



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Wirtschaft, Bildung und Forschung WBF
Staatssekretariat für Wirtschaft SECO

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

**Arbeitsmarkt /
Arbeitslosenversicherung
(TC)
Juristischer Dienst
(TCJD)**

1. Auflage
vom 1. Juli 2018
(Stand 1. Juli 2019)

VORWORT

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. Öffentliche Organe dürfen Daten nur aufgrund einer rechtlichen Grundlage, nur für den angegebenen Zweck und nur soweit erforderlich bearbeiten. Die betroffenen Personen können gegenüber den öffentlichen Organen Rechte geltend machen. Sie haben Anspruch auf Auskunft darüber, welche Daten über sie bearbeitet werden. Unter gewissen Voraussetzungen können sie die Berichtigung, Sperrung oder Löschung der Daten verlangen.

Seit dem 1. Juli 1993 ist das Bundesgesetz über den Datenschutz (DSG) in Kraft. Es regelt das Bearbeiten von Daten natürlicher und juristischer Personen durch Privatpersonen und Bundesorgane. Das DSG ist in den Bereichen der Arbeitslosenversicherung (AVIG) und der Arbeitsvermittlung (AVG) unmittelbar anwendbar für personendatenbearbeitende Bundesorgane, private Arbeitslosenkassen, private Unternehmen (z. B. AMM-Anbietende) und Privatpersonen, die mit öffentlichen Aufgaben des Bundes betraut sind. Die Datenbearbeitung durch die kantonalen und kommunalen Behörden (z. B. RAV, LAM, KAST) oder durch Privatpersonen, die mit öffentlichen Aufgaben des Kantons oder der Gemeinde betraut sind, wird hingegen vom kantonalen Datenschutzrecht geregelt, selbst wenn diese Bundesrecht vollziehen. Spezifische bundesrechtliche Datenschutzbestimmungen (etwa aus dem AVIG, AVG oder ATSG) gehen – als *lex specialis* – wiederum dem kantonalen Datenschutzrecht sowie dem DSG vor.

Als Aufsichtsbehörde hat das SECO für eine einheitliche Rechtsanwendung zu sorgen und den Durchführungsorganen im Zusammenhang mit dem Gesetzesvollzug Weisungen zu erteilen (Art. 110 AVIG). Dies geschieht üblicherweise in Form der AVIG-Praxis, was vorliegend aus genannten föderalistischen Gründen nicht möglich ist: So gesehen ist der Datenschutzleitfaden AVIG & AVG für die einen verbindlicher Weisungstext und für die anderen eine Auslegehilfe.

Der Datenschutzleitfaden AVIG & AVG versteht sich als Hilfsmittel und bietet allen Durchführungsorganen Unterstützung in der Beurteilung von datenschutzrechtlichen Fragen und Verfahren. Er gibt einen Überblick über die zu beachtenden allgemeinen Grundsätze des Datenschutzrechts, definiert die Begriffe und behandelt allgemeine datenschutzrechtliche Themen. Er bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die im Rahmen des Vollzugs der Arbeitslosenversicherung oder der öffentlichen Arbeitsvermittlung Daten bearbeitet werden.

Die datenschutzrechtlichen Normen – seien sie auf Stufe Bund, Kanton oder Gemeinde legiferiert – orientieren sich terminologisch wie inhaltlich weitgehend am DSG. Aus diesem Grund erlauben wir uns, im Datenschutzleitfaden AVIG & AVG exemplarisch auf die entsprechenden DSG-Normen zu verweisen.

Der vorliegende Datenschutzleitfaden AVIG & AVG wird auf arbeit.swiss.ch sowie auf dem TCNet publiziert. Bitte richten Sie Ihre Fragen oder Anregungen an tcjd@seco.admin.ch.

Zitierung: Datenschutzleitfaden AVIG & AVG Rz1.

Ergänzend weisen wir darauf hin, dass am 25. Mai 2018 die neue Datenschutz-Grundverordnung der Europäischen Union (DSGVO) in Kraft getreten ist. Ab diesem Zeitpunkt ist die DSGVO für alle in der EU tätigen schweizerischen Unternehmen unmittelbar anwendbar. Den Verordnungstext sowie weitere Informationen zu den Auswirkungen auf die Schweiz finden Sie hier.

INHALTSÜBERSICHT

VORWORT

INHALTSÜBERSICHT

ABKÜRZUNGSVERZEICHNIS

LITERATURVERZEICHNIS

MATERIALIEN

NÜTZLICHE APP UND LINKS

ZWECK, GELTUNGSBEREICHE UND RECHTSQUELLEN 01 - 09

Zweck 01 - 01

Geltungsbereiche 02 - 05

Kantonale Datenschutzbeauftragte 06 - 08

Rechtsquellen 09 - 09

BEGRIFFE UND GRUNDSÄTZE 10 - 10

BEARBEITEN VON PERSONENDATEN 11 - 20

Grundsatz 11 - 11

Gesetzliche Voraussetzungen 12 - 12

Besonders schützenswerte («sensible») Personendaten 13 - 14

Versichertennummer 15 - 15

Schweigepflicht 16 - 17

Datenerhebung im Internet 18 - 19

Unrechtmässige Datenerhebung durch Private 20 - 20

DATENBEKANNTGABE 21 - 29

Grundsatz 21 - 21

Auskunft, Amts- und Verwaltungshilfe und Schweigepflicht 22 - 22

Regulärer Datenverkehr 23 - 24

Grenzüberschreitende Datenbekanntgabe 25 - 25

Abrufverfahren 26 - 27

Prüfschema Datenbekanntgabe 28 - 28

Übersicht: Datenbekanntgabe gemäss AVIG und AVG 29 - 29

AUSKUNFTSRECHT 30 - 36

Grundsatz 30 - 30

Auskunftsberechtigte Person 31 - 31

Auskunftsverpflichtete Stelle	32 - 33
Objekt	34 - 34
Form	35 - 35
Zulässige Einschränkung	36 - 36
INFORMATIONSSYSTEME DER AUSGLEICHSTELLE	37 - 41
Grundsatz	37 - 39
Die Ausgleichsstelle als Inhaberin der Datensammlung	40 - 40
Eintrag von Daten in die Informationssysteme	41 - 41
DATENMIGRATION	42 - 45
Grundsatz	42 - 42
Voraussetzungen	43 - 43
Gesuch um Datenexport respektive Datenimport	44 - 44
Folgen einer unbefugten Datenbeschaffung	45 - 45
DATENBEARBEITUNG DURCH DRITTE	46 - 55
Grundsatz	46 - 46
Voraussetzungen	47 - 47
Auftraggeber/in bleibt verantwortlich	48 - 49
Sicherstellung einer angemessenen Datensicherheit	50 - 51
Datenschutzvereinbarung	52 - 54
Von den Durchführungsorganen für ihre eigenen Systeme erhobenen Daten	55 - 55
BEARBEITEN FÜR FORSCHUNG, PLANUNG UND STATISTIK (FORSCHUNGSPRIVILEG)	56 - 60
Grundsatz	56 - 56
Ausgleichsstelle und private Arbeitslosenkassen	57 - 58
Kantonale Durchführungsorgane	59 - 59
Beauftragte Private	60 - 60
INTERINSTITUTIONELLE ZUSAMMENARBEIT (IIZ)	61 - 72
Grundsatz	61 - 61
Ziele	62 - 62
Erleichterter Datenaustausch	63 - 63
Einwilligung in die Datenbekanntgabe	64 - 65
Informationspflicht	66 - 66
Fehlendes Gegenrecht: Einzelfallregelung	67 - 67
Datenbekanntgabe an die IV	68 - 68

