



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Wirtschaft, Bildung und Forschung WBF

Staatssekretariat für Wirtschaft SECO
Arbeitsmarkt / Arbeitslosenversicherung

Leitfaden zur Bearbeitung von Personendaten in den Bereichen AVIG und AVG (Datenschutzleitfa- den AVIG / AVG)

Arbeitsmarkt /
Arbeitslosenversicherung (TC)

3. Auflage, Stand: 01.01.2024

Staatssekretariat für Wirtschaft SECO
Direktion für Arbeit
Arbeitsmarkt / Arbeitslosenversicherung (TC)
Holzikofenweg 36, CH-3003 Bern
Tel. 058 462 29 20
www.seco.admin.ch, www.arbeit.swiss; tcjd@seco.admin.ch

VORWORT

Als Aufsichtsbehörde hat die Ausgleichsstelle der Arbeitslosenversicherung (SECO-TC) für eine einheitliche Rechtsanwendung zu sorgen und den Durchführungsstellen im Zusammenhang mit dem Gesetzesvollzug Weisungen zu erteilen (Art. 110 AVIG).

Der vorliegende Leitfaden versteht sich als Arbeits- und Hilfsmittel für alle Durchführungsstellen zur Einschätzung von Fragestellungen und Vorgehensweisen im Zusammenhang mit dem Datenschutz im Rahmen des Vollzugs des AVIG und des AVG.

Der vorliegende Datenschutzleitfaden AVIG & AVG wird auf [arbeit.swiss](https://www.arbeit.swiss) sowie auf dem TCNet publiziert. Bitte richten Sie Ihre Fragen oder Anregungen an tcjd@seco.admin.ch.

Zitierung: Datenschutzleitfaden AVIG & AVG Rz. 1.

Das neue Bundesgesetz über den Datenschutz (DSG) ist am 1. September 2023 in Kraft getreten. Die hauptsächlichen Unterschiede zum alten DSG bestehen in terminologischen Änderungen sowie in der Änderung des Geltungsbereichs: Das revDSG schützt nicht mehr die Daten von juristischen Personen, und die Inhaber der Datensammlung werden neu als Verantwortliche bezeichnet. Ausserdem wird der Begriff des Persönlichkeitsprofils durch die beiden Begriffe Profiling und Profiling mit hohem Risiko ersetzt.

Das revDSG führt neue Pflichten für die Verantwortlichen ein, wie die erweiterte Informationspflicht, die Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten, die Meldung von Verletzungen der Sicherheit oder den Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen sowie die Folgenabschätzung und die vorgängige Konsultation des Datenschutzbeauftragten. Diese Punkte werden im vorliegenden Leitfaden nicht behandelt, da sie ausschliesslich SECO-TC betreffen.

Ergänzend verweisen wir auf die europäische Verordnung zum Datenschutz (DSGVO), die seit dem 25. Mai 2018 in der Europäischen Union in Kraft ist ([Datenschutz-Grundverordnung der Europäischen Union \(admin.ch\)](#)). Die DSGVO ist beim Vollzug der Schweizer Arbeitslosenversicherung zwar nicht anwendbar, kann jedoch als Argumentationsgrundlage dienen.

SECO -TC

INHALTSÜBERSICHT

Vorwort	1
INHALTSÜBERSICHT	2
ABKÜRZUNGSVERZEICHNIS	4
GLOSSAR	6
GRUNDSÄTZE UND BEGRIFFE	8
Zweck des Datenschutzes	8
Geltungsbereiche	8
Kantonale Datenschutzbeauftragte	8
Bearbeiten von Personendaten	8
DATENBEARBEITUNG IN DER ALV UND ÖAV	13
Gesetzliche Grundlagen	13
Zugang zu den von SECO-TC betriebenen Informationssystemen	13
Erhebung und Bearbeitung von Personendaten	14
Auskunftsrecht der betroffenen Person	16
Auskunfts berechtigte Person	16
Zuständige Stelle zur Behandlung von Auskunftsbegehren	16
Gegenstand des Auskunftsrechts	16
Form	17
Frist	17
Datenbekanntgabe	18
Schweigepflicht	18
Auskunft, Amts- und Verwaltungshilfe	18
Regulärer Datenverkehr	19
Bekanntgabe an Behörden auf schriftlich begründetes Gesuch hin	20
Bekanntgabe an Dritte	20
Veröffentlichung	20
Grenzüberschreitende Datenbekanntgabe (Art. 16 DSGVO)	21
Datenverkehr zwischen der Schweiz und den EU/EFTA-Staaten	21
Datenbearbeitung für nicht personenbezogene Zwecke (FORSCHUNGSPRIVILEG)	22
Grundsatz	22
Verfahren	22
Kantonale Durchführungsstellen	23
Arten des Datenaustauschs und Gebühren	24
Arten	24
Gebühren	24
Übersicht: Datenbekanntgabe gemäss AVIG und AVG	25
Datenbearbeitung für nicht personenbezogene Zwecke (Art. 15 ALV-IsV)	25

INTERINSTITUTIONELLE ZUSAMMENARBEIT (IIZ)	26
Grundsatz.....	26
Aufgabendelegation	26
Erleichterter Datenaustausch	26
Einwilligung in die Datenbekanntgabe	27
Fehlendes Gegenrecht: Einzelfallregelung	27
Datenbekanntgabe an die IV	28
Sichtung der AVAM-Daten	28
Schweigepflicht und Geheimnisschutz	28
SECO-TC INFORMATIONSSYSTEME	29
Grundsatz.....	29
SECO-TC als Verantwortlicher	29
Eintrag von Daten in die Informationssysteme.....	29
DATENMIGRATION	30
Grundsatz.....	30
Voraussetzungen	30
Verfahren	30
DATENBEARBEITUNG DURCH einen Auftragsbearbeiter	31
Bedingungen der Bearbeitung durch einen Auftragsbearbeiter.....	31
Verantwortung.....	31
Sicherstellung einer angemessenen Datensicherheit	31
Bearbeitungsvereinbarung	31
Von den Durchführungsstellen für ihre eigenen Systeme erhobene Daten.....	32
DATENSICHERHEIT	33
Grundsatz.....	33
Technische Massnahmen.....	34
Organisatorische Massnahmen	35
AUFBEWAHRUNG, ARCHIVIERUNG UND VERNICHTUNG VON DATEN (INKLUSIVE PAPIERAKTEN)	36
Aufbewahrung	36
Archivierung	36
Vernichtung.....	36
Transparenz und Nachvollziehbarkeit.....	37
DOKUMENTE, APPS UND NÜTZLICHE LINKS	38

ABKÜRZUNGSVERZEICHNIS

Abs.	Absatz
AHVG	Bundesgesetz vom 20. Dezember 1946 über die Alters- und Hinterlassenenversicherung (SR 831.10)
ALE	Arbeitslosenentschädigung
ALV	Arbeitslosenversicherung
ALV-IsV	Verordnung vom 26. Mai 2021 für die von der Ausgleichsstelle der Arbeitslosenversicherung betriebenen Informationssysteme (SR 837.063.1)
Art.	Artikel
ASAL	Informationssystem für die Auszahlung von Leistungen der Arbeitslosenversicherung
ATSG	Bundesgesetz vom 6. Oktober 2000 über den Allgemeinen Teil des Sozialversicherungsrechts (SR 830.1)
ATSV	Verordnung vom 11. September 2002 über den Allgemeinen Teil des Sozialversicherungsrechts (SR 830.11)
AVAM	Informationssystem für die öffentliche Arbeitsvermittlung
AVG	Bundesgesetz vom 6. Oktober 1989 über die Arbeitsvermittlung und den Personalverleih (Arbeitsvermittlungsgesetz, SR 823.11)
AVIG	Bundesgesetz vom 25. Juni 1982 über die obligatorische Arbeitslosenversicherung und die Insolvenzenschädigung (Arbeitslosenversicherungsgesetz, SR 837.0)
AVIV	Verordnung vom 31. August 1983 über die obligatorische Arbeitslosenversicherung und die Insolvenzenschädigung (Arbeitslosenversicherungsverordnung, SR. 837.02)
AVV	Verordnung vom 16. Januar 1991 über die Arbeitsvermittlung und den Personalverleih (Arbeitsvermittlungsverordnung, SR 823.111)
BGE	Bundesgerichtsentscheid
bzw.	beziehungsweise
d.h.	das heisst
DSG	Bundesgesetz vom 25. September 2020 über den Datenschutz (SR 235.1)
DSV	Verordnung vom 31. August 2022 über den Datenschutz (SR 235.11)
E-ALV	Zugangsplattform für elektronische Dienstleistungen
EDÖB	Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte
IIZ	Interinstitutionelle Zusammenarbeit
IV	Invalidenversicherung
Job-Room	Plattform der öffentlichen Arbeitsvermittlung
KAST	Kantonale Amtsstelle

KVG	Bundesgesetz vom 18. März 1994 über die Krankenversicherung (SR 832.10)
LAM	Logistikstelle für arbeitsmarktliche Massnahmen
LAMDA	Informationssystem für die Analyse von Arbeitsmarktdaten
RAV	Regionales Arbeitsvermittlungszentrum
Rz.	Randziffer
SECO-TC	Ausgleichsstelle der Arbeitslosenversicherung
SR	Systematische Sammlung des Bundesrechts
StGB	Schweizerisches Strafgesetzbuch vom 21. September 1937 (SR 311.0)
u.a.	unter anderem
usw.	und so weiter
UVG	Bundesgesetz vom 20. März 1981 über die Unfallversicherung (SR 832.20)
z.B.	zum Beispiel

GLOSSAR

Nachfolgend werden die wichtigsten, auch im kantonalen Datenschutzrecht verwendeten Begriffe definiert. Beispielhaft finden sich Klammervweise auf die entsprechende Norm im DSG:

- **Personendaten** (Art. 5 lit. a DSG)

Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Dies unabhängig davon, ob es sich um objektive Angaben (z.B. Name, Beruf) oder subjektive Angaben (z.B. Angaben zur Arbeitsleistung in einem Arbeitszeugnis, Werturteile) handelt.

Auch wenn solche Angaben keinen direkten Rückschluss auf eine Person zulassen, sondern diese nur reidentifizierbar machen, handelt es sich um Personendaten. Keine Bestimmbarkeit liegt erst vor, wenn nach der allgemeinen Lebenserfahrung der Aufwand, eine Person ausfindig zu machen, derart gross ist, dass eine interessierte Person diesen Aufwand nicht auf sich nehmen wird.

- **Betroffene Person** (Art. 5 lit. b DSG)

Betroffen sein können natürliche Personen, über die Daten bearbeitet werden.

- **Besonders schützenswerte Personendaten** (Art. 5 lit. c DSG)

Es handelt sich um Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten; über die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit; über die Massnahmen der Sozialhilfe oder über administrative oder strafrechtliche Verfolgungen und Sanktionen.

Die Information, dass eine Person bei der ALV gemeldet ist, ist nicht besonders schützenswert (z.B. Absender auf Couvert).

- **Bearbeiten** (Art. 5 lit. d DSG)

Bearbeitung meint jeden Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten.

- **Bekanntgeben** (Art. 5 lit. e DSG)

Bekanntgeben bedeutet das Übermitteln oder Zugänglichmachen von Personendaten

- **Profiling** (Art. 5 lit. f DSG)

Jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.

