Verhaltensregeln / Code of Conduct zum Datenschutz
der Berufsvereinigung der ArbeitgeberInnen
privater Bildungseinrichtungen

BABE CoC

Inhaltsverzeichnis

1. Ziel und Zweck

Seit dem 25. Mai 2018 gilt die Datenschutz-Grundverordnung (DSGVO) in Österreich und ist direkt anwendbar. Ziel der Verordnung ist der Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten und die Vereinheitlichung der Datenschutzstandards in Europa.

Gemäß Art 40 DSGVO können Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, Verhaltensregeln (auch „Code of Conduct“, kurz „CoC“, genannt) ausarbeiten. Verhaltensregeln präzisieren die Vorgaben der DSGVO, indem sie die jeweils relevanten Vorgaben, spezifisch für bestimmte Gruppen von Verarbeitungen auslegen. Verhaltensregeln dienen somit als praxisnahe Interpretationshilfe, erleichtern dadurch den Verantwortlichen und Auftragsverarbeitern die Anwendung der DSGVO und bieten ihnen mehr Rechtssicherheit, welche konkreten Verpflichtungen einzuhalten sind.

Die Berufsvereinigung der ArbeitgeberInnen privater Bildungseinrichtungen (BABE) als Vertretung der österreichischen Bildungsträger hat in Zusammenarbeit mit ihren Mitgliedern, unter Einbeziehung verschiedener öffentlicher Auftraggeber bzw. Fördergeber, sowie mit weiteren maßgeblichen Interessensträgern die nachfolgenden Verhaltensregeln ausgearbeitet, welche bei Bedarf und nach erneuter Vorlage an die Datenschutzbehörde weiterentwickelt und ergänzt werden können.

Die unterzeichnenden Einrichtungen sind sich in diesem Zusammenhang ihrer Rolle hinsichtlich der Gewährleistung des Grundrechts auf Datenschutz bewusst und bekennen sich ausdrücklich zu ihrer gesellschaftlichen Verantwortung im Rahmen ihrer unternehmerischen Tätigkeit.

1.1. Mehrwert der CoC

Durch Erarbeitung eines gemeinsamen Grundverständnisses der branchenspezifischen Ausgestaltung der in der DSGVO enthaltenen Erfordernisse bzw. Verpflichtungen für private Bildungsträger (im Weiteren kurz „Träger“ genannt) sowie durch die Vornahme von Präzisierungen soll eine bestmögliche Umsetzung der DSGVO zur Wahrung der Rechte betroffener Personen sowie Rechtssicherheit für die Träger gewährleistet werden.

Es bestehen zahlreiche branchenspezifische Fragestellungen im Umgang mit (personenbezogenen) Daten, die zum Zweck erhöhter Rechtssicherheit sowie zur Vereinfachung der Compliance sowohl für Träger als auch für Auftrag- und Fördergeber möglichst weitgehend einheitlichen Lösungswegen zugeführt werden sollen.

Die Einhaltung eines bestimmten Schutzniveaus bei der Verarbeitung personenbezogener Daten ist dabei auch ein Qualitätskriterium zur Leistungserbringung für öffentliche Auftrag-/Fördergeber, wie insbesondere für das Arbeitsmarktservice (kurz „AMS“). Auch für die Seite der öffentlichen Auftrag-/Fördergeber – die durchwegs mit öffentlichen Mitteln arbeiten – stellen gegenständliche Verhaltensregeln daher eine wesentliche Erleichterung dar.

Durch einen eigenständigen Kontroll- und Auditierungs-Mechanismus soll gewährleistet werden, dass die sich verpflichtenden Träger auch tatsächlich ein grundlegendes Schutzniveau einhalten, ohne dass es seitens der Auftrag- oder Fördergeber einer weiteren intensiven Kontrolltätigkeit bedarf. Durch die Unterzeichnung und Selbstbindung an diese Verhaltensregeln kann ein Träger zudem objektiviert darstellen, warum ein Auftrag- oder Fördergeber in der Rolle des datenschutzrechtlich Verantwortlichen auf die gebotene Zuverlässigkeit und Eignung dieses Trägers vertrauen darf.

1.2. Adressaten

Die Mitglieder der BABE können sich den vorliegenden Verhaltensregeln auf freiwilliger Basis, durch Abgabe einer Erklärung, unterwerfen.

Jeder Träger gibt eine Erklärung ab, aus der hervorgeht, ob die Selbstverpflichtung durch Beitritt zu den BABE CoC das gesamte Unternehmen mit all seinen Dienstleistungen umfasst oder ob nur bestimmte, abgrenzbare Teile des Unternehmens davon erfasst sein sollen (**Statement of Applicability**, SOA).

Sofern die Regeln nur auf Teile des Unternehmens bezogen sind, hat der Träger kenntlich zu machen, mit welchen Teilbereichen des Unternehmens er sich den CoC unterworfen hat. Die in Art 40 DSGVO vorgesehenen Vereinfachungen werden dann auch nur für diese Teile des Unternehmens wirksam.

2. Einordnung der BABE CoC in den global-rechtlichen Rahmen

2.1. Rechtswirkung der BABE CoC

Die vorliegenden Verhaltensregeln betreffen ausschließlich Verarbeitungstätigkeiten in Österreich und dienen der Präzisierung

- der datenschutzrechtlichen Rolle der Träger in bestimmten Verarbeitungssituationen;
- der Ausübung der Rechte der betroffenen Personen;
- der Erfüllung von Informationspflichten gegenüber betroffenen Personen;
- der Maßnahmen gemäß den Art 24, 25 und 32 DSGVO;
- der Risikoanalyse entsprechenden Maßnahmen.

2.2. Verhältnis zu weiteren Rechtsvorschriften

Die vorliegenden BABE CoC unterliegen der Genehmigung durch die österreichische Datenschutzbehörde. Insofern enthalten die CoC einen normativen Teil, der durch die Genehmigung der Behörde eine konstitutive Rechtswirkung entfaltet – nämlich insofern, als die Einhaltung der Vorgaben dieser CoC nach Art 83 Absatz 2 lit. j DSGVO bei der Verhängung einer Geldbuße gebührend zu berücksichtigen ist. Die normative Wirkung beschränkt sich auf Auslegungsfragen zur DSGVO oder zum DSG und ist nicht präjudiziell im Hinblick auf die Auslegung anderer – für die den Verhaltensregeln Unterworfenen beachtlicher – Rechtsvorschriften (AMSG, BAG, AngG, ArbVG, BVerfG, Förderrichtlinien, Berufsrecht etc.) außerhalb der Zuständigkeit der Datenschutzbehörde.

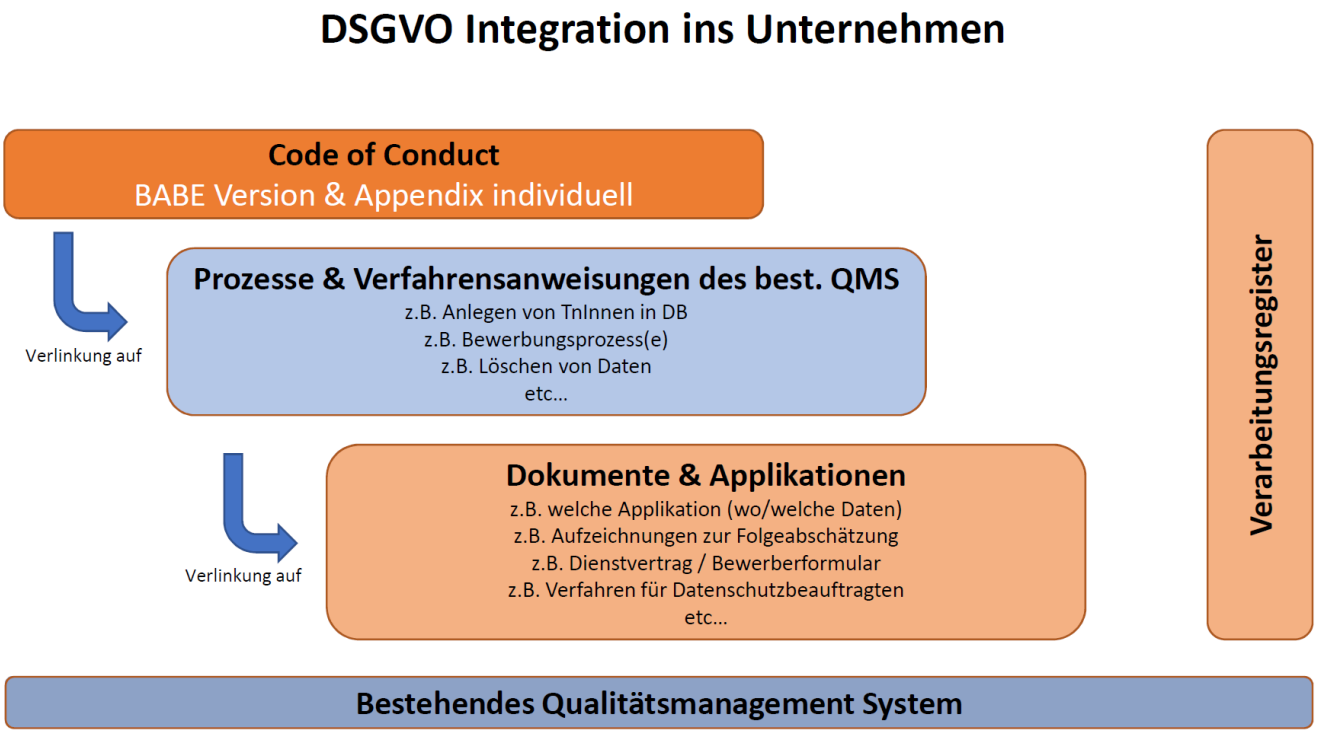
2.3. Verhältnis zu Auftragsverarbeitungsverträgen und Förderverträgen

Auftragsverarbeitungsverträge und Förderverträge wirken als Indikatoren der datenschutzrechtlichen Beurteilung. Darüber hinaus richtet sich die datenschutzrechtliche Beurteilung primär nach der DSGVO, dem DSG und den jeweiligen leges speciales und nicht nach etwaigen Förderverträgen. Sie gestalten die Rechtslage und sind gleichzeitig Gegenstand einer datenschutzrechtlichen Beurteilung. Darüber hinaus sind sie ständigen Änderungen unterworfen und können als solche nicht statisch referenziert werden. Die BABE CoC vermögen nicht, in die rechtsgestaltende Wirkung solcher Verträge einzugreifen.

Soweit auf diese Instrumente Bezug genommen wird, ist dies als Handlungsanleitung für die adressierten Träger zu verstehen und bürdet den Trägern typischerweise bestimmte Sorgfaltspflichten auf, eine bestimmte Frage einer klaren Regelung und Dokumentation zuzuführen – ohne den letztlich gültigen Inhalt der Regel final vorzugeben. Zudem wird im Folgenden mehrfach Bezug v. a. auf Inhalte genommen, die sich in den derzeitigen datenschutzrechtlichen Vorgaben des AMS in der Rolle des Verantwortlichen gegenüber den Trägern als Auftragsverarbeiter finden.

2.4. Verhältnis zu Datenschutz-Managementsystemen

Die nachfolgende Graphik dient der Illustration der Verhältnisse verschiedener Management-Systeme zu den BABE CoC:



Die BABE CoC befinden sich somit eine Regelungsebene über dem Management-System der betroffenen Organisation bzw. des Trägers. Die BABE CoC adressieren dieses Verhältnis jedoch, in dem die Synergieeffekte erkannt und befördert werden, insbesondere im Hinblick auf etablierte Audit- und Zertifizierungssysteme.

3. Umfang der Verarbeitung personenbezogener Daten

3.1. Betroffene Personenkategorien

TeilnehmerInnen von Bildungsaktivitäten stehen im Fokus der hier erfassten Zusammenhänge. Darüber hinaus sind auch die MitarbeiterInnen der Träger betroffen, wobei TrainerInnen hier eine besondere Kategorie bilden. Besonders hervorzuheben sind in diesem Zusammenhang SÖB-MitarbeiterInnen (Transitarbeitskräfte) und ÜBA-Lehrlinge. Diese beiden Gruppen haben gemeinsam, dass sie zugleich sowohl TeilnehmerInnen einer Bildungsmaßnahme als auch – bedingt durch die Natur der Maßnahme – MitarbeiterInnen im Betrieb eines Trägers sind.

Ausnahmsweise können auch außenstehende Dritte von der Verarbeitung betroffen sein, nämlich typischerweise Personen aus dem Familien- oder Freundeskreis insbesondere der TeilnehmerInnen. Die zuletzt genannte Kategorie von Personen ist z. B. bei der Angabe von Notfallkontakten relevant. Darüber hinaus finden sich Daten über solche Personenkategorien mitunter in Protokollen zu Einzelcoachings, wenn Angaben der TeilnehmerInnen dazu gemacht wurden und für die Bildungsmaßnahme relevant erscheinen.