Transparenz	69 - 69
Sichtung der AVAM-Daten	70 - 70
Schweigepflicht und Geheimnisschutz	71 - 71
Übersicht Datenaustausch	72 - 72
DATENSICHERHEIT	73 - 75
Grundsatz	73 - 73
Technische Massnahmen	74 - 74
Organisatorische Massnahmen	75 - 75
AUFBEWAHRUNG, ARCHIVIERUNG UND VERNICHTUNG VON DATEN (INKL. PAPIERAKTEN)	76 - 86
Grundsatz	76 - 76
Aufbewahrung	77 - 81
Archivierung	82 - 82
Vernichtung	83 - 84
Gesuch um Vernichtung	85 - 85
Transparenz und Nachvollziehbarkeit	86 - 86

ABKÜRZUNGSVERZEICHNIS

Abs.	Absatz
AHVG	Bundesgesetz über die Alters- und Hinterlassenenversicherung (SR 831.10)
ALE	Arbeitslosenentschädigung
ALV	Arbeitslosenversicherung
Art.	Artikel
ATSG	Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts (SR 830.1)
ATSV	Verordnung über den Allgemeinen Teil des Sozialversicherungsrechts (SR 830.11)
AVAM	Arbeitsvermittlungs- und Arbeitsmarktstatistik Informationssystem
AVG	Bundesgesetz über die Arbeitsvermittlung und den Personalverleih (Arbeitsvermittlungsgesetz, SR 823.11)
AVV	Verordnung über die Arbeitsvermittlung und den Personalverleih (Arbeitsvermittlungsverordnung, SR 823.111)
AVIG	Bundesgesetz über die obligatorische Arbeitslosenversicherung und die Insolvenzenschädigung (Arbeitslosenversicherungsgesetz, SR 837.0)
AVIV	Verordnung über die obligatorische Arbeitslosenversicherung und die Insolvenzenschädigung (Arbeitslosenversicherungsverordnung, SR. 837.02)
BGE	Bundesgerichtsentscheid
BV	Bundesverfassung (SR 101)
bzw.	beziehungsweise
DSGVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/E (Datenschutz-Grundverordnung)
Datenschutzleitfaden AVIG & AVG	Leitfaden zur Bearbeitung von Personendaten in den Bereichen AVIG und AVG
DMS	Dokumentenmanagementsystem
DSG	Bundesgesetz über den Datenschutz (SR 235.1)
EDÖB	Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte
EMRK	Konvention zum Schutze der Menschenrechte und Grundfreiheiten (Europäische Menschenrechtskonvention, SR 0.101)
EU-GRC	Charta der Grundrechte der Europäischen Union (2000/C 364/01)
EU-Richtlinien	Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates

IIZ	Interinstitutionelle Zusammenarbeit
IV	Invalidenversicherung
KAST	Kantonale Amtsstelle
KVG	Bundesgesetz über die Krankenversicherung (SR 832.10)
LAM	Logistikstelle für arbeitsmarktliche Massnahmen
RAV	Regionales Arbeitsvermittlungszentrum
SAK	Schweizerische Ausgleichskasse in Genf
SECO	Staatssekretariat für Wirtschaft
SR	Systematische Sammlung des Bundesrechts
u. a.	unter anderem
UVG	Bundesgesetz über die Unfallversicherung (SR 832.20)
usw.	und so weiter
V-ASAL	Verordnung über das Informationssystem für die Auszahlung von Leistungen (ASAL-Verordnung, SR 837.063.1)
V-AVAM	Verordnung über das Informationssystem für die Arbeitsvermittlung und Arbeitsmarktstatistik (AVAM-Verordnung, SR 823.114)
VDSG	Verordnung zum Bundesgesetz über den Datenschutz (SR 235.11)
V-LAMDA	Verordnung über das Informationssystem für die Analyse von Arbeitsmarktdaten (LAMDA-Verordnung, SR 837.063.2)
ZAS	Zentrale Ausgleichsstelle (www.zas.admin.ch)
z. B.	zum Beispiel

LITERATURVERZEICHNIS

- BÄNI, EVA-MARIA, in: Michael Kull (Hrsg.), Stämpflis Handkommentar (SHK), 1. Aufl., Bern 2014.
- BAERISWYL BRUNO / PÄRLI KURT, Datenschutzgesetz (DSG), Stämpfli Verlag, Bern 2015.
- BELSER, EVA MARIA / EPINEY, ASTRID / WALDMANN, BERNHARD, Datenschutzrecht Grundlagen und öffentliches Recht, Stämpfli Verlag, Bern 2011.
- EPINEY ASTRID / CIVITELLA TAMARA / ZBINDEN PATRIZIA, Datenschutzrecht in der Schweiz, Eine Einführung in das Datenschutzgesetz des Bundes, mit besonderem Akzent auf den für Bundesorgane relevanten Vorgaben, Freiburg 2009.
- EPINEY, ASTRID / HOBI, PATRICK, Die Revision des Datenschutzgesetzes / La révision de la Loi sur la protection des données, Zürich 2009.
- GLASS, PHILIP, Die rechtsstaatliche Bearbeitung von Personendaten in der Schweiz, DIKE, Basel 2016.
- KIESER, UELI, ATSG Kommentar, 3. Aufl., Zürich 2015.
- KIESER, UELI, Gutachten zu Fragen der Zusammenarbeit gestützt auf Art. 85f AVIG, Bern/St. Gallen 2017.
- KIESER, UELI, Gutachten zu Fragen des Datenschutzes bei der Zusammenarbeit gestützt auf Art. 85f AVIG, Bern/St. Gallen 2017.
- KIESER, UELI / PÄRLI, KURT / UTTINGER URSULA, Datenschutz – Aktuelle Fragen auf dem Weg, IRP-HSG Band 93, St. Gallen 2015.
- KULL MICHAEL, Arbeitsvermittlungsgesetz (AVG), Bundesgesetz vom 6. Oktober 1989 über die Arbeitsvermittlung und den Personalverleih, Stämpfli Verlag, 2014.
- LEU, AGNES, Die arbeitsmarktlichen Massnahmen im Rahmen der Arbeitslosenversicherung in der Schweiz, Schriften zum Sozialversicherungsrecht (SzS) Bd. 15, Zürich 2006.
- MEIER, PHILIPPE, Protection des données, Fondements, principes et droit privé, Stämpfli Editions SA, Bern 2011.
- MAURER-LAMBROU, URS / BLECHTA, GABOR P., Datenschutzgesetz Öffentlichkeitsgesetz, Basler Kommentar, Helbling Lichtenhahn Verlag, Basel 2014.
- MÜLLER, JÖRG PAUL / SCHEFER, MARKUS: Grundrechte in der Schweiz im Rahmen der Bundesverfassung, der EMRK und der UNO-Pakte, 4. Aufl., Bern 2008.
- NUSSBAUMER, THOMAS, in: Ulrich Meyer (Hrsg.), Schweizerisches Bundesverwaltungsrecht, Band XIV, Soziale Sicherheit, 3. Aufl. 2015.
- PÄRLI, KURT, IIZ-Datenaustausch, Datenschutz und Datenaustausch in der Interinstitutionellen Zusammenarbeit (IIZ), digma Schriften zum Datenrecht Band 8, Schulthess §, Zürich, Basel, Genf 2014.
- PASSADELIS, NICOLAS / ROSENTHAL DAVID / THÜR HANSPETER, Datenschutzrecht, Beraten in Privatwirtschaft und öffentlicher Verwaltung, Helbing Lichtenhahn Verlag, Basel 2015.
- RIEDO, CHRISTOPH / FIOKA, GERHARD / NIGGLI, MARCEL ALEXANDER, Strafprozessrecht sowie Rechtshilfe in Strafsachen, 1. Aufl., Basel 2011.
- ROSENTHAL, DAVID / JÖHRI, YVONNE, Handkommentar zum Datenschutzgesetz, Schulthess §, Zürich 2008.
- ROSSNAGEL, ALEXANDER, Handbuch Datenschutzrecht, München 2003.

