1. Vertrag über die Auftragsverarbeitung mit dem AMS ... 9
4.2.3.2. Vertrag über die Auftragsverarbeitung mit dem SMS ... 11
4.2.4. Auswirkungen von datenschutzrechtlichen Rollen auf Maßnahmen für die Sicherheit der Verarbeitung gemäß Art. 32 DSGVO ... 11
5. Risikoanalyse ... 12
5.1. Art, Umfang und Umstände der Datenverarbeitung im Rahmen der Auftragserfüllung ... 13
5.2. Zwecke der Datenverarbeitung ... 15
5.3. Risiken für die Rechte und Freiheiten natürlicher Personen ... 16
5.4. Schutzziele ... 17
5.5. Potenzielle Ereignisse ... 17
5.5.1. Branchenunabhängig ... 18
5.5.2. Branchenspezifisch ... 20
5.6. Risikobewertung ... 22
5.6.1. Eintrittswahrscheinlichkeit ... 23
5.6.2. Schwere des Schadens ... 23
5.6.3. Bestimmung der Risikokategorie ... 24
5.7. Individuelle Risikobewertung ... 29
6. Geeignete technische und organisatorische Maßnahmen ... 29
6.1. Zutrittskontrolle ... 30
6.2. Zugangskontrolle ... 31
6.3. Zugriffskontrolle ... 34
6.4. Weitergabekontrolle ... 35

6.5. Eingabekontrolle 36
6.6. Verfügbarkeitskontrolle 37
6.7. Trennungskontrolle 38
6.8. Sonstige Maßnahmen 38
6.9. Erreichung eines angemessenen Datenschutzniveaus 40
7. Schutzzielerreichung 40
8. Neuerliche Risikobewertung 41
9. Verfahrensbestimmungen 47
9.1. Akkreditierte Stellen 47
9.2. Verfahren zur Überwachung der Einhaltung der Verhaltensregeln 48
10. Änderungen der Verhaltensregeln 49

1. Begriffsbestimmungen

„Verbände“ im Sinn von Art. 40 Abs. 2 DSGVO sind die Vereine „Dachverband Berufliche Integration – Austria“ und „arbeit plus - Soziale Unternehmen Österreich“.

„Verantwortliche“ im Sinn von Art. 4 Ziffer 7 DSGVO sind das „Arbeitsmarktservice“ und das „Sozialministeriumservice“.

„Auftragsverarbeiter“ im Sinn von Art. 4 Ziffer 8 DSGVO sind die Mitglieder der Verbände im Umfang des jeweiligen Vertrages über die Auftragsverarbeitung gemäß Art. 28 DSGVO, der mit dem Arbeitsmarktservice und/oder dem Sozialministeriumservice abgeschlossen wird.

„AdressatInnen“ sind alle Personen, die im Rahmen von arbeitsmarktpolitischen Maßnahmen der Verantwortlichen Leistungen erhalten können und von den Mitgliedern betreut werden. Neben Begünstigten, einschließlich antragstellenden Personen und FörderungswerberInnen im Sinn von § 22 Abs. 4 BEinstG, Arbeitssuchenden im Sinn von § 25 AMSG und Jugendlichen im Sinn von § 15 APflG sind davon z.B. auch NEET-Jugendliche,[1] SchülerInnen und in Beschäftigung stehende Personen umfasst.[2] Da von AdressatInnen im Rahmen der Aufgabenerfüllung zwangsläufig personenbezogene Daten verarbeitet werden, sind diese „betroffene Personen“ im Sinn von Art. 4 Z 1 DSGVO.

„Akkreditierte Stellen“ im Sinn von Art. 41 DSGVO sind Stellen, die gemäß der Verordnung der Datenschutzbehörde über die Anforderungen an eine Stelle für die Überwachung der Einhaltung von Verhaltensregeln (Überwachungsstellenakkreditierungs-Verordnung – ÜStAkk-V) über das geeignete Fachwissen hinsichtlich des Gegenstands der Verhaltensregeln verfügen und die von der Datenschutzbehörde zum Zweck der Überwachung der Verhaltensregeln akkreditiert und von den Mitgliedern entsprechend beauftragt wurden.

„Dritte“ sind Personen, denen personenbezogene Daten von AdressatInnen übermittelt, beauskunftet oder offen gelegt werden, z.B. gesetzliche VertreterInnen, potenzielle ArbeitgeberInnen, Schulen, Ausbildungsstätten oder Behörden im Rahmen gesetzlicher Zuständigkeiten (z.B. Gefährdungsmitteilungen gemäß § 37 B-KJHG 2013, Auskünfte im Rahmen von Ermittlungen nach § 57 SPG oder Anzeigen nach dem Gewaltschutzgesetz 2019).

2. Gegenstand

Im Rahmen der Teilnahme an arbeitsmarktpolitischen Maßnahmen gewährt das Arbeitsmarktservice (im Folgenden „AMS“) Förderungsmaßnahmen für Arbeitssuchende nach Maßgabe des AMSG. Dienstleistungen des AMS zur Vorbereitung, Ermöglichung oder Erleichterung einer Vermittlung oder Beschäftigungssicherung werden entweder vom AMS

[1] Jugendliche und junge Erwachsene die weder in Ausbildung, Beschäftigung oder Training sind (not in employment, education or training).

[2] In der Praxis sind für AdressatInnen auch Bezeichnungen wie z.B. „KlientInnen“, „TeilnehmerInnen“ oder „NutzerInnen“ gebräuchlich. Dabei kann es auch zu Unterschieden in den Bundesländern kommen. Aus Vereinfachungsgründen wird der Begriff „AdressatInnen“ als Sammelbegriff für alle diese Personen herangezogen.

selbst erbracht oder auf Grund vertraglicher Vereinbarungen, z.B. durch Übertragung an geeignete Einrichtungen, zur Verfügung gestellt (§ 32 AMSG).

Das Sozialministeriumservice (im Folgenden „SMS“) fördert Maßnahmen beruflicher Assistenz nach Maßgabe des BEinstG, des APflG und der Allgemeinen Rahmenrichtlinien für die Gewährung von Förderungen aus Bundesmitteln. Darüber hinaus ist das SMS auch für die Durchführung von Beschäftigungsmaßnahmen des Europäischen Sozialfonds, nach Maßgabe der jeweils in Kraft stehenden Verordnungen des europäischen Parlamentes und des Rates über den Europäischen Sozialfonds verantwortlich.

Bei der Erfüllung ihrer gesetzlichen Aufgaben sind das AMS und das SMS jeweils Verantwortliche im Sinn von Art. 4 Ziffer 7 DSGVO und entscheiden über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten der geförderten Personen.

Sowohl das AMS als auch das SMS ziehen zur Erfüllung ihrer gesetzlichen Aufgaben Unternehmen des sozialen Dienstleistungssektors heran, die in Formen des Privatrechts eingerichtet sind. Diese Unternehmen sind Mitglieder der Vereine „Dachverband Berufliche Integration – Austria“ und „arbeit plus - Soziale Unternehmen Österreich“ (im Folgenden „dabei Austria“ und „arbeit plus“ oder gemeinsam „Verbände“).

Die Mitglieder der Verbände (im Folgenden „Mitglieder“) werden entweder für das AMS oder das SMS oder für beide Fördergeber tätig.

Sowohl zwischen dem AMS und den Mitgliedern als auch zwischen dem SMS und den Mitgliedern werden jeweils Verträge über die Auftragsverarbeitung gemäß Art. 28 DSGVO abgeschlossen. Daneben können Mitglieder personenbezogener Daten – abhängig von den spezifischen Rahmenbedingungen – auch als Verantwortlicher im Sinne von Art. 4 Z. 7 DSGVO oder als gemeinsam Verantwortliche im Sinn von Art. 26 DSGVO verarbeiten .

Mitglieder haben gemäß Art. 32 Abs. 1 DSGVO unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten geeignete technische und organisatorische Maßnahmen (im Folgenden „Maßnahmen für die Sicherheit der Verarbeitung“) zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Gegenstand dieser Verhaltensregeln sind präzisierende Vorgaben für Mitglieder zu Maßnahmen für die Sicherheit der Verarbeitung gemäß Art. 32 DSGVO.

Die gegenständlichen Verhaltensregeln wurden von den Verbänden erstellt und im Rahmen von persönlichen Besprechungen sowie in Schriftform laufend mit dem AMS und dem SMS abgestimmt. Die Verbände behalten sich vor, diese Verhaltensregeln künftig um weitere Regelungsinhalte zu ergänzen.

Die Unterwerfung unter diese Verhaltensregeln durch Mitglieder erfolgt freiwillig und kann von ihnen zu jedem Zeitpunkt wieder beendet werden.

3. Zweck

Die Bestimmung von Maßnahmen für die Sicherheit der Verarbeitung gemäß Art. 32 DSGVO und die damit einhergehende Durchführung von Risikoanalysen ist speziell für kleinere und mittelgroße Mitglieder herausfordernd.

Präzisierende Vorgaben zu solchen Maßnahmen für die Sicherheit der Verarbeitung verschaffen Mitgliedern den Vorteil, dass laufende aufwändige individuelle Auseinandersetzungen mit zum Teil kostenintensiver externer Begleitung vermieden werden können. Dies ist insbesondere auch deshalb von Bedeutung, weil Mitglieder im Rahmen der Leistungserbringung in der beruflichen und sozialen Integration häufig besondere Kategorien personenbezogener Daten (insbesondere Gesundheitsdaten) verarbeiten und vor diesem Hintergrund die Risiken für die Rechte und Freiheiten der Betroffenen als potenziell hoch eingeschätzt werden müssen. Darüber hinaus bestehen zu Maßnahmen für die Sicherheit der Verarbeitung – abgesehen von unverbindlichen Empfehlungen und vereinzelter Fachliteratur, wie z.B. dem „Österreichischen Informationssicherheitshandbuch“ – keine substanziellen Hilfsmittel, wie sie etwa für Datenschutz-Folgenabschätzungen in Form von Stellungnahmen des Europäischen Datenschutzausschusses vorliegen. Auch die DSGVO selbst bietet, abgesehen von der Aufzählung im Art. 32 Abs. 1 lit. a bis d, wenig konkrete Hilfestellungen zur Bestimmung von Maßnahmen für die Sicherheit der Verarbeitung.

Präzisierende Vorgaben zu Maßnahmen für die Sicherheit der Verarbeitung ermöglichen Mitgliedern eine gewisse Planungssicherheit, wobei festzuhalten ist, dass die Einhaltung von Verhaltensregeln nicht dazu führt, dass Mitglieder keinen Sanktionen nach der DSGVO (insbesondere Geldbußen) mehr unterliegen können. Ein strafbares Verhalten kann daher weder beseitigt noch obsolet werden. Der Einhaltung von Verhaltensregeln ist aber gebührend – zu Gunsten der Mitglieder – Rechnung zu tragen (vgl. Erwägungsgrund 148 zur DSGVO). Darüber hinaus können Mitglieder die Einhaltung genehmigter Verhaltensregeln als Faktor für den Nachweis heranziehen, dass sie geeignete Maßnahmen für die Sicherheit der Verarbeitung getroffen haben (Art. 32 Abs. 3 DSGVO).

Für die Verbände ergeben sich Vorteile aus der Ausschöpfung von Synergie- und Effizienzpotentialen in Bezug auf den Informations-, Beratungs- und Schulungsbedarf ihrer Mitglieder. Auch die Begleitung bei der Umsetzung gesetzlich und vertraglich verpflichtender Datensicherheitsmaßen wird dadurch planbarer.

Da Mitglieder ihre Leistungen für das AMS und das SMS auf der Grundlage von Verträgen über die Auftragsverarbeitung gemäß Art. 28 DSGVO erbringen, können genehmigte Verhaltensregeln vom AMS und vom SMS als Faktor herangezogen werden, um hinreichende Garantien ihrer Auftragsverarbeiter für die Ergreifung geeigneter Maßnahmen für die Sicherheit der Verarbeitung nachzuweisen (Art. 28 Abs. 5 DSGVO). Wird die Einhaltung der Verhaltensregeln gemäß Art. 41 DSGVO durch akkreditierte Stellen überprüft, können eigenständige Überprüfungen des AMS und des SMS abgestimmt, Doppelgleisigkeiten vermieden und Synergiepotentiale ausgeschöpft werden.

4. Rechtsgrundlagen und datenschutzrechtliche Rollenverteilung

Gemäß Art. 40 Abs. 2 lit. h DSGVO können Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, Verhaltensregeln ausarbeiten, mit denen Maßnahmen für die Sicherheit der Verarbeitung gemäß Art. 32 präzisiert werden.

Die Vereine „dabei Austria“ und „arbeit plus“ sind „Verbände“ im Sinn dieser Vorschrift und vertreten, entweder unmittelbar oder mittelbar über die Landesverbände, Mitglieder im Rahmen ihrer Leistungserbringung gegenüber dem AMS und dem SMS.

4.1. Abgrenzung zur Berufsvereinigung der ArbeitgeberInnen privater Bildungseinrichtungen (BABE) und ihren Verhaltensregeln

Dienstleistungen im Auftrag des AMS können nicht nur von Mitgliedern von „dabei Austria“ und „arbeit plus “, sondern auch von Mitgliedern Berufsvereinigung der ArbeitgeberInnen privater Bildungseinrichtungen („BABE") erbracht werden.

„BABE“ vertritt in diesem Kontext Bildungseinrichtungen, die insbesondere folgende Dienstleistungen erbringen:[3]

- *„Bildungsangebote für Erwachsene und Jugendliche zur Verbesserung der Chancen am Arbeitsmarkt, in Bildung und Gesellschaft.“*
- *„Vermittlung arbeitssuchender Personen am Arbeitsmarkt.“*

Mitglieder von „BABE“ bieten ihren Zielgruppen damit insbesondere Möglichkeiten zur Weiterbildung und Vermittlung am Arbeitsmarkt. Dabei können „*unter Umständen*“ auch besondere Kategorien personenbezogener Daten betroffen sein, z.B. dann, wenn gesundheitliche Umstände die Stellung einer Person am Arbeitsmarkt beeinflussen.[4]

Mitglieder der Verbände „dabei Austria“ und „arbeit plus“ erbringen hingegen Dienstleistungen im Bereich der beruflichen und sozialen Integration.

Konkret erbringen Mitglieder von „dabei Austria“ insbesondere Dienstleistungen für jugendliche oder erwachsene Personen, die eine Behinderung haben oder, z.B. aufgrund von Lernschwächen oder sozialen Phobien, ausgrenzungsgefährdet sind. Primäre Ziele dieser Dienstleistungen sind somit die berufliche Orientierung, das Aufzeigen von Perspektiven, die Erlangung der individuellen Ausbildungsreife sowie die Heranführung an oder die Erlangung und Sicherung von Ausbildungs- bzw. Beschäftigungsverhältnissen am allgemeinen Arbeitsmarkt. Von diesen Dienstleistungen sind auch Beratungs- oder Informationsangebote für Unternehmen umfasst, die jugendliche oder erwachsene Menschen mit Behinderung bzw.

[3] vgl. Verhaltensregeln / Code of Conduct zum Datenschutz der Berufsvereinigung der ArbeitgeberInnen privater Bildungseinrichtungen - BABE CoC, Version 5. November 2020, S 7.
[4] vgl. BABE CoC, S 10.

ausgrenzungsgefährdete Jugendliche und Erwachsene beschäftigen oder beschäftigen wollen. Die dabei angebotenen Maßnahmen sind nicht nur auf eine Wiedereingliederung in den Arbeitsmarkt beschränkt, sondern erstrecken sich insbesondere bei Jugendlichen und jungen Erwachsenen auf die Qualifizierung für den Ersteintritt.