- **Profiling mit hohem Risiko** (Art. 5 lit. g DSG)

Profiling, das ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, indem es zu einer Verknüpfung von Daten führt, die

eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt.

- **Verletzung der Datensicherheit** (Art. 5 lit. h DSGVO)

Eine Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden.

- **Bundesorgan** (Art. 5 lit. i DSGVO)

Behörde oder Dienststelle des Bundes oder Person, die mit öffentlichen Aufgaben des Bundes betraut ist.

- **Verantwortliche/-r** (Art. 5 lit. j DSGVO)

Private Person oder Bundesorgan, die oder das allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet.

- **Auftragsbearbeiter/-in** (Art. 5 lit. k DSGVO)

Private Person oder Bundesorgan, die oder das im Auftrag des Verantwortlichen Personendaten bearbeitet.

Die Bearbeitung von Personendaten kann vertraglich oder durch die Gesetzgebung einer Auftragsbearbeiterin / einem Auftragsbearbeiter übertragen werden, wenn:

- a. die Daten so bearbeitet werden, wie die / der Verantwortliche selbst es tun dürfte;
- b. keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet.

Die / Der Verantwortliche muss sich insbesondere vergewissern, dass die / der Auftragsbearbeitende in der Lage ist, die Datensicherheit zu gewährleisten. Die / der Auftragsbearbeitende darf die Bearbeitung nur mit vorgängiger Genehmigung der / des Verantwortlichen einem Dritten übertragen. Sie / er kann dieselben Rechtfertigungsgründe geltend machen wie die / der Verantwortliche.

GRUNDSÄTZE UND BEGRIFFE

Zweck des Datenschutzes

- 1 Der Datenschutz dient dem Schutz der Persönlichkeitsrechte und der Privatsphäre. Er verpflichtet die Datenbearbeitenden zu rechtmässigem und verhältnismässigem Handeln und verleiht den betroffenen Personen durchsetzbare Rechte.

Geltungsbereiche

- 2 Allgemein kommen Datenschutzvorschriften zur Anwendung, wenn Personendaten in irgendeiner Form bearbeitet werden. Nicht zur Anwendung kommen sie, wenn keine Personendaten, sondern beispielsweise anonymisierte oder statistische Daten bearbeitet werden (Art. 2 DSG).
- 3 Das DSG findet dann Anwendung, wenn Personendaten natürlicher Personen durch Privatpersonen oder Bundesorgane bearbeitet werden (Art. 2 Abs. 1 DSG). Folglich wenden SECO-TC und die privaten Arbeitslosenstellen sowie die AMM-Anbietenden ausschliesslich das DSG an.
- 4 Infolge der verfassungsrechtlich geschützten Organisationsautonomie der Kantone unterstehen die kantonalen Behörden (z.B. die RAV, die LAM, die KAST) bei der Datenbearbeitung dem kantonalen Datenschutzrecht, selbst wenn diese Bundesrecht vollziehen.
- 5 Bestehen auf Bundesebene bereichsspezifische Datenschutzvorschriften (z.B. im AVIG, AVG oder ATSG), so gehen diese Bestimmungen vor.

Kantonale Datenschutzbeauftragte

- 6 Für die Kontrolle der korrekten Anwendung der Gesetzesbestimmungen im Bereich des Datenschutzes durch die kantonalen Vollzugsorgane sind in erster Linie die kantonalen Datenschutzbeauftragten zuständig.

Bearbeiten von Personendaten

- 7 Die Bearbeitung schliesst eine Vielzahl unterschiedlicher, mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgänge im Zusammenhang mit personenbezogenen Daten ein. Die Bearbeitung umfasst das Erheben, das Erfassen, die Organisation, das Ordnen, das Speichern, das Anpassen oder Ändern, das Auslesen, das Abfragen, die Verwendung, das Bekanntgeben, das Auskunftgeben, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung personenbezogener Daten.
- 8 Damit Personendaten bearbeitet werden dürfen, müssen sämtliche der folgenden Grundsätze beachtet werden. Beispielhaft finden sich jeweils Verweise auf die entsprechende DSG-Norm:

- **Rechtmässigkeit, Legalitätsprinzip** (Art. 6 Abs. 1 und 34 DSG)

Personendaten dürfen nur rechtmässig bearbeitet werden.

Im Privatbereich ist die Bearbeitung von Daten rechtmässig und damit erlaubt, wenn kein allgemeiner Datenschutzgrundsatz verletzt wird. Für die Bearbeitung von Personendaten durch eine staatliche Stelle muss hingegen eine gesetzliche Grundlage bestehen (Legalitätsprinzip).

Eine Grundlage in einem Gesetz im formellen Sinn ist in folgenden Fällen erforderlich:

- a. Es handelt sich um die Bearbeitung von besonders schützenswerten Personendaten;
- b. Es handelt sich um ein Profiling;
- c. Der Bearbeitungszweck oder die Art und Weise der Datenbearbeitung können zu einem schwerwiegenden Eingriff in die Grundrechte der betroffenen Person führen.

Für die Bearbeitung von Personendaten ist eine Grundlage in einem Gesetz im materiellen Sinn ausreichend, wenn die folgenden Voraussetzungen erfüllt sind:

- a. Die Bearbeitung ist für eine in einem Gesetz im formellen Sinn festgelegte Aufgabe unentbehrlich.
- b. Der Bearbeitungszweck birgt für die Grundrechte der betroffenen Person keine besonderen Risiken.

Hiervon ist eine Ausnahme in drei Fällen möglich:

- a. Wenn der Bundesrat es im Einzelfall bewilligt, weil die Rechte der betroffenen Person nicht gefährdet sind;
- b. Wenn die betroffene Person im Einzelfall eingewilligt oder ihre Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat;
- c. Die Bearbeitung ist notwendig, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es ist nicht möglich, innerhalb einer angemessenen Frist die Einwilligung der betroffenen Person einzuholen.

- **Treu und Glauben** (Art. 6 Abs. 2 DSG)

Der Grundsatz von Treu und Glauben verlangt einen fairen und vertrauenswürdigen Umgang mit Personendaten. Ihm kommt insbesondere im Zusammenhang mit der aktiven Information eine wichtige Bedeutung zu. So kann von ihm eine allgemeine Verpflichtung abgeleitet werden, wonach betroffene Personen über die Datenbearbeitung zu informieren sind, wenn sich dies angesichts der Umstände unter Zugrundelegung eines loyalen und vertrauenswürdigen Verhaltens aufdrängt. So dürfen personenbezogene Daten nicht erhoben werden, ohne dass die betroffene Person darüber informiert wurde oder gegebenenfalls ihre Einwilligung gegeben hat.

- **Verhältnismässigkeit** (Art. 6 Abs. 2 DSG)

Die Datenbearbeitung muss verhältnismässig sein. Der Grundsatz der Verhältnismässigkeit besagt, dass nur solche Daten erhoben, bearbeitet oder gespeichert werden dürfen, die für die Erreichung des Zwecks notwendig und angemessen sind. Es muss immer eine Interessenabwägung zwischen dem Zweck der Bearbeitung und dem Eingriff in die Persönlichkeit der betroffenen Person vorgenommen werden. Dieser Zweck muss aber auch in einem vernünftigen Verhältnis zum Eingriff in die Grundrechte der betroffenen Person stehen.

- **Zweckbindung, Transparenz bzw. Erkennbarkeit** (Art. 6 Abs. 3 DSG)

Gemäss dem Prinzip der Zweckbestimmung dürfen Personendaten nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Sollen Personendaten über den

ursprünglich angegebenen oder aus den Umständen ersichtlichen Zweck hinaus bearbeitet werden, müssen die betroffenen Personen entsprechend informiert werden.

Die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung müssen für die betroffene Person unter normalen Umständen erkennbar oder voraussehbar sein. Das Erfordernis der Erkennbarkeit konkretisiert den Grundsatz von Treu und Glauben und erhöht die Transparenz einer Datenbearbeitung. Für die Datenbeschaffung durch Bundesorgane ist in diesem Zusammenhang zudem auf die in Art. 19 DSGVO normierte Informationspflicht hinzuweisen, welche über das Erfordernis der blossen Erkennbarkeit hinausgeht.

- **Vernichtung, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind** (Art. 6 Abs. 4 DSGVO)

Personendaten werden vernichtet oder anonymisiert, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind

- **Datenrichtigkeit** (Art. 6 Abs. 5 DSGVO)

Wer Personendaten bearbeitet, muss sich über deren Richtigkeit vergewissern. Sie oder er muss alle angemessenen Massnahmen treffen, damit die Daten berichtigt, gelöscht oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind. Die Angemessenheit der Massnahmen hängt namentlich ab von der Art und dem Umfang der Bearbeitung sowie vom Risiko, das die Bearbeitung für die Persönlichkeit oder Grundrechte der betroffenen Personen mit sich bringt.

- **Gewährleistung der Datenintegrität**

Die Datenintegrität ist ein Teilaspekt der Datensicherheit und bezeichnet die Zuverlässigkeit und Vertrauenswürdigkeit von Daten. Sie bezieht sich auf die Richtigkeit und die Vollständigkeit der Daten. Gleichzeitig gilt es sicherzustellen, dass keine unzulässigen Änderungen vorgenommen werden bzw. die Änderung von Daten festgestellt werden kann.

- **Anonymisierte und pseudonymisierte Personendaten**

Man spricht von anonymisierten Daten, wenn ohne unverhältnismässigen Aufwand kein Rückschluss auf die Person mehr möglich ist und so der Personenbezug irreversibel aufgehoben wurde.

Bei pseudonymisierten Daten gibt es hingegen nach wie vor einen Schlüssel (z.B. in Form einer Konkordanztabelle), mit welchem der Personenbezug wiederhergestellt werden kann.

Für jede Person, die Zugang zum Schlüssel hat, bleiben pseudonymisierte Daten demnach Personendaten. Nur für Aussenstehende ohne Schlüssel sind es keine Personendaten mehr (anonymisierte Daten).

- **Auskunftsrecht der betroffenen Person** (Art. 25 und 26 DSGVO)

Das Auskunftsrecht ist eines der wichtigsten Elemente im Bereich des Datenschutzes. Es bildet die Voraussetzung für die Ausübung anderer Rechte und Ansprüche; so ist es die Grundlage für das Recht auf Berichtigung falscher Personendaten (nach Art. 25 DSGVO), das Recht auf Unterlassung einer unrechtmässigen Datenbearbeitung oder das Recht auf Beseitigung der Folgen einer unrechtmässigen Bearbeitung.

Auf das Auskunftsrecht kann nicht verzichtet werden (Art. 25 Abs. 5 DSGVO).

Die Verantwortlichen können die Auskunft verweigern, einschränken oder aufschieben, wenn:

- ein Gesetz im formellen Sinn dies vorsieht, namentlich um ein Berufsgeheimnis zu schützen;
- dies aufgrund überwiegender Interessen Dritter erforderlich ist;
- das Auskunftsgesuch offensichtlich unbegründet ist, namentlich wenn es einen datenschutzwidrigen Zweck verfolgt, oder offensichtlich querulatorisch ist;
- die Massnahme wegen überwiegender öffentlicher Interessen, insbesondere der inneren oder äusseren Sicherheit der Schweiz erforderlich ist;
- die Mitteilung der Information eine Ermittlung, eine Untersuchung oder ein behördliches oder gerichtliches Verfahren gefährden kann.