RUDIN, BEAT: Datenschutzgesetze – fit für Europa, Europarechtliche Anforderungen an die schweizerischen Datenschutzgesetze, Schulthess Verlag, Zürich 2007.

SCHLAURI, SIMON / JÖRG, FLORIAN S./ ARTER OLIVER, Internet-Recht und Digitale Signaturen, Stämpfli Verlag, Bern 2005.

WEBER, ROLF H., Datenschutz – Zum Aufstieg einer neuen Rechtsdisziplin, Editions Weblaw, Bern 2015.

MATERIALIEN

Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung (Bundesinformatikverordnung, BinfV), SR 172.010.58.

Verordnung über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV), SR 510.411.

Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten SR 0.235.1.

Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23. März 1988, BBl 1988 II 413.

Botschaft zur Änderung des Bundesgesetzes über den Datenschutz (DSG) und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung vom 19. Februar 2003, BBl 2003 2101.

Weisungen des Bundesrates über die IKT-Sicherheit in der Bundesverwaltung vom 1. Juli 2015.

SECO, Weisungen und Erläuterungen zum Arbeitsvermittlungsgesetz, zur Arbeitsvermittlungsverordnung und der Gebührenverordnung zum Arbeitsvermittlungsgesetz, 6. Oktober 1989.

SECO, AVIG-Praxis ALE, Arbeitsmarkt und Arbeitslosenversicherung (TC).

BSV, Kreisschreiben über die Schweigepflicht und die Datenbekanntgabe in der AHV/IV/EO/FamZLw/FamZ, 1.1.2014.

EDÖB, Leitfaden für die Bearbeitung von Personendaten in der Bundesverwaltung, August 2009.

EDÖB, Leitfaden über Internet- und E-Mailüberwachung am Arbeitsplatz, Für die Bundesverwaltung, September 2013.

EDÖB, Leitfaden über die Rechte der betroffenen Personen bei der Bearbeitung von Personendaten, Mai 2014.

EDÖB, Was muss in einem Bearbeitungsreglement eines Bundesorgans aufgeführt werden? Mai 2014.

EDÖB, Datenvermittlung ins Ausland kurz erklärt, September 2014.

EDÖB, Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes, EDÖB, August 2015.

EDÖB, Erläuterungen zur Übermittlung von Personendaten ins Ausland nach revidiertem DSG, Januar 2017.

EDÖB, Die Datenübermittlung ins Ausland kurz erklärt, zuhanden Bundesbehörden und Privatwirtschaft, Januar 2017.

EDÖB; Datenschutzkonformes Social Media Monitoring.

NÜTZLICHE APP UND LINKS

- www.edoeb.admin.ch (Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB))
- EDÖB-Newsletter
- EDÖB-Raster zur Datenschutz-Folgenabschätzung
- www.iiz.ch
- www.arbeit.swiss
- Datenschutzbehörden der Schweiz mit eigenem Internetauftritt
- www.privatim.ch/de (Konferenz der Schweizer Datenschutz-Beauftragten)
- App «Datenschutz.ch» des Datenschutzbeauftragten vom Kanton Zürich: Enthält umfassende Werkzeuge zu datenschutzrechtlichen Themen, inklusive Passwortcheck und Datenschutzlexika
- www.edps.europa.eu (Der Europäische Datenschutzbeauftragte)

ZWECK, GELTUNGSBEREICHE UND RECHTSQUELLEN

Zweck

- 1 Datenschutznormen bezwecken den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden.

Der Datenschutzleitfaden AVIG & AVG dient den Bundesorganen und den Durchführungsorganen nach Art. 76 Abs. 1 AVIG – direkt oder indirekt – dazu, die Datenbearbeitung datenschutzrechtskonform zu gestalten.

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 und juristischer Personen (z. B. Privatperson, AMM-Anbietende) durch Privatpersonen oder Bundesorgane bearbeitet werden (Art. 2 Abs. 1 DSG). Die Ausgleichsstelle (SECO) ist als Bundesorgan dem DSG unterstellt. Auch für die privaten Arbeitslosenkassen findet das DSG Anwendung, da diese bei der Durchführung des AVIG wie Bundesorgane behandelt werden.

- 4 Die Datenbearbeitung durch kantonale oder kommunale Behörden ist grundsätzlich nicht Gegenstand des DSG. Infolge der verfassungsrechtlich geschützten Organisationsautonomie der Kantone gilt beim Vollzug von Bundesrecht respektive in Erfüllung von Bundesaufgaben durch die Kantone (oder kantonale öffentlich-rechtliche Anstalten) kantonales Datenschutzrecht.

Die kantonalen Datenschutzvorschriften gelten für den kantonalen oder kommunalen öffentlichen Bereich (z. B. Sozialhilfe, öffentliche Arbeitslosenkassen, RAV, LAM und KAST).

Voraussetzung ist nach Art. 37 Abs. 1 DSG allerdings, dass das kantonale Datenschutzrecht einen angemessenen Schutz gewährt. Ist dies nicht der Fall, gelten gemäss Art. 37 Abs. 1 DSG für das Bearbeiten von Personendaten durch kantonale Organe beim Vollzug von Bundesrecht die Art. 1 bis 11a, 16, 17, 18 bis 22 und 25 Abs. 1 bis 3 DSG.