Mitglieder von „arbeit plus“ unterstützen am Arbeitsmarkt benachteiligte Personen, indem ihnen Beschäftigung, Beratung und Qualifizierung auf den Weg zurück ins Erwerbsleben angeboten werden. Diese Angebote richten sich dabei an unterschiedliche benachteiligte Gruppen, wie z.B. langzeitbeschäftigungslose Personen, Menschen mit Beeinträchtigungen, Mädchen und Frauen, Jugendliche, ältere Menschen, MigrantInnen, Personen mit Suchterkrankungen oder Haftentlassene. Mitglieder bieten arbeitssuchenden Personen einen Entwicklungsrahmen auf Zeit. Sie unterstützen dabei, bestehende Probleme im persönlichen Umfeld zu lösen (Wohnungssuche, Schulden, Suchterkrankung, familiäre Schwierigkeiten etc.) und vermitteln praxisorientiertes Wissen, was insbesondere Menschen mit niedrigem formalen Bildungsstand zugutekommt. Außerdem kooperieren sie mit anderen Unternehmen bei der Suche nach passenden Arbeitsplätzen und beraten sie in Fragen von Gleichstellung, Diversität und sozialer Integration.

Im Ergebnis betreuen Mitglieder der Verbände primär Menschen mit Behinderungen und sonstige benachteiligte Menschen. Die damit verbundene Verarbeitung besonderer Kategorien personenbezogener Daten erfolgt – anders als bei Mitgliedern von „BABE“ – nicht nur „*unter Umständen*“ (d.h. gelegentlich bzw. in Einzelfällen), sondern regelmäßig. Gerade in Bezug auf die Erbringung von Leistungen nach dem BEinstG gegenüber dem SMS muss die Verarbeitung von Gesundheitsdaten als immanent angesehen werden. Daneben werden auch häufig Daten verarbeitet, die zwar keine besonderen Kategorien personenbezogener Daten im Sinn der DSGVO darstellen, aufgrund ihrer persönlichen Bedeutung für die betroffenen Personen aber ebenfalls als besonders vertraulich einzustufen sind. In der Praxis kann dies z.B. Informationen über wirtschaftliche und soziale Rahmenbedingungen, Hinweise zur Arbeitslosigkeit oder strafrelevante Daten betreffen.

Die Zielgruppen von Mitgliedern der Verbände unterscheiden sich damit grundlegend von jenen der Mitgliedern von „BABE“, die ihre Leistungen in der Weiterbildung und Vermittlung am Arbeitsmarkt generell für alle arbeitslosen Menschen und damit insbesondere auch für jene Personen anbieten, die nicht aufgrund einer Behinderung oder eines sonstigen Grundes benachteilig sind.

Auch die Mitgliederkreise selbst unterscheiden sich grundlegend voneinander. Während „BABE“ eine Berufsvereinigung für grundsätzlich alle privaten Bildungseinrichtungen ist, vertreten „dabei Austria“ und „arbeit plus“ ausschließlich Unternehmen des sozialen Dienstleistungssektors, die Leistungen im Rahmen der beruflichen und sozialen Integration erbringen. In Einzelfällen kann es zwar sein, dass Mitglieder der Verbände auch Mitglied bei „BABE“ sind, und zwar dann, wenn diese neben ihrer Leistungserbringung in der beruflichen und sozialen Integration auch eine Bildungseinrichtung betreiben, diese gemeinsame Schnittmenge ist jedoch quantitativ nicht bedeutsam.

4.2. Datenschutzrechtliche Rollenverteilung

4.2.1. Unterschiedliche Tätigkeitsbereiche

Mitglieder der Verbände werden entweder für das AMS oder das SMS oder für beide Fördergeber tätig. Je nach individuellem Leistungsangebot können Mitglieder aber auch für andere FördergeberInnen tätig werden, so z.B. für die für sie zuständige Landesregierung im Rahmen der Behindertenhilfe,der Kinder- und Jugendhilfe oder der Mindestsicherung.

Über alle diese Leistungserbringungen werden zwischen den Fördergebern und den Mitgliedern in der Regel zivilrechtliche Verträge – entweder in Form von Förderungsverträgen, Werkverträgen, Auftragsverträgen bzw. Mischformen daraus oder Rahmenvereinbarungen – abgeschlossen. Werden dabei personenbezogene Daten im Auftrag eines Fördergebers gemäß Art. 28 DSGVO verarbeitet, werden zusätzlich entsprechende Verträge über die Auftragsverarbeitung abgeschlossen.

Bei der Leistungserbringung gegenüber dem AMS und dem SMS und somit in der beruflichen und sozialen Integration werden Daten standardmäßig im Auftrag der Fördergeber verarbeitet und dementsprechend Verträge über die Auftragsverarbeitung gemäß Art. 28 DSGVO abgeschlossen. Bei anderen Fördergebern, wie z.B. Landesregierungen ist das nur vereinzelt der Fall (z.B. bei Leistungen, die im Bereich der Kinder- und Jugendhilfe erbracht werden), in anderen Bereichen, wie z.B. der Behindertenhilfe oder der Mindestsicherung ist das in der Regel nicht der Fall.

4.2.2. Applikationen der FördergeberInnen

Das AMS und das SMS stellen Mitgliedern zur Aufgabenerfüllung eigene Applikationen zur Verfügung. Dabei handelt es sich insbesondere um die Applikation „eAMS-Konto“ des AMS und um die Applikationen „MBI - Monitoring berufliche Integration“, „MAB - Monitoring AusBildung bis 18“, „Be-FIT“, „WABA“ (Wirkungs- und Aktivitätsmonitoring der Beruflichen Assistenzen) und „Betriebsservice Datenbank“ des SMS.

Über diese Applikationen erfolgt die Leistungsdokumentation und die zentrale Kommunikation zwischen Fördergebern und Mitgliedern. Für die Verarbeitung personenbezogener Daten stehen Mitgliedern damit sichere elektronische Plattformen und Kommunikationswege zur Verfügung.

4.2.3. Rolle als Verantwortlicher und Auftragsverarbeiter

Da Mitglieder häufig ein breites Spektrum an sozialen Dienstleistungen für öffentliche AuftraggeberInnen erbringen, ist von ihnen im Einzelfall zu prüfen, bei welchen Verarbeitungstätigkeiten sie jeweils „Verantwortlicher“ im Sinne von Art. 4 Z. 7 DSGVO sind. Eine solche Eigenverantwortlichkeit kann zunächst für alle Verarbeitungstätigkeiten angenommen werden, die nicht im Auftrag eines Fördergebers erfolgen, so z.B. die betriebsinterne Personalverwaltung oder eigene Marketingmaßnahmen.

Bei der Auftragserfüllung gegenüber dem SMS beschränkt sich die Auftragsverarbeitung gemäß Art. 28 DSGVO auf die Verwendung der vom SMS zur Verfügung gestellten Applikationen. In Bezug auf alle anderen Verarbeitungen, die in Zusammenhang mit der Leistungserbringung für das SMS stattfinden (z.B. E-Mail-Versand, Kommunikation mit System- und KooperationspartnerInnen, eigenständige Dokumentationen, Zusendung von Newslettern, etc.), legt das SMS weder Zwecke noch Mittel der Datenverarbeitung fest. Somit sind Mitglieder in allen Bereichen außerhalb der vom SMS zur Verfügung gestellten Applikationen eigenständige Verantwortliche und haben z.B. ihre Informationspflichten nach Art. 13 und 14 DSGVO selbst zu erfüllen.

Bei der Auftragserfüllung gegenüber dem AMS stellt sich die Auftragsverarbeitung gemäß Art. 28 DSGVO umfangreicher dar und umfasst nicht nur die Verwendung der zur Verfügung gestellten Applikation „eAMS-Konto“, sondern grundsätzlich alle Datenverarbeitungen, die im Rahmen der Auftragserfüllung (z.B. sozialpädagogische Betreuung inklusive Outplacement von Transitarbeitskräften im Fall von GBP/SÖB) gegenüber dem AMS erfolgen. Von der Auftragsverarbeitung gegenüber dem AMS ist daher z.B. auch die Kommunikation mit potenziellen Ausbildungsträgern und Arbeitgebern erfasst.

Die Details zum Umfang der Auftragsverarbeitung ergeben sich aus dem jeweiligen Vertrag über die Auftragsverarbeitung gemäß Art. 28 DSGVO, der von Mitgliedern mit dem AMS und/oder dem SMS standardmäßig abgeschlossen wird.

Ob Mitglieder im Rahmen Ihrer Leistungserbringung als „Verantwortlicher“ oder als „Auftragsverarbeiter“ zu qualifizieren sind, hängt letztlich aber nicht von formellen Gesichtspunkten ab, sondern ist immer aus den faktischen Gegebenheiten der jeweiligen Datenverarbeitung abzuleiten.[5] Aus diesem Grund haben Mitglieder auch im Einzelfall zu prüfen, welche datenschutzrechtliche Rolle sie konkret einnehmen .

Aus dem Vertrag über die Auftragsverarbeitung des AMS und des SMS ergeben sich nachfolgende Besonderheiten.

4.2.3.1. Vertrag über die Auftragsverarbeitung mit dem AMS

Neben den allgemeinen Vorgaben in Art. 28 DSGVO werden im Vertrag über die Auftragsverarbeitung mit dem AMS insbesondere folgende Punkte geregelt:

- Mitglieder haben die Verschwiegenheitsverpflichtung für MitarbeiterInnen so auszugestalten, dass diese auch nach Beendigung der Tätigkeit aufrecht bleibt.

- Die konkreten Datenkategorien, die von Mitgliedern im Rahmen der Auftragserfüllung verarbeitet werden dürfen, werden vorgegeben.

- Eine Verarbeitung von Daten für andere Zwecke ist nur nach Rücksprache mit dem AMS möglich und setzt grundsätzlich voraus, dass dafür eine Rechtsgrundlage im Unionsrecht

[5] Vgl. EDPB, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, Version 2.0 Rz 12ff.

oder in nationalen Rechtsvorschriften vorliegt oder die Einwilligung der betroffenen Personen eingeholt wird. Eine diesbezügliche Rücksprache mit dem AMS darf nur dann unterbleiben, wenn die Datenverarbeitung zur Erfüllung der Vertragsbeziehung zwischen Auftragsverarbeiter und der betroffenen Person (Art. 6 Abs. 1 lit b DSGVO) erfolgt oder auf berechtigte Interessen im unmittelbaren Zusammenhang mit der Leistungserbringung für das AMS gestützt werden kann (Art. 6 Abs. 1 lit f DSGVO, etwa in Bezug auf die Einhaltung der Hausordnung oder die Wahrung der Informationssicherheit). In diesen Fällen sind Mitglieder eigenständige Verantwortliche für die Datenverarbeitung und haben ihre datenschutzrechtlichen Pflichten eigenverantwortlich zu erfüllen. Insbesondere sind die Vorgaben zur Zweckänderung nach Art. 6 Abs. 4 DSGVO einzuhalten.

- Geeignete technische und organisatorische Maßnahmen sind spätestens alle drei Jahre auf ihre Wirksamkeit hin zu überprüfen, zu bewerten und zu evaluieren und werden zum Teil vom AMS auch unmittelbar vorgegeben. Dieser 3-Jahreszeitraum stellt eine Maximalfrist dar. Eine zwischenzeitliche Anpassung innerhalb dieses 3-Jahreszeitraums ist immer dann vorzunehmen, wenn sich die Risikoeinschätzung (z.B. durch die Einführung einer neuen Datenanwendung oder durch einen gröberen Datenschutzvorfall) verändert oder von Seiten des AMS eine Anpassung als erforderlich erachtet wird. Mitglieder sind daher nicht davon befreit, laufend zu evaluieren, ob sich ein materieller Anpassungsbedarf ihrer implementierten technischen und organisatorischen Maßnahmen aus gegebenem Anlass ergibt). Der Nachweis über die Umsetzung solcher geeigneten technischen und organisatorischen Maßnahmen kann auch durch die Anwendung von genehmigten Verhaltensregeln gemäß Art. 40 DSGVO erbracht werden.

- Eine Hinzuziehung von Sub-AuftragsverarbeiterInnen ist grundsätzlich möglich, Mitglieder haben das AMS in diesem Fall vorab (mindestens 2 Wochen) über die Inanspruchnahme unter Angabe des Einsatzzeitpunktes schriftlich zu informieren. Wenn vom AMS bis zum Zeitpunkt des Einsatzes kein schriftlicher Einspruch erhoben und von Mitgliedern mit Sub-AuftragsverarbeiterInnen eine Vereinbarung gemäß Art. 28 Abs. 4 DSGVO abgeschlossen wird, gilt die Genehmigung des AMS für die Hinzuziehung als erteilt. Einzelpersonen, die aufgrund eines freien Dienstvertrages oder eines Werkvertrages als TrainerIn oder BeraterIn arbeiten und die über keine für Mitglieder typische betriebliche Struktur verfügen, gelten nicht als Sub-AuftragsverarbeiterIn. Sie sind datenschutzrechtlich als MitarbeiterInnen des betreffenden Mitglieds zu behandeln und zur Verschwiegenheit zu verpflichten.

- Mitglieder haben das AMS als Verantwortlichen für die Erfüllung der Betroffenenrechte zu unterstützen und insbesondere den betroffenen Personen vor Ort die Muster des AMS zur Erfüllung der Informationspflichten nach Art. 13 und 14 DSGVO zu überreichen (Übernahme der Funktion eines „Briefträgers“, da Mitglieder im direkten Erstkontakt mit den betroffenen Personen stehen).

- Da Mitglieder die Daten betroffener Personen unmittelbar vor Ort verarbeiten und von diesen in der Regel als erste Ansprechpersonen für Nachfragen herangezogen werden, haben sie – im Auftrag und im Namen des AMS als Verantwortlicher – eine DSGVO-konforme Auskunft unmittelbar gegenüber der AuskunftswerberIn zu erteilen. Wenn dabei erkennbar ist, dass vom Auskunftsbegehren auch Daten umfasst sind, die direkt vom AMS verarbeitet werden, haben Mitglieder den Antrag unverzüglich an das AMS weiterzuleiten und dies dem Antragsteller entsprechend mitzuteilen. Unabhängig davon können betroffene Personen entsprechende Anfragen bzw. Anträge immer auch unmittelbar beim AMS einbringen.

- Mitglieder sind verpflichtet, vom AMS übermittelte bzw. bereitgestellte Daten für die Dauer von 6 Monaten nach Vertragsende aufzubewahren und anschließend unverzüglich zu löschen bzw. zu vernichten.

- Das AMS ist ermächtigt, bei Mitgliedern jederzeit Überprüfungen einschließlich Inspektionen durchzuführen. Diese können vom Verantwortlichen selbst oder von einem beauftragten Prüfer vorgenommen werden. Dabei sind auch Vorort-Kontrollen möglich.

4.2.3.2. Vertrag über die Auftragsverarbeitung mit dem SMS

Neben den allgemeinen Vorgaben in Art. 28 DSGVO werden im Vertrag über die Auftragsverarbeitung mit dem SMS insbesondere folgende Punkte geregelt:

- Mitglieder haben die Verschwiegenheitsverpflichtung für MitarbeiterInnen so auszugestalten, dass diese auch nach Beendigung der Tätigkeit aufrecht bleibt.