- **Rechtsgültige Einwilligung** (Art. 6 Abs. 6 DSG)

Ist die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur gültig, wenn sie für eine oder mehrere bestimmte Bearbeitungen nach angemessener Information freiwillig erteilt wird.

Die Information ist angemessen, wenn die betroffene Person transparent und umfassend darüber informiert wurde, was mit ihren Daten geschieht. Auch muss sie die Konsequenzen ihrer Entscheidung verstehen, insbesondere auch die Tragweite einer Nichteinwilligung. Auf die Person darf kein Druck ausgeübt werden, um ihr Einverständnis zu erhalten. Druck ist jedoch nur dann anzunehmen, wenn der mit der Verweigerung der Einwilligung zu der Datenbearbeitung verbundene Nachteil in keinem Zusammenhang mit der Datenbearbeitung und der mit ihr verfolgten Zielsetzung steht oder wenn der damit verbundene Nachteil unverhältnismässig ist.

Die Gültigkeit der Einwilligung hängt sodann von der allgemeinen rechtlichen Anforderung der Urteilsfähigkeit der einwilligenden Person ab. Minderjährige können ihre Einwilligung rechtsgültig erteilen, wenn sie bezüglich des Gegenstands der Einwilligung urteilsfähig sind. Je nach Menge und Art der Daten muss aber auch der gesetzliche Vertreter einwilligen. Personen unter Beistandschaft können rechtsgültig in die Datenbearbeitung einwilligen, wenn sie diesbezüglich urteilsfähig sind. Dies ist im Einzelfall zu prüfen. Wird die Urteilsfähigkeit mit Blick auf die Einwilligung in die Datenbearbeitung verneint, ist die Einwilligung von der Beiständin oder dem Beistand einzuholen.

Die Einwilligung muss ausdrücklich erfolgen für (Art. 6 Abs. 7 DSG):

- a. die Bearbeitung von besonders schützenswerten Personendaten;
- b. ein Profiling mit hohem Risiko durch eine private Person; oder
- c. ein Profiling durch ein Bundesorgan

Die Einwilligung hat grundsätzlich vor der Datenbearbeitung vorzuliegen. Eine Ausnahme ist möglich, wenn die Datenbearbeitung im klaren Interesse der betroffenen Person liegt (Art. 34 Abs. 4 Bst. c DSG). Die Einwilligung kann schliesslich jederzeit widerrufen werden.

Sie kann schriftlich oder mündlich erfolgen und ist an keine bestimmte Form gebunden. Aus Transparenz- und Beweisgründen ist die schriftliche Festhaltung und Unterzeichnung allerdings empfohlen.

- **Datenbearbeitung für nicht personenbezogene Zwecke**

Art. 39 DSGVO ist eine Spezialbestimmung für das Bearbeiten von Personendaten durch Bundesorgane zu nicht personenbezogenen Zwecken. Bei dieser «privilegierten» Personendatenbearbeitung fällt der Personenbezug im Verlauf der Bearbeitung weg.

DATENBEARBEITUNG IN DER ALV UND ÖAV

Gesetzliche Grundlagen

- 9** Die gesetzlichen Grundlagen zum Datenschutz in der Arbeitslosenversicherung und der öffentlichen Arbeitsvermittlung sind in folgenden Texten festgehalten:
- Bundesgesetz vom 25. Juni 1982 über die obligatorische Arbeitslosenversicherung und die Insolvenzenschädigung (AVIG; SR 837.0)
 - Verordnung vom 31. August 1983 über die obligatorische Arbeitslosenversicherung und die Insolvenzenschädigung (AVIV; SR 837.02)
 - Bundesgesetz vom 6. Oktober 1989 über die Arbeitsvermittlung und den Personalverleih (AVG; SR 823.11)
 - Verordnung vom 16. Januar 1991 über die Arbeitsvermittlung und den Personalverleih (AVV; SR 823.111)
 - Verordnung vom 26. Mai 2021 für die von der Ausgleichsstelle der Arbeitslosenversicherung betriebenen Informationssysteme (ALV-IsV; SR 837.063.1)
 - Bundesgesetz vom 6. Oktober 2000 über den allgemeinen Teil des Sozialversicherungsrechts (ATSG; SR 830.1)
 - Verordnung vom 11. September 2002 über den allgemeinen Teil des Sozialversicherungsrechts (ATSV; SR 830.11)

Die anwendbaren gesetzlichen Grundlagen für die Bearbeitung von Daten gemäss AVIG und AVG sind in den Artikeln 96b AVIG und 33a AVG festgehalten. Diejenigen Punkte betreffend den Datenschutz, die nicht ausdrücklich in den Bestimmungen der oben genannten Gesetzestexte bestimmt sind, werden durch das DSG sowie die DSV geregelt.

Zugang zu den von SECO-TC betriebenen Informationssystemen

- 10** Die in Art. 96c AVIG und Art. 35 Abs. 3 AVG erwähnten Stellen haben einen direkten Zugriff auf die von SECO-TC genutzten Informationssysteme, ohne dass letztere daran beteiligt ist. Da die Nutzung des Zugriffs definitionsgemäss wiederholt, regelmässig und automatisiert erfolgt, kann sie grundsätzlich nicht mit einem Einzelfall in Verbindung gebracht werden (Online-Zugriff).

SECO-TC betreibt folgende Informationssysteme (Art. 83 Abs. 1^{bis} AVIG):

- Das Informationssystem für die Auszahlung von Leistungen der ALV [**ASAL**] (Art. 8 ALV-IsV): Es dient der Abrechnung und Auszahlung von Leistungen der ALV durch die Arbeitslosenkassen;
- Das Informationssystem für die öffentliche Arbeitsvermittlung [**AVAM**] (Art. 10 ALV-IsV): Es dient der öffentlichen Stellenvermittlung sowie den arbeitsmarktlichen Massnahmen und umfasst alle einschlägigen Daten von gemäss AVIG versicherten und gemäss AVG stellensuchenden Personen;
- Das Informationssystem für die Analyse von Arbeitsmarktdaten [**LAMDA**] (Art. 12 ALV-IsV): Es ist eine zentrale Datenbank (Data Warehouse), welche die Daten der

anderen Systeme der ALV zu statistischen Reporting- und Analysezwecken zusammenführt und in der die Daten aggregiert, formatiert und im Hinblick auf die spätere Bearbeitung Dritten unter gewissen Voraussetzungen zur Verfügung gestellt werden;

- Die Online-Serviceplattform [**eALV**] (Art. 17 ALV-IsV): Sie dient als Kontaktpunkt zwischen den Bezüglern von ALV-Leistungen oder der öffentlichen Arbeitsvermittlung und den Durchführungsstellen. Sie ermöglicht den Benutzenden die Übermittlung der Daten, welche für die Inanspruchnahme der Leistungen benötigt werden.
- Die Plattform der öffentlichen Arbeitsvermittlung [**Job-Room**] (Art. 21 ALV-IsV): Sie ist eine Online-Börse für offene Stellen.

Die jeweiligen Zugangsrechte sind in der ALV-IsV geregelt.

Erhebung und Bearbeitung von Personendaten
(Art. 96b AVIG; Art. 33a AVG)

Erhobene Daten

11 Im Rahmen der ALV dürfen folgende besonders schützenswerte Personendaten bearbeitet werden (vgl. Art. 5 lit. c DSGVO):

- nachgewiesene Einschränkung der Arbeitsfähigkeit aufgrund der religiösen Zugehörigkeit oder philosophischer Überzeugungen (z.B. bezüglich Bekleidung, Kontakt mit Lebensmitteln, Arbeitszeiten);
- nachgewiesene Einschränkung der Arbeitsfähigkeit aufgrund des Gesundheitszustandes (z.B. bezüglich Tragen von Lasten, Kontakt zu Werkstoffen, sitzende Tätigkeit, Schwangerschaft);
- nachgewiesene Schwangerschaft ohne Einschränkung der Arbeitsfähigkeit (arbeitsgesetzliche Vorgaben);
- nachgewiesene Massnahmen der Sozialhilfe oder anderer Versicherungen (z.B. KVG, UVG, IVG, Beistandsschafts- und Fürsorgemassnahmen zur Leistungskoordination);
- nachgewiesene administrative oder strafrechtliche Sanktionen, sofern ein direkter Bezug zur gesuchten Tätigkeit vorhanden ist (z.B. laufender Führerausweisentzug eines Chauffeurs);
- vorgelegte Gerichtsurteile, sofern sie einen Bezug zum Versicherungsanspruch aufweisen (z.B. das Scheidungsurteil, wenn ab diesem Tag ein Taggeldanspruch gegeben ist).

Informationspflicht

12 Die allgemeine Informationspflicht gemäss Art. 19 DSGVO wird im Bereich der ALV in Art. 126 AVIV und Art. 58 AVV konkretisiert. Danach werden die betroffenen Personen orientiert über:

- den Zweck der Informationssysteme;
- die bearbeiteten Daten und über deren regelmässige Empfänger;

- die Identität und die Kontaktdaten des Verantwortlichen;
- ihre Rechte.

Die Information wird zum Zeitpunkt der Anmeldung zur Arbeitslosigkeit abgegeben, sei dies online oder beim RAV (vgl. Informationen zur Bearbeitung von Personendaten in den Informationssystemen der ALV).

Einwilligung in die Datenerhebung

- 13** Im Bereich der ALV ist der Leistungsanspruch eng mit der Einwilligung der versicherten Person zur Datenbearbeitung verknüpft. Wenn die Person ihre Einwilligung zurückzieht, beendet sie faktisch die Bearbeitung ihres Dossiers und verzichtet somit auf den Bezug von Leistungen der ALV.

Die Veröffentlichung des anonymisierten Profils auf Job-Room erfordert keine ausdrückliche Einwilligung. Um direkt durch private Stellenvermittler kontaktiert werden zu können, muss jedoch die Einwilligung der betroffenen Person eingeholt werden. Die betroffene Person erlaubt zudem fallweise den direkten Kontakt mit einem möglichen Arbeitgeber.

Erhebung und Bearbeitung von Personendaten

- 14** Art. 96b AVIG in Verbindung mit Art. 76 Abs. 1 AVIG legt fest, wer zur Datenerhebung und -bearbeitung legitimiert ist. Für eine rechtskonforme Datenbearbeitung sind auch im Bereich der ALV die allgemeinen Grundsätze der Datenbearbeitung einzuhalten.

Aus diesem Grund ist es verboten, die betroffene Person mittels Profils der Durchführungsstellen, auch mittels privater Profile von Mitarbeitenden oder falscher Profile auf den sozialen Medien zu suchen und auf diese Weise Daten zu erheben.

Ausserdem ist es untersagt, Daten auf Vorrat ohne konkreten Verwendungszweck zu erheben (sog. «Fishing Expeditions») oder um sie zu kopieren oder auch, um sie mit anderen Datenbanken zu verknüpfen (z.B. den mit den Sozialversicherungen verbundenen kantonalen Informationssystemen).

Verwendung der AHV-Nummer

- 15** Bei der 13-stelligen AHV-Nummer handelt es sich um eine anonyme, zufällig generierte und nichtsprechende Nummer, die keine Rückschlüsse auf bestimmte personenbezogene Merkmale zulässt. In Kombination mit zusätzlichen Informationen wird die Identität der betroffenen Person allerdings bestimmbar, weshalb die AHV-Nummer im Rahmen des Datenschutzes von Bedeutung ist.