3.2. Betroffene Datenkategorien

Zur Erfüllung der Verpflichtungen aus einer „Auftragsverarbeitung“ dürfen grundsätzlich nur die vom Auftrag- oder Fördergeber angegebenen Datenarten verarbeitet werden. Im Auftrag des AMS dürfen nur die gemäß § 25 AMSG in der jeweils geltenden Fassung aufgezählten Datenarten verarbeitet werden und dies auch nur, soweit sie im Einzelfall für die Erbringung der dem Träger vertraglich überbundenen Tätigkeiten eine wesentliche Voraussetzung bilden.

In der Rolle des „Verantwortlichen“ stellt der Träger sicher, dass durch ein effektives Datenschutz-Management-System nur jene Daten verarbeiten werden, die im Hinblick auf die jeweiligen Zwecke ihrer Verarbeitung notwendig und verhältnismäßig sind. Der für die jeweilige Anwendung zulässige Umfang personenbezogener Daten ist aber im Hinblick auf jede Fördermaßnahme oder Auftragsvergabe nach den entsprechenden Vertrags- und Rechtsgrundlagen zu prüfen und in der Dokumentation des Trägers festzulegen.

4. Datenschutzrechtliche Rollenverteilung

4.1. Relevanz der datenschutzrechtlichen Rollenverteilung allgemein

Der datenschutzrechtlichen Rollenverteilung kommt besondere Bedeutung zu. Den Verantwortlichen trifft die gesamte in der DSGVO für diesen normierte Verantwortung. So ist dieser u. a. für die Einhaltung der Betroffenenrechte verantwortlich.

Auftragsverarbeiter sind Empfänger im Sinne von Art 4 Z 9 DSGVO. Die Eigenschaft als Empfänger führt zu gesonderten Informations- (vgl. u. a. Art 13 Abs. 1 lit. e DSGVO) und Mitteilungspflichten (Art 19 DSGVO) des Verantwortlichen sowie zu Auskunftsrechten (Art 15 DSGVO) der betroffenen Person gegenüber dem Verantwortlichen. Empfänger von Daten

müssen im Verzeichnis von Verarbeitungstätigkeiten (vgl. Art 30 Abs. 1 lit. d DSGVO) geführt werden. Das bedeutet insbesondere, dass im Rahmen eines Auskunftsbegehrens auch über den gewählten Auftragsverarbeiter eine Auskunft zu erteilen ist (Namhaftmachung).

4.2. Akteure und deren Zuordnung zu den datenschutzrechtlichen Rollen

4.2.1. Allgemeines

Ein Großteil der in der BABE repräsentierten Unternehmen erbringt Dienstleistungen insbesondere in zwei Bereichen:

1. Bildungsangebote für Erwachsene und Jugendliche zur Verbesserung der Chancen am Arbeitsmarkt, in Bildung und Gesellschaft.
2. Vermittlung arbeitssuchender Personen am Arbeitsmarkt.

Manche Träger sind auf einen der Bereiche spezialisiert, während vor allem größere Unternehmen der Branche die gesamte Bandbreite mit spezifischen Angeboten abdeckt.

Das genannte Leistungsspektrum wird dabei sehr stark durch öffentliche Förderungen oder öffentliche Aufträge bestimmt. Allerdings verfügen viele Träger daneben – vereinzelte auch ausschließlich – über ein rein privates Angebot an Dienstleistungen zur Fortbildung sowie zur Arbeitsvermittlung, die nicht aus öffentlichen Mitteln finanziert, sondern entgeltlich gegenüber den betroffenen Personen (B2C) oder deren Dienstgeber (B2B) als Endkunden erbracht werden.

Ein beachtlicher Teil der von der Branche erbrachten Dienstleistungen basiert auf öffentlichen Ausschreibungen des AMS iSd des Bundesvergabegesetzes idgF. In diesen Fällen ist der Bund, vertreten durch das AMS, dieses wiederum vertreten durch die jeweilige Landesgeschäftsstelle des AMS, öffentlicher Auftrag-/Fördergeber und schließt Werkverträge oder Rahmenvereinbarungen mit den Trägern zur Erbringung der Bildungsdienstleistungen.

Darüber hinaus werden Dienstleistungen auch im Rahmen von Förderprogrammen des Bundes (z. B. des Sozialministeriums und des Bildungsministeriums) und der Länder, des Wiener ArbeitnehmerInnen Förderungsfonds (WAFF), verschiedener Magistratsabteilungen oder Gemeinden sowie auf Grundlage entsprechender Programme der EU bzw. des Europäischen Sozialfonds (ESF) gemäß jeweils geltenden gesetzlichen Förderbedingungen und Richtlinien erbracht. Einheitliche, konkrete Vorgaben zum Datenschutz liegen hier bisher nicht oder nur vereinzelt vor.

Da das AMS ein für viele Träger bedeutender Auftrag- und/oder Fördergeber der Branche ist, sind die nachfolgenden Verhaltensregeln unter besonderer Berücksichtigung auf das Verhältnis zwischen Träger und AMS erarbeitet, sollen aber gegenüber allen Auftrag- und Fördergebern gleiche Wirkung entfalten.

4.2.2. Träger in der Rolle des Verantwortlichen

Viele Träger haben eigene, rein private Bildungsangebote ohne einen öffentlichen Förderungshintergrund. Der Träger muss für jede Verarbeitungstätigkeit im Verzeichnis nach Artikel 30 DSGVO nachvollziehbar dokumentieren, ob er die Verarbeitung als Verantwortlicher oder als Auftragsverarbeiter durchführt. Das hat er immer im Einzelfall zu prüfen. Zur Orientierung gilt: Alle mit einem rein privaten Bildungsangebot einhergehenden Verarbeitungen personenbezogener Daten, bei denen es keine Dokumentationspflichten gegenüber einem Fördergeber gibt und auch sonst niemand rechtlich zulässige Entscheidungen über die Zwecke oder die Mittel der jeweiligen Verarbeitung für den Träger trifft, sind dem Träger als Verantwortlichen zuzurechnen. Dies gilt insbesondere für die Personaldatenverarbeitung des beim Träger (als Dienstgeber) unmittelbar beschäftigten Personals. Für den Fall, dass die Beschäftigung im Betrieb des Trägers zugleich Teil einer geförderten Maßnahme ist (wie insbesondere in einem Sozialökonomischen Betrieb), sind alle Verarbeitungstätigkeiten (Aufzeichnungen, Übermittlungen etc.) aufgrund der Handlungspflichten des Trägers im Auftrag des Fördergebers (z. B. AMS) als gesonderte Verarbeitungstätigkeit gemäß Art 30 DSGVO eigenständig unter Bezeichnung des Verantwortlichen zu dokumentieren.

Zur besseren Nachvollziehbarkeit kann es nützlich sein, zwischen den Stammdaten und Leistungsdaten zu unterscheiden. Leistungsdaten sind solche Daten im Zusammenhang mit der Leistungserbringung, die zugleich einen bestimmten Geschäftsfall dokumentieren. Diese Daten sind typischerweise unmittelbar mit Daten der TeilnehmerInnen verbunden.

Die Verarbeitung von Kontaktdaten (Stammdaten) der Arbeitgeberseite im Rahmen des durch die Tätigkeit aufgebauten Netzwerks liegt in der Verantwortung der Träger. Sehr viele der Bildungsmaßnahmen im privaten und öffentlich geförderten Sektor erfordern den regelmäßigen Kontakt der Träger zur Arbeitgeberseite. Schließlich sind die Bildungsprogramme nicht Selbstzweck, vielmehr sollen sie die Chancen der TeilnehmerInnen in diesen Programmen am Arbeitsmarkt und im Wirtschaftsleben steigern. Die Entscheidung zur Bildung eines Netzwerks zur Arbeitgeberseite (mit oder ohne bestimmte Branchenausprägung) ist daher für die meisten Träger notwendiger Bestandteil eines Erwachsenenbildungsbetriebs. Daraus folgt, dass die datenschutzrechtliche Verantwortung für die im Zusammenhang mit einem solchen Netzwerk zur Arbeitgeberseite aufgebauten Kontakte und Informationsbeziehungen beim Träger liegt. Die Träger trifft insbesondere die Pflicht, für jede Verarbeitungstätigkeit auch eine Dokumentation der Zwecke sowie der dazu gehörigen Rechtfertigung für die Verarbeitung zu führen, aus der nachvollziehbar ist, warum solche Stammdaten zulässig durch den Träger als Verantwortlichen verarbeitet werden und von den Verarbeitungsvorgängen im Rahmen allfälliger Auftragsverarbeitungen abgegrenzt sind.

4.2.3. Auftragsverarbeitung im Auftrag des „öffentlichen Auftraggebers / Fördergebers“

Im Bereich der Finanzierung aus öffentlichen Mitteln ist zwischen öffentlicher Auftragsvergabe nach BVergG und „Förderungsvergabe“ bzw. Förderung nach nationalen und/oder EU-Förderbedingungen zu unterscheiden. Die in der Praxis bestehende Unterscheidung zwischen Förderung und öffentlicher Auftragsvergabe ist im Hinblick auf die datenschutz-

rechtliche Rollenverteilung allerdings nur von nachrangiger Bedeutung. Im Endeffekt werden in beiden Fällen Verträge mit dem „Geldgeber“ geschlossen. Dieser formale Aspekt ist für die Rollendefinition weniger wichtig als der Inhalt eben dieser Verträge, bspw. eine Befugnis zur Anweisung einer Datenlöschung oder Korrektur oder das Ausmaß an Eigenverantwortung. Der Begriff „Auftraggeber“ oder „Fördergeber“ im Rahmen dieser CoC umfasst in Bezug auf die Träger sowohl öffentliche Auftragsvergaben als auch Fördervergaben. Es wird ausdrücklich festgehalten, dass nicht die formale Bezeichnung der Rolle (also Verantwortlicher oder Auftragsverarbeiter) ausschlaggebend ist, sondern die inhaltliche Ausgestaltung der Entscheidungsbefugnis über die Verarbeitung der Daten.

In den derzeitigen Förderbedingungen des Bundes/der EU ist dies nicht immer so klar geregelt, wie es das AMS in seinen Datenschutz-Vereinbarungen für Förderungs- und Werkverträge gemäß § 32 Abs. 3 AMSG festhält. Die Vorgehensweise des AMS wird daher im Folgenden – als das präziseste einschlägige Regelwerk im öffentlich-rechtlichen Bereich – als Modell betrachtet, soweit konkrete Vorgaben aus Förderverträgen dem nicht entgegenstehen. Dass sich darüber hinaus Träger in Förderprojekten als Fördernehmer bewerben, wird in diesen CoC ergänzend dargestellt, mit dem Ziel der Klarstellung, dass die Träger auch in Förderprojekten datenschutzrechtlich Auftragsverarbeiter sind. Die branchentypische Konstellation beinhaltet dabei, dass ein Fördergeber (z. B. AMS, ESF, Sozialministerium, Bildungsministerium etc.) nicht nur die Mittel zur Durchführung arbeitsmarkt- und/oder bildungspolitischer Maßnahmen bereitstellt, sondern dabei selbst unmittelbar die Verantwortung trägt. Deshalb ist es üblich, dass der Fördergeber auch alle maßgeblichen Entscheidungen zur Verarbeitung der personenbezogenen Daten der TeilnehmerInnen im Rahmen der Bildungsmaßnahmen trifft und entsprechende Vorgaben an die Träger macht. Der Träger verarbeitet dabei die Daten ausschließlich zur Erbringung der im Vertrag mit dem Fördergeber vorgesehenen Aufgaben sowie zur Erfüllung von darüberhinausgehenden vertragsbezogenen und dokumentierten Weisungen des Fördergebers. Der Träger hat den Fördergeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Fördergebers verstößt gegen Datenschutzbestimmungen der EU oder der Mitgliedstaaten. In diesem Umfang liegt die Entscheidung über die Zwecke und (jedenfalls normativ) auch über die Mittel der Verarbeitung beim Fördergeber, dem damit im Hinblick auf die diesbezüglichen Datenanwendungen die Rolle des Verantwortlichen zukommt.

Im Rahmen von Ausschreibungen und Förderungen durch den Bund, Länder, AMS, ESF oder andere öffentlich-rechtliche Körperschaften und Auftrag-/Fördergeber erfolgt die Verarbeitung personenbezogener Daten somit regelmäßig als Auftragsverarbeitung in der Verantwortung des jeweiligen Auftrag-/Fördergebers. In jedem Einzelfall einer Auftrags- oder Fördervergabe ist jedoch durch den Träger konkret zu prüfen, wer nach allfälligen einschlägigen Vorgaben die Entscheidung über Zwecke und Mittel der Datenverarbeitung trifft und in welcher Rolle der Träger daher Daten verarbeitet. Den Träger trifft die Verpflichtung, dies im eigenen Datenschutz-Management jeweils von Beginn einer Verarbeitungstätigkeit an klar festzulegen.