- Die Hinzuziehung von Sub-AuftragsverarbeiterInnen ist nicht gestattet, wobei dies nur im Umfang der Auftragsverarbeitung (Verwendung der vom SMS zur Verfügung gestellten Applikationen) gilt. Da Mitglieder für alle anderen Verarbeitungstätigkeiten im Zusammenhang mit der Leistungserbringung selbst die Zwecke und Mittel der Verarbeitung festlegen und damit eigenständige Verantwortliche sind, können für diese Tätigkeiten Sub-AuftragsverarbeiterInnen nach den Vorgaben der DSGVO beigezogen werden.

- Mitglieder sind verpflichtet, ausreichende Sicherheitsmaßnahmen gemäß Art. 32 DSGVO zu ergreifen, um zu verhindern, dass Daten ordnungswidrig verwendet oder Dritten unbefugt zugänglich werden.

4.2.4. Auswirkungen von datenschutzrechtlichen Rollen auf Maßnahmen für die Sicherheit der Verarbeitung gemäß Art. 32 DSGVO

Werden Leistungen aufgrund einer vertraglichen Vereinbarung mit AMS, SMS oder anderen öffentlichen Fördergebern erbracht, kann die mit der Aufgabenerfüllung einhergehende Verarbeitung personenbezogener Daten wie oben dargestellt entweder als Verantwortlicher oder als Auftragsverarbeiter erfolgen. Abhängig von den spezifischen Rahmenbedingungen

einer Beauftragung kann in der Praxis auch eine gemeinsame Verantwortlichkeit im Sinn von Art. 26 DSGVO vorliegen. Mitglieder haben daher immer im Einzelfall zu prüfen, im Rahmen welcher Leistungserbringung gegenüber welchem Fördergeber sie welche datenschutzrechtliche Rolle einnehmen und dies nachvollziehbar zu dokumentieren (z.B. im Verarbeitungsverzeichnis nach Art. 30 DSGVO).

Abhängig von der konkreten datenschutzrechtlichen Rolle eines Mitglieds können sich unterschiedliche Pflichten ergeben, so sind z.B. in Bezug auf die Erstellung des Verzeichnisses von Verarbeitungstätigkeiten [6] oder hinsichtlich der Verletzung des Schutzes personenbezogener Daten, bei der ein Auftragsverarbeiter unverzüglich den Verantwortlichen informieren muss, während ein Verantwortlicher gegebenenfalls eine Meldung an die Datenschutzbehörde zu erstatten hat.[7]

Bei einem Verstoß gegen die DSGVO bzw. das DSG ist zu beachten, dass der Betroffene Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter hat.[8] Damit bleibt der Verantwortliche auch bei Hinzuziehung eines Auftragsverarbeiters haftbar.

Mit den gegenständlichen Verhaltensregeln sollen Mitgliedern im Zuge der Leistungserbringung für das AMS und das SMS im Rahmen der beruflichen und sozialen Integration geeignete technische und organisatorische Maßnahmen für die Sicherheit der Datenverarbeitung gemäß Art. 32 DSGVO vorgegeben werden. Da diese Maßnahmen unter Berücksichtigung der oben dargestellten Besonderheiten bei der Leistungserbringung in der beruflichen und sozialen Integration beschrieben werden (regelmäßige Verarbeitung besonderer Kategorien personenbezogener Daten und anderer als besonders vertraulich einzustufender Daten), stellen sie eine Orientierungshilfe für alle Verarbeitungstätigkeiten im Zusammenhang mit der Leistungserbringung für das AMS und das SMS, unabhängig davon ob diese als Verantwortlicher oder als Auftragsverarbeiter durchgeführt werden. Da sich die Anordnungen in Art. 32 DSGVO gleichermaßen an den Verantwortlichen und den Auftragsverarbeiter richten („*Unter Berücksichtigung… treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen*“), bieten die Verhaltensregeln daher in jedem Fall eine Hilfestellung für Mitglieder.

5. Risikoanalyse

Auftragsverarbeiter haben nach Art. 32 DSGVO geeignete Maßnahmen für die Sicherheit der Verarbeitung zu treffen, um ein dem Risiko angemessenes Schutzniveau der im Auftrag verarbeiteten personenbezogenen Daten zu gewährleisten.

Bei der Bestimmung der Maßnahmen für die Sicherheit der Verarbeitung sind nach Art. 32 Abs. 1 DSGVO der Stand der Technik, die Implementierungskosten, die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche

[6] Vgl. Art. 30 Abs.1 und 2 DSGVO.
[7] Vgl. Art. 33 Abs. 1 und 2 DSGVO.
[8] Vgl. Art. 82 Abs. 1 DSGVO und § 29 Abs. 1 DSG.

Eintrittswahrscheinlichkeit und die Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen.

Nach Erwägungsgrund 76 zur DSGVO sollen die Eintrittswahrscheinlichkeit und die Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person 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. Mit der nachfolgenden Analyse werden als Hilfestellung für Mitglieder Risiken anhand von potenziellen Ereignissen bewertet, die sowohl branchenunabhängig als auch branchenspezifisch eintreten können.

5.1. Art, Umfang und Umstände der Datenverarbeitung im Rahmen der Auftragserfüllung

Die gegenständlichen Verhaltensregeln stellen keine Rechtsgrundlage im Sinn der Art. 6 und 9 DSGVO dar. Im Rahmen der Auftragserfüllung gegenüber dem AMS und/oder dem SMS dürfen Mitglieder personenbezogene Daten vielmehr nur in jenem Umfang verarbeiten, in dem auch für das AMS bzw. das SMS eine gesetzliche Grundlage zur Datenverarbeitung vorliegt. Die einschlägigen Bestimmungen dafür finden sich im BEinstG, im AMSG, im AMFG und im APflG.

Bei der Datenverarbeitung im Rahmen der Auftragserfüllung können insbesondere folgende Kategorien personenbezogener Daten von AdressatInnen relevant sein:[9]

- Stammdaten (Namen, Sozialversicherungsnummer und Geburtsdatum, Geschlecht, Staatsangehörigkeit, Aufenthalts- und Arbeitsberechtigungen, Adresse des Wohnsitzes oder Aufenthaltsortes, Telefon- und Faxnummer, E-Mail-Adresse, sonstige Kontaktmöglichkeiten, Bankverbindung und Kontonummer, beruflich verwertbare Fähigkeiten und Fertigkeiten, sonstige persönliche Umstände, die die berufliche Verwendung berühren).

- Daten über Beruf, Bildung und Ausbildung (Erwerbstätigkeit und Status der Person, Berufs-, Beschäftigungs- und Ausbildungswünsche, Schulbildung, außerschulische Bildung, berufliche Ausbildung, Ausbildungswünsche, bisherige berufliche Tätigkeiten, beruflich verwertbare Fähigkeiten und Fertigkeiten, Umstände des Nichtzustandekommens oder der vorzeitigen Beendigung von Ausbildungen oder des Ruhens der Ausbildungspflicht).

- Daten über wirtschaftliche und soziale Rahmenbedingungen (Familienstand, unterhaltsberechtigte Kinder, Art und Umfang von Sorgepflichten, die die Verfügbarkeit am Arbeitsmarkt berühren, sonstige Umstände, die die Verfügbarkeit am Arbeitsmarkt berühren, ausgeübte Erwerbstätigkeiten, Einkommen, außerordentliche Aufwendungen, Versicherungszeiten, Bemessungsgrundlagen, Art, Inhalt, Dauer und Höhe gewährter Leistungen, Zeiten der Arbeitsuche).

[9] Vgl. § 22 Abs. 4 BEinstG, § 25 AMSG und § 15 APflG.

- Gesundheitsdaten (Funktionseinschränkungen, Grad der Behinderung, gesundheitliche Einschränkungen, die die Arbeitsfähigkeit oder die Verfügbarkeit in Frage stellen oder die berufliche Verwendung berühren, gesundheitliche Einschränkungen der AdressatInnen und ihrer Angehörigen, die einen finanziellen Mehraufwand erfordern).

- Daten über Beschäftigungsverläufe, Arbeitsuche und Betreuungsverläufe (Pläne und Ergebnisse der Arbeitsuche und Betreuung, Hindernisse, welche die Betreuung erschweren oder verhindern, Umstände der Auflösung von Arbeitsverhältnissen, Umstände des Nichtzustandekommens von Arbeitsverhältnissen, Sanktionen wegen Fehlverhaltens, Betroffenheit von Streik oder Aussperrung).

Im Rahmen ihrer Auftragserfüllung gegenüber dem AMS und dem SMS werden von Mitgliedern häufig Gesundheitsdaten gemäß Art. 4 Z 15 DSGVO und damit besondere Kategorien personenbezogener Daten von AdressatInnen verarbeitet. Darüber hinaus werden auch Daten verarbeitet, die zwar nicht als besondere Kategorien personenbezogener Daten zu qualifizieren sind, aufgrund ihrer persönlichen Bedeutung für betroffene Personen aber dennoch als besonders vertraulich anzusehen sind. Dies kann z.B. Informationen über wirtschaftliche und soziale Rahmenbedingungen, Hinweise zur Arbeitslosigkeit oder strafrelevante Daten betreffen. Alle diese Daten können zur Bloßstellung und Diskriminierung von AdressatInnen sowie zu anderen unerwünschten Folgen führen, wenn sie etwa Unbefugten gegenüber offengelegt werden.

Mitglieder müssen im Rahmen ihrer Aufgabenerfüllung auch häufig Gesundheitsdaten und andere besonders vertrauliche Informationen mit unterschiedlichen externen Stakeholdern austauschen, z.B. im Rahmen der Auskunftserteilung gegenüber gesetzlichen VertreterInnen, dem Kinder- und Jugendhilfeträger und anderen gesetzlich zuständigen Behörden und Institutionen oder wenn dies im Einzelfall nach vorhergehender Aufklärung, Abstimmung und erteilter Einwilligung der AdressatInnen, z.B. gegenüber Schulen, Ausbildungsstätten, potenziellen ArbeitgeberInnen sowie involvierten GesundheitsdienstleisterInnen und anderen sozialen DienstleisterInnen, zur Zielerreichung jeweils erforderlich ist.

Der Umstand, dass Mitglieder im Zusammenhang mit der beruflichen und sozialen Integration von betroffenen Personen und unter Berücksichtigung von Grundsätzen wie Zweckbindung, Datenminimierung und Verhältnismäßigkeit von einfachen Stammdaten über Daten zu wirtschaftlichen und sozialen Rahmenbedingen bis hin zu Gesundheitsdaten und anderen sensiblen Daten verarbeiten und im Rahmen der Aufgabenerfüllung sich häufig auch mit unterschiedlichsten externen Stakeholdern abstimmen müssen, stellt eine branchenspezifische Besonderheit dar, die so z.B. weder auf Bildungseinrichtungen oder Sozialberatungsstellen noch auf Alten- und Pflegeheime oder Krankenanstalten zutrifft.

So werden z.B. in einer Krankenanstalt laufend gesundheitsrelevante Daten verarbeitet, ein Datenaustausch mit externen Stakeholdern findet aber grundsätzlich nur in vordefinierten Konstellationen statt (z.B. Anforderung einer Diagnose durch die HausärztIn oder Anfrage eines Versicherers nach einem Personenschaden mit Aufenthalt in der Krankenanstalt) und regelmäßig nur mit Personen bzw. Institutionen, die einer besonderen berufsrechtlichen

Verschwiegenheitspflicht (z.B. nach dem ÄrzteG, dem KAKuG oder dem MTD-Gesetz) unterliegen.

Im Unterschied dazu können im Rahmen der beruflichen und sozialen Integration unterschiedlichste Fallkonstellationen auftreten, bei denen Mitglieder – abhängig vom Fördergeber und dem jeweiligen Umfang der Auftragsverarbeitung – und gegebenenfalls nach erfolgter Abstimmung und Einwilligung durch die betroffene Person personenbezogene Daten anderen involvierten Personen und Institutionen gegenüber offen legen müssen, die regelmäßig keiner besonderen berufsrechtlichen Verschwiegenheitspflicht unterliegen. So z.B., wenn ein Unternehmen, zu dem die AdressatIn erfolgreich vermittelt wurde, in der Probezeit auf die zuständige BetreuerIn des betreffenden Mitglieds zukommt und eine Abklärung von Problemen im Zusammenhang mit einer Verhaltensauffälligkeit der AdressatIn wünscht.

Abhängig von der Größe der Mitglieder werden auch entsprechend viele AdressatInnen von ihnen betreut, was wiederum zwangsläufig zur Folge hat, dass eine entsprechend hohe Anzahl von MitarbeiterInnen Zugriff auf Gesundheitsdaten und andere besonders vertrauliche Daten von AdressatInnen haben muss.

Für die Verarbeitung personenbezogener Daten werden den Mitgliedern vom AMS und vom SMS eigene Applikationen wie „eAMS-Konto“ „MBI-Monitoring berufliche Integration“, „MAB Monitoring AusBildung bis 18“, „Be-FIT“, „WABA“ (Wirkungs- und Aktivitätsmonitoring der Beruflichen Assistenzen) und „Betriebsservice Datenbank“ zur Verfügung gestellt. Darüber hinaus erfolgen Datenverarbeitungen zwangsläufig auch in eigenen IT-Systemen der Mitglieder, wie z.B. E-Mail-Diensten und zum Teil auch in manueller Form, etwa wenn von AdressatInnen persönliche Dokumente in Papierform übergeben werden oder im Rahmen der Aufgabenerfüllung mit externen Stakeholdern, wie z.B. Schulen, Ausbildungsstätten, potenziellen ArbeitgeberInnen, involvierten GesundheitsdienstleisterInnen, anderen sozialen DienstleisterInnen oder Behörden kommuniziert werden muss.

Die Verarbeitung von personenbezogenen Daten im Rahmen der Auftragserfüllung gegenüber dem AMS und dem SMS erfolgt daher unter den besonderen Umständen, dass häufig besondere Kategorien personenbezogener Daten und andere besonders vertrauliche Informationen verarbeitet und in unterschiedlichsten Fallkonstellationen mit externen Stakeholdern, die keiner besonderen berufsrechtlichen Verschwiegenheitsverpflichtung unterliegen, ausgetauscht werden und diese Datenverarbeitungen auf Grund der regelmäßig hohen Anzahl an betreuten AdressatInnen auch als umfangreich anzusehen sind. Entsprechende Datenverarbeitungen erfolgen dabei überwiegend elektronisch, zum Teil aber auch manuell.

5.2. Zwecke der Datenverarbeitung

Die Datenverarbeitung von Mitgliedern im Rahmen der Auftragserfüllung gegenüber dem AMS und dem SMS erfolgt nach Maßgabe der in den Verträgen über die Auftragsverarbeitung angeführten Verarbeitungszwecke, die sich wiederum unmittelbar aus den gesetzlichen Grundlagen für arbeitsmarktpolitische Maßnahmen im Sinn der Art. 6 Abs. 1 lit. c und

Art. 9 Abs. 2 lit. g DSGVO ableiten.[10] Damit entspricht die Datenverarbeitung auch den Grundsätzen der Zweckbindung und der Datenminimierung und liegt im hohen öffentlichen Interesse.