- 5 Bestehen auf Bundesebene bereichsspezifische Datenschutzvorschriften (z. B. im AVIG, AVG oder ATSG), so gehen diese Bestimmungen vor. Dabei ist es möglich, dass die bereichsspezifischen Datenschutzvorschriften einen weitergehenden oder weniger weitgehenden Schutz als die formellen Datenschutzgesetze enthalten.

Kantonale Datenschutzbeauftragte

- 6 Gemäss Art. 37 Abs. 2 DSG bestimmen die Kantone ein Kontrollorgan, welches für die Einhaltung des Datenschutzes sorgt (Datenschutzbeauftragte). Dabei sind Art. 27 DSG (Aufsicht über Bundesorgane), Art. 30 DSG (Information) und Art. 31 DSG (Weitere Aufgaben) sinngemäss anwendbar.

- 7 Bei der Anwendung von kantonalem Datenschutzrecht für Sachverhalte, die die ALV oder die öffentliche Arbeitsvermittlung betreffen, sind – neben der Ausgleichsstelle (als Aufsichtsorgan) – in erster Linie die kantonalen Datenschutzbeauftragten zuständig.

Sämtliche Datenschutzanfragen aus den Kantonen (ohne Anfragen der privaten ALK) werden zuständigkeitshalber zuerst den kantonalen Datenschutzbeauftragten unterbreitet. Diese begutachten das Vorhaben nach kantonalem Datenschutzrecht. Deren Stellungnahme ist einer allfälligen Datenschutzanfrage an die Ausgleichsstelle (tcjd@seco.admin.ch) beizulegen.

- 8 Der EDÖB stellt ein Evaluationsraster zur Früherkennung von Datenschutzrisiken zur Verfügung, mit dem sich sehr früh im Erarbeitungsprozess eines Projekts diejenigen Punkte identifizieren lassen, die aus der Sicht des (nationalen) Datenschutzes heikel sind. Der Fragebogen thematisiert die verschiedenen Datenschutzaspekte, die es bei Projekten, wo Personendaten bearbeitet werden, zu beachten gilt.

Die Auswertung vermittelt ein objektives Bild der Auswirkungen, die der Datenschutz auf kantonale Projekte haben kann, und gibt diesbezügliche Ratschläge. Den Kantonen sei empfohlen, bei geplanten Projekten das Evaluationsraster zu konsultieren (www.apps.e-doeb.admin.ch/dsfa/de/index.html).

Rechtsquellen

- 9 Die Rechtsquellen des verfassungsmässigen und des formellen Datenschutzrechts sind:

- Art. 13 Abs. 2 BV und kantonale Verfassungsbestimmungen;
- Datenschutzgesetze, -verordnungen, -reglemente und -richtlinien von Bund und Kantonen;

Für die Schweiz von Bedeutung sind folgende internationale Rechtsquellen:

- Art. 8 EMRK;
- Datenschutzkonvention des Europarates samt Zusatzprotokoll (ER-Konv sowie ZP-ER-Konv 108);
- EU-Datenschutzrichtlinie (EU-Richtlinie 95/46/EG, EU-Datenschutzgrundverordnung, EU-Richtlinie 2016/680) und Art. 8 EU-GRC;
- Art. 17 UNO-Pakt II.

Für die Belange der Arbeitslosenversicherung und der öffentlichen Arbeitsvermittlung massgebendes materielles Datenschutzrecht findet sich in:

- ATSG und ATSV;
- AVIG und AVIV;
- AVG und AVV;
- V-ASAL;
- V-AVAM;
- V-LAMDA.

Auflistung der wichtigsten bundesrechtlichen Datenschutznormen im Bereich der Sozialversicherung:

- Art. 32 und Art. 33 ATSG (SR 830.1);
- Art. 49a, 50a, 50b, 71 AHVG (SR 831.10);
- Art. 83, 96b, 96c, 97a AVIG (SR 837.0);

- Art. 29, 29a EOG (SR 834.1);
- Art. 66b IVG (SR 831.20);
- Art. 21, 22a, 23, 42a, 84, 84a KVG (SR 832.10);
- Art. 94a, 95a, 95b MVG (SR 833.1);
- Art. 96, 97 UVG (SR 832.20);
- Art. 10 V-ASAL (SR 837.063.1);
- Art. 13 V-LAMDA (SR 837.063.2);
- VVK (832.105).

Der Datenschutz im Informationssystem für die Arbeitsvermittlung und Arbeitsmarktstatistik:

- Art. 33a, 34, 34a, 34b, 35, 35a, 35b AVG (SR 823.11);
- Art. 9-11 V-AVAM (SR 823.114).

Die Datenbearbeitung im Bereich der Bundesverwaltung:

- Art. 6-11 GEVER-Verordnung (SR 172.010.441);
- Art. 57h-57q RVOG (SR 172.010);
- Verordnung über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen (SR 172.010.442).

BEGRIFFE UND GRUNDSÄTZE

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

- **Personendaten** (Art. 3 lit. a DSG)
- Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare 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 Personen** (Art. 3 lit. b DSG)
Betroffen sein können natürliche Personen (Individuen) oder juristische Personen (Unternehmen), über die Daten bearbeitet werden.
- **Besonders schützenswerte Personendaten** (Art. 3 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 (Bsp. Absender auf Couvert).

- **Persönlichkeitsprofil** (Art. 3 lit. d DSGVO)
Als Persönlichkeitsprofil gilt eine Zusammenstellung oder Sammlung von Informationen respektive Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt.
- **Bearbeiten** (Art. 3 lit. e DSGVO)
Bearbeitung meint jeden Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten.
- **Bekanntgeben** (Art. 3 lit. f DSGVO)
Bekanntgeben bedeutet das Zugänglichmachen von Personendaten wie etwa das Einsicht gewähren, Weitergeben oder Veröffentlichen.
- **Datensammlung** (Art. 3 lit. g DSGVO)
Eine Datensammlung meint jeden Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach betroffenen Personen erschliessbar sind. Dabei bedeutet erschliessbar, dass die Daten gefunden werden können.
- **Bundesorgane** (Art. 3 lit. h DSGVO)
Gemeint sind Behörden oder Dienststellen des Bundes sowie Personen, soweit sie mit öffentlichen Aufgaben des Bundes betraut sind.
- **Inhaber/in der Datensammlung** (Art. 3 lit. i DSGVO)
Inhaber/in oder Datenherr/in kann eine Privatperson oder ein Bundesorgan sein, welche über den Zweck und den Inhalt der Datensammlung entscheiden.
- **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 Konkordanztafel), 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).
- **Verhältnismässigkeit** (Art. 4 Abs. 2 DSGVO)
Eine Datenbearbeitung ist verhältnismässig, wenn die bearbeiteten Daten geeignet sind, den verfolgten Zweck zu erreichen. Es dürfen nur Daten bearbeitet werden, die hierzu erforderlich sind. Zudem muss der Zweck der Datenbearbeitung in einem vernünftigen Verhältnis zum Eingriff in die Grundrechte der betroffenen Person stehen.
- **Einzelfall / Einzelfallanfrage** (Art. 19 Abs. 1 DSGVO)
Der Einzelfall im datenschutzrechtlichen Sinne ist eine Datenbekanntgabe zu einem einmaligen Zweck, in einer bestimmten, einmaligen Situation. Nicht relevant ist, wie viele Personen von dieser einmaligen Situation betroffen sind (von der Einzelfallanfrage können auch mehrere Personen gleichzeitig betroffen sein). Mehrere Bekanntgaben hintereinander oder der Transfer einer unbestimmten Zahl von Daten sind nicht erlaubt, wenn der Einzelfall gefordert ist. Rechtsungültig ist z. B. eine vom Durchführungsorgan bei der betroffenen Person eingeholte Einwilligung in noch undefinierte Datenbekanntgaben an noch unbekannte Dritte (Pauschaleinwilligung). Auch Onlinezugriffe, bei welchen die anfragende Stelle unkontrolliert beliebig viele Daten beliebig oft abrufen kann, stellen keinen Einzelfall dar.