Die Verwendung der AHV-Nummer als administrativer Personenidentifikator ist für die ALV in Art. 96 AVIG geregelt. Danach dürfen die mit der Durchführung des AVIG beauftragten Stellen die AHV-Nummer für die Erfüllung ihrer gesetzlichen Aufgaben systematisch verwenden.

Auskunftsrecht der betroffenen Person
(Art. 126 AVIV; Art. 28, 31 und 47 ATSG; Art. 58 AVV)

- 16** Art. 126 AVIV deckt das Recht auf Orientierung bezüglich der Verwendung der eigenen Daten sowie das Auskunftsrecht über diese Daten ab.

Art. 126 Abs. 2 AVIV entwickelt eine hybride Auffassung des Auskunftsrechts, die sowohl dem Recht auf Akteneinsicht nach Art. 47 ATSG als auch dem Auskunftsrecht nach Art. 25 DSG entspricht. Eine analoge Bestimmung in Bezug auf die öffentliche Arbeitsvermittlung findet sich in Art. 58 AVV.

Auskunfts berechtigte Person

- 17** Art. 126 Abs. 2 lit. a AVIV gibt der betroffenen Person ein Recht auf datenschutzrechtliche Auskunft darüber, welche Daten die ALV über sie bearbeitet. Das datenschutzrechtliche Auskunftsrecht ermöglicht es, die Kontrolle über die eigenen Personendaten zu behalten.

Zuständige Stelle zur Behandlung von Auskunftsbegehren

- 18** Wenn mehrere Verantwortliche Personendaten gemeinsam bearbeiten, kann die betroffene Person ihr Auskunftsrecht bei jedem von ihnen ausüben.

Falls das Auskunftsgesuch von einem Auftragsbearbeiter bearbeitete Daten betrifft, unterstützt dieser den Verantwortlichen bei der Erteilung der Auskunft, sofern er das Gesuch nicht selbst im Namen des Verantwortlichen beantwortet. Im Rahmen der ALV ist die Zuständigkeit wie folgt:

Aktives Dossier:

Wenn eine Rahmenfrist für den Leistungsbezug läuft, hat das zuständige RAV und/oder die Arbeitslosenkasse, jeweils für diejenigen Daten, auf die sie Zugriff haben, das Auskunftsgesuch zu behandeln. Falls das Gesuch allgemein gehalten ist (z. B. «ich möchte mein Arbeitslosendossier einsehen»), koordinieren das RAV und die Arbeitslosenkasse ihre Tätigkeit.

Abgeschlossenes Dossier:

Wenn keine Rahmenfrist für den Leistungsbezug läuft, ist das Auskunftsgesuch an die folgende Adresse zu richten:

Ausgleichsstelle der Arbeitslosenversicherung
Staatssekretariat für Wirtschaft SECO
Direktion für Arbeit DA
Arbeitsmarkt und Arbeitslosenversicherung
Holzikofenweg 36, 3003 Berne

Gegenstand des Auskunftsrechts

- 19** Im Rahmen des datenschutzrechtlichen Auskunftsrechts kann die gesuchstellende Person Auskunft über alle über sie in der Datensammlung vorhandenen Daten verlangen.

Daten über Dritte können nicht Gegenstand des datenschutzrechtlichen Auskunftsrechts sein.

Die Auskunft muss vollständig sein, also alle über die Person vorhandenen Daten umfassen. Dies ungeachtet der Form ihrer Aufzeichnung (z.B. Text, Bild, Ton oder sonstige Form) und unabhängig der Form ihrer Speicherung (z.B. Handnotiz in Papierdossier).

Im Bereich der ALV dient das Auskunftsrecht in erster Linie der Aktualisierung und der Korrektur von Daten im Rahmen eines laufenden Verfahrens (aktives Dossier). Jede Korrektur, Ergänzung oder Vernichtung von Daten muss den Amtsstellen, an welche die Daten üblicherweise weitergegeben werden, mitgeteilt werden, ebenso wie weiteren Stellen, wenn die betroffene Person dies wünscht. Wenn die Richtigkeit oder Unrichtigkeit von Daten nicht bewiesen werden kann, so hat die datenbearbeitende Stelle einen Vermerk hinzuzufügen, dass es sich um umstrittene Daten handelt.

Sobald das/die Dossier/s inaktiv ist/sind, bleibt das Auskunftsrecht gewährleistet, ohne dass weitere Änderungen möglich sind.

Form

- 20** Art. 126 AVIV sieht keine bestimmte Form vor, um Auskunft über ein Dossier zu verlangen.

Allerdings gilt als Regel, dass die Anfrage einer Person an den Verantwortlichen, ob sie betreffende Personendaten bearbeitet werden, schriftlich unter Beilegung der Kopie eines amtlichen Ausweises (Identitätskarte oder Pass) zu erfolgen hat. Mit Zustimmung des Verantwortlichen kann die Anfrage auch mündlich gestellt werden. Die angefragte Behörde kann auf das Vorweisen eines Ausweises verzichten, wenn die anfragende Person bekannt ist oder wenn sich deren Identität anderweitig feststellen lässt.

Der/die Vertreter/in hat sich durch eine Vollmacht auszuweisen.

Das Verfahren kann auf elektronischem Weg erfolgen, sofern die Person eine gesicherte Plattform benutzt.

Die Auskunft wird schriftlich erteilt oder in der Form, in der die Daten vorliegen. In Absprache mit dem Verantwortlichen kann die betroffene Person ihre Daten vor Ort einsehen. Falls sie damit einverstanden ist, kann ihr die Auskunft auch mündlich erteilt werden.

Die Auskunft wird in einer für die betroffene Person verständlichen Form erteilt.

Frist

- 21** Die Auskunft wird innerhalb von 30 Tagen nach Erhalt des Gesuchs erteilt.

Falls die Auskunft nicht innerhalb von 30 Tagen erteilt werden kann, informiert die zuständige Behörde die betroffene Person und gibt dabei an, innert welcher Frist die Auskunft erteilt wird.

Falls der Verantwortliche die Auskunft verweigert, einschränkt oder aufschiebt, teilt er dies innerhalb der gleichen Frist mit.

Datenbekanntgabe

(Art. 97a AVIG; Art. 32 und 33 ATSG; Art. 34a und 34b AVG)

22 Das Gesetz unterscheidet sowohl in Art. 97a AVIG wie auch in Art. 34a AVG zwei Formen der Datenbekanntgabe:

- Datenbekanntgabe, für welche die datenersuchende Stelle ein schriftlich begründetes Gesuch stellen muss und die nur im Einzelfall vorgenommen werden darf; oder
- Datenbekanntgabe, die auch ohne Gesuch und nicht nur im Einzelfall, wiederholt regelmässig und automatisch vorgenommen werden darf.

In jedem Fall können nur die für den fraglichen Zweck notwendigen Daten bekannt gegeben werden.

Wenn die Durchführungsstellen Daten in ihren eigenen Informationssystemen oder Dokumenten erfasst haben, so müssen sie gemäss jener Rechtsgrundlage Auskunft erteilen, die für sie im Bereich Datenschutz gilt.

Schweigepflicht

23 Die Mitarbeitenden, die an der Durchführung sowie der Kontrolle oder der Beaufsichtigung der Durchführung der ALV beteiligt sind, haben Verschwiegenheit zu bewahren (Art. 33 ATSG und Art. 34 AVG). Sie müssen Informationen, die sie bei ihrer Tätigkeit erlangen, vertraulich behandeln und sind zum Stillschweigen verpflichtet. Die Schweigepflicht gilt sowohl Dritten gegenüber (z. B. anderen Sozialversicherungen, Behörden oder Arbeitgebenden) wie auch innerhalb der Behörde.

Von der Schweigepflicht sind auch externe Personen, die zur Datenbearbeitung beigezogen wurden, betroffen. Soll von der Schweigepflicht abgewichen werden, muss eine gesetzliche Grundlage vorhanden sein (z. B. das verfahrensrechtliche Akteneinsichtsrecht nach Art. 47 ATSG oder die Amts- und Verwaltungshilfe nach Art. 32 ATSG). Eine entgegen der Schweigepflicht erfolgte Bekanntgabe von Personendaten kann den Tatbestand von Art. 105 AVIG, Art. 34 AVG oder Art. 320 StGB (Verletzung des Amtsgeheimnisses) erfüllen.

Auskunft, Amts- und Verwaltungshilfe

24 Art. 32 ATSG regelt die Amts- und Verwaltungshilfe: So geben die Verwaltungs- und Rechtspflegebehörden des Bundes, der Kantone, Bezirke, Kreise und Gemeinden den Organen der einzelnen Sozialversicherungen auf schriftliche und begründete Anfrage im Einzelfall kostenlos diejenigen Daten bekannt, die erforderlich sind für die Festsetzung, Änderung oder Rückforderung von Leistungen, für die Verhinderung ungerechtfertigter Bezüge, für die Festsetzung und den Bezug der Beiträge sowie für den Rückgriff auf haftpflichtige Dritte (Abs. 1). Gemäss Abs. 2 leisten die Organe der einzelnen Sozialversicherungen einander unter den gleichen Bedingungen Verwaltungshilfe.

Wichtig ist der für die gesamte sozialversicherungsrechtliche Verwaltungstätigkeit gültige Hinweis, dass Amtshilfe die Hilfe von Behörden (z.B. Sozialdienst) an Versicherungsträger meint und Verwaltungshilfe die Hilfe des einen Versicherungsträgers zugunsten eines anderen Versicherungsträgers.

Regulärer Datenverkehr

- 25** Nach Art. 97a AVIG und Art. 34a AVG dürfen die Durchführungsstellen den dort aufgelisteten Institutionen in Abweichung von Art. 33 ATSG Daten bekanntgeben, sofern kein überwiegendes Privatinteresse entgegensteht.

Die Daten dürfen den folgenden Behörden bekanntgegeben werden (Art. 97a Abs. 1 lit. a bis e^{bis}, Abs. 2 AVIG; Art. 34a Abs. 2 AVG):

- a) zwischen Durchführungsstellen des AVIG/AVG, wenn es für die Erfüllung der ihnen nach diesen Gesetzen übertragenen Aufgaben erforderlich ist;
- b) * den Durchführungsorganen der kantonalen Arbeitslosenhilfegesetze;
- c) den Organen einer anderen Sozialversicherung, wenn sich in Abweichung von Art. 32 Abs. 2 ATSG eine Pflicht zur Bekanntgabe aus einem Bundesgesetz ergibt oder für die Zuweisung oder Verifizierung der AHV-Nummer;
- d) den für Ausländerfragen zuständigen Behörden nach Art. 97 Abs. 3 des Bundesgesetzes vom 16. Dezember 2005 über die Ausländerinnen und Ausländer und über die Integration (AIG);
- e) * den für die Quellensteuer zuständigen Behörden nach Art. 88 und 100 des Bundesgesetzes vom 14. Dezember 1990 über die direkte Bundessteuer und den entsprechenden kantonalen Bestimmungen;
- f) * den kantonalen Steuerbehörden, sofern das kantonale Recht eine direkte Übermittlung der Leistungsabrechnung** an diese vorsieht
- g) den Organen der Bundesstatistik nach dem Bundesstatistikgesetz vom 9. Oktober 1992;
- h) den Strafuntersuchungsbehörden, wenn die Anzeige oder die Abwendung eines Verbrechens es erfordert;
- i) * dem Nachrichtendienst des Bundes (NDB) oder den Sicherheitsbehörden der Kantone zuhanden des NDB, wenn eine konkrete Bedrohung der inneren oder äusseren Sicherheit nach Art. 19 Abs. 2 des Bundesgesetzes vom 25. September 2015 über den Nachrichtendienst gegeben ist.
- j) den für die Bekämpfung der Schwarzarbeit zuständigen Behörden gemäss Artikel 11 und 12 des Bundesgesetzes vom 17. Juni 2005 gegen die Schwarzarbeit.
- l) * Die öffentlichen und privaten Arbeitslosenkassen dürfen an die Organe nach Art. 7 des Bundesgesetzes vom 8. Oktober 1999 über die in die Schweiz entsandten Arbeitnehmerinnen und Arbeitnehmer die für die Kontrolle der Einhaltung der minimalen Arbeits- und Lohnbedingungen erforderlichen Daten bekanntgeben.