Die Verarbeitung personenbezogener Daten durch Mitglieder ist zur Auftragserfüllung gegenüber dem AMS und dem SMS auch zwingend erforderlich und damit alternativlos. Eine Verwendung anonymisierter Daten ist nicht möglich.

5.3. Risiken für die Rechte und Freiheiten natürlicher Personen

Eine Verletzung des Schutzes personenbezogener Daten kann gemäß Art. 4 Z 12 DSGVO in Form einer Verletzung der Sicherheit erfolgen, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt.

Nach Erwägungsgrund 75 zur DSGVO können die Risiken für die Rechte und Freiheiten natürlicher Personen — mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere —aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, und zwar insbesondere dann, wenn

a) die Verarbeitung

   - zu einer Bloßstellung oder einer Diskriminierung,
   - einem Identitätsdiebstahl oder -betrug,
   - einem finanziellen Verlust,
   - einer Rufschädigung oder
   - zu anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen

   führen kann;

b) die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren;

c) besondere Kategorien personenbezogener Daten wie Gesundheitsdaten verarbeitet werden;

d) personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden;

[10] Beispielsweise betrifft dies § 25 und § 32 Abs. 2 AMSG, § 4 und § 6 AMFG § 15 APflG, §§ 6 Abs. 2, 10a und 22 Abs. 4 und 5 BEinStG sowiedie VO (EU) Nr. 1303/2013 und die VO (EU) Nr. 1304/2013.

e) oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.

Auf die Datenverarbeitung von Mitgliedern im Rahmen der Auftragserfüllung gegenüber dem AMS und dem SMS treffen viele dieser Tatbestände zu. Sind von einem Datenschutzvorfall Gesundheitsdaten betroffen, kann dies beispielsweise zu einer Diskriminierung, einer Bloßstellung und anderen erheblichen gesellschaftlichen Nachteilen sowie finanziellen Verlusten führen. Betroffene Personen können auch die Kontrolle über ihre personenbezogenen Daten verlieren und ihre Rechte nicht mehr wahrnehmen. Darüber hinaus sind von der Datenverarbeitung auch Gesundheitsdaten und andere sensible Daten von besonders schutzbedürftigen Personen, wie Menschen mit Behinderungen und Minderjährige betroffen, auf die auch viele Personen (MitarbeiterInnen der Mitglieder und – im Wege gesetzlich geregelter Auskunftserteilungen und Offenlegungen – dritte Personen) zugreifen können.

Vor diesem Hintergrund können Datenschutzvorfälle zweifellos zu einem physischen, materiellen oder immateriellen Schaden für AdressatInnen führen und zwar insbesondere dann, wenn besondere Kategorien personenbezogener Daten betroffen sind.[11]

5.4. Schutzziele

Folgende Schutzziele gelten im Standard-Datenschutzmodell als anerkannt:[12]

- „Verfügbarkeit“: Schutz vor Vernichtung und Verlust.
- „Integrität“: Schutz vor Veränderung.
- „Vertraulichkeit“: Schutz vor unbefugter Offenlegung und unbefugtem Zugang.
- „Nichtverkettbarkeit“: Schutz der Zweckbindung.
- „Transparenz“: Schutz der Revisionsfähigkeit (Nachprüfbarkeit und Nachvollziehbarkeit).
- „Intervenierbarkeit“: Schutz der Betroffenenrechte.

5.5. Potenzielle Ereignisse

Bei der Verarbeitung personenbezogener Daten im Rahmen der Auftragserfüllung gegenüber dem AMS und dem SMS sind insbesondere folgende potenzielle Datenschutzvorfälle vorstellbar, die aus Gründen der besseren Übersicht in tabellarischer Form dargestellt werden.

[11] Vgl. OGH vom 27.2.2013, 6 Ob 25/13i zur ungewollten Offenlegung von Gesundheitsdaten gegenüber Unbefugten.

[12] *Jandt* in *Kühling/Buchner*, Kommentar zur DSGVO[2], Art. 35, Rz. 45, mit weiteren Nachweisen, und *Baumgartner* in *Ehmann/Selmayr*, Kommentar zur DSGVO, Art. 35, Rz. 34. Dazu auch *Bedner/Ackermann*, Schutzziele der IT-Sicherheit, DuD - Datenschutz und Datensicherheit 5/2010, Seiten 323 ff, und andere.

Der Beschreibung möglicher Ereignisse werden dabei die jeweils betroffenen Schutzziele und die möglichen Folgen für Betroffene gegenübergestellt.

In der Praxis sind dabei Ereignisse möglich, die grundsätzlich in jedem Unternehmen und damit branchenunabhängig eintreten können. Darüber hinaus sind auch branchenspezifische Ereignisse vorstellbar, die typischerweise im Rahmen der Aufgabenerfüllung von Mitgliedern eintreten. Um Mitgliedern eine Hilfestellung zur Entwicklung einer ganzheitlichen Sicherheitsstrategie im Sinn von Art. 32 DSGVO zu bieten, werden zunächst jene Ereignisse aufgezeigt, die branchenunabhängig eintreten können, und in der Folge die Ereignisse, die als branchenspezifisch anzusehen sind.

5.5.1. Branchenunabhängig

Liste	Potenzielles Ereignis	Verletzte Schutzziele	Mögliche Folgen
A	Unbefugte Personen dringen in Netzwerke und Systeme ein (Cyber-Crime und Malware-Attacken) und drohen z.B. mit der Löschung von Daten oder der Veröffentlichung vertraulicher Daten im Internet.	Vertraulichkeit, Integrität, Verfügbarkeit, Nichtverkettbarkeit und Transparenz.	Bloßstellung, Diskriminierung, Identitätsdiebstahl, finanzieller Verlust, Rufschädigung und sonstige erhebliche gesellschaftliche Nachteile.
B	Durch Naturgewalten, unvorhersehbare Schadensereignisse oder technische Gebrechen werden Daten zerstört, gelöscht oder können nicht mehr wiederhergestellt werden (Einwirkungen auf Räumlichkeiten, Verarbeitungsanlagen oder technische Infrastrukturen).	Verfügbarkeit, Transparenz und Intervenierbarkeit.	Finanzieller Verlust und sonstige erhebliche gesellschaftliche Nachteile.
C	Unbefugte Personen verschaffen sich Zutritt zu Räumlichkeiten, Verarbeitungsanlagen oder Datenaufbewahrungsorten und gelangen in den Besitz vertraulicher Daten in elektronischer oder manueller Form, etwa durch Einbruchsdiebstahl.	Vertraulichkeit, Integrität, Verfügbarkeit und Nichtverkettbarkeit.	Bloßstellung, Diskriminierung, Identitätsdiebstahl, Rufschädigung und sonstige erhebliche gesellschaftliche Nachteile.
D	Anwesende Personen haben unbefugten Zugang zu vertraulichen Dokumenten in Papierform, die z.B.	Vertraulichkeit und Verfügbarkeit.	Bloßstellung, Diskriminierung, Identitätsdiebstahl,

	in Büros, in Besprechungszimmern oder an Arbeitsplätzen aufliegen.		Rufschädigung und sonstige erhebliche gesellschaftliche Nachteile.
E	Anwesende Personen sehen unbefugt Bildschirme ein.	Vertraulichkeit.	Bloßstellung, Diskriminierung, Rufschädigung und sonstige erhebliche gesellschaftliche Nachteile.
F	Anwesende Personen hören unbefugt vertrauliche Gespräche oder Telefonate mit.	Vertraulichkeit.	Bloßstellung, Diskriminierung, Rufschädigung und sonstige erhebliche gesellschaftliche Nachteile.
G	Vertrauliche Dokumente und Informationen gehen verloren (z.B. Verlust von mobilen Datenträgern oder Dokumenten in Papierform im Außendienst oder im Homeoffice).	Vertraulichkeit und Verfügbarkeit.	Bloßstellung, Diskriminierung, Rufschädigung und sonstige erhebliche gesellschaftliche Nachteile.
H	Vertrauliche Informationen werden von MitarbeiterInnen unbewusst gegenüber unbefugten Personen beauskunftet oder offengelegt, etwa im Zuge von Telefonaten mit Personen, deren Identität und Funktion nicht geklärt wurde.	Vertraulichkeit.	Bloßstellung, Diskriminierung, Rufschädigung und sonstige erhebliche gesellschaftliche Nachteile.
I	Vertrauliche Informationen werden von MitarbeiterInnen bewusst oder unbewusst gegenüber unbefugten Personen im Privatleben offengelegt, etwa im Zuge von Erzählungen im Familien- und Freundeskreis.	Vertraulichkeit.	Bloßstellung, Diskriminierung, Rufschädigung und sonstige erhebliche gesellschaftliche Nachteile.
J	Vertrauliche Informationen werden von MitarbeiterInnen im Homeoffice unbewusst gegenüber unbefugten	Vertraulichkeit.	Bloßstellung, Diskriminierung, Rufschädigung und

	Personen offengelegt, etwa im Zuge von Videokonferenzen oder Telefonaten, die in nicht vertraulicher Umgebung durchgeführt werden.		sonstige erhebliche gesellschaftliche Nachteile.
K	(Ehemalige) MitarbeiterInnen oder AdressatInnen verschaffen sich zum Zweck der persönlichen Vorteilsnahme unbefugt vertrauliche Informationen über betroffene Personen.	Vertraulichkeit.	Bloßstellung, Diskriminierung, Rufschädigung und sonstige erhebliche gesellschaftliche Nachteile.
L	Zulässigerweise verarbeitete personenbezogene Daten werden für unbefugte Zwecke, wie z.B. Profilbildung, weiterverwendet.	Vertraulichkeit, Integrität, Nichtverkettbarkeit, Transparenz und Intervenierbarkeit	Bloßstellung, Diskriminierung, Identitätsdiebstahl, Rufschädigung und sonstige erhebliche gesellschaftliche Nachteile
M	Beigezogene Dienstleister gehen nicht ordnungsgemäß mit personenbezogenen Daten um, die ihnen zur Auftragserfüllung über-lassen wurden bzw. auf die sie zu diesem Zweck zugreifen können.	Vertraulichkeit, Integrität, Verfügbarkeit, Nichtverkettbarkeit, Transparenz und Intervenierbarkeit.	Bloßstellung, Diskriminierung, Identitätsdiebstahl, Rufschädigung und sonstige erhebliche gesellschaftliche Nachteile.

5.5.2. Branchenspezifisch

Liste	Potenzielles Ereignis	Verletzte Schutzziele	Mögliche Folgen
N	Aufgrund der Vielzahl an externen involvierten Stakeholdern kommt es zu Unklarheiten, Missverständnissen und Zweifelsfällen gegenüber welchen Personen bzw. Institutionen welche Informationen beauskunftet oder übermittelt werden dürfen. Im Arbeitsalltag kann dadurch eine Offenlegung von	Vertraulichkeit.	Bloßstellung, Diskriminierung, Rufschädigung und sonstige erhebliche gesellschaftliche Nachteile.

	Daten gegenüber unbefugten Dritten erfolgen.		
O	Im Zuge der Erbringung von Leistungen in einer Gruppe (z.B. Schulung, Workshop oder Ausübung von Beschäftigungen beim Mitglied als geförderte Maßnahme) werden bewusst oder unbewusst Informationen von AdressatInnen gegenüber unbefugten Personen (insbesondere anderen teilnehmenden AdressatInnen) offengelegt.	Vertraulichkeit.	Bloßstellung, Diskriminierung, Rufschädigung und sonstige erhebliche gesellschaftliche Nachteile.
P	Informationen werden bewusst oder aufgrund eines Versehens in den von den Fördergebern zur Verfügung gestellten Applikationen nicht oder nicht vollständig erfasst und dokumentiert. Dadurch sind notwendige Informationen für den Auftragsverarbeiter und den Verantwortlichen in der weiteren Betreuung nicht mehr verfügbar. Können dann z.B. durchgeführte Maßnahmen nicht mehr nachgewiesen werden (etwa die Teilnahme einer AdressatIn an einer internen Fortbildung) könnte dies eine Kürzung oder Streichung von Förderungen bewirken.	Verfügbarkeit, Transparenz und Intervenierbarkeit.	Finanzieller Verlust und sonstige erhebliche gesellschaftliche Nachteile.
Q	Die interne Rechtevergabe für die Verwendung der von den Fördergebern zur Verfügung gestellten Applikationen erfolgt in Einzelfällen nicht nach dem „Need-to-know“-Prinzip oder wird nicht laufend auf ihre Aktualität hin überprüft. So können MitarbeiterInnen Einsicht in Projekte mit AdressatInnen haben, für die sie nicht zuständig sind oder es wird nach dem internen Wechsel des	Nichtverkettbarkeit, Transparenz, Intervenierbarkeit	Betroffene Person wird um ihre Rechte und Freiheiten gebracht und daran gehindert, die sie betreffenden personenbezogenen Daten zu kontrollieren, sonstige erhebliche

	Aufgabenbereichs einer MitarbeiterIn die Rechteverwaltung nicht angepasst. Dadurch kann eine Offenlegung von Daten gegenüber unbefugten Personen erfolgen.		gesellschaftlichen Nachteile
R	Die Stellung besonders schutzbedürftiger Personen (z.B. Jugendliche, Menschen mit Behinderungen, MigrantInnen oder AdressatInnen, die im Zuge eines Beschäftigungsprojektes als ArbeitnehmerInnen angestellt werden) wird von Mitgliedern im Zuge der Aufgabenerfüllung ausgenützt, etwa um eine Einwilligung für eigene Verarbeitungszwecke zu erlangen (z.B. Fotoverwendung für Marketingzwecke) oder die Geltendmachung von Rechten zu erschweren.	Verfügbarkeit, Nichtverkettbarkeit, Transparenz, Intervenierbarkeit.	Bloßstellung, Diskriminierung, Rufschädigung und sonstige erhebliche gesellschaftliche Nachteile.

5.6. Risikobewertung

Nach anerkannten Bewertungsmethoden[13] können die Eintrittswahrscheinlichkeit und die Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen anhand von vier Stufen klassifiziert werden:

- „Vernachlässigbar“ (Stufe 1)
- „Begrenzt“ (Stufe 2)
- „Wesentlich“ (Stufe 3)
- „Maximal“ (Stufe 4)

Die nachfolgende Musterbewertung von Risiken soll eine Orientierungshilfe bieten. Unabhängig davon haben Mitglieder im Einzelfall zu prüfen, ob spezifische und individuelle

[13] Vgl. z.B. die Ausführungen des Bayrischen Landesamtes für Datenschutzaufsicht zu einer auf der ISO/IEC 29134 basierenden Risikoanalyse im Rahmen einer Datenschutz-Folgenabschätzung (https://www.lda.bayern.de/media/04_dsfa_praesentation_baylda_iso29134.pdf), die der gegenständlichen Risikoanalyse zu Grunde gelegt werden.

Rahmenbedingungen vorliegen, die Einfluss auf die Risikobewertung nehmen, und diese gegebenenfalls zu berücksichtigen.

5.6.1. Eintrittswahrscheinlichkeit

Die oben beschriebenen potenziellen Ereignisse A bis C, K bis M und R können hinsichtlich ihrer Eintrittswahrscheinlichkeit als „Begrenzt“ angesehen werden, weil sie eine erhebliche kriminelle Energie voraussetzen (z.B. Cyber-Crime-Attacke), nach allgemeinen Erfahrungswerten selten auftreten (z.B. Naturgewalt), ein vertragswidriges Verhalten erfordern (z.B. Verfehlung einer beigezogenen DienstleisterIn) oder ein vorsätzliches Handeln des potenziellen Schädigers bedingen (z.B. Einbruchsdiebstahl, persönliche Vorteilsnahme, unbefugte Profilbildung).