Eine Besonderheit in der Branche besteht im Hinblick auf sogenannte „Einzelcoachings“. Es handelt sich um Einzelgespräche der TrainerInnen im Rahmen von Bildungsprogrammen mit den TeilnehmerInnen. Solche Gespräche werden durch die TrainerInnen dokumentiert, wobei die Aufzeichnungen zunächst nur in der Informationssphäre zwischen TrainerInnen und TeilnehmerInnen verbleiben und ausschließlich einer humanen und zielführenden Begegnung der beiden Gruppen in ihrer jeweiligen Rolle dienen. Nur wenn im Rahmen

dieser Aufzeichnungen Umstände hervorgehen, welche für die Bildungsmaßnahme in einem grundsätzlichen Ausmaß relevant wird, das heißt vor allem, wenn diese Umstände Einfluss auf die Verfügbarkeit oder die Vermittelbarkeit am Arbeitsmarkt haben, kann es zu einer Ausweitung des Informationszirkels kommen. In den Programmen des AMS bedeutet dies dann typischerweise, dass die Aufzeichnungen in einen Eintrag im eAMS resultieren, der die für die Betreuung durch das AMS wesentlichen Umstände zusammenfasst und dem die Einzelaufzeichnungen zugrunde liegen. Solche Aufzeichnungen können unter Umständen auch besondere Kategorien personenbezogener Daten iSv Art. 9 DSGVO beinhalten, beispielsweise wenn es um gesundheitliche Gründe (physischer oder psychischer Natur) geht, welche die Verfügbarkeit und Vermittelbarkeit am Arbeitsmarkt beeinflussen. Je nachdem, wie schwerwiegend die Konsequenzen sind, die sich an solche Informationen knüpfen (z. B. Änderung des Betreuungsplans, Leistungsreduktion, Beendigung einer Maßnahme etc.), kann es erforderlich sein, dass die detaillierten Aufzeichnungen der TrainerInnen an den Auftrag-/Fördergeber der Maßnahme (als Verantwortlichen der Datenverarbeitung) zu übermitteln sind. Die Rechtsgrundlage für die Einzelaufzeichnungen der Gespräche zwischen den TrainerInnen und den TeilnehmerInnen bietet das Bundesgesetz über das Arbeitsmarktservice, BGBl. I Nr. 100/2018 (Arbeitsmarktservicegesetz, AMSG), konkret § 25 AMSG (Datenverarbeitung) in Verbindung mit § 29 AMSG (Ziel und Aufgabenerfüllung) sowie – im Hinblick auf die Beauftragung der Träger durch das AMS – § 32 AMSG (Dienstleistungen).

In der Regel ist aber im Sinne des aus der Informationssicherheit stammenden „need to know“ Prinzips von allen Beteiligten gewünscht, dass solche Aufzeichnungen und deren Informationsgehalt im engsten Kreis zwischen TrainerInnen und TeilnehmerInnen verbleiben und – unbeschadet der Stellung als Verantwortliche – auch an die Auftrag-/Fördergeber nur dann herausgegeben werden, wenn der Zweck der Verarbeitung dies unbedingt erfordert, zumal solche Aufzeichnungen häufig Informationen aus dem höchstpersönlichen Lebensbereich der betroffenen Personen enthalten und daher auf den engsten Kreis der Zugangsberechtigten reduziert werden sollten.

Alle im Zusammenhang mit der Erfüllung des Vertrages verarbeiteten Daten sind vom Träger dem Auftrag-/Fördergeber zu überlassen, falls diese angefordert werden. Davon unberührt sind absolute gesetzliche Verschwiegenheitsverpflichtungen (z. B. § 37 Psychologengesetz 2013 unter Berücksichtigung von § 36 Abs. 3 Psychologengesetz 2013), welchen der Träger oder die auf Rechnung und Gefahr des Trägers handelnden Personen bei der Erfüllung seiner ihm vom Auftrag-/Fördergeber überbundenen Leistungen allenfalls unterliegt.

4.2.4. Mehrfachrollen desselben Akteurs

Im Rahmen der SÖB bzw. GBP sowie bei überbetrieblichen Lehrausbildungen (ÜBA) ist zu berücksichtigen, dass die von der arbeitsmarktpolitischen Bildungsmaßnahme betroffenen Personen einerseits TeilnehmerInnen einer Bildungsmaßnahme und andererseits zugleich (mit derselben Tätigkeit) ArbeitnehmerInnen im Betrieb des Trägers sind. Es liegen also zwei unterschiedliche Zwecke zur Verarbeitung der Daten dieser Personengruppe vor. Davon sind insbesondere auch die ÜBA nach den §§ 8c, 30b BAG oder nach anderen entsprechenden Rechtsgrundlagen betroffen. Daraus folgt, dass die mit den jeweiligen Zwecken verbundenen Verarbeitungstätigkeiten (Datenanwendung) zu differenzieren sind, weil zumindest zwei voneinander zu unterscheidende Verarbeitungstätigkeiten vorliegen.

Diese Personen sind einerseits TeilnehmerInnen einer Ausbildungsmaßnahme des öffentlichen Auftrag-/Fördergebers. Die damit verbundene Datenverarbeitung erfolgt in der Verantwortung des öffentlichen Auftrag-/Fördergebers und durch den Träger nur in Erfüllung des ihm erteilten Auftrags. Der Träger ist im Umfang des Auftrags nur als Auftragsverarbeiter tätig und hat dies in der Dokumentation der Verarbeitungstätigkeit nach Artikel 30 DSGVO unter Angabe des Verantwortlichen erkennbar zu machen.

Zugleich werden andererseits die im Rahmen eines SÖB oder GBP beschäftigten Personen – als Bestandteil der Ausbildungsmaßnahme – als MitarbeiterInnen im Betrieb des Trägers angestellt. Wie bei anderen im Betrieb des Trägers angestellten MitarbeiterInnen erfolgt auch die Verarbeitung der Daten dieser Personen im Rahmen der Verarbeitungstätigkeit „Personaldatenverarbeitung“ und daher in der Eigenverantwortung des Trägers auf Basis des Arbeitsvertrags. Unmittelbarer Adressat der arbeits- und sozialrechtlichen Pflichten ist der Träger als Dienstgeber. Daraus folgt, dass alle aufgrund dieser Verpflichtungen erforderlichen Datenverarbeitungen dem Träger als Verantwortlichen im Sinne der DSGVO zuzurechnen sind – dies unbeschadet der Verarbeitungsvorgänge im Auftrag des AMS.

Der Träger hat bei der Gestaltung und Dokumentation seines Datenschutz-Managements zu beachten, dass diese Unterscheidung erkennbar ist und er im Falle der Geltendmachung von Betroffenenrechten jederzeit eine bestimmte Verarbeitungstätigkeit dem jeweils richtigen Verantwortungsbereich zuordnen kann.

5. Materielle Datenschutzvorgaben der CoC

5.1. Umgang mit Daten von TrainerInnen

Neben den allgemeinen Vorgaben des Arbeitsrechts zum Datenschutz besteht in der Branche eine Besonderheit in Bezug auf die Bewerbung der Träger um vergaberechtlich ausgeschriebene Projekte und bei Förderprogrammen öffentlicher Einrichtungen. Die Besonderheit besteht hier darin, dass auch regelmäßig Daten von TrainerInnen, die noch nicht oder nicht mehr als MitarbeiterInnen bei einem bestimmten Träger angestellt sind oder auf Werkvertragsbasis fakultativ für einen Träger tätig werden, in den Bewerbungen um Projekte mit Lebenslauf und Angaben zur Qualifikation verarbeitet (d. h., insbesondere auch an öffentliche Auftrag-/Fördergeber weitergegeben bzw. übermittelt) werden.

In diesem Fall gilt als Rechtsgrundlage für die Verarbeitung der Daten der betroffenen TrainerInnen die Durchführung vorvertraglicher Maßnahmen (im Hinblick auf den künftigen Arbeits- oder Werkvertrag zwischen Träger und dem/r TrainerIn) im Sinne des Art 6 Abs. 1 lit. b DSGVO als Rechtsgrundlage, sofern der Träger sichergestellt hat, dass die Initiative zur Aufnahme in die jeweilige Bewerbung von dem/r TrainerIn ausgegangen ist, z. B. durch eine Initiativbewerbung, Bewerbung auf ein Stelleninserat oder durch die Eintragung in einen TrainerInnen-Pool. Der Abschluss eines Vertrages zwischen Träger und TrainerIn ist durch die Erteilung des Zuschlags in Vergabeverfahren oder durch Abschluss des Fördervertrages in Bezug auf eine Projektbewerbung aufschiebend bedingt. Geht die Initiative nicht von der potentiellen TrainerIn aus, hat der Träger eine den Art 7 und 8 DSGVO entsprechende Einwilligung der TrainerIn zur Verarbeitung seiner/ihrer Daten in diesem Sinne einzuholen.

Dabei gilt aufgrund der teilweise längeren Zeiträume bis zur rechtskräftigen Zuschlagserteilung eine Aufbewahrungsdauer von drei Jahren als angemessen. Wenn die betroffenen TrainerInnen bereits MitarbeiterInnen im Betrieb des Trägers sind, könnte auch Art 6. Abs. 1 lit. f DSGVO (berechtigtes Interesse) zutreffend sein. Die Rechtsgrundlage (Erlaubnistatbestand zur Verarbeitung) muss durch den Träger jedenfalls klar festgehalten werden und es muss ersichtlich sein, auf welche Rechtsgründe die Verarbeitung im Einzelfall gestützt wird.

5.2. TeilnehmerInnenverwaltung

Sämtliche Auftrag- oder Fördergeber verlangen von den Trägern ein bestimmtes Minimum an Dokumentation zur Betreuung der TeilnehmerInnen sowie zum Nachweis der widmungsgemäßen Verwendung der Finanzierungmittel. Alle öffentlichen Auftrag- oder Fördergeber sind – schon durch die DSGVO – angehalten, gegenüber den Trägern möglichst präzise und bestenfalls abschließend vorzugeben, welche Daten für diese Zwecke zu verarbeiten sind. Dies sollte grundsätzlich auch für die sichere Übermittlung von (insbesondere sensiblen) personenbezogenen Daten gelten.

In der Regel ist in allen Dienstleistungsaufträgen und Förderschienen die An- und Abwesenheit der TeilnehmerInnen zu dokumentieren. Diese Dokumentation erfolgt zwar im Auftrag des jeweiligen Auftrag- oder Fördergebers, jedoch in den Systemen des Trägers ist sie dennoch Teil der Auftragsverarbeitung durch den Träger. Beispielsweise sind diese Daten in den Systemen des AMS (eAMS) durch den Träger kumuliert und in der Regel ohne Details zu dokumentieren. Wenn die Abwesenheitszeiten eine für die Förderung der betroffenen Person relevante Dimension erreichen, sind dem AMS regelmäßig Aufzeichnungen oder Auskünfte über die Gründe der Abwesenheit zu überlassen. In diesem Fall können darunter auch sensible Daten, etwa die näheren Informationen über eine Erkrankung als Grund des Fernbleibens, dokumentiert werden, die ansonsten typischerweise nur dem Träger bzw. den für diesen handelnden TrainerInnen bekannt sind.

Gemäß dem Grundsatz der Datenminimierung hat der Träger im Zuge dieser Dokumentation darauf zu achten, dass die – in den Abwesenheitsmeldungen regelmäßig enthaltenen – sensiblen Daten (Art 9 DSGVO) oder sonstige Informationen über den höchstpersönlichen Lebensbereich der Betroffenen nur im unbedingt erforderlichen Ausmaß im Hinblick auf den jeweiligen Zweck an den Auftrag- oder Fördergeber weitergeleitet werden, obwohl die Erhebung dieser Daten in dessen Auftrag und Verantwortung erfolgt. Der Rechtsgrund der Verarbeitung der Daten iSv Art. 9 DSGVO besteht hier typischerweise in den gesetzlichen Grundlagen, die den Auftrag- oder Fördergeber in der Rolle des Verantwortlichen determinieren (z. B. AMSG) und werden durch den Träger nur aufgrund einer Auftragsverarbeitung verarbeitet. Wenn der Auftrag- oder Fördergeber als Verantwortlicher den vollen Zugriff oder die Herausgabe verlangt, hat der Träger dies als Auftragsverarbeiter zu gewähren. Soweit der Träger solche Daten in der Rolle des Verantwortlichen verarbeitet, hat er hierfür die wirksame Einwilligung der Betroffenen einzuholen (Art. 7 und 8 DSGVO).

5.3. Verarbeitung von Daten von ÜBA-Lehrlingen und in SÖB/GBP

Im Rahmen einer Überbetrieblichen Lehrausbildung (überwiegend Minderjährige) sowie in SÖB bzw. GBP werden zunächst von Betroffenen zur Verfügung gestellte personenbezogene Daten (z. B. Lebensläufe, Ausbildungsnachweise, Nachweise zur Berufserfahrung, Stammdaten, Bankverbindungen etc.), aber auch jene Daten, die aufgrund des infolgedessen eingegangenen Lehrausbildungsverhältnisses anfallen (z. B. Gehaltsdaten, Krankenstände, Pflegefreistellung, Zeiterfassungsdaten, Karenzzeiten), verarbeitet.