Eine Ausnahme gilt für die IIZ (Art. 85f AVIG): Hier stimmt die versicherte Person der Datenbekanntgabe z. B. an einen ersuchenden Sozialdienst (Abs. 1 lit. b) für die Gesamtdauer der IIZ (z. B. während 6 Monaten) zu.

- **Rechtsgültige Einwilligung** (Art. 4 Abs. 5 DSG)

Ist für die Bearbeitung von Personendaten die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur gültig, wenn sie nach angemessener Information freiwillig erfolgte. Bei der Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen muss die Einwilligung zudem ausdrücklich erfolgen.

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. Dadurch wird die Einwilligung Ausdruck eines frei gebildeten Willens. Die Einwilligung kann jederzeit widerrufen oder auch verweigert werden. Sie kann schriftlich oder mündlich erfolgen und ist an keine bestimmte Form gebunden. Aus Transparenz- und Beweisgründen sei die schriftliche Festhaltung und Unterzeichnung allerdings empfohlen.

Pauschalermächtigungen sind nicht rechtsgenügend, denn sie schaffen keine genügende Transparenz.

- **Gesetz im formellen Sinn** (Art. 3 lit. j DSG)

Bundesbehörden (auch kantonale oder kommunale Behörden) benötigen für die Datenbearbeitung besonders schützenswerter Personendaten eine formell gesetzliche Grundlage, sofern nicht einer der gesetzlich vorgesehenen Ausnahmetatbestände vorliegt.

BEARBEITEN VON PERSONENDATEN

Grundsatz

- 11 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.

Gesetzliche Voraussetzungen

- 12 Damit Personendaten bearbeitet werden dürfen, müssen folgende Bedingungen kumulativ erfüllt sein. Beispielhaft finden sich jeweils Verweise auf die entsprechende DSG-Norm:
- **Rechtmässigkeit, Legalitätsprinzip** (Art. 4 Abs. 1 DSG)
Personendaten dürfen nur rechtmässig bearbeitet werden. Während im öffentlich-rechtlichen Bereich die Gesetzmässigkeit des staatlichen Handelns das Grundprinzip darstellt und somit auch das Bearbeiten von Personendaten einer gesetzlichen

Grundlage bedarf (Art. 17 DSG verlangt ein Gesetz im formellen Sinn), ist privatrechtliches Handeln und das Bearbeiten von Personendaten erlaubt, soweit nicht gegen Rechtsnormen verstossen wird.

Liegt keine explizite gesetzliche Grundlage nach Art. 17 Abs. 1 DSG vor, dürfen Bundesorgane (oder auf kantonaler Ebene analog kantonale oder kommunale Organe) besonders schützenswerte Personendaten sowie Persönlichkeitsprofile nur bearbeiten, wenn ein in Abs. 2 erwähnter Rechtfertigungsgrund vorliegt:

- Unentbehrlichkeit für die Aufgabenerfüllung (lit. a);
- Bewilligung des Bundesrates im Einzelfall (lit. b) oder
- Einwilligung im Einzelfall oder Zugänglichmachung der Daten (lit. c)

Insbesondere muss die formell gesetzliche Grundlage auch die Bekanntgabe besonders schützenswerter Personendaten erlauben. Die gleiche Anforderung gilt auch für besonders schützenswerte Personendaten, die im Rahmen eines Abrufverfahrens beschafft bzw. bekanntgegeben werden.

Die gesetzlichen Grundlagen für die Datenbearbeitung in den Bereichen AVIG und AVG finden sich grundsätzlich in Art. 96b AVIG sowie Art. 33a AVG.

- **Ausnahmen**

Bundesorgane dürfen besonders schützenswerte Personendaten oder Persönlichkeitsprofile nur ausnahmsweise ohne Vorliegen einer formell gesetzlichen Grundlage bearbeiten.

Nur in drei Fällen können solche Daten ausnahmsweise ohne formelle gesetzliche Grundlage bearbeitet werden (Art. 17 Abs. 2 DSG):

- wenn es für eine in einem formellen Gesetz klar umschriebene Aufgabe unentbehrlich ist; oder
- wenn der Bundesrat es bewilligt, weil im Einzelfall die Rechte der betroffenen Person nicht gefährdet ist; oder
- wenn die betroffene Person im Einzelfall eingewilligt oder ihre Daten allgemein zugänglich gemacht hat und deren Bearbeitung nicht ausdrücklich untersagt hat.

- **Treu und Glauben** (Art. 4 Abs. 2 DSG)

Die Datenbearbeitung hat nach Treu und Glauben zu erfolgen. Personendaten dürfen nicht ohne Wissen oder gegen den Willen der betroffenen Person beschafft werden. Wer die betroffene Person bei der Datenbeschaffung absichtlich täuscht – z. B. indem die Daten unter Angabe einer falschen Identität beschafft oder falsche Angaben über den Zweck der Bearbeitung erteilt wurden – verletzt das Prinzip von Treu und Glauben. Dieses ist auch verletzt, wenn Personendaten verdeckt beschafft werden, beispielsweise durch Belauschen eines Gesprächs oder Abhören von Kommunikationsverbindungen.

- **Verhältnismässigkeit** (Art. 4 Abs. 2 DSG)

Die Datenbearbeitung muss verhältnismässig sein. Das Verhältnismässigkeitsprinzip besagt, dass nur diejenigen Daten bearbeitet werden dürfen, die benötigt werden und geeignet sind, den vorgesehenen Zweck zu erfüllen. 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 Rechte der betroffenen Person stehen.

- **Zweckbindung** (Art. 4 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.

- **Transparenz bzw. Erkennbarkeit** (Art. 4 Abs. 4 DSGVO)

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.

- **Datenrichtigkeit und Datensicherheit** (Art. 5 und 7 DSGVO)

Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern. Dies bedeutet auch, dass die Daten vollständig und aktuell sind, soweit es die Umstände erlauben.