Die oben beschriebenen potenziellen Ereignisse D bis J und N bis Q hingegen können im Arbeitsalltag von Mitgliedern unter Bedachtnahme auf die oben festgestellte umfangreiche Datenverarbeitung grundsätzlich jederzeit eintreten und müssen daher als „Wesentlich“ eingestuft werden.

5.6.2. Schwere des Schadens

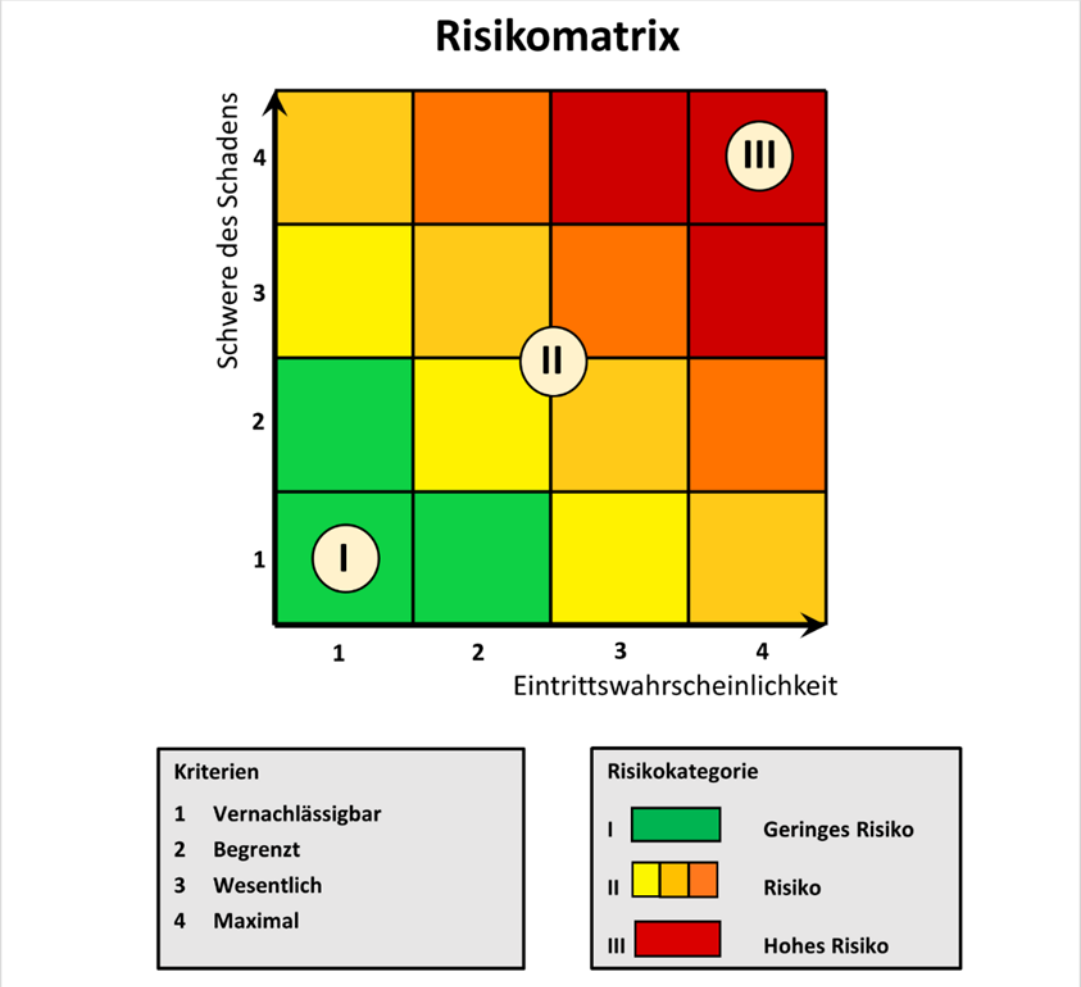
Die oben aufgezeigten Lebenssachverhalte können in völlig unterschiedlichen Ausprägungen auftreten. So kann z.B. der Mitarbeiter eines Mitglieds, der sich auf dem Weg zu einem Vernetzungstreffen in einem öffentlichen Verkehrsmittel befindet, seine Tasche verlieren, in der sich auch ein Firmenhandy mit personenbezogene Daten von AdressatInnen befinden. Der Finder des Firmenhandys hat zahlreiche Möglichkeiten damit umzugehen. Er könnte es bei nächster Gelegenheit im Müll entsorgen, in einen Briefkasten einwerfen oder beim Fundamt abgeben. Er könnte aus Neugierde versuchen, in das Handy einzusteigen, um Rückschlüsse auf den Besitzer und darin gespeicherte Daten zu ziehen. In diesem Fall könnte er das Handy entweder, weil die Daten für ihn nutzlos sind, auf seine Werkeinstellungen zurücksetzen und für private Zwecke weiterverwenden, veräußern oder verschenken. Er könnte aber z.B. auch in krimineller Absicht Erpressungs- oder Betrugshandlungen versuchen. Abhängig von der konkreten Ausprägung des Sachverhalts kann auch die Schwere des Schadens divergieren. Sollte das Handy im Müll entsorgt und niemals mehr in Betrieb genommen werden, kann die Schwere des Schadens für die betroffenen Personen vernachlässigbar sein. Sollten hingegen böswillige oder kriminelle Handlungen unternommen werden, kann aus Sicht der Betroffenen – abhängig von den betroffenen Datenkategorien – ein maximaler Schaden eintreten.

Alle diese Varianten können in einer Risikoanalyse nicht vollumfänglich dargestellt werden. Da der Verarbeitung besonderer Kategorien personenbezogener Daten (insbesondere von Gesundheitsdaten) im Rahmen der Auftragserfüllung gegenüber dem AMS und dem SMS eine zentrale Bedeutung zukommt und die höchstgerichtliche Judikatur bei Datenschutzvorfällen im Zusammenhang mit Gesundheitsdaten bereits Schadenersatzansprüche aufgrund von erlittenen gesellschaftlichen Nachteilen bestätigt hat, werden sämtliche der oben beschriebenen potenziellen Ereignisse A bis R hinsichtlich ihrer möglichen Auswirkungen auf die Rechte und Freiheiten der betroffenen AdressatInnen im Zweifel immer als „Maximal“ eingestuft.

5.6.3. Bestimmung der Risikokategorie

In der Risikobestimmung werden die quantitativen und die qualitativen Bewertungsstufen in einer Risikomatrix zu folgenden drei Risikokategorien zusammengeführt:[14]

- „Geringes Risiko“ (Risikokategorie 1)
- „Risiko“ (Risikokategorie 2)
- „Hohes Risiko“ (Risikokategorie 3)



In der Gesamtbeurteilung führt dies in Bezug auf die oben beschriebenen potenziellen Datenschutzvorfälle zu folgender Risikobestimmung:

[14] Vgl. Rz. 13 und die „Muster-Datenschutz-Folgenabschätzung“ des Vereins privacy officers (https://privacyofficers.at/checklisten-arbeitsunterlagen/#acc-bkod241-0).

Liste	Potenzielles Ereignis	Eintrittswahr-scheinlichkeit	Schwere des Schadens	Risikokategorie
A	Unbefugte Personen dringen in Netzwerke und Systeme ein (Cyber-Crime und Malware-Attacken).	Begrenzt	Maximal	II Orange (Risiko)
B	Durch Naturgewalten oder unvorhersehbare Schadens-ereignisse werden Daten zerstört, gelöscht oder können nicht mehr wieder-hergestellt werden.	Begrenzt	Maximal	II Orange (Risiko)
C	Unbefugte Personen verschaffen sich Zutritt zu Räumlichkeiten, Verarbeitungsanlagen oder Datenaufbewahrungsorten.	Begrenzt	Maximal	II Orange (Risiko)
D	Anwesende Personen haben unbefugten Zugang zu vertraulichen Dokumenten in Papierform, die z.B. in Büros, in Besprechungszimmern oder an Arbeitsplätzen aufliegen.	Wesentlich	Maximal	III Rot (Hohes Risiko)
E	Anwesende Personen sehen unbefugt Bildschirme ein.	Wesentlich	Maximal	III Rot (Hohes Risiko)
F	Anwesende Personen hören unbefugt vertrauliche Gespräche oder Telefonate mit.	Wesentlich	Maximal	III Rot (Hohes Risiko)

G	Vertrauliche Dokumente und Informationen gehen verloren (z.B. Verlust von mobilen Datenträgern oder Dokumenten in Papierform im Außendienst oder im Homeoffice).	Wesentlich	Maximal	III Rot (Hohes Risiko)
H	Vertrauliche Informationen werden von MitarbeiterInnen unbewusst gegenüber unbefugten Personen beauskunftet oder offengelegt.	Wesentlich	Maximal	III Rot (Hohes Risiko)
I	Vertrauliche Informationen werden von MitarbeiterInnen bewusst oder unbewusst gegenüber unbefugten Personen im Privatleben offengelegt.	Wesentlich	Maximal	III Rot (Hohes Risiko)
J	Vertrauliche Informationen werden von MitarbeiterInnen im Homeoffice unbewusst gegenüber unbefugten Personen offengelegt.	Wesentlich	Maximal	III Rot (Hohes Risiko)
K	(Ehemalige) MitarbeiterInnen oder AdressatInnen verschaffen sich zum Zweck der persönlichen Vorteilsnahme unbefugt vertrauliche Informationen über betroffene Personen.	Begrenzt	Maximal	II Orange (Risiko)
L	Zulässigerweise verarbeitete personenbezogene Daten werden für unbefugte Zwecke, wie z.B.	Begrenzt	Maximal	II Orange (Risiko)

	Profilbildung, weiterverwendet.			
M	Beigezogene Dienstleister gehen nicht ordnungsgemäß mit personenbezogenen Daten um, die ihnen zur Auftragserfüllung über-lassen wurden bzw. auf die sie zu diesem Zweck zugreifen können.	Begrenzt	Maximal	II Orange (Risiko)
N	Aufgrund der Vielzahl an externen involvierten Stakeholdern kommt es zu Unklarheiten, Missverständnissen und Zweifelsfällen gegenüber welchen Personen bzw. Institutionen welche Informationen beauskunftet oder übermittelt werden dürfen. Im Arbeitsalltag kann dadurch eine Offenlegung von Daten gegenüber unbefugten Dritten erfolgen.	Wesentlich	Maximal	III Rot (Hohes Risiko)
O	Im Zuge der Erbringung von Leistungen in einer Gruppe (z.B. Schulung, Workshop oder Ausübung von Beschäftigungen beim Mitglied als geförderte Maßnahme) werden bewusst oder unbewusst Informationen von AdressatInnen gegenüber unbefugten Personen (insbesondere anderen teilnehmenden AdressatInnen) offengelegt..	Wesentlich	Maximal	III Rot (Hohes Risiko)

P	Informationen werden bewusst oder aufgrund eines Versehens in den von den Fördergebern zur Verfügung gestellten Applikationen nicht oder nicht vollständig erfasst und dokumentiert. Dadurch sind notwendige Informationen im weiteren Betreuungsverlauf nicht mehr verfügbar. Können dann z.B. durchgeführte Maßnahmen nicht mehr nachgewiesen werden (etwa die Teilnahme einer AdressatIn an einer internen Fortbildung) könnte dies eine Kürzung oder Streichung von Förderungen bewirken.	Wesentlich	Maximal	III Rot (Hohes Risiko)
Q	Die interne Rechtevergabe für die Verwendung der von den Fördergebern zur Verfügung gestellten Applikationen erfolgt in Einzelfällen nicht nach dem „Need-to-know“-Prinzip oder wird nicht laufend auf ihre Aktualität hin überprüft. So können MitarbeiterInnen Einsicht in Projekte mit AdressatInnen haben, für die sie nicht zuständig sind oder es wirdnach dem internen Wechsel des Aufgabenbereichs einer MitarbeiterIn die Rechteverwaltung nicht angepasst. Dadurch kann eine Offenlegung von Daten	Wesentlich	Maximal	III Rot (Hohes Risiko)

	gegenüber unbefugten Personen erfolgen.			
R	Die Stellung besonders schutzbedürftiger Personen (z.B. Jugendliche, Menschen mit Behinderungen, MigrantInnen oder AdressatInnen, die im Zuge eines Beschäftigungsprojektes als ArbeitnehmerInnen angestellt werden) wird von Mitgliedern im Zuge der Aufgabenerfüllung dazu ausgenützt, um z.B. eine Einwilligung für eigene Verarbeitungszwecke zu erlangen (etwa Fotoverwendungen für Marketingzwecke) oder die Geltendmachung von Rechten zu erschweren.	Begrenzt	Maximal	II Orange (Risiko)

5.7. Individuelle Risikobewertung

In der oben durchgeführten Risikobewertung wurden potenzielle Ereignisse berücksichtigt, die sowohl branchenunabhängig als auch branchenspezifisch typischerweise auftreten können. Da im Rahmen dieser Verhaltensregeln aber keine Risiken berücksichtigt werden können, die aufgrund von spezifischen und individuellen Rahmenbedingungen einzelner Mitglieder zusätzlich auftreten können (etwa im Zusammenhang mit bau- oder miertvertragsrechtlichen Besonderheiten eines bestimmten Standortes, einer betreuten Personengruppe oder einer bestimmten Leistungserbringung), haben Mitglieder immer auch zu prüfen, ob und gegebenenfalls noch welche anderen spezifischen Risiken für sie bestehen („mitgliederspezifische Risiken“).

Bei Vorliegen solcher mitgliederspezifischer Risiken, kann die obige Risikobewertung als Orientierungshilfe herangezogen werden.

6. Geeignete technische und organisatorische Maßnahmen

Von den Mitgliedern werden die im Folgenden beschriebenen technischen und organisatorischen Maßnahmen getroffen, die ein der oben dargestellten Risikobewertung angemessenes Schutzniveau gemäß Art. 32 Abs. 1 DSGVO gewährleisten.

6.1. Zutrittskontrolle

Für den Fall, dass Mitglieder an einem bestimmten Standort im Rahmen ihrer Auftragserfüllung gegenüber dem AMS und dem SMS personenbezogene Daten elektronisch oder in manueller Form (z.B. Papierakten) verarbeiten, werden von ihnen folgende technische und organisatorische Maßnahmen getroffen, die verhindern, dass unbefugte Personen Zutritt zu Datenverarbeitungssystemen, Datenverarbeitungsanlagen und Datenaufbewahrungsorten haben (Gebäude- und Raumsicherung):

1. Zugänge werden insbesondere durch eine der folgenden alternativen Maßnahmen geschützt: [15]

   - Elektronisches Zutrittssystem, z.B. in Form von Identifikationsmerkmalträgern, wobei die Berechtigungen (Festlegung welche MitarbeiterInnen Zutritt zu welchen Räumlichkeiten haben) protokolliert und verwaltet werden.

   - Mechanisches Schließsystem, wobei die Berechtigungen (Festlegung welche MitarbeiterInnen Zutritt zu welchen Räumlichkeiten haben) protokolliert und verwaltet werden.