Die Verarbeitung und Übermittlung der Daten erfolgt für die Lohn-, Gehalts-, Entgeltsverrechnung und Einhaltung von Aufzeichnungs-, Auskunfts- und Meldepflichten. Der Träger verarbeitet und speichert in diesem Zusammenhang automationsunterstützt erstellte und archivierte Textdokumente (wie z. B. Korrespondenz) in diesen Angelegenheiten. Ohne diese Daten kann der Träger den Lehr- und Ausbildungsvertrag im Auftrag des AMS oder einer anderen öffentlichen Einrichtung bzw. eines anderen Fördergebers mit dem Betroffenen nicht abschließen bzw. seinen Arbeitgeberpflichten nicht nachkommen. Dies gilt auch für allfällige, freiwillige Sozialleistungen durch den Träger und für Leistungen, die wenn auch nicht unmittelbar mit der Ausbildung in Zusammenhang stehen, aber als wesentlich erachtet werden, um die Teilnahme in einer modernen Gesellschaft zu ermöglichen und dadurch das berufliche Fortkommen zu unterstützen. Beispielsweise würden darunter Datenverarbeitungen fallen, die erforderlich sind, um Betroffene für den Kulturpass anzumelden oder um Wahlen zum Jugendvertrauensrat für Betroffene zu organisieren.

Rechtsgrundlagen der Verarbeitung sind der mit dem Lehrling abgeschlossene Ausbildungs- und Lehrvertrag sowie überwiegende berechtigte Interessen des Trägers. Eine Einwilligung zur Datenverarbeitung im Ausbildungsverhältnis benötigt der Träger nur im Ausnahmefall. Ausnahmefälle sind beispielsweise das Foto eines/r MitarbeiterIn auf der Webseite oder im Intranet (wenn kein betriebliches überwiegendes Interesse besteht), Verarbeitungen mit rein freiwilligem, sozialem Charakter wie die Teilnahme an freiwilligen gemeinsamen Ausflügen und damit verbundene Bilddokumentationen etc.

Eine Übermittlung der im jeweiligen Einzelfall relevanten Daten an Dritte erfolgt nur auf Grundlage der gesetzlichen Bestimmungen, insbesondere nach den §§ 8b und 30b BAG bzw. gemäß vertraglichen Vereinbarungen (so z. B. Krankenstände zur Berechnung der Ausbildungsbeihilfe durch das AMS). Abhängig von der Gestaltung der öffentlich-rechtlichen Förderung ist dabei möglich, dass solche Übermittlungen im Rahmen einer Auftragsverarbeitung stattfinden, die ein Träger im Auftrag des Fördergebers vornimmt (zur datenschutzrechtlichen Rollenverteilung siehe oben Punkt 4.2.4. Mehrfachrollen desselben Akteurs).

Der Träger hat im Rahmen seiner Dokumentation nach Artikel 30 DSGVO die Differenzierung nachvollziehbar zu machen, welche Verarbeitungstätigkeiten in seiner eigenen Verantwortung erfolgen und welche Verarbeitung er als Auftragsverarbeiter – unter Bezeichnung des Verantwortlichen – durchführt. Im Rahmen der Erfüllung seiner Informationspflichten hat der Träger gegenüber den Betroffenen (MitarbeiterInnen) nachvollziehbar im durch Artikel 13 und 14 DSGVO vorgeschriebenen Umfang für die Betroffenen klar erkennbar zu machen, welche Verarbeitungstätigkeiten der Träger als

Verantwortlicher durchführt und welche Verarbeitungstätigkeiten der Träger nur als Auftragsverarbeiter für einen Auftrag-/Fördergeber verarbeitet.

6. Auftragsverarbeitung und Informationspflichten

Im Sinne der Rechenschaftspflicht hat jeder Träger die Erfüllung der Informationspflicht entsprechend zu dokumentieren.

Gibt es keine Vorgaben durch einen Auftrag-/Fördergeber, trifft die Informationspflicht primär den Auftrag-/Fördergeber als datenschutzrechtlich Verantwortlichen, und hat der Träger mit diesem Rücksprache zu halten sowie gegebenenfalls bei der ordentlichen Erfüllung der Informationspflichten mitzuwirken.

Darüber hinaus hat der Träger eigenständig Informationen zur Verarbeitung personenbezogener Daten in seiner Verantwortung zu erteilen. Dies betrifft insbesondere sicherheitsrelevante Aufzeichnungen (Benutzerkennzeichen, Zutrittskontrolle etc.), Datenverarbeitungen zur Durchführung eigener Verträge mit den Betroffenen, insbesondere im Zuge von Personen-Zertifizierungen.

Falls ein Träger in zulässiger Weise von Betroffenen, zu denen er ansonsten als Auftragsverarbeiter in Beziehung steht, eine Einwilligung (Art 4 Z 11 DSGVO) für legitime Zwecke einholt, hat er das Koppelungsverbot des Art 7 Abs. 4 DSGVO besonders zu beachten. Eine solche Einwilligung hat zur Klarstellung, dass keine unzulässige Koppelung zur Auftragsverarbeitung besteht, einen entsprechenden Hinweistext wiederzugeben. Das AMS hat hierzu einen Vorschlag im Rahmen der Standardverträge mit den Trägern vorgelegt:

„*Ich wurde darüber informiert, dass diese Verarbeitungen nicht für Zwecke des AMS erfolgen und dass der Fördergeber diese Verarbeitung nicht beauftragt hat. Die Verweigerung einer Einwilligung führt zu keinen Konsequenzen aus dem Arbeitslosenversicherungsgesetz, dem Arbeitsmarktservicegesetz oder anderen gesetzlichen Grundlagen zur Förderung der Bildungsmaßnahme*."

6.1. Dokumentation der Auftragsverarbeitung

Der Träger hat für vorliegende Auftragsverarbeitungen ein Verzeichnis von Verarbeitungstätigkeiten (Verarbeitungsverzeichnis) nach Art 30 Abs. 2 DSGVO zu errichten. Des Weiteren unterstützt der Träger den Auftrag-/Fördergeber bei Erstellung und Fortschreibung seines Verarbeitungsverzeichnisses im Zusammenhang mit der beauftragten Verarbeitung. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Verantwortlichen auf Anforderung unverzüglich zuzuleiten. Falls eine Verarbeitung für andere rechtmäßige Zwecke außerhalb der Auftragsverarbeitung erfolgt, sind die entsprechenden Anwendungen gemäß Art 30 Abs. 1 DSGVO im Verzeichnis der Verarbeitungstätigkeiten unter Bezeichnung des Verantwortlichen zu dokumentieren. Der Träger hat – falls erforderlich auch auf eigene Initiative – mit jedem Auftrag-/Fördergeber einen schriftlichen Vertrag zur Verarbeitung der personenbezogenen Daten im Auftrag des Auftrag-/Fördergebers mit allen zwingenden Inhalten gemäß Art 28 Abs. 3 DSGVO abzuschließen.

6.1.1. Exkurs: Einsatz von Sub-Auftragsverarbeitern und andere Formen der Zusammenarbeit

Sub-Auftragsverarbeiter sind ausschließlich solche Unternehmen, deren Leistungen einen direkten Zusammenhang mit der Erbringung der durch den Auftrag-/Fördergeber an einen Träger in Auftrag gegebenen Hauptleistung aufweisen und die zur Leistungserbringung personenbezogene Daten der TeilnehmerInnen verarbeiten müssen.

Der Einsatz von Sub-Auftragsverarbeitern zur Erfüllung des Auftrags ist zulässig, wenn

- der Träger eine solche Inanspruchnahme dem Auftrag-/Fördergeber eine angemessene Zeit (zwei Wochen) vorab schriftlich mitteilt und
- falls der Auftrag-/Fördergeber den Einsatz von Sub-Auftragsverarbeitern bereits grundsätzlich schriftlich genehmigt hat nicht bis zum Zeitpunkt des Einsatzes schriftlich Einspruch gegen die konkret mitgeteilten Sub-Auftragsverarbeiter erhebt oder ansonsten eine ausdrückliche schriftliche Zustimmung zur Heranziehung der konkret mitgeteilten Sub-Auftragsverarbeiter erteilt und
- der Träger eine Vereinbarung im Sinne des Art 28 Abs. 4 DSGVO mit dem Sub-Auftragsverarbeiter abschließt. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Träger auf Grund dieser Vereinbarung obliegen.

Die Vereinbarungen hat der Träger nach Aufforderung unverzüglich dem Auftrag-/Fördergeber vorzulegen. Kommt der Sub-Auftragsverarbeiter seinen aus dem Datenschutzrecht erwachsenden Pflichten nicht nach, so haftet der Träger als erster Auftragsverarbeiter gegenüber dem Auftrag-/Fördergeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

Nicht in die Rolle eines (Sub-)Auftragsverarbeiters fallen jedoch Unternehmen/Träger, soweit sie aufgrund eines Vertrages unmittelbar mit dem/r TeilnehmerIn eine Personenzertifizierung durchführen (z. B. ECDL, Österreichisches Sprachdiplom, Staplerführerschein, andere Schulungsunternehmen, Akkreditierungsstellen, Prüfungsabnahme-Stellen, WKO etc.). Diese sind im Hinblick auf die den/die TeilnehmerIn betreffenden Datenverarbeitungen daher selbst „Verantwortliche“.

Partner (Träger) einer Bietergemeinschaft, die in Vergabeverfahren gemeinsam zur Beauftragung einer Bildungsdienstleistung benannt wurden, sind keine Sub-Auftragsverarbeiter. Diese sind bei Zustandekommen eines Vertrages mit dem Auftrag-/Fördergeber datenschutzrechtlich als eigenständige Auftragsverarbeiter des Auftrag-/Fördergebers zu betrachten.

Einzelpersonen, die auf Basis eines freien Dienstvertrages oder eines Werkvertrages als TrainerIn arbeiten, und die über keine für Träger typische betriebliche Struktur verfügen, gelten nicht als Sub-Auftragsverarbeiter. Diese sind datenschutzrechtlich als MitarbeiterIn des Trägers zu behandeln, sie sind also einerseits selbst Betroffene und handeln auf Rechnung und Gefahr des Dienstgebers (des Trägers), der für dieses Handeln in der Rolle des Verantwortlichen oder in der Rolle des Auftragsverarbeiters haftet. Daher entfällt auch die Pflicht einer schriftlichen Mitteilung vor Inanspruchnahme. Es ist von solchen Personen

jedenfalls eine Verschwiegenheits-Verpflichtungserklärung zur Wahrung des Datengeheimnisses gemäß § 6 DSG einzuholen.

6.1.2. Datenaustausch mit dem Auftraggeber/Fördergeber

Für die Kommunikation mit dem Auftrag-/Fördergeber über personenbezogene Daten von TeilnehmerInnen im Rahmen der Projektumsetzungen sind die durch den Auftrag-/ Fördergeber bereitgestellten, sicheren Übertragungswege zu nutzen. Beispielsweise hat das AMS als der in der Praxis mit Abstand bedeutendste Auftrag-/Fördergeber mit dem eAMS hierfür entsprechende Services geschaffen, die nach den Vorgaben des AMS auch zwingend zu nutzen sind. Ein Informationsaustausch zu personenbezogenen Daten via E-Mail ist daher im Regelfall nicht vorgesehen. Dies gilt insbesondere für sensible Daten zum Gesundheitszustand von TeilnehmerInnen, Berichte, Lebensläufe, Prüfungserfolge etc.

Sofern der Auftrag-/Fördergeber keinen sicheren Übertragungsweg zur Verfügung stellt bzw. eine Übermittlung der Daten via E-Mail wünscht, wird er vom Träger vor der Übermittlung auf das Risiko hingewiesen.

Vom Auftrag-/Fördergeber einlangende E-Mails mit personenbezogenen Inhalten betreffend TeilnehmerInnen (z. B. mit Zubuchungslisten, TeilnehmerInnen-Informationen, Sozialversicherungsnummern etc.) sind umgehend nach Bearbeitung zu löschen. Die für die weitere Kursdurchführung relevanten Informationen sind als Dokument in den vom Träger dafür vorgesehenen Ablagesystemen zur Dokumentation zu speichern (damit unterliegen diese einer unternehmensintern vorzusehenden Löschroutine gemäß den Auftraggeber-Vorgaben).