* Nur ASAL-Daten

** *recte*: der Bescheinigung über die erhaltenen Leistungen (s. art. 30 Abs. 3 AVIV)

Bekanntgabe an Behörden auf schriftlich begründetes Gesuch hin

(Art. 97a Abs. 1 lit. f AVIG; Art. 34a Abs. 1 AVG)

- 26** Die Daten dürfen den folgenden Behörden bekanntgegeben werden:
- a) den Organen der Invalidenversicherung, wenn sich eine Pflicht zur Bekanntgabe aus dem Bundesgesetz vom 19. Juni 1959 über die Invalidenversicherung ergibt (IVG; SR 831.20);
 - b) den Sozialhilfebehörden, wenn die Daten für die Festsetzung, Änderung oder Rückforderung von Leistungen beziehungsweise für die Verhinderung ungerechtfertigter Bezüge erforderlich sind;
 - c) den Zivilgerichten, wenn die Daten für die Beurteilung eines familien- oder erbrechtlichen Streitfalles erforderlich sind;
 - d) den Strafgerichten und Strafuntersuchungsbehörden, wenn die Daten für die Abklärung eines Verbrechens oder eines Vergehens erforderlich sind;
 - e) * den Betreibungsämtern nach den Art. 91, 163 und 222 des Bundesgesetzes vom 11. April 1889 über die Schuldbetreibung und Konkurs;
 - f) * Steuerbehörden, wenn die Daten für die Anwendung der Steuergesetze erforderlich sind;
 - g) den Kindes- und Erwachsenenschutzbehörden nach Art. 448 Abs. 4 Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907 (Art. 34a Abs. 1 lit. e AVG);
 - h) den zuständigen Behörden für den Vollzug des Abkommens vom 21. Juni 1999 zwischen der Europäischen Gemeinschaft und ihren Mitgliedstaaten einerseits und der Schweizerischen Eidgenossenschaft andererseits über die Freizügigkeit samt Anhängen und Protokollen sowie der dazugehörigen schweizerischen Ausführungsgesetzgebung.

* Nur ASAL-Daten

Bekanntgabe an Dritte (Art. 97a Abs. 4 AVIG; Art. 34a Abs. 4 AVG)

- 27** In den übrigen Fällen dürfen Daten in Abweichung von Art. 33 ATSG an Dritte wie folgt bekannt gegeben werden:
- a. nicht personenbezogene Daten, sofern die Bekanntgabe einem überwiegenden Interesse entspricht;
 - b. Personendaten, sofern die betroffene Person im Einzelfall schriftlich eingewilligt hat oder, wenn das Einholen der Einwilligung nicht möglich ist, diese nach den Umständen als im Interesse des Versicherten vorausgesetzt werden darf.

Dieser Punkt wird insbesondere im Rahmen der Ausführungen zum Forschungsprivileg konkretisiert (vgl. Rz. 31 ff.).

Veröffentlichung (Art. 97a Abs. 3 AVIG; Art. 34a Abs. 3 AVG)

- 28** Daten, die von allgemeinem Interesse sind und sich auf die Anwendung des AVIG und des AVG beziehen, dürfen in Abweichung von Art. 33 ATSG veröffentlicht werden. Die Anonymität der Versicherten muss gewährleistet sein, in dem Sinne, dass Einzelpersonen nicht mehr reidentifiziert werden können, insbesondere durch die Rekombination von Daten.

Grenzüberschreitende Datenbekanntgabe (Art. 16 DSGVO)

- 29** Personendaten dürfen ins Ausland bekanntgegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates oder das internationale Organ einen angemessenen Schutz gewährleistet.

Wenn Personendaten ins Ausland bekanntgegeben werden, teilt der Verantwortliche der betroffenen Person auch den Namen des Staates oder der internationalen Organisation mit, dem oder der diese bekanntgegeben wurden und gegebenenfalls die in Artikel 16 Absatz 2 vorgesehenen Garantien oder die Anwendung einer der Ausnahmen gemäss Artikel 17 DSGVO.

Für jede Auskunft zu in den Systemen AVAM oder ASAL gespeicherten Daten ist das Auskunftsgesuch SECO-TC zur Prüfung zu unterbreiten.

Datenverkehr zwischen der Schweiz und den EU/EFTA-Staaten

(Art. 97a Abs. 1 lit. f Ziff. 7 AVIG; Art. 17e ATSV)

- 30** Bezüglich des ALV-Datenverkehrs mit der EU/EFTA verweisen wir auf Weisung ALE 883 Rz. B55 ff.

DATENBEARBEITUNG FÜR NICHT PERSONENBEZOGENE ZWECKE (FORSCHUNGSPRIVILEG)

(Art. 97a Abs. 4 AVIG; Art. 34a Abs. 4 AVG; Art. 15 ALV-IsV)

Grundsatz

- 31** Spezifische Personendaten können einmalig an Forschungsinstitutionen übermittelt werden, sofern die betroffenen Personen schriftlich ihre Einwilligung dazu gegeben haben. Keine Einwilligung ist notwendig für rein statistische oder anonymisierte Daten, wenn die Bekanntgabe einem überwiegenden Interesse entspricht (z.B. einer Publikation in AMSTAT).

Durchführungsbehörden der ALV und der öffentlichen Arbeitsvermittlung

- 32** Soweit eine gesetzliche Grundlage besteht (AVIG, AVG), können die Durchführungsbehörden der ALV und der öffentlichen Arbeitsvermittlung Personendaten für nicht personenbezogene Zwecke bearbeiten bzw. zur Bearbeitung weitergeben (z.B. für Forschung, Planung, Statistik, Gutachten oder Expertisen). Dafür können sie von gewissen gesetzlichen Vorgaben abweichen (Art. 39 Abs. 2 DSGVO).
- 33** Vom Forschungsprivileg darf nur Gebrauch gemacht werden, wenn folgende Voraussetzungen kumulativ erfüllt sind (Art. 39 Abs. 1 DSGVO), d.h. wenn:
- die Daten anonymisiert werden, sobald der Bearbeitungszweck dies erlaubt;
 - das Bundesorgan privaten Personen besonders schützenswerte Personendaten nur so bekanntgibt, dass die betroffenen Personen nicht bestimmbar sind;
 - die Empfängerin oder der Empfänger Dritten die Daten nur mit der Zustimmung des Bundesorgans weitergibt, das die Daten bekanntgegeben hat; und
 - die Ergebnisse nur so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind.

Verfahren

Form des Gesuchs

- 34** Das Gesuch muss schriftlich und mit Nachweisunterlagen eingereicht werden. Als Nachweisunterlagen gelten alle Dokumente, die es erlauben festzustellen, welche Daten zur Bekanntgabe notwendig sind (z.B. Mandatsvereinbarung, Dokumentation im Zusammenhang mit einem genehmigten Forschungsprojekt). Ein Zuschlagsentscheid in einem öffentlichen Ausschreibungsverfahren wird in der Regel nicht als ausreichend beurteilt.

Das Dokument muss zwingend die Zielsetzung/en der Bearbeitung, die Art der mit den Daten durchgeführten Operationen, die Kategorien der behandelten Personendaten, die Kategorien und die Anzahl der betroffenen Personen sowie die Dauer der Bearbeitung beschreiben.

Verantwortliche Stelle:

- 35** Ausgleichsstelle der Arbeitslosenversicherung
Staatssekretariat für Wirtschaft SECO
Direktion für Arbeit DA
Arbeitsmarkt und Arbeitslosenversicherung
Holzikofenweg 36, 3003 Bern

Kantonale Durchführungsstellen

- 36** Das in den kantonalen Datenschutzgesetzen erwähnte Forschungsprivileg ist nicht gültig für übermittelte Daten, die von den durch SECO-TC betriebenen Informationssystemen stammen.

ARTEN DES DATENAUSTAUSCHS UND GEBÜHREN

Arten

37 Die Daten werden auf gesicherte Weise grundsätzlich schriftlich und kostenlos übermittelt. Ausser der Übermittlung in Papierform sind folgende Arten des Datenaustauschs möglich:

a) Datenaustausch zwischen Systemen
Der Datenaustausch zwischen Systemen muss vom Gesetz vorgesehen sein. Zurzeit ist dies formell nur zwischen den von SECO-TC betriebenen Informationssystemen vorgesehen.

b) Auf elektronischem Weg (Art. 96c Abs. 2^{bis} AVIG)
Das AVIG sieht vor, dass die Datenbekanntgabe auf elektronischem Weg erfolgen kann. Dies ermöglicht die Verwendung der gebräuchlichen Benutzerschnittstellen (Sunet UVAL, Portal LPP, ELM usw.) sowie den Versand über geschützten Mailverkehr. Allerdings betrifft diese Bestimmung nur die ASAL- und eALV-Daten (vgl. Rz. 26).

Tatsächlich gibt es bis anhin keine spezifische Bestimmung, welche den elektronischen Datenaustausch im Rahmen der dem DSG unterstellten Systeme regelt. Deshalb dürfen die von AVAM und Job-Room stammenden Daten nicht Gegenstand einer elektronischen Datenbekanntgabe an Dritte sein. Eine Revision des AVG zu diesem Punkt ist allerdings im Gang.

Hinweis: Die Datenbekanntgabe auf elektronischem Weg (Art. 97a Abs. 8 AVIG) ist nicht mit dem in Artikel 1 AVIV vorgesehenen elektronischen Verkehr mit Behörden zu verwechseln. Dieser unterliegt besonderen Regeln und ist nicht Gegenstand dieses Leitfadens.