   - Einsatz von Sicherheitsschlüsseln, die ohne Genehmigung des Verfügungsberechtigten nicht dupliziert werden können, wobei die Berechtigungen (Festlegung welche MitarbeiterInnen Zutritt zu welchen Räumlichkeiten haben) protokolliert und verwaltet werden.

2. Die Zuteilung und Ausgabe von Identifikationsmerkmalträgern / Schlüsseln wird protokolliert und verwaltet.

3. Schlüssel / Identifikationsmerkmalträger, die in Räumlichkeiten der Mitglieder verbleiben (insbesondere nach Dienstende), werden sicher verwahrt.

4. Schlüssel / Identifikationsmerkmalträger werden nur dann an trägerfremde Personen (z.B. an DienstleisterInnen, HandwerkerInnen) ausgefolgt, wenn und solange dies zur Aufgabenerledigung unbedingt erforderlich ist. Entsprechende Ausfolgungen werden protokolliert und verwaltet.

5. Büroräumlichkeiten sind bei Abwesenheit von MitarbeiterInnen grundsätzlich zu versperren. Ist dies nicht möglich, sind Aktenschränke und andere Aufbewahrungsorte für personenbezogene Daten in Papierform ausreichend vor unbefugten Zugriffen zu sichern.

[15] Diese Maßnahmen setzen grundsätzlich voraus, dass Mitglieder eine entsprechende zivilrechtliche Verfügungsmacht bzw. Gestaltungsmöglichkeit in Bezug auf die von ihnen genutzte Liegenschaft haben. Liegt eine solche Verfügungsmacht bzw. Gestaltungsmöglichkeit nicht vor, ist der Entscheidungsbefugte (in der Regel der Vermieter) nachweislich über die Notwendigkeit solcher Maßnahmen in Kenntnis zu setzen. Können entsprechende Maßnahmen auch nach erfolgter Informierung des Entscheidungsbefugten nicht getroffen werden, führen Mitglieder eine Verhältnismäßigkeitsprüfung in Bezug auf den Wechsel betroffener Standorte durch (z.B. durch Kündigung von Mietverhältnissen und Verlagerung der Auftragsverarbeitung in geeignetere Objekte).

Insbesondere gilt dies dann, wenn darin besondere Kategorien personenbezogener Daten in Papierform aufbewahrt werden.

6. Für den Fall des Verlustes von Identifikationsmerkmalträgern / Schlüsseln sind MitarbeiterInnen angewiesen, einen intern verbindlich zu regelnden Informationsfluss einzuhalten, der sicherstellt, dass der/die IT-Verantwortliche(n) und der/die Datenschutzverantwortliche(n) ohne Aufschub über den Verlust informiert werden.

7. Serveranlagen werden insbesondere durch eine der folgenden alternativen Maßnahmen geschützt:

   - Schutzmaßnahmen für im Haus befindliche Serveranlagen (z.B. Sicherheitstüre, zusätzliche Schließvorrichtung, Serverreck, Alarmanlage, Videoüberwachung, 2-Faktor-Authentifizierung oder sonstige geeignete Zugangsbeschränkungen).

   - Auslagerung an geeignete DienstleisterInnen (z.B. Rechenzentrum) mit denen ein Vertrag über die Auftragsverarbeitung nach Art. 28 DSGVO abgeschlossen wird.

8. Dritte Personen dürfen sich grundsätzlich nicht unbegleitet/ungeregelt in Räumlichkeiten von Mitgliedern bewegen, in denen regelmäßig personenbezogene Daten verarbeitet werden (z.B. Anmeldung beim Empfang und Abholung durch zuständige MitarbeiterInnen).

9. MitarbeiterInnen im Homeoffice, die personenbezogene Daten außerhalb der Betriebsräumlichkeiten der Mitglieder bearbeiten, sind (z.B. mittels Homeoffice-Vereinbarung oder arbeitsrechtlich verbindlichen Homeoffice-Richtlinien) angewiesen, ausreichende Datensicherheitsmaßnahmen einzuhalten (z.B. versperrte Aufbewahrung von mobilen IT-Geräten sowie Ordnern und Mappen und Führen von Telefonaten und Videotelefonkonferenzen in vertraulicher Umgebung).

10. MitarbeiterInnen sind zur Einhaltung der „Closed Door“-Policy angewiesen, sofern dies zur Wahrung der Vertraulichkeit von Gesprächen und zum Schutz vor unbefugten Zugriffen auf personenbezogene Daten erforderlich und möglich ist.

11. Mitglieder treffen sonstige geeignete (alternative oder zusätzliche) Maßnahmen, die eine wirksame Zutrittskontrolle gewährleisten.

6.2. Zugangskontrolle

Für den Fall, dass Mitglieder an einem bestimmten Standort im Rahmen ihrer Auftragserfüllung gegenüber dem AMS und dem SMS personenbezogene Daten elektronisch oder in manueller Form (z.B. Papierakten) verarbeiten, werden von ihnen folgende technische und organisatorische Maßnahmen getroffen, die verhindern, dass unbefugte Personen Zugang zu Datenverarbeitungsanlagen und Datenaufbewahrungsorten von Mitgliedern haben (Schutz vor unbefugter Nutzung):

12. Einrichtung von Desktop- bzw. Bildschirmsperren durch eine der folgenden alternativen Maßnahmen:

    - Automatische Desktopsperren nach Ablauf bestimmter Zeitabstände.

    - MitarbeiterInnen sind zur Einhaltung der „Clear Screen"-Policy angewiesen, nach der beim vorübergehenden Verlassen von Desktop-Computern (z.B. Rauchpause, Teambesprechung) oder der vorübergehenden Nichtverwendung von Laptops/Notebooks die Desktopsperre manuell (z.B. durch die Tastenkombination „Windows + L") herbeizuführen ist.

13. Bei Smartphones und Tablets, die zur Erfüllung beruflicher Aufgaben eingesetzt werden, ist die passwort- oder kennzahlgesicherte Displaysperre in möglichst kurzen Zeitintervallen sicherzustellen.

14. Die Passwortsicherheit wird durch eine intern verbindliche Passwortrichtlinie gewährleistet.

15. Die Passwortverwaltung von privilegierten oder administrativen Benutzerkonten erfolgt zentralisiert und entspricht erhöhten Sicherheitsanforderungen.

16. MitarbeiterInnen sind zur Einhaltung der „Clear Desk"-Policy angewiesen (Ordner, Mappen, Notizbücher, etc. dürfen nicht offen herumliegen und sind bei Verlassen des Arbeitsplatzes sicher aufzubewahren). Insbesondere gilt dies dann, wenn darin besondere Kategorien personenbezogener Daten in Papierform verarbeitet werden.

17. MitarbeiterInnen sind angewiesen, bei Außendiensten Dokumente, Ordner, Mappen, Notizbücher und Kalenderbücher sowie mobile IT-Geräte sicher zu verwahren und zu transportieren.

18. Bildschirme in Räumlichkeiten, die für Dritte zugänglich sind, sind blickdicht aufgestellt bzw. ausgerichtet.

19. MitarbeiterInnen sind angewiesen, persönliche Gespräche oder Telefonate mit AdressatInnen oder sonstigen involvierten Personen so zu führen, dass die Vertraulichkeit gewahrt wird.

20. Unter Berücksichtigung der Auswahlkriterien gemäß Art. 32 Abs. 1 DSGVO werden geeignete technische Abwehrmaßnahmen gegen Schadprogramme und -funktionen getroffen. Diese sind insbesondere[16]:

    - Einsatz einer geeigneten Firewall, die Datenpakete nur nach vordefinierten Regeln zulässt, sodass z.B. Dateitypen (wie insbesondere *.vbs, *.wsh, *.bat, *.exe), die im täglichen Arbeitsablauf nicht vorkommen, zentral blockiert werden.

[16] Vgl. Österreichisches Informationssicherheitshandbuch Version 4.3.1. vom 2.2.2022, S. 365 ff.

- Einsatz eines aktuellen Anti-Viren/-Trojaner/-Malware-Schutzprogramms mit aktuellen Signaturdateien, das im Hintergrund läuft und bei bekannter Schadsoftware Alarm schlägt.

- Aktivierung des Makrovirenschutzes von Anwendungsprogrammen (z.B. bei MS Office Anwendungen).

- Auswahl entsprechender Einstellungsoptionen in E-Mail-Programmen, sodass die Ausführung von aktiven Inhalten unterbunden wird.

- Scan von eingehenden E-Mails auf Schadsoftware.

- Im Fall der Auslagerung werden geeignete DienstleisterInnen herangezogen, mit denen ein Vertrag über die Auftragsverarbeitung nach Art. 28 DSGVO abgeschlossen wird.

21. Für alle MitarbeiterInnen, die EDV-mäßig personenbezogene Daten verarbeiten, wird ein Benutzerkonto eingerichtet (Benutzerstammsatz).

22. MitarbeiterInnen müssen sich beim Zugang zu Verarbeitungsanlagen mittels Benutzerkennung und Passwort identifizieren (keine Gruppenkennungen).

23. Sicherheitsupdates werden durch eine der folgenden alternativen Maßnahmen gewährleistet:

    - Automatische Durchführung.

    - Verpflichtende manuelle Durchführung.

24. Mobile Datenträger (z.B. Festplatten von Laptops/Notebooks, USB-Sticks), die für berufliche Zwecke eingesetzt werden, sind verschlüsselt.

25. Homeoffice Zugriffe erfolgen über eine sichere Verbindung (z.B. VPN).

26. Die Sicherheit von mobilen IT-Geräten wird durch eine der folgenden alternativen Maßnahmen sichergestellt:

    - Einsatz eines zentralisierten System zur Verwaltung (Mobile-Device-Management).

    - Einsatz eines Sicherheitsdienstes zum Löschen oder Sperren von Smartphones aus der Distanz (Fernzugriff).

    - MitarbeiterInnen sind zur Einhaltung einer intern verbindlichen Richtlinie zur Nutzung mobiler IT-Geräte angewiesen.

27. Der Austausch (Entsorgung) und die Reparatur von IT-Geräten erfolgt durch befugte MitarbeiterInnen oder durch externe Fachkräfte, mit denen ein Vertrag über die Auftragsverarbeitung nach Art. 28 DSGVO abgeschlossen wird.

28. Geräte, die auszutauschen oder zu reparieren sind, werden so gelagert, dass sie vor dem Zugriff unbefugter Personen geschützt sind.

29. Für den Fall des Diebstahls (Verlustes) eines IT-Gerätes sind MitarbeiterInnen angewiesen, einen intern verbindlich zu regelnden Informationsfluss einzuhalten, der sicherstellt, dass der/die IT-Verantwortliche und der/die Datenschutzbeauftragte ohne Aufschub über den Diebstahl (Verlust) informiert werden.

30. Mitglieder treffen sonstige geeignete (alternative oder zusätzliche) Maßnahmen, die eine wirksame Zugangskontrolle gewährleisten.

6.3. Zugriffskontrolle

Für den Fall, dass Mitglieder an einem bestimmten Standort im Rahmen ihrer Auftragserfüllung gegenüber dem AMS und dem SMS personenbezogene Daten elektronisch oder in manueller Form (z.B. Papierakten) verarbeiten, werden von ihnen folgende technische und organisatorische Maßnahmen getroffen, die sicherstellen, dass Personen nur dann auf Daten von AdressatInnen zugreifen können, sofern und soweit sie hierzu berechtigt sind (Schutz vor unbefugter Verarbeitung):

31. Zugriffsberechtigungen für MitarbeiterInnen auf die vom AMS und SMS zur Verfügung gestellten Applikationen werden ausschließlich nach den schriftlichen Vorgaben des AMS und des SMS vergeben. Liegen keine solchen Vorgaben vor oder werden Daten außerhalb der vom AMS und SMS zur Verfügung gestellten Applikationen verarbeitet, dürfen Zugriffsberechtigungen nur nach dem „Need-to-know"-Prinzip (rollenbasierte Benutzerverwaltung) vergeben werden. Auch Zugriffsberechtigungen auf Daten von AdressatInnen, die über eigene Applikationen von Mitgliedern erfolgen, dürfen nur nach dem „Need-to-know"-Prinzip vergeben werden.

32. Postfächer und Faxablagefächer sind für unbefugte Personen nicht frei zugänglich.

33. MitarbeiterInnen sind angewiesen, gesetzliche oder vertraglich verpflichtende Aufbewahrungsfristen bzw. Fristen zur Vernichtung manueller Daten einzuhalten und diese auf sichere Weise zu vernichten. Zu diesem Zweck sind für MitarbeiterInnen verbindliche Handlungsanleitungen vorzusehen, deren Einhaltung regelmäßig, zumindest stichprobenweise, zu kontrollieren ist.

34. Zur Vernichtung besonderer Kategorien personenbezogener Daten in manueller Form werden Aktenvernichter der Sicherheitsstufe „P-4" nach „DIN 66399"[17] oder höher eingesetzt. Werden manuelle Daten an externe DienstleisterInnen zur ordnungsgemäßen Vernichtung übergeben, wird mit diesen ein Vertrag über die Auftragsverarbeitung nach Art. 28 DSGVO abgeschlossen.

[17] In den gegenständlichen Verhaltensregeln wird auf den deutschen Standard „DIN 66399" Bezug genommen, da dieser in den internationalen Standard ISO/IEC 21964 überführt wurde.

35. Mit externen DienstleisterInnen, die Zugang zu personenbezogenen Daten des Mitgliedes haben, wird ein Vertrag über die Auftragsverarbeitung nach Art. 28 DSGVO abgeschlossen. Sind vom Zugriff besondere Kategorien personenbezogener Daten betroffen (z.B. Betreuungsverläufe), wird dies im Vertrag gesondert angeführt.

36. Durch interne verbindliche Regelungen zur Berechtigungsverwaltung wird sichergestellt, dass bei Abwesenheit (z.B. Urlaub oder Karenz) und beim Ausscheiden von MitarbeiterInnen keine unbefugten Zugriffe erfolgen, die nicht dem „Need-to-know"-Prinzip entsprechen.

37. Mitglieder treffen sonstige geeignete (alternative oder zusätzliche) Maßnahmen, die eine wirksame Zugriffskontrolle gewährleisten. So kann unter Berücksichtigung möglicher Vorfälle, die branchenspezifisch auftreten können (vgl. etwa das oben beschriebene potenzielle Ereignis Q), z.B. folgende Maßnahme geeignet sein:

    - Erlassung verbindlicher Richtlinien für Führungskräfte für die Vergabe und Entziehung von Lese- und Schreibberechtigungen für die von den Fördergebern zur Aufgabenerfüllung zur Verfügung gestellten Applikationen (Rechtevergabe und -verwaltung nach dem „Need-to-know"-Prinzip).

6.4. Weitergabekontrolle

Für den Fall, dass Mitglieder an einem bestimmten Standort im Rahmen ihrer Auftragserfüllung gegenüber dem AMS und dem SMS personenbezogene Daten elektronisch oder in manueller Form (z.B. Papierakten) verarbeiten, werden von ihnen folgende Maßnahmen getroffen, die sicherstellen, dass personenbezogene Daten sicher weitergegeben werden (Übermittlungsschutz):

38. MitarbeiterInnen sind angewiesen, in E-Mails nur dann einen Personenbezug herzustellen, wenn dies zur Aufgabenerfüllung im Einzelfall jeweils erforderlich ist.