Einzelanfragen des Auftrag-/Fördergebers per E-Mail bzw. telefonischer Kommunikation: Wenn eine Datenübermittlung über die speziellen, sicheren Übertragungswege aus zeitlichen oder sonstigen Gründen nicht möglich ist, oder wenn der betreffende Kommunikationspartner (ausnahmsweise) nicht über den vorgesehenen Übertragungskanal erreichbar ist, sind vor dem Hintergrund einer zeitökonomischen Zusammenarbeit auf Anfrage des Auftrag-/ Fördergebers weiterhin E-Mail-Kommunikation und/oder telefonischer Kontakt zulässig. In diesen Fällen ist die Anordnung eines bestimmten, weniger sicheren Kommunikationskanals als Weisung des Verantwortlichen gegenüber dem Auftragsverarbeiter zu verstehen. Festzuhalten ist, dass sich der Umfang und die Art der zu übermittelnden Daten aus den Förderverträgen und den Aufträgen im Rahmen der für die Auftrag-/Fördergeber einschlägigen gesetzlichen Grundlagen (insbesondere § 25 AMSG) richtet.

Eine dementsprechende Datenübermittlung bzw. ein Informationsaustausch ist unter folgenden Bedingungen zulässig:

- Telefonische Anfragen eines/r MitarbeiterIn des Auftrag-/Fördergebers können weiterhin telefonisch beantwortet werden, wenn seitens des Trägers kein Zweifel daran besteht, dass der/die KommunikationspartnerIn ein/e zur Datenerhebung befugte/r MitarbeiterIn des Auftrag-/Fördergebers ist, d. h., es ist sicherzustellen, dass es sich hierbei auch tatsächlich um eine/n MitarbeiterIn des Auftrag-/Fördergebers handelt (z. B. Telefonnummer am Display oder persönlich bekannt).
- Im Fall von Einzelanfragen eines/r MitarbeiterIn des Auftrag-/Fördergebers per E-Mail (z. B. über die Anwesenheit eines/r TeilnehmerIn) kann der Kommunikationsweg per

E-Mail verwendet werden, sofern der/die MitarbeiterIn des Auftrag-/Fördergebers dies vorab gewünscht hat. Eine schriftliche Aufforderung durch einen Auftrag-/Fördergeber per Rundschreiben an die Träger ist dem gleichzuhalten.

- Eine Informationserteilung durch MitarbeiterInnen des Trägers per unverschlüsselter E-Mail ohne vorherige Anfrage bzw. Wunsch seitens des Auftrag-/Fördergebers ist jedenfalls unzulässig.
- Per unverschlüsselter E-Mail dürfen keine sensiblen Daten übermittelt werden (z. B. Gesundheitsdaten, wobei darunter nicht die Bekanntgabe eines Krankenstandes zu verstehen ist, da hierbei nur eine Statusmeldung ohne Diagnose erfolgt).
- Im Falle eines Informationsaustausches per E-Mail ist der gesamte E-Mail-Verkehr, der personenbezogene Daten enthält, zu demselben Betreff umgehend nach Bearbeitung zu löschen. Die für die weitere Kursdurchführung relevanten Informationen sind in den vom Träger dafür vorgesehenen Ablagesystemen zur Dokumentation zu speichern (damit unterliegen diese der Löschroutine).

7. Wahrnehmung der Betroffenenrechte von TeilnehmerInnen an Bildungsmaßnahmen

7.1. Betroffenenrechte im Verhältnis zwischen Träger und Auftrag-/Fördergebern

Wird ein Antrag auf Auskunft an einen Träger gerichtet, hat dieser nach der Auftragsverarbeitungsvereinbarung im Innenverhältnis zu prüfen, ob er eine DSGVO-konforme Auskunft auch über die im Auftrag des Auftrag-/Fördergebers verarbeiteten Daten direkt zu erteilen hat. Der Auftrag-/Fördergeber ist zeitgleich über eine direkte Auskunft an den Betroffenen zu informieren, soweit dies nach dem Innenverhältnis zulässig ist.

Lässt der Antrag auf Auskunft erkennen, dass auch Daten beauskunftet werden sollen, die direkt durch den Auftrag-/Fördergeber verarbeitet werden, darf der Träger den Antrag unverzüglich an den Auftrag-/Fördergeber als datenschutzrechtlich Verantwortlichen weiterleiten und dies dem Antragsteller mitteilen.

Soweit das Auskunftsersuchen Daten des Anfragenden betrifft, die zwar im Auftrag des Auftrag-/Fördergebers aber – zum Zeitpunkt der Anfrage – ausschließlich in den Systemen des Trägers verarbeitet werden, besteht eine Wahlfreiheit seitens des Trägers: Er kann die Anfrage entweder gemeinsam mit solchen Daten an den Auftrag-/Fördergeber weitergeben, der die Auskunft selbst vornimmt, oder der Träger führt die Auskunft über die diesbezüglichen Daten selbst durch und informiert den Auftrag-/Fördergeber und datenschutzrechtlich Verantwortlichen über die erfolgte Auskunft. Der betroffenen Person dürfen im Außenverhältnis jedenfalls keine Nachteile entstehen, die die Ausübung ihrer Betroffenenrechte erschweren.

Der Träger ist durch den Auftrag-/Fördergeber im Rahmen der Vereinbarung zur Auftragsverarbeitung zusätzlich ermächtigt, einer betroffenen Person, Einsicht über die von ihm zu dieser Person verarbeiteten Daten zu geben. Sofern Zweifel an der Identität der betroffenen Person bestehen, kann die betroffene Person ihre Identität gemäß Punkt 7.2.1. der BABE CoC nachweisen.

Bei Anträgen auf Berichtigung und Löschung ist sinngemäß vorzugehen. Wird ein Antrag auf Berichtigung, Löschung oder Einschränkung der Verarbeitung und Widerspruch eingebracht, dann ist dieser in Bezug auf die Daten, die für den Auftrag-/Fördergeber verarbeitet werden, an den Auftrag-/Fördergeber unverzüglich weiterzuleiten und dies dem Antragsteller mitzuteilen.

7.2. Wahrnehmung des Rechts auf Auskunft durch TeilnehmerInnen an Bildungsmaßnahmen

Die DSGVO enthält in Art 15 ein Recht auf Auskunft der betroffenen Person (z. B. Kunde, MitarbeiterIn, StellenbewerberIn, PatientIn, im Weiteren kurz „Betroffener“) gegenüber dem Verantwortlichen. Sinn und Zweck dieses Rechts ist es, kurz zusammengefasst, dass sich der Betroffene über den Inhalt und die näheren Umstände der über ihn verarbeiteten Daten informieren kann, mit dem Ziel, eventuell weitere Betroffenenrechte geltend zu machen bzw. die Rechtmäßigkeit der Verarbeitung zu kontrollieren. Die nachfolgenden Ausführungen geben die Rechtslage nach der DSGVO unter Berücksichtigung der Erwägungsgründe wieder und sollen vor allem dem Verständnis und der Klarheit dienen.

Es besteht kein Formzwang. Das Auskunftsbegehren kann mündlich, schriftlich oder in digitaler Form gestellt werden (z. B. per E-Mail). Die Beantwortung eines Auskunftsverlangens kann in jeder angemessenen Form erfolgen, wobei jedoch Folgendes zu beachten ist:

- Eine schriftliche Anfrage wird am besten schriftlich beantwortet. Eine gängige Methode ist es, dass der Auskunftswerber seinem Antrag eine Kopie eines Identitätsnachweises (amtlicher Ausweis) beilegt und der Verantwortliche die Beantwortung durch Zustellung mittels eingeschriebenen Briefs erfolgt.
- Falls vom Auskunftswerber verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde.
- Stellt die betroffene Person den Antrag elektronisch (z. B. per E-Mail), so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts anderes angibt. Nach Möglichkeit kann der Verantwortliche auch den Fernzugang zu einem sicheren System bereitstellen, der der betroffenen Person direkten Zugang zu ihren personenbezogenen Daten ermöglicht. Ein sicheres System bedeutet, dass der Träger auf eigenen IT Systemen oder durch Beauftragung eines geeigneten Dienstleisters einen in seiner Kontrolle befindlichen Datenspeicher zur Verfügung stellt, auf den die betroffene Person über das Internet über eine verschlüsselte Verbindung (Transportverschlüsselung) auf die sie betreffenden Daten zugreifen kann. Die Absicherung hat zumindest durch einen Nutzernamen und ein Passwort zu erfolgen, welche zuverlässig nur der betroffenen Person auf einem nach außen sicheren Übertragungskanal übergeben werden.

Alle Mitteilungen sind in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Dies gilt insbesondere für Informationen, die sich speziell an Jugendliche richten. Wie schon bisher sind in den Daten enthaltene Abkürzungen etc. dem Betroffenen in der Auskunftsbeantwortung zu erklären.

7.2.1. Identitätsnachweis des Auskunftswerbers

Es ist davon auszugehen, dass die Identität des Auskunftswerbers (betroffene Person) klar sein muss, da der Verantwortliche zusätzliche Informationen anfordern kann, wenn er „begründete Zweifel“ an der Identität der natürlichen Person, die den Antrag stellt, hat.[1]

Der Verantwortliche soll alle vertretbaren Mittel nutzen, um die Identität einer Auskunft suchenden betroffenen Person zu überprüfen, insbesondere im Rahmen von Online-Diensten und im Fall von Online-Kennungen. Die Identitätsfeststellung sollte so ausgestaltet sein, dass sie die Pflicht erfüllt, eine dem jeweiligen Risiko angemessene Datensicherheit zu gewährleisten, sonst könnte es zu einer Datenschutzverletzung/einem Data Breach kommen, wenn die Daten einem unbefugten/falschen Empfänger übermittelt werden.

Eine zulässige Praxis ist beispielsweise, dass der Auskunftswerber seinem Antrag eine Kopie eines Identitätsnachweises (amtlicher Ausweis) beilegt und der Verantwortliche die Beantwortung als „eigenhändig“ zuzustellendes Einschreiben (unter Ausschluss von Zustellbevollmächtigten) mit der Post übermittelt. Die Identität kann jedoch auch aus der Situation klar sein, z. B. wenn mit dem Auskunftswerber laufender Kontakt besteht und dieser (und dessen Adresse) daher bekannt ist.[2]

7.2.2. Kostenersatz

Die Auskunft wird grundsätzlich unentgeltlich erteilt (siehe Art 12 Abs 5 DSGVO). Bei offenkundig unbegründeten oder insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person – kann der Verantwortliche jedoch entweder
a) ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder
b) sich weigern, aufgrund des Antrags tätig zu werden.

7.2.3. Berücksichtigung der Rechte Dritter bei der Auskunftserteilung

Art 15 Abs. 4 DSGVO sieht vor, dass das Recht auf Erhalt einer Kopie die Rechte und Freiheiten anderer Personen nicht beeinträchtigen darf. An dieser Stelle wird auch auf § 4 Abs. 6 DSG verwiesen, welcher festlegt, dass das Recht auf Auskunft der betroffenen Person gemäß Art. 15 DSGVO gegenüber einem Verantwortlichen unbeschadet anderer gesetzlicher Beschränkungen in der Regel dann nicht besteht, wenn durch die Erteilung dieser Auskunft ein Geschäfts- oder Betriebsgeheimnis des Verantwortlichen bzw. Dritter gefährdet würde. Dies darf jedoch nicht dazu führen, dass der betroffenen Person jegliche Auskunft verweigert wird.

[1] Siehe Art. 12 Abs 6; so auch *Souhrada-Kirchmayer*, Das Auskunftsrecht nach der DSGVO, in Jahnel [Hrsg], Jahrbuch 17. Datenschutzrecht [2017] 86 f).

[2] Siehe dazu die Rechtsprechung: VwGH 4.7.2016, Ra 2016/04/0014; OGH 25.2.1993, 6 Ob 6/93).

Es ist daher erforderlich, die zu beauskunftenden Daten zu kontrollieren, im Regelfall werden personenbezogene Daten Dritter (z. B. der Name des Sachbearbeiters/der Sachbearbeiterin, der/die den Kunden betreut hat und in der Kundenkartei angeführt ist) aus der Datenkopie zu schwärzen, bzw. sofern dies nicht möglich ist, zu löschen sein.

Rechte Dritter können insbesondere dann einen Auskunftsanspruch beschränken, wenn die konkret verarbeiteten Daten im Hinblick auf den Dokumentationszweck personenbezogene Daten anderer Betroffener (Dritter) enthalten, diese Datensätze in einer bestimmten Verarbeitungsform nicht voneinander trennbar sind und zugleich kein legitimes Interesse des Auskunftswerbers besteht, die Daten der anderen Betroffenen einzusehen (z. B. bei Teilnahmelisten, die in Papierform als Nachweis der Anwesenheit von allen TeilnehmerInnen im Rundlauf zur Unterschrift durchgegeben werden).

7.2.4. Wahrnehmung des Rechts auf Datenübertragbarkeit durch TeilnehmerInnen an Bildungsmaßnahmen

Das Recht auf Datenübertragbarkeit besteht im Hinblick auf solche Daten, die der Betroffene selbst in den Systemen des Trägers erzeugt hat. Dies betrifft insbesondere Lebensläufe und Bewerbungsschreiben des Betroffenen. Solche Dokumente sind den Betroffenen im Format, in dem diese erstellt wurden, auch in gängiger elektronischer Form zu überlassen.