Nach dem in Art. 7 DSGVO verankerten Grundsatz der Datensicherheit müssen Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. Die betroffene Person kann die Berichtigung oder Löschung unrichtiger Daten verlangen.

Besonders schützenswerte («sensible») Personendaten

13 Art. 96b AVIG wie auch Art. 33a AVG erlauben den genannten Organen zur Erfüllung ihrer gesetzlichen Aufgaben die Bearbeitung von besonders schützenswerten Personendaten unter den gleichen Voraussetzungen wie sonstige Personendaten. An die Bearbeitung von besonders schützenswerten Personendaten werden jedoch in den meisten Datenschutzgesetzen erhöhte Anforderungen gestellt. Das DSGVO verlangt beispielsweise, dass deren Bearbeitung in einem Gesetz im formellen Sinn ausdrücklich vorgesehen ist (Art. 17 Abs. 2 DSGVO, Art. 19 Abs. 3 DSGVO). Weiter sind die Anforderungen an die Einwilligung erhöht (Art. 4 Abs. 5 DSGVO), sowie auch die Informationspflicht bei deren Erhebung separat geregelt (Art. 14 DSGVO).

14 Im Rahmen der ALV dürfen folgende besonders schützenswerte Personendaten bearbeitet werden (vgl. Art. 3 lit. c DSGVO):

- nachgewiesene Einschränkung der Arbeitsfähigkeit aufgrund der religiösen Zugehörigkeit (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 Leistungscoordination);
- 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).

Bei jeder Bearbeitung ist eine einzelfallbezogene Prüfung vorzunehmen. Im konkreten Einzelfall muss deshalb nochmals geprüft werden, ob eine Erfassung oder Bearbeitung verhältnismässig ist.

Versichertennummer

- 15** Die Verwendung der 13-stelligen Versichertennummer gemäss Versicherungsausweis AHV-IV oder Krankenversicherungskarte KVG (auch AHV-Nummer, AHV-Versichertennummer oder Sozialversicherungsnummer genannt) als administrativer Personenidentifikator ist für die ALV in Art. 96 AVIG geregelt. Verwenden die Durchführungsorgane der ALV die Versichertennummer, müssen sie die im AHVG vorgeschriebenen technischen und organisatorischen Mindestanforderungen beachten (vgl. Art. 50c bis 50g AHVG).

Die Versichertennummer gemäss Art. 49a lit. g AHVG benutzen u. a. folgende Stellen (und benennen sie teilweise jedoch anders):

- Gemeindeverwaltungen (siehe auch www.upiviewer.zas.admin.ch);
- Krankenkassen (AHV-Nummer auf der Krankenversicherungskarte, die etwa auch bei der Anmeldung zum Bezug von ALE vorgebracht werden kann);
- Arbeitgebende, deren Ausgleichskassen sowie Verbandsausgleichskassen; oder
- SAK.

Gemäss Art. 50e AHVG darf die Versichertennummer ausserhalb der Sozialversicherung des Bundes systematische nur verwendet werden, wenn ein Bundesgesetz dies vorsieht und der Verwendungszweck sowie die Nutzungsberechtigten bestimmt sind. So darf eine Durchführungsstelle z. B. dem SEM eine bestimmte Versichertennummer nicht bekannt geben.

Schweigepflicht

- 16** Die Mitarbeitenden, die an der Durchführung sowie der Kontrolle oder der Beaufsichtigung der Durchführung der ALV beteiligt sind, haben Verschwiegenheit zu bewahren. Sie unterstehen der Schweigepflicht nach Art. 33 ATSG und Art. 34 AVG (vgl. auch Art. 105 und Art. 85f AVIG). 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.
- 17** Von der Schweigepflicht können auch externe Personen, die zur Datenbearbeitung beigezogen wurden, betroffen sein. Soll von der Schweigepflicht abgewichen werden, muss eine gesetzliche Grundlage vorhanden sein (z. B. das 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. 35 DSG, Art. 105 AVIG, 39 AVG oder Art. 320 StGB (Verletzung des Amtsgeheimnisses) erfüllen.

Datenerhebung im Internet

- 18** Im Internet, insbesondere in den sozialen Medien (Netzwerkplattformen wie Facebook, Xing, LinkedIn oder Multimediaplattformen oder Weblogs) hinterlegen die Nutzer/innen eine Unmenge von (Personen-) Daten. Grundsätzlich dürfen die Durchführungsorgane solche Daten nur erheben, wenn diese öffentlich zugänglich sind (= ohne Login).

Bei Mitgliederplattformen mit Zugangsschutz (z. B. Facebook) ist dies nur bedingt der Fall. Nicht erlaubt ist es, über Profile von Durchführungsorganen oder sogar über private Profile der Mitarbeitenden in sozialen Netzwerken nach der betroffenen Person zu suchen und auf diese Weise Daten zu erheben (vgl. Art. 17 Abs. 2 lit. c DSGVO).

- 19 Durchführungsorgane dürfen im Internet erhobene Daten nur verwenden, wenn diese verifiziert sind und den Voraussetzungen der Datenbearbeitung genügen. Die Durchführungsorgane müssen nach Treu und Glauben (Art. 4 Abs. 2 DSGVO) und im Rahmen der Verhältnismässigkeit die Richtigkeit der erhobenen Daten überprüfen und garantieren können.

Unrechtmässige Datenerhebung durch Private

- 20 Von Privaten unrechtmässig erhobene Daten dürfen von den Durchführungsorganen weder zur Kenntnis genommen noch weiterverwendet werden und daher auch nicht in die Fallbearbeitung einfließen. Hierzu gehören insbesondere:

- Daten, deren Erhebung für die betroffene Person nicht ersichtlich war oder deren Erhebung sie nicht erwarten musste;
- Daten, deren Erhebung nicht verhältnismässig war; oder
- Daten, die entgegen Treu und Glauben erhoben wurden.

So dürfen beispielsweise heimlich von einer Privatperson gemachte Filmaufnahmen oder gestohlene Schriftstücke von den Durchführungsorganen nicht verwendet werden.

Bei begründetem Missbrauchsverdacht hat das Durchführungsorgan nach den Regeln des ordentlichen Strafverfahrens Anzeige bei der zuständigen Strafbehörde (i.d.R. Polizei) zu erstatten.

DATENBEKANNTGABE

Grundsatz

- 21 Die Datenbekanntgabe ist eine besondere Form der Datenbearbeitung. Deshalb sind für Datenbekanntgaben immer auch die Voraussetzungen der Datenbearbeitung zu beachten.

Auskunft, Amts- und Verwaltungshilfe und Schweigepflicht

- 22 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 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.

Die in Art. 33 ATSG definierte Schweigepflicht verpflichtet Personen, die an der Durchführung sowie der Kontrolle oder der Beaufsichtigung der Durchführung der Sozialversicherungsgesetze beteiligt sind, zur Verschwiegenheit gegenüber Dritten.