39. Besondere Kategorien personenbezogener Daten von AdressatInnen (z.B. in Form von Befunden, Gutachten oder Bewerbungen mit ausdrücklichen Hinweisen auf den Gesundheitszustand) werden ausschließlich nach den Vorgaben der Verantwortlichen AMS und SMS an Dritte übermittelt. Liegen keine solchen Vorgaben vor, wird die Sicherheit der Übermittlung von besonderen Kategorien personenbezogener Daten insbesondere durch eine der folgenden alternativen Maßnahmen bzw. gegebenenfalls durch eine Kombination solcher Maßnahmen sichergestellt:

    - Erzwungene Transportverschlüsselung (Forced TLS - Transport Layer Security).

    - E-Mail-Verschlüsselung (Verschlüsselungsprotokoll S/MIME oder [Open]PGP).

    - Verschlüsselter Cloud-Dienst (Bereitstellung und Abholung von Dokumenten).

    - Sonstige sichere elektronische Übertragungsarten.

- Übermittlung im Postweg per Einschreiben.

40. Postsendungen werden ordnungsgemäß verschlossen. In Sichtfenstern von Postsendungen werden keine Informationen ersichtlich gemacht, die für die AdressatIn nicht unbedingt erforderlich sind (z.B. Sozialversicherungsnummer).

41. MitarbeiterInnen sind angewiesen, Dokumente, Ordner, Mappen, Notizbücher und mobile IT-Geräte während des Transports in öffentlichen Verkehrsmitteln und auf Fußwegen sicher zu verwahren und nicht unbeaufsichtigt zu lassen.

42. Mitglieder treffen sonstige geeignete (alternative oder zusätzliche) Maßnahmen, die eine wirksame Weitergabekontrolle gewährleisten. So können unter Berücksichtigung möglicher Vorfälle, die branchenspezifisch auftreten können (vgl. etwa die oben beschriebenen potenziellen Ereignisse N und O), z.B. folgende Maßnahmen geeignet sein:

    - Identifikation und Führung einer aktuellen Liste von möglichen System- und KooperationspartnerInnen im Arbeitsalltag, insbesondere zur Orientierung für MitarbeiterInnen ohne Berufserfahrung.

    - Berücksichtigung unterschiedlichster Fallkonstellationen für Datenübermittlungen sowie System- und KooperationspartnerInnen bei der Einschulung von MitarbeiterInnen.

    - Festlegung verpflichteter Workflows in Bezug auf (un-)typische, unklare oder zweifelhafte Datenübermittlungen, wie z.B. Rücksprache mit Vorgesetzten und/oder dem/der Datenschutzbeauftragten.

6.5. Eingabekontrolle

Für den Fall, dass Mitglieder an einem bestimmten Standort im Rahmen ihrer Auftragserfüllung gegenüber dem AMS und dem SMS personenbezogene Daten elektronisch und außerhalb der vom AMS und SMS zur Verfügung gestellten Applikationen verarbeiten, werden von ihnen folgende Maßnahmen getroffen, die sicherstellen, dass Verarbeitungsvorgänge ausreichend dokumentiert werden (Protokollierung von Zugriffen):

43. Elektronische Verarbeitungsvorgänge werden protokolliert, um zur Aufklärung eines Datenschutzvorfalls (z.B. infolge einer unbefugten Datenlöschung oder Datenveränderung) die erforderlichen Feststellungen treffen zu können.

44. Über die Rechteverwaltung (rollenbasierte Benutzerverwaltung) wird sichergestellt, dass nur befugte MitarbeiterInnen besondere Kategorien personenbezogener Daten löschen oder übermitteln können. Löschungen erfolgen ausschließlich nach den schriftlichen Vorgaben des AMS und des SMS.

45. Mitglieder treffen sonstige geeignete (alternative oder zusätzliche) Maßnahmen, die eine wirksame Eingabekontrolle gewährleisten. Unter Berücksichtigung auf mögliche Vorfälle,

die branchenspezifisch auftreten können (insbesondere Ereignis P), sind z.B. folgende Maßnahmen möglich:.

Verbindliche Richtlinien für den Umgang mit den von den Fördergebern zur Aufgabenerfüllung zur Verfügung gestellten Applikationen und Einschulung neu eintretender MitarbeiterInnen.

6.6. Verfügbarkeitskontrolle

Für den Fall, dass Mitglieder an einem bestimmten Standort im Rahmen ihrer Auftragserfüllung gegenüber dem AMS und dem SMS personenbezogene Daten außerhalb der vom AMS und vom SMS zur Verfügung gestellten eigenen Applikationen elektronisch oder in manueller Form (z.B. Papierakten) verarbeiten, werden von ihnen folgende Maßnahmen getroffen, die sicherstellen, dass personenbezogene Daten vor Beschädigung, Zerstörung oder Verlust geschützt werden, Systeme wiederhergestellt und auftretende Fehlfunktionen gemeldet werden (Integrität, Zuverlässigkeit und Wiederherstellung):

46. Der Brandschutz wird insbesondere durch eine der folgenden alternativen Maßnahmen bzw. gegebenenfalls durch eine Kombination solcher Maßnahmen sichergestellt:

    - Einsatz von Rauch- oder Brandmeldern.
    - Einsatz von Sprinkleranlagen.
    - Bereitstellung einer ausreichenden Anzahl an Feuerlöschern und Löschdecken.

47. Räumlichkeiten, die der Unterbringung von Servern dienen, werden durch geeignete Maßnahmen in Bezug auf Temperatur und Feuchtigkeit überwacht und vor unbefugtem Zutritt und Zugriff geschützt.

48. Es werden Maßnahmen für eine unterbrechungsfreie Stromversorgung ergriffen.

49. Es werden ausreichende Maßnahmen zur Daten- und Systemsicherung getroffen (Backup-Systeme, Recovery-Systeme und Archivierungs-Systeme). Im Fall der Auslagerung werden geeignete DienstleisterInnen herangezogen, mit denen ein Vertrag über die Auftragsverarbeitung nach Art. 28 DSGVO abgeschlossen wird.

50. Es liegen Konzepte für die Datenarchivierung, die Datensicherheit und die Datenwiederherstellung vor. Für den Fall des Eintretens von Notfallsituationen wird sichergestellt, dass erforderliche Kontaktdaten (z.B. IT-Verantwortlicher und Datenschutzbeauftragter) jederzeit zur Verfügung stehen.

51. Sicherungsmedien werden auf sichere Weise, insbesondere verschlüsselt, aufbewahrt. Im Fall der Auslagerung werden geeignete DienstleisterInnen herangezogen, mit denen ein Vertrag über die Auftragsverarbeitung nach Art. 28 DSGVO abgeschlossen wird.

52. Mitglieder treffen sonstige geeignete (alternative oder zusätzliche) Maßnahmen, die eine wirksame Verfügbarkeitskontrolle gewährleisten.

6.7. Trennungskontrolle

Für den Fall, dass Mitglieder an einem bestimmten Standort im Rahmen ihrer Auftragserfüllung gegenüber dem AMS und dem SMS personenbezogene Daten elektronisch oder in manueller Form (z.B. Papierakten) verarbeiten, werden von ihnen folgende Maßnahmen getroffen, die sicherstellen, dass personenbezogene Daten von AdressatInnen getrennt bearbeitet werden können (Separierung von Geschäftsbereichen):

53. Unterschiedliche Verarbeitungszwecke (z.B. die Betreuung ein- und derselben AdressatIn für mehrere Auftraggeber) werden insbesondere durch eine der folgenden alternativen Maßnahmen sichergestellt:

    - Einsatz getrennter Systeme oder unterschiedlicher Datenträger.

    - Bei der Verwaltung der Zugriffsberechtigungen (rollenbasierte Benutzerverwaltung) werden unterschiedliche Verarbeitungszwecke berücksichtigt. Auch auf AdressatInnenebene (z.B. gleichzeitige Betreuung in mehreren voneinander unabhängigen Projekten) werden Zugriffsberechtigungen nur nach dem „Need-to-know"-Prinzip" vergeben.

54. Personenbezogene Daten in manueller Form werden getrennt voneinander verarbeitet, z.B. durch Verwendung von eigenen Ordnern für AdressatInnen und individuellen Personalordnern.

55. Personenbezogene Daten in manueller Form werden so archiviert, dass Löschfristen (Vernichtungsfristen) entsprochen werden kann.

56. Mitglieder treffen sonstige geeignete (alternative oder zusätzliche) Maßnahmen, die eine wirksame Trennungskontrolle gewährleisten.

6.8. Sonstige Maßnahmen

57. MitarbeiterInnen werden schriftlich auf das Datengeheimnis gemäß § 6 DSG verpflichtet. Externe Personen, denen Zugriff auf personenbezogene Daten ermöglicht wird (z.B. DolmetscherInnen, Zivildiener, PraktikantInnen, ehrenamtliche MitarbeiterInnen, beigezogenen TrainerInnen, Coaches) haben im Vorfeld eine Verschwiegenheitserklärung zu unterfertigen, die inhaltlich dem Datengeheimnis nach § 6 DSG entspricht, sofern diese externen Personen nicht bereits einer berufsrechtlichen Verschwiegenheitspflicht unterliegen, wie z.B. PsychologInnen nach dem Psychologengesetz 2013 und TherapeutInnen nach dem MTD-Gesetz.

58. Mitglieder richten ein standardisiertes und intern verbindliches Verfahren zur Sicherstellung ein, dass Rechte betroffener Personen rechtzeitig gewahrt und das AMS und das SMS bei der Geltendmachung von Rechten entsprechend unterstützt werden

können. Erfolgen vom AMS und dem SMS dazu schriftliche Vorgaben, werden diese eingehalten.

59. Mitglieder richten ein standardisiertes und intern verbindliches Verfahren zur Sicherstellung ein, dass das AMS und das SMS unverzüglich über Datenschutzvorfälle gemäß Art. 33 DSGVO informiert werden. Erfolgen vom AMS und dem SMS dazu schriftliche Vorgaben, werden diese eingehalten.

60. Mitglieder schließen mit DienstleisterInnen, die im Rahmen der Auftragserfüllung gegenüber dem AMS und dem SMS personenbezogene Daten verarbeiten, Verträge über die Auftragsverarbeitung gemäß Art. 28 DSGVO ab (z.B. betreffend der Webseite, Marketing- und EDV-Dienstleistungen).

61. Soweit MitarbeiterInnen private Geräte für berufliche Zwecke nutzen („Bring Your Own Device – BYOB"), sind diese angewiesen (insbesondere mittels BYOB-Vereinbarung), ausreichende Datensicherheitsmaßnahmen umzusetzen, z.B. die Verwendung eines aktuellen Betriebssystems sowie Anti-Viren/-Trojaner/-Malware-Schutzprogramms, eine Festplattenverschlüsselung oder eine Container-Lösung zur Trennung von privaten und beruflichen Daten. Mitglieder unterstützen ihre MitarbeiterInnen bei der Umsetzung geeigneter Maßnahmen.

62. Mitglieder richten ein Schulungssystem für MitarbeiterInnen ein, das jedenfalls folgende Inhalte aufweist und vorsieht, dass einmal jährlich Auffrischungen erfolgen:

    - Vertraulicher Umgang mit personenbezogenen Daten und insbesondere mit besonderen Kategorien personenbezogener Daten.

    - Erledigung von Aufgaben im Rahmen der Auftragserfüllung gegenüber dem AMS und dem SMS.

    - Beschreibung typischer Lebenssachverhalte im sozialen Dienstleistungsbereich, die zu Datenschutzvorfällen führen können (Sensibilisierung).

    - Grundlegende Datensicherheitsmaßnahmen im Arbeitsalltag (Closed Door, Clear Desk, Clear Screen, sichere Aufbewahrung von Ordnern, Mappen, Dokumenten, Umgang mit mobilen IT-Geräten).

    - Aufklärung über aktuelle Bedrohungslagen bei Cybercrime-Attacken, wie z.B. „Phishing"-Angriffe.

    - Verhaltensregeln im Umgang mit Datenschutzvorfällen und Rechten der Betroffenen.

6.9. Erreichung eines angemessenen Datenschutzniveaus

Mit den in den Punkten 6.1. bis 6.8. aufgezählten Maßnahmen werden neben allgemeinen Risiken, die in jedem Unternehmen auftreten können, auch branchenspezifische Risiken berücksichtigt. Die Maßnahmen wurden unter Bezugnahme von risikoerhöhenden Faktoren wie insbesondere die Verarbeitung von besonderen Kategorien personenbezogener Daten und sonstigen besonders vertraulichen Daten von besonders schützenswerten Personengruppen erstellt. Alle diese Faktoren führen dazu, dass die dargestellten, umfangreichen technischen und organisatorischen Maßnahmen notwendig sind, um dem besonderen Schutzbedürfnis im Zuge der Datenverarbeitung in der beruflichen und sozialen Integration Rechnung zu tragen, die Schutzziele zu erreichen und das vorhandene Risiko zu minimieren.

Mit der Umsetzung der oben aufgezählten und bei Bedarf von weiteren Maßnahmen, mit denen spezifische und individuelle Rahmenbedingungen berücksichtigt werden, können diese Ziele erreicht und ein angemessenes Datenschutzniveau gewährleistet werden.

Wie oben im Punkt 5.7. ausgeführt können im Rahmen dieser Verhaltensregeln keine Risiken berücksichtigt werden, die aufgrund von spezifischen Rahmenbedingungen einzelner Mitglieder zusätzlich auftreten können („mitgliederspezifische Risiken“). Mitglieder haben daher im Einzelfall zu prüfen, ob weitere Risiken bestehen und die in diesen Verhaltensregeln getroffenen Schutzmaßnahmen dafür ausreichen oder ob sonstige geeignete (alternative oder zusätzliche) Maßnahmen getroffen werden müssen, um auch im Hinblick auf diese „mitgliederspezifischen Risiken“ ein angemessenes Datenschutzniveau zu gewährleisten.

7. Schutzzielerreichung

Mit den dargestellten technischen und organisatorischen Maßnahmen Nr. 1 bis 62 werden die oben unter Punkt 5.4. beschriebenen Schutzziele erreicht:

Durchgeführte Maßnahmen	**Erreichte Schutzziele**
Zutrittskontrolle	Verfügbarkeit, Vertraulichkeit, Integrität, Nichtverkettbarkeit
Zugangskontrolle	Vertraulichkeit, Integrität, Nichtverkettbarkeit
Zugriffskontrolle	Vertraulichkeit, Integrität, Nichtverkettbarkeit
Weitergabekontrolle	Verfügbarkeit, Vertraulichkeit, Transparenz

Eingabekontrolle	Vertraulichkeit, Nichtverkettbarkeit, Transparenz
Verfügbarkeitskontrolle	Verfügbarkeit, Transparenz, Intervenierbarkeit
Trennungskontrolle	Nichtverkettbarkeit, Transparenz
Auftragskontrolle	Nichtverkettbarkeit, Intervenierbarkeit
Sonstige Maßnahmen	Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettbarkeit, Transparenz, Intervenierbarkeit

8. Neuerliche Risikobewertung

Die dargestellten technischen und organisatorischen Maßnahmen Nr. 1 bis 62 sehen Garantien, Schutzmaßnahmen und Verfahren vor, die geeignet sind, die oben unter Punkt 5.6.3. bewerteten Risiken einer neuen Beurteilung zu unterziehen.