7.2.5. Wahrnehmung des Rechts auf Löschung durch TeilnehmerInnen an Bildungsmaßnahmen

Sofern eine betroffene Person ihr Recht auf Löschung im Hinblick auf bestimmte, sie betreffende Daten geltend macht, hat der Träger unverzüglich zu prüfen, ob dem Träger im Hinblick auf die adressierte Datenanwendung die Rolle des Verantwortlichen zukommt. Falls sich das Löschbegehren auf eine Verarbeitungstätigkeit bezieht, die für den Träger eine Auftragsverarbeitung darstellt, hat der Träger das Begehren unverzüglich dem Verantwortlichen weiterzuleiten und das Datum zu bezeichnen, an dem das Begehren dem Träger zugegangen ist. Selbiges gilt auch, wenn die Löschung auf sämtliche Daten gerichtet ist. Über eine solche Weiterleitung an den Verantwortlichen ist die betroffene Person unverzüglich, jedoch längstens binnen einer Woche ab Antragstellung zu verständigen. Die Verständigung hat die korrekte Bezeichnung und die Kontaktdaten des Verantwortlichen sowie das Datum der Weiterleitung des Löschbegehrens an den Verantwortlichen zu enthalten.

8. Risikoanalyse und technisch-organisatorische Maßnahmen (TOM) der Träger

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

8.1. Anforderungen gemäß Art 32 Abs. 2 DSGVO

Die Träger werden die erforderlichen technischen und organisatorischen Maßnahmen unter Berücksichtigung

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

treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Bei der Risikoanalyse werden physische, materielle und immaterielle Schäden berücksichtigt, zu denen die Verarbeitung personenbezogener Daten führen kann (vgl. dazu ErwGr 75). Folgende Risiken sind dabei branchentypisch im Hinblick auf die möglichen physischen, materiellen oder immateriellen Schäden und daher im Rahmen der TOM jedes Trägers zu adressieren:

1. **Diskriminierung**: Es besteht potentiell das Risiko einer Diskriminierung aufgrund der ausgewerteten Daten insbesondere hinsichtlich der Herkunft und aufgrund von Aspekten, die die wirtschaftliche/berufliche/gesundheitliche Lage bzw. das Verhalten betreffen (diese können analysiert oder prognostiziert werden, um persönliche Profile zu erstellen bzw. zu nutzen).

2. **Rufschädigung:** Szenarien einer Rufschädigung sind denkbar, wenn bestimmte Informationen aus der Datenverarbeitung des Trägers an unbefugte Personen geraten. Letztlich ist diese Art des Schadens sehr subjektiv. Es hängt von der besonderen Situation des Betroffenen ab, ob das Bekanntwerden des Umstands, dass diese Person eine bestimmten Bildungsmaßnahme absolviert, oder das Bekanntwerden bestimmter Informationen aus dem Zusammenhang mit der Bildungsmaßnahme für diesen Betroffenen nachteilige Folgen hat. Das Faktum, dass jemand z. B. an einer AMS Maßnahme teilnimmt, in einem sozialökonomischen Betrieb beschäftigt ist oder eine überbetriebliche Lehrausbildung bei einem Träger absolviert, kann – vor allem in Zusammenhang mit den Umständen, warum ein Betroffener diesen Vermittlungsweg/Bildungsweg eingeschlagen hat – zu einer rechtlich relevanten Rufschädigung führen.

3. **Andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile:** Aufzeichnungen und Rückmeldungen der Träger können darüber entscheiden, ob der Betroffene Unterstützungsleistungen im vollen Umfang weiter erhalten. Zwar ist dieser Aspekt den durch die Träger übernommenen Aufgaben häufig geradezu immanent, weil ja insbesondere gegenüber Fördergebern oder Auftraggebern in der Regel eine Verpflichtung besteht, solche Aufzeichnungen zu führen und zurückzumelden. Dennoch bedeutet diese (notwendige) Verarbeitung für die Betroffenen ein Risiko. Für die Träger bedeutet dies, dass

insbesondere die Richtigkeit der Daten zu gewährleisten ist und auch die Vertraulichkeit entsprechend zu wahren ist.

4. **Einschränkung der Rechte**: Es können Entscheidungen erfolgen, die den Betroffenen gegenüber rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen können.

5. **Identitätsdiebstahl**: Aus der Sicht der Betroffenen liegt das Risiko eines Identitätsdiebstals nicht ausschließlich in den Auswirkungen im Zusammenhang mit der Datenverarbeitung durch den Träger begründet. Vielmehr geht es darum, dass in der vorliegenden Anwendung eine große Zahl an Informationen zu Personen vorliegen, die es einem böswilligen Täter ermöglichen würden, in Verbindung mit anderen Informationen und Tathandlungen einen schweren Identitätsdiebstahl zu begehen. Die besonders im Bereich der Cyberkriminalität schwerwiegenden Fälle sind typischerweise komplexe, über längere Zeiträume verteilte und oft für sich genommen unscheinbare einzelne Angriffe, die in Summe schwere Schäden mit sich bringen können (sog. Advanced Persistent Threats, APT).

   In dieser Hinsicht ist der wichtigste und effektivste Grundsatz der Datenminimierung in der Umsetzung der vorliegenden Anwendung optimiert. Initial sowie bei jeder künftigen Ergänzung wird genau geprüft, ob ein Datum notwendig ist und die Pseudonymisierung optimiert ist. Der Kreis der Zugangsberechtigten ist strikt eng gehalten, wodurch auch die Integrität der Daten bestmöglich gewährleistet wird.

6. **Überwachung des höchstpersönlichen Lebensbereichs**: Mit der Durchführung von Bildungsmaßnahmen geht nicht selten einher, dass im Rahmen einer persönlichen Betreuung Betroffene auch Daten und Informationen aus ihrem höchstpersönlichen Lebensbereich preisgeben. Insbesondere im Verhältnis zu einem unmittelbaren Betreuer kann ein Vertrauensverhältnis entstehen.

8.2. Faktoren der Risikoerhöhung

Grundsätzlich birgt jede Verarbeitungstätigkeit ein Risiko, es bestehen jedoch risikoerhöhende Verarbeitungsvorgänge die ebenfalls in Erwägungsgrund 75 aufgezählt[3] werden:

8.2.1. Allgemeine Faktoren der Risikoerhöhung

1. **Profilerstellung (Bewertung persönlicher Aspekte):** Persönliche Aspekte können hier verarbeitet werden, die sich auf eine natürliche Person beziehen, um diese zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen

[3] Hinweis: Die Einstufung als risikoerhöhender Verarbeitungsvorgang führt jedoch nicht automatisch dazu, dass ein hohes Risiko im Sinne der DSGVO vorliegt.

Person zu analysieren oder vorherzusagen. Dazu zählen insbesondere Aufzeichnungen über die Abwesenheit von TeilnehmerInnen, bei denen auch persönliche/private Gründe (z. B. Krankheit) mit aufgezeichnet werden und einer systematischen Auswertung (z. B. tabellarisch festgehalten und vergleichbar) zugänglich sind. Die Verwendung des Worts „Bewertung“ legt nahe, dass es beim Profiling um eine Art Einschätzung oder Beurteilung einer Person geht. Die Profilerstellung kann auch unabhängig vorliegen, ob die Prozesse dazu gänzlich oder auch nur teilweise automatisiert sind. Zwar sind die hier beispielhaft genannten Aufzeichnungen branchentypisch, nicht typisch ist jedoch, dass Träger mit solchen Aufzeichnungen Profile erstellen.

Von der Frage, ob eine Profilerstellung vorliegt, sollte auch getrennt werden, ob an die Zuordnung von Profilen zu Personen automatisierte Einzelentscheidungen geknüpft werden. Wenn auch diese Elemente und damit ein Profiling im Sinne des Art 22 DSGVO vorliegt, ist ohnehin eine Folgenabschätzung nach Art 35 DSGVO erforderlich.

2. **Automatisierte Einzelentscheidung:** Verarbeitungen, die eine Bewertung oder Einstufung natürlicher Personen – einschließlich des Erstellens von Profilen und Prognosen – umfasst für Zwecke, welche die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben und Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel der Person betreffen und ausschließlich auf einer automatisierten Verarbeitung beruhen und negative rechtliche, physische oder finanzielle Auswirkungen haben können.

8.2.2. Branchentypische Faktoren der Risikoerhöhung

1. **ArbeitnehmerInnen/Jugendliche:** Verarbeitung von Daten besonders schutzbedürftiger Personen (insb. Kinder/Minderjähriger und ArbeitnehmerInnen): Es erfolgt eine Verarbeitung von personenbezogenen Daten schutzbedürftiger Personen. Träger könnten ihre Position als Erfüllungsgehilfen des AMS missbrauchen und dem Betroffenen – unter Missachtung des Koppelungsverbots – eine Einwilligung zur rein privatwirtschaftlichen Datenverwendung abverlangen oder Daten aus der Auftragsverarbeitung für eigene Zwecke ohne Rechtsgrundlage missbrauchen.

2. **Verarbeitung sensibler (besondere Kategorien personenbezogener) Daten:** Erfolgt teilweise, um Einschränkungen, die die Arbeitsfähigkeit bzw. Ausbildungsfähigkeit betreffen, gebührend berücksichtigen zu können. Hierzu zählen vor allem Aufzeichnungen über die Gründe einer Abwesenheit von einer Bildungsmaßnahme.

3. **Große Reichweite (große Datenmenge, große Anzahl Betroffener):** Eine große Reichweite könnte vorliegen und bildet ein Kriterium für die Durchführung der vorliegenden Datenschutz-Folgenabschätzung.

8.3. Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit/Belastbarkeit als Schutzziele gemäß Artikel 32 Abs. 1 lit b DSGVO

Risiken für die Rechte und Freiheiten der betroffenen Personen und daraus resultierender potenzieller Folgen, können u. a. vorliegen, wenn die Gewährleistung folgender Schutzziele aus dem Bereich der Datensicherheit gemäß Artikel 32 Abs. 1 lit b DSGVO gefährdet sein könnte:

1. **Wahrung der Vertraulichkeit:** Welche Auswirkungen der Verlust der Vertraulichkeit für die einzelnen TeilnehmerInnen hat, lässt sich allgemein nur für bestimmte Problemstellungen beschreiben. Darüber hinaus kann es für die TeilnehmerInnen im Einzelfall jeweils spezifische, in der konkreten Person begründete Gründe geben, warum ein Verlust der Vertraulichkeit nachteilige Auswirkungen für sie hat. Die typischerweise bestehenden Risiken sind: Rufschädigung, erhebliche wirtschaftliche oder gesellschaftliche Nachteile, Einschränkung von Rechten oder ein Eingriff in den Kernbereich der Intimsphäre (in Bezug auf „sensible Daten“). In einzelnen Projekten ist auch denkbar, dass durch den Verlust der Vertraulichkeit eine Verletzung einer gesetzlichen Verschwiegenheitspflicht („Berufsgeheimnis“, z. B. nach Ärztegesetz, Psychotherapiegesetz etc.) eintritt. Ein Spezialfall des Verlusts der Vertraulichkeit ist die **unbefugte Aufhebung der Pseudonymisierung.**

2. **Wahrung der Datenverfügbarkeit/Belastbarkeit:** Die Verletzung der Datenverfügbarkeit/Belastbarkeit, hat für betroffene TeilnehmerInnen möglicherweise Auswirkungen auf den rechtzeitigen Erhalt von Zahlungen.

3. **Wahrung der Integrität der Daten**: Daten werden ungewollt oder gewollt aber ohne Befugnis geändert. Die Auswirkungen der Verletzung der Datenintegrität können unterschiedlich sein. So können manipulierte Daten Auswirkungen auf den Erhalt von Zahlungen durch das AMS dem Grunde nach oder hinsichtlich der Höhe haben. Dies könnte in Konstellationen der Fall sein, in denen sich unbefugte Personen Zugriff auf personenbezogene Daten verschaffen und diese verändern oder zerstören.

8.4. Verpflichtende Maßnahmen

8.4.1. Risikoanalyse und Datenschutz-Folgenabschätzung – TOM

Es ist nach den oben genannten Kriterien eine Risikoanalyse zur Datenverarbeitung durchzuführen. Falls im Einzelfall erforderlich, ist eine Datenschutz-Folgenabschätzung gemäß Art 35 DSGVO durchzuführen. Für andere Auftragsverarbeitungen ist zu prüfen, ob eine vergleichbare, privatautonom vereinbarte Verpflichtung existiert.