Gebühren (Art. 126a AVIV; Art. 18a ATSV; Art. 57a AVV)

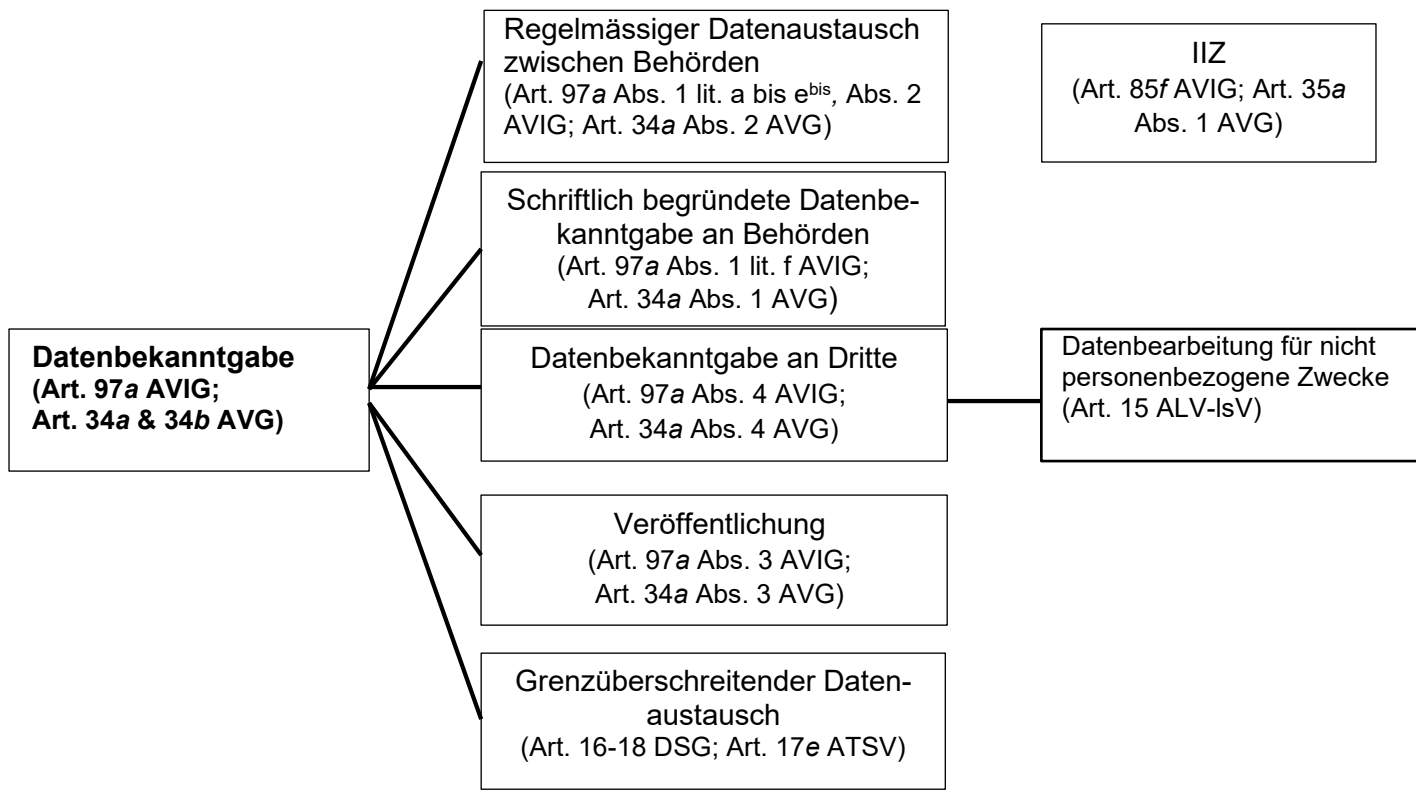
38 Eine Erhebung kostendeckender Gebühren ist für die in Art. 97a Abs. 3 AVIG sowie Art. 34a Abs. 3 AVG genannten Leistungen vorgesehen.

Eine Erhebung von Gebühren ist für die Fälle in Art. 97a Abs. 4 AVIG sowie in Art. 34a Abs. 4 AVG vorgesehen, wenn die Datenbekanntgabe zahlreiche Kopien oder andere Vervielfältigungen oder besondere Nachforschungen erfordert. Die Höhe dieser Gebühr wird entsprechend den in der allgemeinen Gebührenverordnung vom 8. September 2004 vorgesehenen Beträgen festgesetzt (SR 172.041.1).

SECO-TC hat bis anhin noch keine Weisung bezüglich der zu erhebenden Gebühren veröffentlicht.

ÜBERSICHT: DATENBEKANNTGABE GEMÄSS AVIG UND AVG

39



Je nach System anwendbares Gesetz:
 AVIG: ASAL, eALV
 AVG: AVAM, Job-Room

INTERINSTITUTIONELLE ZUSAMMENARBEIT (IIZ)

Grundsatz

- 40** Gemäss Art. 85f AVIG regelt und fördert die IIZ – im Interesse der betroffenen Person sowie der Effizienz des Gesamtsystems – die Zusammenarbeit der involvierten Institutionen. Diese können unter gewissen Voraussetzungen untereinander Informationen austauschen, die nach datenschutzrechtlichen Grundsätzen als besonders schützenswert gelten. Die Regelung nach Art. 85f AVIG stellt somit eine Ausnahme von der beruflichen Schweigepflicht und eine Erleichterung der Amts- und Verwaltungshilfe dar.

Die Zusammenarbeit im Rahmen der IIZ erfolgt zeitlich befristet und dient dem eng umrissenen Zweck der (Wieder-)Eingliederung im Einzelfall. Die betroffene Person ist über die möglichen sowie geplanten Arten der Zusammenarbeit zu informieren. Eine Datenbekanntgabe bzw. ein Datenaustausch sind gegenüber der betroffenen Person offenzulegen.

Aufgabendelegation

- 41** Um die Zielsetzungen der einzelnen Institutionen, insbesondere die Ausbildungs- und Arbeitsintegration, zu unterstützen, kann bei der IIZ den in Art. 85f Abs. 1 AVIG erwähnten Stellen während einer gewissen Zeit die Fallverantwortung übertragen werden. Dabei interessiert insbesondere, ob bei einer Aufgabendelegation an eine andere Behörde, Institution oder an eine gemeinsame Wiedereingliederungsstelle Besonderheiten gelten und wie die Anforderungen des Datenschutzes bezogen auf diese Beziehungen zu konkretisieren sind. Ausgangspunkt bildet damit die Frage, inwieweit die Aufgabenerfüllung durch solche Behörden, Institutionen und Stellen zulässig ist.

Erleichterter Datenaustausch

- 42** Neben den allgemeinen datenschutzrechtlichen Normen im AVIG und AVG sind weitere Normen verankert, die den Datenaustausch erleichtern und damit insbesondere die IIZ fördern sollen (Art. 85f AVIG und Art. 35a AVG).

Wenn die ALV (KAST, RAV, LAM für AMM und die Arbeitslosenkassen) im Rahmen der IIZ mit einer der in Art. 85f Abs. 1 AVIG abschliessend aufgeführten Stellen eng zusammenarbeiten möchte, ist den genannten Stellen der Datenaustausch zu ermöglichen. Voraussetzung ist jedoch, dass eine Datenbekanntgabe auf Gesuch hin und nur im Einzelfall, d.h. für die Dauer der IIZ erfolgt (Art. 85f Abs. 2 AVIG). Dazu müssen gemäss Abs. 2 lit. a und b folgende Voraussetzungen kumulativ erfüllt sein:

- a. die betroffene Person bezieht Leistungen von einer dieser Stellen und stimmt der Gewährung des Zugriffs zu; und
- b. die genannten Stellen gewähren den Durchführungsstellen der ALV Gegenrecht.

Im Zusammenhang mit den erwähnten Voraussetzungen gilt es darauf hinzuweisen, dass eine betroffene Person gleichzeitig Leistungen von mehreren in Art. 85f Abs. 1 AVIG erwähnten Stellen beziehen kann. Die Voraussetzung des Leistungsbezuges beschränkt sich sodann nicht auf Leistungen monetärer Art, sondern umfasst auch Beratungsleistungen usw.

Einwilligung in die Datenbekanntgabe

- 43** Die Einwilligung im Rahmen der IIZ richtet sich nach den allgemeinen Voraussetzungen der Einwilligung bei der Bearbeitung von Personendaten. Zudem besteht auch bei der IIZ eine Informationspflicht gegenüber der einwilligenden Person. Allerdings kann die Information der betroffenen Person auch nach ergangener Einwilligung erfolgen.

Die Informationspflicht gegenüber der betroffenen Person bezogen auf die Datenbekanntgabe bei der IIZ umfasst Informationen bezüglich:

- Ziel und Zweck der IIZ im konkreten Fall;
- der involvierten Stellen und Personen;
- des vorgesehenen Ausmasses und der Form der Datenbekanntgabe;
- der Dauer der Aufbewahrung;
- der Massnahmen zur Datensicherheit;
- des Auskunfts- bzw. Akteneinsichtsrechts; und
- des jederzeitigen Widerrufsrechts der Vollmacht einschliesslich des Aufzeigens der Konsequenzen eines Widerrufs.

Zudem muss der betroffenen Person im Rahmen der Informationspflicht deutlich gemacht worden sein, dass sie in eine Datenbearbeitung einwilligt. Zu dieser ist sie von Gesetzes wegen nicht verpflichtet. So zieht die IIZ auch keine spezifischen Pflichten der versicherten Person nach sich. Mit anderen Worten: Die Einwilligung in die IIZ kann nicht eingefordert werden und die Verweigerung der Einwilligung führt zu keinen Konsequenzen für die versicherte Person.

- 44** Keine Einwilligung ist erforderlich:

- beim Datenaustausch mit der IV-Stelle nach Art. 85f Abs. 3 und Abs. 4 AVIG;
- bei der Datenbekanntgabe an Sozialhilfebehörden nach Art. 97a Abs. 1 lit. f Ziff. 1 AVIG;
- bei der Datenbekanntgabe an Dritte nach Art. 97a Abs. 4 lit. b AVIG (wenn die Einwilligung nicht eingeholt, aber vorausgesetzt werden kann); sowie
- bei verweigerter Zustimmung, wenn bestimmte Voraussetzungen nach Art. 36 Abs. 2 lit. e DSGVO erfüllt sind.

Fehlendes Gegenrecht: Einzelfallregelung

- 45** Die Datenbekanntgabe seitens der ALV an IIZ-Stellen ist grundsätzlich nur unter den kumulativ zu erfüllenden Voraussetzungen der Einwilligung der betroffenen Person und des Gegenrechts der datenempfangenden Stelle zulässig.

Fehlt es an einer gesetzlichen Verankerung des Gegenrechts eines Datenaustauschs zwischen ALV-Behörde und einer anderen in Art. 85f Abs. 1 AVIG genannten Institution, darf die ALV-Behörde gestützt auf Art. 97a Abs. 4 lit. b AVIG Personendaten im Einzelfall anderen IIZ-Stellen nur bekanntgeben, wenn die betroffene Person schriftlich eingewilligt hat oder, falls das Einholen der Einwilligung nicht möglich ist, wenn diese Einwilligung nach den Umständen als im Interesse des Versicherten liegend vorausgesetzt werden kann. Die hier geregelte Datenbekanntgabe bezieht sich auf «Dritte».

Vorbehalten bleibt schliesslich Art. 97a Abs. 1 lit. f Ziff. 1 AVIG, wonach Sozialhilfebehörden unter gewissen Voraussetzungen Daten bekannt gegeben werden können.

Datenbekanntgabe an die IV

46 Art. 85f Abs. 3 AVIG und Art. 35a Abs. 1^{bis} AVG regeln die Datenbekanntgabe an die IV separat. Danach können den IV-Stellen im Rahmen der IIZ wiederholt, regelmässig und automatisch (nicht nur im Einzelfall und auf schriftlich begründetes Gesuch hin) Daten der betroffenen Personen bekanntgegeben werden. Die Bekanntgabe kann auch ohne deren Zustimmung erfolgen. Sie müssen jedoch nachträglich über den Datenaustausch und dessen Inhalt informiert werden. Dazu müssen folgende Voraussetzungen kumulativ erfüllt sein:

- Es darf kein überwiegendes Privatinteresse entgegenstehen;
- es ist noch nicht klar bestimmt, ob die ALV oder die IV die Kosten trägt; und
- die Auskünfte dienen der Feststellung, ob Eingliederungsmassnahmen der IV oder der ALV besser geeignet sind oder ob bei einer anderen Versicherung Ansprüche bestehen.