Liste	Potenzielles Ereignis	Getroffene Maßnahmen	Risikokategorie
A	Unbefugte Personen dringen in Netzwerke und Systeme ein (Cyber-Crime und Malware-Attacken).	Zutrittskontrolle (1-4, 6, 7) Zugangskontrolle (14, 15, 20-27, 29, 30) Zugriffskontrolle (31, 35-37) Weitergabekontrolle (38, 39, 41, 42) Eingabekontrolle (43-45) Verfügbarkeitskontrolle (49-52) Trennungskontrolle (53, 56) Sonstige Maßnahmen (58-62)	II Gelb (Verringerte Eintritts-wahrscheinlichkeit, Risiko innerhalb der Kategorie II abgeschwächt).

B	Durch Naturgewalten oder unvorhersehbare Schadensereignisse werden Daten zerstört, gelöscht oder können nicht mehr wiederhergestellt werden.	Zutrittskontrolle (7, 11) Verfügbarkeitskontrolle (46-52) Trennungskontrolle (53-56) Sonstige Maßnahmen (58,59)	II Gelb (Verringerte Eintritts-wahrscheinlichkeit, Risiko innerhalb der Kategorie II abgeschwächt).
C	Unbefugte Personen verschaffen sich Zutritt zu Räumlichkeiten, Verarbeitungsanlagen oder Datenaufbewahrungsorten.	Zutrittskontrolle (1-11) Zugangskontrolle (12-17, 20-22, 24, 26, 28, 30) Zugriffskontrolle (31-34, 37) Eingabekontrolle (43-45) Verfügbarkeitskontrolle (49-52) Trennungskontrolle (52-56) Sonstige Maßnahmen (57-62)	II Gelb (Verringerte Eintritts-wahrscheinlichkeit, Risiko innerhalb der Kategorie II abgeschwächt).
D	Anwesende Personen haben unbefugten Zugang zu vertraulichen Dokumenten in Papierform, die z.B. in Büros, in Besprechungs-zimmern oder an Arbeitsplätzen aufliegen.	Zutrittskontrolle (5, 8-11) Zugangskontrolle (16, 17) Zugriffskontrolle (32-34, 37) Weitergabekontrolle (40-42) Trennungskontrolle (54-56) Sonstige Maßnahmen (58, 59, 62)	II Orange (Verringerte Eintritts-wahrscheinlichkeit, Risiko um eine Kategorie herabgestuft).
E	Anwesende Personen sehen unbefugt Bildschirme ein.	Zutrittskontrolle (8, 10) Zugangskontrolle (12, 13,18) Zugriffskontrolle (39, 42, 47, 51) Weitergabekontrolle (41)	II Orange (Verringerte Eintritts-wahrscheinlichkeit, Risiko um eine Kategorie herabgestuft).

		Sonstige Maßnahmen (57-59, 62)	
F	Anwesende Personen hören unbefugt vertrauliche Gespräche oder Telefonate mit.	Zutrittskontrolle (8, 10, 11) Zugangskontrolle (19, 30) Sonstige Maßnahmen (57-59, 62)	II Orange (Verringerte Eintritts-wahrscheinlichkeit, Risiko um eine Kategorie herabgestuft).
G	Vertrauliche Dokumente und Informationen gehen verloren..	Zutrittskontrolle (9, 11) Zugangskontrolle (12-15, 17, 24-26, 29, 30) Weitergabekontrolle (39-42) Verfügbarkeitskontrolle (49-52) Sonstige Maßnahmen (57-59, 61, 62)	II Orange (Verringerte Eintritts-wahrscheinlichkeit, Risiko um eine Kategorie herabgestuft).
H	Vertrauliche Informationen werden von MitarbeiterInnen unbewusst gegenüber unbefugten Personen beauskunftet oder offengelegt.	Zutrittskontrolle (8-11) Zugangskontrolle (13, 16-19, 29, 30) Zugriffskontrolle (32-34, 36, 37) Weitergabekontrolle (38, 40-42) Eingabekontrolle (43) Trennungskontrolle (53, 54) Sonstige Maßnahmen (57-59, 62)	II Orange (Verringerte Eintritts-wahrscheinlichkeit, Risiko um eine Kategorie herabgestuft).

I	Vertrauliche Informationen werden von MitarbeiterInnen bewusst oder unbewusst gegenüber unbefugten Personen im Privatleben offengelegt.	Zugangskontrolle (13, 14, 24, 26, 29, 30) Weitergabekontrolle (41) Sonstige Maßnahmen (57, 59, 60, 62)	II Orange (Verringerte Eintritts-wahrscheinlichkeit, Risiko um eine Kategorie herabgestuft).
J	Vertrauliche Informationen werden von MitarbeiterInnen im Homeoffice unbewusst gegenüber unbefugten Personen offengelegt.	Zutrittskontrolle (2, 6, 9-11) Zugangskontrolle (12-26, 28, 29, 30) Weitergabekontrolle (38-42) Eingabekontrolle (43-45) Trennungskontrolle (53, 54) Sonstige Maßnahmen (57-59, 61, 62)	II Orange (Verringerte Eintritts-wahrscheinlichkeit, Risiko um eine Kategorie herabgestuft).
K	(Ehemalige) MitarbeiterInnen oder AdressatInnen verschaffen sich zum Zweck der persönlichen Vorteilsnahme unbefugt vertrauliche Informationen über betroffene Personen.	Zutrittskontrolle (1-11) Zugangskontrolle (12-19, 21, 22, 24, 29, 30) Zugriffskontrolle (31, 32, 34, 36, 37) Weitergabekontrolle (38, 41) Eingabekontrolle (43-45) Verfügbarkeitskontrolle (49-52) Trennungskontrolle (53-56) Sonstige Maßnahmen (57-59, 61, 62)	II Gelb (Verringerte Eintritts-wahrscheinlichkeit, Risiko innerhalb der Kategorie II abgeschwächt).

L	Zulässigerweise verarbeitete personenbezogene Daten werden für unbefugte Zwecke weiterverwendet.	Zugriffskontrolle (31, 36, 37) Eingabekontrolle (43-45) Trennungskontrolle (53-56) Sonstige Maßnahmen (57-60, 62)	II Gelb (Verringerte Eintritts-wahrscheinlichkeit, Risiko innerhalb der Kategorie II abgeschwächt).
M	Beigezogene Dienstleister gehen nicht ordnungsgemäß mit personenbezogenen Daten um, die ihnen zur Auftragserfüllung überlassen wurden bzw. auf die sie zu diesem Zweck zugreifen können.	Zutrittskontrolle (4, 5) Zugangskontrolle (14, 15, 16, 20, 23, 27-30) Zugriffskontrolle (34, 35, 37) Eingabekontrolle (43-45) Verfügbarkeitskontrolle (49-51) Sonstige Maßnahmen (57-60, 62)	II Gelb (Verringerte Eintritts-wahrscheinlichkeit, Risiko innerhalb der Kategorie II abgeschwächt).
N	Aufgrund der Vielzahl an externen involvierten Stakeholdern kommt es zu Unklarheiten, Missverständnissen und Zweifelsfällen gegenüber welchen Personen bzw. Institutionen welche Informationen beauskunftet oder übermittelt werden dürfen.	Zugangskontrolle (27) Zugriffskontrolle (34, 35, 37) Weitergabekontrolle (38, 42) Eingabekontrolle (43, 44) Trennungskontrolle (53, 54, 56) Sonstige Maßnahmen (57, 60, 62)	II Orange (Verringerte Eintritts-wahrscheinlichkeit, Risiko um eine Kategorie herabgestuft).

O	Im Zuge der Erbringung von Leistungen in einer Gruppe (z.B. Schulung, Workshop oder Ausübung von Beschäftigungen beim Mitglied als geförderte Maßnahme) werden bewusst oder unbewusst Informationen von AdressatInnen gegenüber unbefugten Personen (insbesondere anderen teilnehmenden AdressatInnen) offengelegt..	Zutrittskontrolle (5, 8, 10) Zugangskontrolle (12, 16, 17, 19) Zugriffskontrolle (32) Weitergabekontrolle (42) Sonstige Maßnahmen (57, 62)	II Orange (Verringerte Eintritts-wahrscheinlichkeit, Risiko um eine Kategorie herabgestuft).
P	Informationen werden bewusst oder aufgrund eines Versehens in den von den Fördergebern zur Verfügung gestellten Applikationen nicht oder nicht vollständig erfasst und dokumentiert. Dadurch sind notwendige Informationen im weiteren Betreuungsverlauf nicht mehr verfügbar..	Zugriffskontrolle (31, 36, 37) Eingabekontrolle (43-45) Verfügbarkeitskontrolle (49-52) Sonstige Maßnahmen (58, 59, 62)	II Orange (Verringerte Eintritts-wahrscheinlichkeit, Risiko um eine Kategorie herabgestuft).
Q	Die interne Rechtevergabe für die Verwendung der von den Fördergebern zur Verfügung gestellten Applikationen erfolgt in Einzelfällen nicht nach dem „Need-to-know“-Prinzip oder wird nicht laufend auf ihre Aktualität hin überprüft..	Zugangskontrolle (21, 22) Zugriffskontrolle (31, 36, 37) Eingabekontrolle (43-45) Trennungskontrolle (53, 56) Sonstige Maßnahmen (57, 62)	II Orange (Verringerte Eintritts-wahrscheinlichkeit, Risiko um eine Kategorie herabgestuft).
R	Die Stellung besonders schutzbedürftiger Personen wird von Mitgliedern im Zuge der Aufgabenerfüllung dazu	Zugriffskontrolle (31, 36, 37) Eingabekontrolle (43-45) Trennungskontrolle (53)	II Gelb (Verringerte Eintritts-wahrscheinlichkeit, Risiko innerhalb der

	ausgenützt, um z.B. eine Einwilligung für eigene Verarbeitungszwecke zu erlangen oder die Geltendmachung von Rechten zu erschweren.	Sonstige Maßnahmen (58, 59, 62)	Kategorie II abgeschwächt).

Im Ergebnis können die oben beschriebenen potenziellen Ereignisse A bis C, K bis M und R hinsichtlich des Bewertungskriteriums Eintrittswahrscheinlichkeit von Stufe 2 „Begrenzt“ auf Stufe 1 „Vernachlässigbar“ herabgesetzt werden. Dies führt innerhalb der Risikokategorie II zu einer Risikoabschwächung von „Orange“ auf „Gelb“.

Die oben beschriebenen potenziellen Ereignisse D bis J und N bis Q können hinsichtlich des Bewertungskriteriums Eintrittswahrscheinlichkeit von Stufe 3 „Wesentlich“ auf Stufe 2 „Begrenzt“ herabgesetzt werden. Dies führt zu einer Herabstufung von Risikokategorie III (Rot) auf Risikokategorie II (Orange).

Das verbleibende Risiko der Kategorie II muss angesichts der alternativlosen Verarbeitung besonderer Kategorien personenbezogener Daten (insbesondere Gesundheitsdaten von AdressatInnen) im Rahmen der Auftragserfüllung gegenüber dem AMS und dem SMS als vertretbar angesehen werden. Den Schutzzielen

- Verfügbarkeit (Schutz vor Vernichtung und Verlust),
- Integrität (Schutz vor Veränderung),
- Vertraulichkeit (Schutz vor unbefugter Offenlegung und unbefugtem Zugang),
- Nichtverkettbarkeit (Schutz der Zweckbindung),
- Transparenz (Schutz der Revisionsfähigkeit (Nachprüfbarkeit und Nachvollziehbarkeit) und
- Intervenierbarkeit (Schutz der Betroffenenrechte)

wird durch die getroffenen technischen und organisatorischen Maßnahmen ausreichend Rechnung getragen.

9. Verfahrensbestimmungen

9.1. Akkreditierte Stellen

Die Überwachung der Einhaltung der gegenständlichen Verhaltensregeln wird von Stellen durchgeführt, die – unbeschadet der Aufgaben und Befugnisse der Datenschutzbehörde – über das geeignete Fachwissen hinsichtlich des Gegenstands der Verhaltensregeln verfügen

und von der Datenschutzbehörde zu diesem Zweck akkreditiert wurden (Art. 41 Abs. 1 DSGVO). Das Akkreditierungsverfahren vor der Datenschutzbehörde wird durch die ÜStAkk-V geregelt.

Da die Verbände Mitglieder österreichweit vertreten und in allen Bundesländern Vorort-Kontrollen ermöglicht werden sollen, wird im Interesse einer Kostenneutralität (etwa in Bezug auf Anfahrts- und Reisekosten) angestrebt, in jedem Bundesland zumindest eine akkreditierte Stelle zur Verfügung stellen zu können. Die Verbände werden daher, wenn möglich, in jedem Bundesland geeignete Unternehmen oder Institutionen, die über das notwendige Fachwissen auf dem Gebiet der Datensicherheitsmaßnahmen gemäß Art. 32 DSGVO verfügen, einladen, die Akkreditierung durch die Datenschutzbehörde zu erlangen (Überwachungsstellen im Sinn der ÜStAkk-V).

9.2. Verfahren zur Überwachung der Einhaltung der Verhaltensregeln

Das Verfahren zur Überwachung der Einhaltung der Verfahrensregeln richtet sich nach der ÜStAkk-V. Daneben sind folgende Grundsätze zu beachten:

- Die akkreditierten Stellen haben das Überwachungsverfahren nach § 5 ÜStAkk-V mit den Verbänden abzustimmen.

- Mitglieder, die sich den gegenständlichen Verhaltensregeln unterwerfen, sind verpflichtet, akkreditierten Stellen im Rahmen der Erfüllung ihres Prüfauftrages alle notwendigen Informationen und Unterlagen, wie z.B. Verträge über die Auftragsverarbeitung gemäß Art. 28 DSGVO, bereitzustellen und Einsicht in Informationen zu Datenverarbeitungen zu gewähren.

- Erlangen akkreditierte Stellen im Rahmen der Erfüllung ihres Prüfauftrages Einblick in Geschäfts- und Betriebsgeheimnisse von Mitgliedern, sind sie im entsprechenden Umfang zur Verschwiegenheit verpflichtet.

- Mitglieder, die sich den gegenständlichen Verhaltensregeln unterwerfen, haben Anfragen von akkreditierten Stellen, die im Rahmen der Erfüllung ihres Prüfauftrages an sie gerichtet werden, innerhalb einer Frist von 6 Wochen zu beantworten. In begründeten Fällen kann diese Frist für 2 Wochen verlängert werden. In diesem Fall hat das betreffende Mitglied die akkreditierte Stelle vor Ablauf der Frist von 6 Wochen über die Verzögerung und die Gründe hierfür zu unterrichten.

- Die zuständige akkreditierte Stelle ist berechtigt, Vorort-Kontrollen durchzuführen. Vorort-Kontrollen sind unter größtmöglicher Schonung der Geschäftsabläufe des überprüften Mitgliedes und der Achtung von Persönlichkeitsrechten und der Privatsphäre von MitarbeiterInnen durchzuführen und mit dem Mitglied im Vorfeld terminlich abzustimmen.

10. Änderungen der Verhaltensregeln

Für den Fall einer künftigen inhaltlichen Änderung eines maßgeblichen Vertrages über die Auftragsverarbeitung gemäß Art. 28 DSGVO werden die Verbände in Abstimmung mit dem AMS und dem SMS überprüfen, ob eine Anpassung der gegenständlichen Verhaltensregeln erfolgen muss.

Ein Änderungsbedarf der Verhaltensregeln kann sich auch nach Maßgabe von § 9 ÜStAkk-V ergeben.