Eine Datenschutz-Folgenabschätzung ist gemäß Art 35 DSGVO erforderlich, wenn eine Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen birgt. Von den in Art 35 Abs. 3 DSGVO sowie ErwGr 91 enthaltenen und von der Art-29-Datenschutzgruppe zusammengestellten Kriterien zur Beurteilung, ob ein hohes Risiko besteht, sind im vorliegenden Zusammenhang insbesondere folgende Kriterien relevant:

- Verarbeitung besonderer Kategorien personenbezogener Daten oder sonst besonders vertraulicher Daten nicht nur im Einzelfall
- Bewerten persönlicher Aspekte natürlicher Personen (allerdings grundsätzlich nicht in automatisierter Form)
- Abhängig von der Anzahl der betroffenen Personen: Datenverarbeitung in großem Umfang

Ein Träger hat daher ab einer bestimmten Größe, d. h., abhängig von der Anzahl der Personen, die pro Jahr von seiner Datenverarbeitung betroffen sind, eine Datenschutz-Folgenabschätzung durchzuführen sofern der Träger Verantwortlicher der Datenverarbeitung ist oder vom Verantwortlichen an den Träger als Auftragsverarbeiter eine entsprechende Verpflichtung auferlegt wird. Bei einer Verarbeitung von 10.000 betroffenen Personen pro Jahr und mehr liegt auf jeden Fall eine Verarbeitung im großen Umfang vor. Hinsichtlich der Datenschutz-Folgeabschätzung ist zu bemerken, dass die Datenschutzfolgeabschätzungs-Ausnahmenverordnung, BGBl. II Nr. 108/2018 (DSFA-AV) bereits kundgemacht wurde und unter https://www.dsb.gv.at/verordnungen-in-osterreich abrufbar ist. Zudem wurde die Verordnung über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V), BGBl. II Nr. 278/2018, bereits kundgemacht.

Diese Risikoanalyse bzw. Datenschutz-Folgenabschätzung und die technischen und organisatorischen Maßnahmen sind regelmäßig (spätestens alle drei Jahre) zu überprüfen und erforderlichenfalls anzupassen.

8.4.2. Mindestanforderungen an die Risikoanalyse

Bei der Risikoanalyse hat jeder Träger folgende Mindestanforderungen zu berücksichtigen:

1. Risikoanalyse liegt vor
2. Risikoanalyse ist schlüssig
   Schlüssig bedeutet: die wesentlichsten (zentralen) Risiken sind identifiziert bzw. definiert und durch eine oder mehrere technisch- organisatorische Maßnahme(n) adressiert (Erkennbarkeit des Zusammenhangs zwischen Risiko und Maßnahme zur besseren Beherrschung des Risikos).
3. Risikoanalyse ist vollständig
   Vollständig: Es müssen jedenfalls die zentralen Schutzziele des Art 32 Abs. 1 lit b DSGVO (Vertraulichkeit, Verfügbarkeit/Belastbarkeit und Integrität) durch bestimmte TOMs erkennbar adressiert sein. Außerdem muss eine – wie immer geartete – Bewertung der Risiken vorliegen. Diese kann (idealerweise) quantifiziert und in eine Skala eingeteilt sein oder zumindest in einer qualitativen (prosaisch ausgeführten) Beschreibung der Risikolage bestehen.

8.5. Risikomaßnahmenplan zur Sicherstellung der Vertraulichkeit, Verfügbarkeit und Belastbarkeit der Systeme

Nachfolgend steht eine Auflistung geeigneter **technischer und organisatorischer Maßnahmen** (TOM) zur Risikoreduktion. Diese dient der Unterstützung für die Identifikation und Beschreibung von risikoangemessenen Maßnahmen und ist keinesfalls als abschließende Aufzählung zu verstehen. Jeder Träger hat individuell für seinen Betrieb zu prüfen, welche weiteren Risiken – in Ergänzung des vorstehenden Katalogs – in seinem

Betrieb allenfalls bestehen und welche Maßnahmen – in Ergänzung der nachstehenden Vorschläge gesetzt werden, um den bestehenden und ausgewiesenen Risiken zu begegnen. Jeder Träger hat die für seinen Betrieb getroffenen technischen und organisatorischen Maßnahmen mit einer Risikoanalyse zu verbinden. Das bedeutet, dass die Risiken ausgewiesen werden müssen – allenfalls auch durch ausdrückliche Referenz auf den vorstehenden Katalog und die Nummerierung dort – und ein Bezug zwischen den technischen und organisatorischen Maßnahmen und den Risiken im Kontext der jeweiligen Schutzziele herzustellen ist.

Datenschutzschulungen:

Die mit der Verarbeitung personenbezogener Daten betrauten MitarbeiterInnen sind (ein)zu schulen und es sind zumindest alle drei Jahre Auffrischungsschulungen durchzuführen. Zusätzlich sind schriftliche Informationen den MitarbeiterInnen zum Datenschutz und zur Datensicherheit zur Verfügung zu stellen. Entsprechende Verpflichtungen zur Wahrung des Datengeheimnisses im Sinne des § 6 Datenschutzgesetzes sind vorzusehen.

Datensicherheit bei der elektronischen Kommunikation mit dem AMS:

Für die elektronische Kommunikation mit dem AMS sind die vertraglich vorgeschriebenen eServices des eAMS-Kontos zu verwenden. Die betroffenen MitarbeiterInnen sind darüber schriftlich zu informieren. Ausnahmen hierzu siehe 6.1.2.

Gemäß der Empfehlung der Datenschutzbehörde vom 17. Jänner 2018, GZ. DSB-D213.503/0004-DSB/2017 an das AMS betreffend Zugang auf das eAMS-Konto für Weiterbildungsinstitutionen („Partnerinstitutionen“) haben die Träger sicherzustellen, dass für das AMS tätige TrainerInnen über das eAMS-Konto nicht mehr auf die Geschäftsfälle aller anderen TrainerInnen und somit auf die Daten von deren KursteilnehmerInnen zugreifen können. Die eService „Projekt/Veranstaltungszuordnung“ des eAMS-Kontos ist daher zwingend zu verwenden und laufend zu warten. Als Grundlage ist ein Berechtigungskonzept zu erstellen.

Zugriffsbeschränkungen bei EDV-Geräten:

Es sind Vorkehrungen zu treffen, dass personenbezogene Daten auf EDV-Geräten, die von unterschiedlichen TeilnehmerInnen benutzt werden, vor unberechtigtem Zugriff geschützt sind. Dem Verlust von Daten wird u. a. durch regelmäßige Backups der Daten und redundante Datenhaltung entgegengewirkt.

Jeder Träger unterhält umfassende technisch-organisatorische Maßnahmen (verschlüsselte Verbindungen, Zugriffsbeschränkungen etc.), die einem Datenmissbrauch bzw. Datendiebstahl effektiv entgegenwirken.

Der Zugang zum Verwaltungsbereich erfordert zumindest ein Kennwort, wodurch eine Missbrauchsmöglichkeit vermieden bzw. jedenfalls stark reduziert wird. Initial sowie bei jeder künftigen Ergänzung wird genau geprüft, ob ein Datum notwendig ist und die Pseudonymisierung optimiert ist. Der Kreis der Zugangsberechtigten ist strikt eng gehalten („need to know“ Prinzip), wodurch auch die Integrität der Daten bestmöglich gewährleistet wird.

A. Vertraulichkeit gem. Art. 32 Abs. 1 lit b. DSGVO

Zutrittskontrolle

Folgende Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren, wurden getroffen.

- ☐ Alarmanlage
- ☐ Absicherung von Gebäudeschächten
- ☐ Automatisches Zugangskontrollsystem
- ☐ Chipkarten-/Transponder-Schließsystem
- ☐ Schließsystem mit Codesperre
- ☐ Manuelles Schließsystem
- ☐ Biometrische Zugangssperren
- ☐ Videoüberwachung der Zugänge
- ☐ Lichtschranken / Bewegungsmelder
- ☐ Sicherheitsschlösser
- ☐ Schlüsselregelung (Schlüsselausgabe etc.)
- ☐ Personenkontrolle beim Pförtner / Empfang
- ☐ Protokollierung der Besucher
- ☐ Sorgfältige Auswahl von Reinigungspersonal
- ☐ Sorgfältige Auswahl von Wachpersonal
- ☐ Tragepflicht von Berechtigungsausweisen

Zugangskontrolle

Folgende Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können, wurden getroffen.

- ☐ Zuordnung von Benutzerrechten
- ☐ Erstellen von Benutzerprofilen
- ☐ Passwortvergabe
- ☐ Authentifikation mit biometrischen Verfahren
- ☐ Authentifikation mit Benutzername / Passwort
- ☐ Zuordnung von Benutzerprofilen zu IT-Systemen
- ☐ Gehäuseverriegelungen
- ☐ Einsatz von VPN-Technologie
- ☐ Sperren von externen Schnittstellen (USB etc.)
- ☐ Sicherheitsschlösser
- ☐ Schlüsselregelung (Schlüsselausgabe etc.)
- ☐ Personenkontrolle beim Pförtner / Empfang

☐ Protokollierung der Besucher

☐ Sorgfältige Auswahl von Reinigungspersonal

☐ Sorgfältige Auswahl von Wachpersonal

☐ Tragepflicht von Berechtigungsausweisen

☐ Einsatz von Intrustion-Detection-Systemen

☐ Verschlüsselung von mobilen Datenträgern

☐ Verschlüsselung von Smartphone-Inhalten

☐ Einsatz von zentraler Smartphone-Administrations-Software (z. B. zum externen Löschen von Daten)

☐ Einsatz von Anti-Viren-Software

☐ Verschlüsselung von Datenträgern in Laptops / Notebooks

☐ Einsatz einer Hardware-Firewall

☐ Einsatz einer Software-Firewall

Zugriffskontrolle

Es sind Vorkehrungen zu treffen, dass personenbezogene Daten auf EDV-Geräten, die von unterschiedlichen TeilnehmerInnen benutzt werden, vor unberechtigtem Zugriff geschützt sind. Jeder Träger unterhält umfassende technisch-organisatorische Maßnahmen (verschlüsselte Verbindungen, Zugriffsbeschränkungen etc.), die einem Datenmissbrauch bzw. Datendiebstahl effektiv entgegenwirken. Der Zugang zum Verwaltungsbereich erfordert zumindest ein Kennwort, wodurch eine Missbrauchsmöglichkeit vermieden bzw. jedenfalls stark reduziert wird. Initial sowie bei jeder künftigen Ergänzung wird genau geprüft, ob ein Datum notwendig ist und die Pseudonymisierung optimiert ist. Der Kreis der Zugangsberechtigten ist strikt eng gehalten („need to know“ Prinzip), wodurch auch die Integrität der Daten bestmöglich gewährleistet wird.

Folgende Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, wurden getroffen.

☐ Erstellen eines Berechtigungskonzepts

☐ Verwaltung der Rechte durch Systemadministrator

☐ Anzahl der Administratoren auf das „Notwendigste“ reduziert

☐ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel

☐ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten

☐ Sichere Aufbewahrung von Datenträgern

☐ physische Löschung von Datenträgern vor Wiederverwendung

☐ ordnungsgemäße Vernichtung von Datenträgern

☐ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)

☐ Protokollierung der Vernichtung

☐ Verschlüsselung von Datenträgern

Trennungsgebot

Folgende Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können, wurden getroffen.

☐ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern

☐ Logische Mandantentrennung (softwareseitig)

☐ Verwendung der eServices des eAMS-Kontos

☐ Verwendung des eService „Projekt/Veranstaltungszuordnung“

☐ Erstellung eines Berechtigungskonzepts

☐ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden

☐ Versehen der Datensätze mit Zweckattributen/Datenfeldern

☐ Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System

☐ Festlegung von Datenbankrechten

☐ Trennung von Produktiv- und Testsystem

B. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Folgende Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind, wurden getroffen.

☐ Unterbrechungsfreie Stromversorgung (USV)

☐ Klimaanlage in Serverräumen

☐ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen

☐ Schutzsteckdosenleisten in Serverräumen

☐ Feuer- und Rauchmeldeanlagen

☐ Feuerlöschgeräte in Serverräumen

- ☐ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☐ Erstellen eines Backup- & Recoverykonzepts
- ☐ Testen von Datenwiederherstellung
- ☐ Erstellen eines Notfallplans
- ☐ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ☐ Serverräume nicht unter sanitären Anlagen
- ☐ In Hochwassergebieten: Serverräume über der Wassergrenze

C. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle

Folgende Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist, wurden getroffen.

- ☐ Einrichtungen von Standleitungen bzw. VPN-Tunneln
- ☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- ☐ Verwendung der eServices des eAMS-Kontos
- ☐ Verwendung des eService „Projekt/Veranstaltungszuordnung“
- ☐ E-Mail-Verschlüsselung
- ☐ Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- ☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- ☐ Beim physischen Transport: sichere Transportbehälter/-verpackungen
- ☐ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –fahrzeugen

Eingabekontrolle

Folgende Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, wurden getroffen.

☐ Protokollierung der Eingabe, Änderung und Löschung von Daten

☐ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.

☐ Verwendung der eServices des eAMS-Kontos

☐ Verwendung des eService „Projekt/Veranstaltungszuordnung“

☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind

☐ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

8.6. Risikobewertung

Eine Risikobewertung muss nicht zwingend mit einer ausdrücklichen quantifizierten Bewertung erfolgen. Wenn eine prosaische Beschreibung existiert und erkennbar ist, mit welchen Maßnahmen welchen Risiken minimiert werden, wird dies den Mindestanforderungen gerecht.