Im Hinblick auf die berufliche Wiedereingliederung von Personen haben die Organe der IV im Rahmen der IIZ nach Art. 35 Abs. 3 lit. g AVG zudem Zugriff auf AVAM und können Daten bearbeiten.

Sichtung der AVAM-Daten

47 Die Sichtung der AVAM-Daten durch die in Art. 85f Abs. 1 AVIG – bzw. den in Art. 35 Abs. 3 lit. g und j^{bis} AVG – genannten Institutionen ist unter den oben beschriebenen Voraussetzungen möglich. Erlaubt ist demnach das Lesen, nicht aber das Abändern von Daten durch die genannten Institutionen (vgl. Art. 96c AVIG, welcher sich auf die Organe und Stellen bezieht, welche das AVIG unmittelbar vollziehen, sowie Anhang II ALV-IsV).

Schweigepflicht und Geheimnisschutz

48 Was die Geheimhaltung von Informationen in der IIZ anbelangt, ist vorab der strafrechtliche Geheimnisschutz massgebend (Art. 320 und 321 StGB). Die Schweigepflichtnorm in Art. 33 ATSG bindet die IV und die ALV. Art. 34 AVG stipuliert eine Schweigepflicht für Personen, die an der Durchführung der öffentlichen Arbeitsvermittlung beteiligt sind. Schweigepflichtnormen finden sich auch in den kantonalen Sozialhilfegesetzen.

SECO-TC INFORMATIONSSYSTEME

Grundsatz

- 49** SECO-TC betreibt verschiedene Informationssysteme zur Erfüllung der gesetzlichen Aufgaben und für statistische Zwecke (Art. 83 Abs. 1bis AVIG).

SECO-TC als Verantwortlicher

- 50** Als Verantwortlicher ist SECO-TC dazu verpflichtet, umfassend für die Einhaltung der datenschutzrechtlichen Anforderungen zu sorgen, und die Rechtmässigkeit der Datenbearbeitung zu überwachen. SECO-TC muss dafür sorgen, dass die Art und Weise des Bearbeitens die Betroffenen zu keinem Zeitpunkt in ihrer Persönlichkeit verletzt.

Die Durchführungsbehörden sind für die Datenbearbeitung mitverantwortlich, denn es sind vor allem sie, welche die Daten in die Systeme eingeben und Änderungen daran vornehmen. Sie haben demnach für die Einhaltung der Grundsätze zum Datenschutz und der von SECO-TC erlassenen Richtlinien zu sorgen.

Eintrag von Daten in die Informationssysteme

- 51** Alle über die betroffene Person gesammelten Daten sind in den von SECO-TC betriebenen Informationssystemen abzulegen (so z.B. Formulare, Verfügungen, Beratungsprotokolle, Arztzeugnisse, Dokumente bezüglich der Arbeitsfähigkeit oder -unfähigkeit, medizinische Gutachten). Die Informationssysteme enthalten ausschliesslich Felder für Personendaten, die von den Durchführungsstellen benötigt werden, um die ihnen gesetzlich übertragenen Aufgaben zu erfüllen (Art. 96b AVIG, Art. 33a AVG).

Umgekehrt sollten Informationen, für die die von SECO-TC verwalteten Informationssysteme kein Eingabefeld vorsehen, weder gesammelt noch gespeichert werden.

DATENMIGRATION

(Art. 5 ALV-IsV)

Grundsatz

- 52** Datenmigration, Datenexport und Datenimport sind besondere Formen der Datenbearbeitung.

Als Datenmigration bezeichnet man den Prozess, bei dem Personendaten transferiert werden. Die Datenmigration lässt sich grob in drei Phasen unterteilen:

1. Export und Bereinigung der alten Daten;
2. Mapping alter und neuer Datenstrukturen; und
3. Import der Daten ins neue System.

Die Durchführungsstellen dürfen keine Daten erheben oder festhalten, für die in den von SECO-TC verwalteten Informationssystemen keine Datenfelder vorgesehen sind. Erlaubt ist ihnen unter gewissen Voraussetzungen, die Daten aus den Informationssystemen in eigene Systeme zu importieren.

Voraussetzungen

- 53** Der Export von Daten aus den Informationssystemen nach Art. 83 Abs. 1^{bis} AVIG in die Informationssysteme der Durchführungsstellen bedarf vor dem ersten Export in das jeweilige Informationssystem einer Genehmigung durch SECO-TC.

Die Genehmigung wird nur erteilt, wenn die folgenden Voraussetzungen erfüllt sind:

- a. Der Export und die Nutzung der Daten sind für den Vollzug des AVIG oder des AVG notwendig.
- b. Die Durchführungsstellen gewährleisten für die exportierten Daten die Einhaltung der Datenschutzbestimmungen.
- c. Im Falle kantonaler Durchführungsstellen verfügen diese für ihr eigenes Informationssystem und für die Bearbeitung von Daten aus Drittsystemen über eine Grundlage in einem kantonalen Gesetz im formellen Sinn.

Die Durchführungsstellen müssen sich jederzeit über die Richtigkeit der Daten versichern.

Verfahren

- 54** Die Durchführungsstellen unterbreiten ihre Gesuche der SECO-TC. Sie müssen darin präzisieren, welche Daten betroffen sind und die Notwendigkeit des Datenexports in ihre Systeme zur Erfüllung ihrer Aufgabe darlegen. Überdies müssen sie einen angemessenen Datenschutz gewährleisten.

Die Kantone müssen ausserdem die Existenz einer Rechtsgrundlage aufzeigen, und zwar sowohl für das Informationssystem, in welches die Daten zu importieren sind, als auch für das Prinzip des Datentransfers von den Informationssystemen der ALV in das betroffene kantonale System.

Die Nutzung der Daten ist streng beschränkt auf das, was für den Vollzug des AVIG und des AVG notwendig ist (vgl. Erläuterungen Änderung der Arbeitslosenversicherungsverordnung und ALV-Informationssystemeverordnung, 26. Mai 2021, S. 19).

DATENBEARBEITUNG DURCH EINEN AUFTRAGSBEARBEITER

(Art. 96b AVIG; Art. 33a AVG)

- 55** Das AVIG und das AVG erlauben unter bestimmten Umständen eine Datenbearbeitung durch einen Auftragsbearbeiter, insbesondere im Bereich der Aufsicht über die Durchführung des AVG (Art. 33a Abs. 1 lit. e AVG) sowie bei der Datenbekanntgabe für die Forschung (Art. 15 ALV-IsV).

Der Umfang der Bearbeitung durch Dritte wird in einer Bearbeitungsvereinbarung festgelegt (Art. 9 Abs. 1 DSGVO).

Bedingungen der Bearbeitung durch einen Auftragsbearbeiter

Verantwortung

- 56** Wenn die Bearbeitung durch einen Auftragsbearbeiter erfolgt, behält der Verantwortliche die ursprüngliche Verantwortung für die Daten.

Der Verantwortliche sorgt für die Einhaltung des Datenschutzes und dafür, dass die Daten auftragsgemäss bearbeitet werden, insbesondere was deren Verwendung und Bekanntgabe betrifft. Auch müssen die Datensicherheit und deren Überwachung gewährleistet sein. Für die Auftragsbearbeiterin / den Auftragsbearbeiter gelten die gleichen datenschutzrechtlichen Grundsätze wie für den Verantwortlichen.

Sicherstellung einer angemessenen Datensicherheit

- 57** Sachgerechte Massnahmen zur Sicherstellung einer angemessenen Datensicherheit sind etwa:

- sorgfältige Auswahl der Auftragsbearbeiter;
- gründliche Instruktion der Auftragsbearbeiter sowie ausreichende Information über die Sensitivität der Daten;
- Beendigung des Auftragsverhältnisses im Falle, dass die Auftragsbearbeiter trotz entsprechender Abmahnung nicht die nötige Sicherheit bieten;
- vertragliche Zusicherung der Auftragsbearbeiter, dass sie über angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten verfügen;
- Verpflichtung der Auftragsbearbeiter, über die von ihnen getroffenen Massnahmen im Bereich der Datensicherheit regelmässig oder auf Verlangen Bericht zu erstatten (getroffene Massnahmen, Effektivität, Verbesserungen, etwaige sicherheitsrelevante Vorfälle); und
- regelmässige Audits bei den Auftragsbearbeitern durch stichprobeweise Kontrollen (Vermeidung eines Verschuldens von SECO-TC, sollte es aufgrund erkennbar mangelhafter Datensicherheit seitens der Auftragsbearbeiter zu einer unrechtmässigen Persönlichkeitsverletzung kommen).

Bearbeitungsvereinbarung

- 58** Jede Datenbearbeitung durch Dritte setzt eine detaillierte Vereinbarung für den Datenschutz voraus. Dies gilt insbesondere bei der Weitergabe von Daten im Rahmen der Bearbeitung für nicht personenbezogene Zwecke.

59 Die datenschutzrechtlichen Vorgaben und Vereinbarungen sind vertraglich festzulegen, z.B.:

- Ausgangslage;
- Gegenstand und Umfang der Datenbearbeitung;
- Verantwortlichkeiten;
- Informationssicherheit;
- Kontrolle (Berichts- und Informationspflichten);
- Zweck der Datenbearbeitung;
- Zugriff auf die Daten durch das berechnigte Personal und seine Instruktion im Bereich des Datenschutzes;
- Geheimhaltungs- und Schweigepflicht;
- Wahrnehmung der Rechte betroffener Personen;
- Datensicherheitsmassnahmen;
- Fragen der Datenbekanntgabe und -weitergabe;
- Pflicht zur regelmässigen Berichterstattung;
- Datenverknüpfungen;
- Kontrollmöglichkeiten oder Vereinbarung externer Prüfungen;
- Unterauftragsverhältnisse;
- Ort der Bearbeitung und Aufbewahrung der Daten;
- spezifische Massnahmen;
- Haftung und Konventionalstrafen;
- Verhältnis zu anderen AGB;
- Vertragsdauer und Vertragsauflösung;
- Anonymisierung, Pseudonymisierung und Löschung der Daten;
- Anwendbares Recht und Gerichtsstand.

Von den Durchführungsstellen für ihre eigenen Systeme erhobene Daten

60 Den Durchführungsstellen ist es nicht gestattet, Daten aus den Informationssystemen der Ausgleichsstelle an Dritte zur Bearbeitung weiterzugeben. Dies gilt auch für Daten, die sie mit Zustimmung von SECO-TC in ihre eigenen Systeme importiert haben.