Regulärer Datenverkehr

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

24 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.

☞ Beispiel:

Wechselt die Zuständigkeit für eine betroffene Person z. B. aufgrund eines Wohnortwechsels von einem RAV zum andern, erhält das neu zuständige RAV die notwendigen Systemberechtigungen, um alle Dokumente im elektronischen Dossier einzusehen. Existiert zudem noch ein schriftliches Dossier, muss das bisherige RAV dem neu zuständigen RAV eine vollständige Kopie des schriftlichen Dossiers weitergeben. Bei einem Arbeitslosenkassenwechsel gilt dasselbe.

Grenzüberschreitende Datenbekanntgabe

25 Grundsätzlich dürfen Personendaten nicht ins Ausland bekanntgegeben werden, wenn dadurch die Persönlichkeit der Betroffenen schwerwiegend gefährdet würde. Die betroffene Person kann allerdings in eine solche Datenbekanntgabe einwilligen.

Für Auskünfte über die in AVAM, ASAL und LAMDA gespeicherten Daten ist das Auskunftsbegehren der Ausgleichsstelle als Dateninhaberin zu unterbreiten. Geht ein Auskunftsbegehren irrtümlicherweise bei einem Durchführungsorgan ein, so leitet es dieses zuständigkeitshalber der Ausgleichsstelle (tcjd@seco.admin.ch) weiter.

Haben die Durchführungsorgane Daten in ihren eigenen Systemen oder Dokumenten erfasst, müssen sie nach dem auf sie anwendbaren Datenschutzrecht Auskunft geben.

Informationen zur Datenübermittlung ins Ausland finden sich auf der Seite des EDÖB (www.edoeb.admin.ch/datenschutz/00626/00753/index.html?lang=de). Zu beachten ist insbesondere auch die Liste der Staaten, deren Gesetzgebung (k)einen angemessenen Datenschutz gewährleistet.

Bezüglich des ALV-Datenverkehrs mit der EU/EFTA verweisen wir auf KS ALE 883.

Abrufverfahren

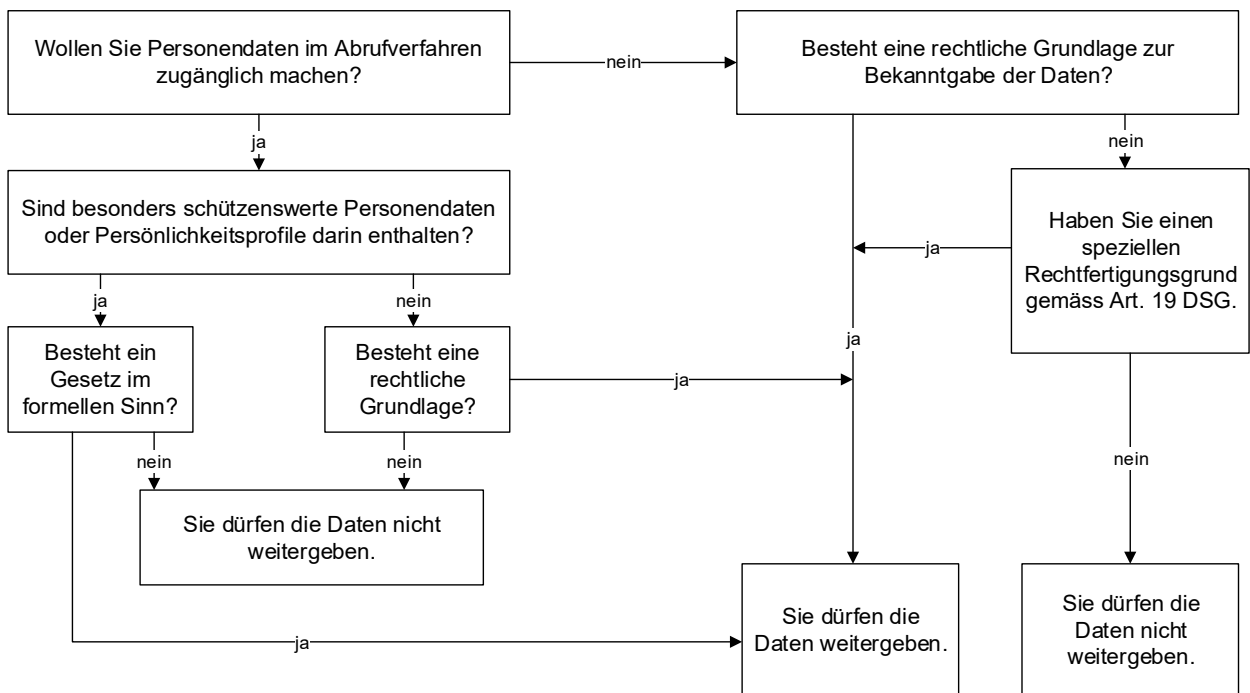
26 Ein Sonderfall der Datenbekanntgabe ist das Abrufverfahren. Darunter ist ein automatisiertes Verfahren zu verstehen, das einem/einer Dritten den Zugriff auf Daten ermöglicht, ohne dass beim Inhaber oder bei der Inhaberin der Datensammlung dazu die Erlaubnis eingeholt werden muss.

Gemäss Art. 19 Abs. 3 DSGVO muss die Bekanntgabe durch ein Abrufverfahren ausdrücklich in einer Rechtsgrundlage (mindestens in einer bundesrätlichen Verordnung) vorgesehen sein. Für die Bekanntgabe von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen durch ein Abrufverfahren ist sogar eine ausdrückliche gesetzliche Grundlage im formellen Sinn erforderlich, auf Gesetzes- oder sogar Verfassungsebene.

- 27 Die in Art. 96c AVIG oder Art. 35 Abs. 3 AVG aufgeführten Stellen können direkt auf die von der Ausgleichsstelle betriebenen Informationssysteme zugreifen, ohne dass die Ausgleichsstelle mitwirkt. Da der Zugriff definitionsgemäss wiederholt, regelmässig und automatisch ist, kann er grundsätzlich nicht einzelfallbezogen sein.