Optimal ist eine ausdrückliche und ausführliche Risikobewertung. Beispielhaft hier eine Beschreibung betreffend die Schwere der Auswirkungen der Risikoverwirklichung und die Eintrittswahrscheinlichkeit der Risiken, mit einer Einteilung in jeweils vier Kategorien: unbedeutend, spürbar, kritisch, katastrophal; Eintrittswahrscheinlichkeit: häufig, eher häufig, eher selten, unwahrscheinlich

Risiko-objekt 1 Dokumente in Papierform

häufig (4)	4	8	12	16
eher häufig (3)	3	6	9	12
eher selten (2)	2	4	6	8
unwahrscheinlich (1)	1	2	3	4
Eintrittswahr-scheinlich-keit / Auswirkung	unbedeutend (1)	spürbar (2)	kritisch (3)	katastrophal (4)

9. Prüfraster zu Risikoanalyse und Maßnahmenplan für Verarbeitungsvorgänge im Auftrag des AMS

9.1. Einführung

Der vorliegende Prüfraster dient zur Vereinfachung einer internen oder externen Überprüfung der Risikoanalyse und des Maßnahmenplans im Hinblick auf Datenverarbeitungen im Auftrag des AMS. Der Prüfraster ist im Vergleich zum Katalog von Maßnahmen in Kapitel 8 in den Formulierungen allgemeiner gehalten und in Form einer Checkliste geführt.

9.2. Risikoanalyse

Rechtsgrundlage: Art. 32 Abs. 2 DSGVO

Ja	Nein	Es liegt eine Risikoanalyse zur Datenverarbeitung für die vom AMS beauftragte Dienstleistungen vor. Im Einzelfall würde eine Datenschutzfolgenabschätzung gemäß Art. 35 falls erforderlich durchgeführt.

Ja	Nein	Die Ergebnissen der Risikoanalyse finden sich in den technischen und organisatorischen Maßnahmen wieder.

9.3. Datenschutzrechtliche Schulungen

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

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

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

Verpflichtende Maßnahmen:

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

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

9.4. Zutrittsbeschränkungen

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

Führen Sie bitte aus, durch welche **technischen Maßnahmen** die Räume, in denen sich personenbezogene Daten von AMS Kundinnen und Kunden befinden, angemessen vor unberechtigtem Zutritt geschützt werden (z. B. Sicherheitsschlösser, Schließsysteme, Alarmanlage etc).

Ja	Nein	Sicherheitsschlösser

Ja	Nein	Schließsysteme

Ja	Nein	Alarmanlage

Ja	Nein	

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

Ja	Nein	Schließregelung für die Räumlichkeiten

Ja	Nein	Schlüsselbuch/Schlüsselregelung

Ja	Nein	Ausweisregelung

Ja	Nein	Sorgfältige Auswahl von Sicherheits-/Reinigungs-/IT-Personal bzw. –Firmen

Ja	Nein	

9.5. Zugangs-, Zugriffs- und Betriebsbeschränkungen

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

Führen Sie bitte aus, durch welche **technischen Maßnahmen** personenbezogene Daten in Ihren EDV-Systemen vor unberechtigtem Zugang und Zugriff als auch unbefugter Inbetriebnahme geschützt werden (z. B. durch Einstieg mittels Benutzer/Passwort,

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

Ja	Nein	Einstieg mittels Benutzer/Passwort

Ja	Nein	Automatische Sperrmechanismen

Ja	Nein	Einsatz von Anti-Viren Software

Ja	Nein	Firewall

Ja	Nein	VPN Technologien

Ja	Nein	Sperren von externen Schnittstellen

Ja	Nein	E-Mail Verschlüsselungen

Ja	Nein	Verschlüsselung von Datenträgern

Ja	Nein	Frühestmögliche Pseudonymisierung der Daten

Ja	Nein	Ablage von Papierakten in versperrten Schränken

Ja	Nein	

Verpflichtende AMS-spezifische Maßnahmen:

- Die vertraglich vorgeschriebenen eServices des eAMS-Kontos sind für die elektronische Kommunikation mit dem AMS zu verwenden. Die betroffenen Mitarbeiterinnen und Mitarbeiter sind darüber schriftlich zu informieren.
- Das eService „Projekt/Veranstaltungszuordnung“ des eAMS-Kontos ist zwingend zu verwenden und laufend zu warten. Als Grundlage ist ein Berechtigungskonzept zu erstellen.

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

Die Aktivitäten sind zu dokumentieren und auf Aufforderung vorzulegen.

Führen Sie bitte aus, durch welche organisatorischen Maßnahmen Ihre EDV-Systeme vor unberechtigtem Zugang und Zugriff als auch unbefugte Inbetriebnahme geschützt werden (z. B. durch ein laufend gewartetes Berechtigungskonzept, Standardprozess für Berechtigungsvergabe, Passwort-Richtlinie, Telearbeit-Richtlinie, Nutzungsverbot von nichtbetrieblicher Soft- und Hardware, Installationsberechtigung von Programmen ausschließlich durch IT-AdministratorInnen, laufende Softwareaktualisierung, insbesondere von sicherheitsrelevanter Software [Antiviren-Programme, Browser etc.], Datenträgerverwaltung, Mobile Device Management, Regelungen beim Ausscheiden von MitarbeiterInnen etc.) und die manuell geführten personenbezogenen Daten („Papierakt“) vor unberechtigtem Zugriff geschützt werden.

Ja	Nein	Ein Berechtigungskonzept wird eingesetzt

Ja	Nein	Standardprozess für Berechtigungsvorgabe ist beschrieben

Ja	Nein	Eine Passwort-Richtlinie oder ähnliches ist vorgesehen.

Ja	Nein	Eine Telearbeit-Richtlinie oder ähnliches ist vorgesehen.

Ja	Nein	Es gibt ein Nutzungsverbot von nichtbetrieblicher Soft- und Hardware.

Ja	Nein	Die Installationsberechtigung von Programmen liegt ausschließlich bei IT-AdministratorInnen

Ja	Nein	Laufende Software-Aktualisierungen sind vorgesehen, insbesondere von sicherheitsrelevanter Software (Antiviren-Programme, Browser etc.)

Ja	Nein	Es ist eine Datenträgerverwaltung vorgesehen

Ja	Nein	Es ist ein Mobile Device Management vorgesehen

Ja	Nein	Es gibt eine Regelung zum Auscheiden von MitarbeiterInnen

Ja	Nein	Es gibt Regelungen wie manuell geführte personenbezogenen Daten von unberechtigtem Zugriff geschützt werden.

9.6. Verfügbarkeit, Belastbarkeit und Löschung

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

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

Ja	Nein	Es wird auf eine ausreichende EDV-Kapazität geachtet.

Ja	Nein	Es ist eine Klimatisierung der Serverräume vorgesehen.

Ja	Nein	Es ist eine unterbrechungsfreie Stromversorgung (USV) der Server vorgesehen.

Ja	Nein	Es sind Maßnahmen gegen Feuer, Wasser und elektromagnetische Felder vorgesehen, die die Daten auf den Servern beeinträchtigen könnten.

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

Ja	Nein	Es wird ein (getestetes) Backup- und Recoverykonzept eingesetzt.

Ja	Nein	Datensicherungen werden an einem externen sicheren Ort aufgewahrt.

Ja	Nein	Es liegt ein Notfallplan vor.

Ja	Nein	

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

Ja	Nein	Eine automatisierte Löschungsroutine liegt vor.

Ja	Nein	Eine manuelle Löschung liegt vor

Ja	Nein	Eine verlässliche und effektive Vernichtung von nicht mehr benötigten Datenträgern (Papier, CD, DVD, USB-Stick, Festplatten etc.) ist vorgesehen.

Ja	Nein	Es kommen geeignete Löschprogramme zur Anwendung, die Daten auf Datenträgern, die wiederverwendet werden sollen, irreversibel löschen.

Ja	Nein	

9.7. Überprüfungsmöglichkeiten der rechtmäßigen Datenverarbeitung

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

Führen Sie bitte aus, durch welche Maßnahmen Sie feststellen, ob und von wem personenbezogene Daten eingegeben, eingesehen, verändert oder entfernt worden sind (z. B. durch Protokollierung auf Ebene der individuellen Benutzernamen, stichprobenartige Auswertung durch befugte Personen, Dokumentation der Datenübermittlungen, Dokumentenmanagement etc.), um die rechtmäßige Verarbeitung zu überprüfen.

Ja	Nein	Es ist eine (automatische) Protokollierung auf Ebene der individuellen Benutzernamen vorgesehen.

Ja	Nein	Es ist eine stichprobenartige Auswertung durch befugte Personen vorgesehen.
Ja	Nein	Es ist eine Dokumentation der Datenübermittlungen vorgesehen.

Ja	Nein	Es wird ein Dokumentenmanagement beschrieben.

Ja	Nein	

10. Transparenz und Verfahrensregeln zu den BABE CoC

Nach Art. 40 Abs. 4 DSGVO sind zwingend konkrete Verfahren vorzusehen, die die obligatorische Überwachung der Einhaltung ihrer Bestimmungen durch die Verantwortlichen oder die Auftragsverarbeiter, die sich zur Anwendung der Verhaltensregeln verpflichten, ermöglichen. Die Überwachung muss durch eine private Stelle durchgeführt werden. Diese Stelle muss rechtsfähig sein. Die „zwingenden Verfahren“ erfassen die Aufnahme der Unterwerfung unter die Verhaltensregeln, die Durchführung von Beschwerdeverfahren wegen eines Verstoßes gegen die Verhaltensregeln, die Durchführung von Prüfungen, ob die Verhaltensregeln eingehalten wurden und auch Sanktionen, die die Überwachungsstelle gegenüber Unterworfenen bei Verstößen gegen die dort normierten Regeln aussprechen kann (z. B. der Ausschluss von den Verhaltensregeln).

10.1. Publizität der BABE CoC

Die BABE CoC sind auf der Website der BABE zu publizieren. Die BABE publiziert auf ihrer Website außerdem eine aktuelle Liste der den BABE CoC beigetretenen Mitglieder.

10.2. Regeln zur Überwachung der Einhaltung der BABE CoC[4]

10.3. Mechanismen zur Überprüfung[4]

[4] Eine zur Überwachung der BABE CoC vorgesehene Überwachungsstelle im Sinne von Art. 41 Abs. 1 und 2 DSGVO muss unter den in der ÜStAkk-V normierten Voraussetzungen noch akkreditiert werden. Die vorgesehene Überwachungsstelle wird dann durch einen Änderungsantrag an die DSB in die vorliegenden BABE CoC eingefügt.

11. Abkürzungs- und Begriffsverzeichnis

SÖB… Sozialökonomische Betriebe

GBP… Gemeinnützige Beschäftigungsprojekte

SÖBÜ/GBPÜ… gemeinnützige Arbeitskräfteüberlassungs-Betriebe

BBE… Arbeitsmarktbezogene Beratungs- und Betreuungseinrichtungen des AMS. Von diesen werden individuelle Leistungen für Personen, die aufgrund unterschiedlicher Problemstellungen keinen Zugang zum Arbeitsmarkt finden, angeboten

ÜBA… Überbetriebliche Lehrausbildung

AMS… Arbeitsmarktservice Österreich sowie sämtliche Landesorganisationen mit regionalen Geschäftsstellen (BGS, LGS, RGS)

eAMS… elektronisches AMS, Tool zur Kommunikation und elektronischen Abwicklung von Geschäftsfällen (z. B. Berichte zu Personen, Teilnahmelisten, Inserate zu den Personen, Abwesenheiten etc.) mit entsprechenden eServices für Bildungspartner des AMS

Träger (Bildungsträger)… Einrichtungen, deren Hauptzweck in der außerbetrieblichen Erwachsenenbildung liegt, soweit sie nach arbeitsmarktrechtlichen Vorschriften oder bundes- oder landesrechtlichen Fördervorschriften oder Förderverein-barungen als Einrichtungen der außerbetrieblichen Erwachsenenbildung anerkannt sind (gemäß Erklärung des BABE-KV zur Satzung).

TrainerInnen… natürliche Personen, die auf Rechnung und Gefahr eines Trägers die Bildungsdienstleistung als AusbildnerInnen, TrainerInnen oder BetreuerInnen in Form von Kursen, Trainings, Coachings, Workshops oder ähnlichen Formaten erbringen, unabhängig davon, ob diese im Rahmen eines echten Dienstverhältnisses oder auf Basis eines anderen Vertragstyps für den Träger tätig werden

TeilnehmerInnen… natürliche Personen, die an von Auftraggebern oder Fördergebern beauftragten bzw. zugewiesenen oder privat angebotenen Bildungsmaßnahmen teilnehmen

MitarbeiterInnen… MitarbeiterInnen von Trägern, die nicht Transitarbeitskräfte sind

Einzelcoaching… Einzelsettings von TrainerInnen im Rahmen von Bildungsmaßnahmen gemeinsam mit TeilnehmerInnen