DATENSICHERHEIT

Grundsatz

- 61** Die Schutzmassnahmen werden anhand der Risikoanalyse festgelegt. Das DSG beschäftigt sich mit den Risiken für die Privatsphäre der betroffenen Personen. Es beschränkt sich allerdings auf den Hinweis, dass im Fall von «hohem Risiko» besondere Massnahmen getroffen werden müssen. Das hohe Risiko ergibt sich aus verschiedenen Faktoren (der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung) und liegt namentlich unter zwei Umständen vor: bei der umfangreichen Bearbeitung besonders schützenswerter Personendaten und wenn systematisch umfangreiche öffentliche Bereiche überwacht werden.
- 62** Im Bereich der ALV basiert die Datensicherheit nicht nur auf dem DSG, sondern berücksichtigt auch die allgemeinen Sicherheitsvorschriften des Bundes für die kritischen Infrastrukturen gemäss Informationssicherheitsgesetz vom 18. Dezember 2020 (ISG, SR 128, in Kraft seit 1. Mai 2022). Das ISG stützt sich auf das Risiko für die Ausübung der Tätigkeit der ALV.
- 63** Die Durchführungsstellen, welche Daten bearbeiten, müssen die Vertraulichkeit, die Verfügbarkeit und die Integrität der von ihnen bearbeiteten Personendaten gewährleisten. Sie haben geeignete technische und organisatorische Massnahmen zu treffen, um Personendaten vor jeglicher unbefugten Bearbeitung zu schützen (Art. 3 DSV).

Um die Vertraulichkeit zu gewährleisten, müssen geeignete Massnahmen getroffen werden, damit:

- a. berechnete Personen nur auf diejenigen Personendaten Zugriff haben, die sie zur Erfüllung ihrer Aufgaben benötigen (Zugriffskontrolle);
- b. nur berechnete Personen Zugang zu den Räumlichkeiten und Anlagen haben, in denen Personendaten bearbeitet werden (Zugangskontrolle);
- c. unbefugte Personen automatisierte Datenbearbeitungssysteme nicht mittels Einrichtungen zur Datenübertragung nutzen können (Benutzerkontrolle).

Um die Verfügbarkeit und Integrität der Daten zu gewährleisten, müssen geeignete Massnahmen getroffen werden, damit:

- a. unbefugte Personen Datenträger nicht lesen, kopieren, verändern, verschieben, löschen oder vernichten können (Datenträgerkontrolle);
- b. unbefugte Personen Personendaten im Speicher nicht speichern, lesen, ändern, löschen oder vernichten können (Speicherkontrolle);
- c. unbefugte Personen bei der Bekanntgabe von Personendaten oder beim Transport von Datenträgern Personendaten nicht lesen, kopieren, verändern, löschen oder vernichten können (Transportkontrolle);
- d. die Verfügbarkeit der Personendaten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können (Wiederherstellung);

- e. alle Funktionen des automatisierten Datenbearbeitungssystems zur Verfügung stehen (Verfügbarkeit), Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte Personendaten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität);
- f. Betriebssysteme und Anwendungssoftware stets auf dem neusten Sicherheitsstand gehalten und bekannte kritische Lücken geschlossen werden (Systemsicherheit).

Um die Nachvollziehbarkeit zu gewährleisten, muss dafür gesorgt werden, dass:

- a. überprüft werden kann, welche Personendaten zu welcher Zeit und von welcher Person im automatisierten Datenbearbeitungssystem eingegeben oder verändert werden (Eingabekontrolle);
- b. überprüft werden kann, wem Personendaten mit Hilfe von Einrichtungen zur Datenübertragung bekanntgegeben werden (Bekanntgabekontrolle);
- c. Verletzungen der Datensicherheit rasch erkannt (Erkennung) und Massnahmen zur Minderung oder Beseitigung der Folgen ergriffen werden können (Beseitigung).

64 Zu diesem Zweck halten sich die Durchführungsbehörden an die einschlägigen Richtlinien von SECO-TC:

- Internes Kontrollsystem (IKS) in den AVIG Durchführungsstellen
- Organisationshandbuch für das IKS der Arbeitslosenversicherung (ALV)

Technische Massnahmen

65 Unter technischen Massnahmen sind Mittel der Technik oder physische Mittel zu verstehen, die die Sicherheit der Daten zu gewährleisten vermögen, etwa folgende:

- Der Zugang zu den Personendaten ist geschützt (z.B. durch Passwort oder Fingerscan). Falls ein Passwort verwendet wird, soll dieses eine Mindestkomplexität aufweisen (Kombination von Gross- und Kleinbuchstaben, Zahlen und Zeichen);
- das System verunmöglicht eine unbefugte Datenweitergabe durch Mitarbeitende;
- die Datenbewirtschaftung ist gewährleistet;
- die Systeme sind so konzipiert, dass der betroffenen Person innert vernünftiger Frist Auskunft erteilt werden kann, welche Personendaten über sie bearbeitet werden (Auskunftsrecht);
- die Datenbearbeitungsprogramme sowie die Software zum Schutz vor Hacker/innenangriffen (Firewall usw.) sind aktuell (Update) und entsprechen dem neusten Stand der Technik, der auf dem Markt erhältlich ist;
- für die elektronische Kommunikation gilt, dass Personendaten zur Sicherstellung der Vertraulichkeit und Korrektheit mit geeigneten technischen Massnahmen geschützt werden müssen. Bei der Datenübertragung darf es nicht zu Datenverlusten, Datenverfälschungen oder zu unberechtigten Zugriffen kommen.

Organisatorische Massnahmen

- 66** Organisatorische Massnahmen sind Strukturen oder Prozesse, die zur Erhöhung der Datensicherheit Aufgaben und Verantwortlichkeiten festlegen, z.B.:
- Mitarbeitende können nur Personendaten einsehen, die sie zur Erfüllung ihrer betrieblichen Aufgaben benötigen. Innerhalb der meisten Kantone oder privaten Arbeitslosenstellen haben wohl alle zugangsberechtigten Personen rein technisch Zugriff auf sämtliche Versichertendaten, d.h. es besteht in der Regel keine dynamische Zuordnung der Zugriffsberechtigungen. Aus diesem Grund sind die Mitarbeitenden anzuleiten, dass sie nur diejenigen Daten abrufen, die sie zur Erfüllung ihres Auftrags zwingend benötigen;
 - das Vorgehen, nach welchem Personen Systemberechtigungen erhalten und ihnen diese auch wieder entzogen werden (Prozess der Benutzendenfreigabe), ist festgelegt und nachvollziehbar, zudem muss es dokumentiert werden;
 - es wird in regelmässigen Abständen kontrolliert, ob alle zugelassenen Benutzenden sowie deren Berechtigungen noch aktuell sind;
 - alle vorgenommenen Kontrollen sowie kritischen Aktivitäten, Fehler oder missglückte Prozesse werden dokumentiert;
 - die Verantwortlichkeiten für die Daten sind klar zugewiesen; ein möglicher Missbrauch und eine daraus folgende Persönlichkeitsverletzung müssen zugewiesen werden können;
 - die betrieblichen Strukturen sind so festgelegt, dass die Daten nicht unnötig transportiert oder verschoben werden müssen; und
 - die Mitarbeitenden werden im Umgang mit Daten geschult und behandeln diese vertraulich.

AUFBEWAHRUNG, ARCHIVIERUNG UND VERNICHTUNG VON DATEN (INKLUSIVE PAPIERAKTEN)

Aufbewahrung

- 67** Personendaten dürfen nur so lange aufbewahrt werden, wie sie für den Zweck, für den sie erhoben wurden, benötigt werden (Zweckbindung). Wann genau dieser Zeitpunkt ist, muss im Einzelfall bestimmt werden. Eine Datenaufbewahrung oder Archivierung auf unbestimmte Zeit ist aber nicht möglich (BGE 113 Ia 257). Sofern keine explizite Rechtsgrundlage besteht, müssen nach gängiger Praxis die personenbezogenen Daten spätestens nach zehn Jahren anonymisiert oder vernichtet werden.
- 68** Anonymisierte Daten dürfen weiterhin aufbewahrt werden, denn die Anonymisierung hat zur Folge, dass die Daten keinen Personenbezug mehr aufweisen. Bezüglich der Wahrung der Privatsphäre und des Persönlichkeitsschutzes hat sie die gleiche Wirkung wie die Vernichtung.
- 60** Art. 125 AVIV widmet sich der Aktenaufbewahrung:
- Daten aus Geschäftsbüchern und Buchungsbelegen sind zehn Jahre aufzubewahren.
 - Daten über die Versicherungsfälle sind nach ihrer letzten Bearbeitung fünf Jahre aufzubewahren.

Archivierung

- 70** Archivwürdig im Sinne des Bundesgesetzes über die Archivierung (Archivierungsgesetz, BGA; SR 152.1) sind Unterlagen, die von juristischer oder administrativer Bedeutung sind oder einen grossen Informationswert haben (vgl. Art. 3 BGA). Archivwürdige Unterlagen des Bundes werden im Bundesarchiv archiviert. Die in den Informationssystemen der ALV enthaltenen Personendaten werden nicht als archivwürdig qualifiziert.

Die kantonalen Durchführungsstellen der ALV sind berechtigt, Daten aus den durch SECO-TC verwalteten Informationssystemen zu extrahieren, um ihre Dossiers den kantonalen Archiven anzubieten, sofern es sich dabei um eine im kantonalen Archivierungsgesetz vorgesehene Pflicht handelt.

Vernichtung

- 71** Daten, die nicht archivwürdig sind und nicht in anonymisierter Form aufbewahrt werden, müssen nach Ablauf ihrer Aufbewahrungsdauer vernichtet werden (vgl. Art. 9a ATSV, Art. 38 DSG).

SECO-TC ist verantwortlich für die Löschung von Daten aus den von ihm verwalteten Informationssystemen. Die Vernichtung von Daten muss den Durchführungsstellen mitgeteilt werden, damit diese die Daten in ihren eigenen Systemen sowie in allen anderen Formaten, die sich in ihrem Besitz befinden, vernichten (z. B. Papier, CD, USB-Sticks usw.). Schliesslich sind die Vollzugsorgane verpflichtet, die in ihrem Besitz befindlichen Daten unaufgefordert zu vernichten, sobald sie diese nicht mehr benötigen.

Transparenz und Nachvollziehbarkeit

- 72** Die Anonymisierung oder Vernichtung der Daten muss transparent und nachvollziehbar sein. Die Durchführungsstellen tragen die Verantwortung für die fachgerechte Anonymisierung oder Vernichtung der Daten, welche in ihren jeweiligen Informationssystemen oder Akten erfasst sind. Sie haben sicherzustellen, dass ihre betrieblichen Prozesse so ausgestaltet sind, dass Daten nicht fälschlicherweise weiterbestehen. So erfolgt die Löschung z.B. idealerweise zentral und nicht etwa individuell durch die einzelnen Mitarbeitenden.

DOKUMENTE, APPS UND NÜTZLICHE LINKS

- Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (<http://www.edoeb.admin.ch/>)
- Konferenz der schweizerischen Datenschutzbeauftragten (<http://www.privatim.ch/de>)
- Europäischer Datenschutzbeauftragter (https://edps.europa.eu/_de)

BIBLIOGRAPHIE

Blechta, Gabor P., PD Dr. iur.; Vasella, David, Dr. iur. - Datenschutzgesetz /Öffentlichkeitsgesetz - Helbing Lichtenhahn Verlag, Basel 2023

Uttinger, Ursula, lic. iur., MBA HSG; Geiser, Thomas, Prof. Dr. iur., Dr. h.c. - Das neue Datenschutzrecht, Helbing Lichtenhahn Verlag, Basel 2023

Meier, Philippe, Prof. Dr. iur.; Métille, Sylvain, Prof. Dr. iur., Avocat - Loi sur la protection des données - Helbing Lichtenhahn Verlag, Bâle 2023

Benhamou, Yaniv, Prof. Dr. iur.; Cottier, Bertil, Prof. Dr. - Petit commentaire LPD- Helbing Lichtenhahn Verlag, Bâle 2023