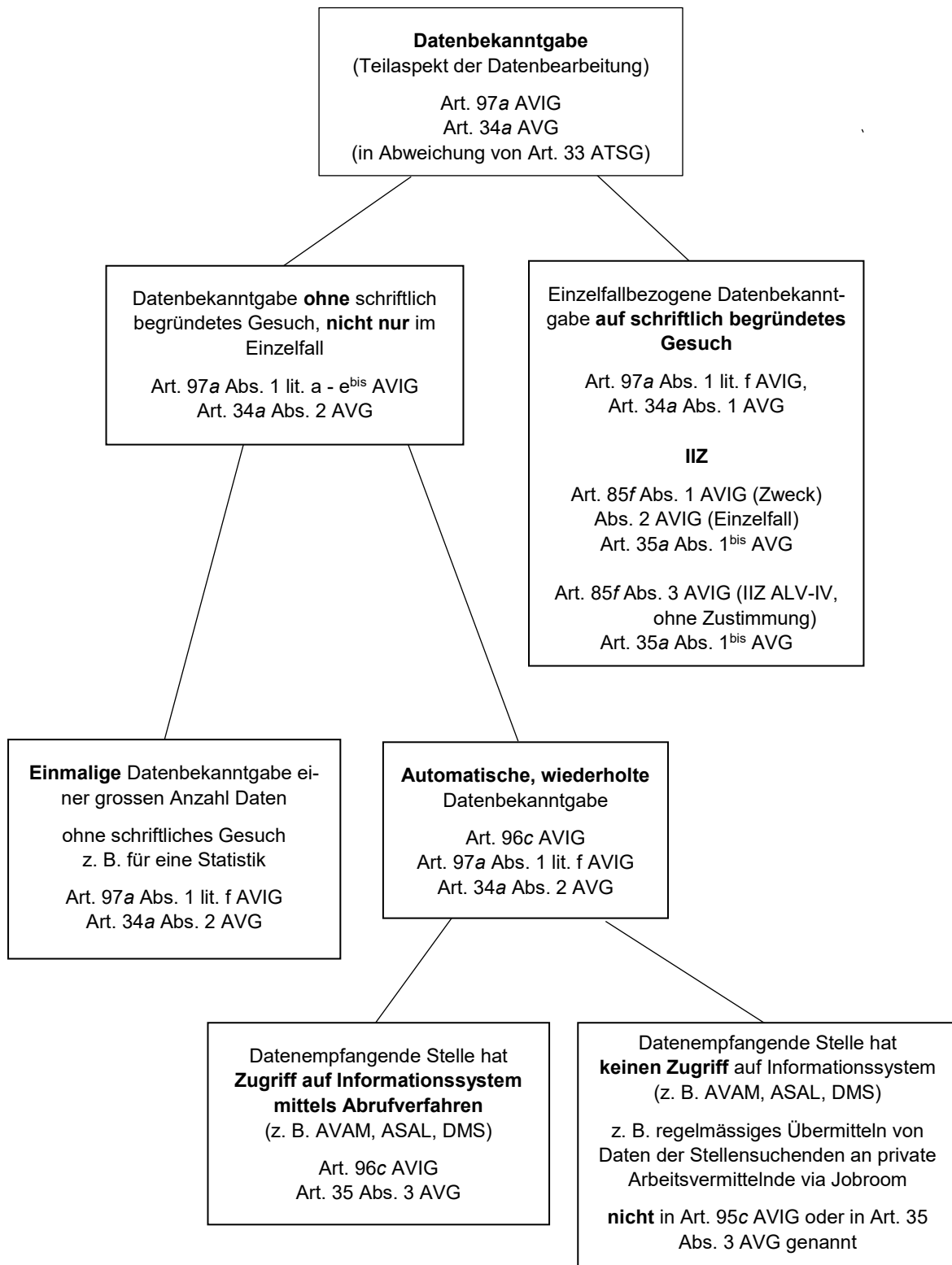
Prüfschema Datenbekanntgabe

- 28 Ist ein Bundes- oder Durchführungsorgan mit der Frage konfrontiert, ob eine bestimmte Datenbearbeitung, insbesondere eine Datenbekanntgabe, zulässig ist oder nicht, ist gemäss nachfolgender Übersicht vorzugehen (Quelle: «Leitfaden für die Bearbeitung von Personendaten in der Bundesverwaltung» des EDÖB vom August 2009):



Übersicht: Datenbekanntgabe gemäss AVIG und AVG

29



AUSKUNFTSRECHT

Grundsatz

- 30** Eine Auskunft ist eine besondere Form der Datenbearbeitung. Deshalb sind immer auch die Voraussetzungen der Datenbearbeitung zu beachten.

Das Auskunftsrecht ist eines der zentralen Elemente des Datenschutzrechts. Es ist die Voraussetzung für die Wahrnehmung weiterer Rechte und Ansprüche: So ergeben sich daraus das Recht auf Berichtigung unrichtiger Personendaten (Art. 5, 15 und 25 DSGVO), das Recht auf Unterlassung widerrechtlicher Datenbearbeitung sowie das Recht auf Beseitigung der Folgen eines widerrechtlichen Bearbeitens (Art. 15 und 25 DSGVO).

Beim Inhaber oder bei der Inhaberin einer Datensammlung kann um Auskunft über die eigenen Daten (einschliesslich der Angaben, woher sie stammen) ersucht werden. Auch die Berichtigung oder Löschung kann verlangt werden. Die Anfrage muss weder begründet sein noch muss ein Interesse an der Auskunftserteilung nachgewiesen werden (Art. 8 DSGVO).

Das Auskunftsrecht ist unverzichtbar und unverjährbar.

Auskunfts berechtigte Person

- 31** Art. 126 Abs. 2 lit. a AVIV gibt der betroffenen Person ein Recht auf Auskunft darüber, welche Daten die ALV über sie bearbeitet. Das Auskunftsrecht ermöglicht es, die Kontrolle über die eigenen Personendaten zu behalten. Ähnlich geregelt ist die Auskunftspflicht in Art. 58 Abs. 2 AVV.

Auch juristische Personen können ein Auskunftsrecht geltend machen.

Lässt sich die betroffene natürliche oder juristische Person anwaltlich vertreten, muss eine Vollmacht vorliegen respektive einverlangt werden.

Auskunfts verpflichtete Stelle

- 32** Auskunftspflichtig ist der Inhaber oder die Inhaberin einer Datensammlung, auch wenn die Daten durch Dritte bearbeitet werden (Outsourcing, vgl. Art. 8, insbesondere Abs. 4 DSGVO).

- 33** Für Auskünfte bezüglich der in den Informationssystemen der Ausgleichsstelle gespeicherten Daten ist die Ausgleichsstelle als Dateninhaberin zuständig. Geht ein Auskunftsbegehren irrtümlicherweise bei einem Durchführungsorgan ein, so leitet es dieses der Ausgleichsstelle (tcjd@seco.admin.ch) weiter.

Haben die Durchführungsorgane Daten in ihren eigenen Systemen oder Dokumenten erfasst, müssen sie nach dem auf sie anwendbaren Datenschutzrecht Auskunft geben.

Objekt

- 34** Im Rahmen des Auskunftsrechts kann die gesuchstellende Person Auskunft über alle über sie in der Datensammlung vorhandenen Daten verlangen. Daten über Dritte können nicht Gegenstand des 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).

Es muss insbesondere auch über Personendaten Auskunft erteilt werden, welche:

- Bei Dritten erhoben wurden (inklusive Angaben über die Herkunft der Daten);
- bereits gelöscht sein sollten; oder
- in von den Durchführungsorganen erstellten Dokumenten festgehalten sind (egal ob als intern qualifiziert oder nicht).

Form

- 35** Das Auskunftsbegehren hat schriftlich zu erfolgen (E-Mail oder Brief). Der EDÖB stellt Musterbriefe zur Verfügung, die es den Versicherten ermöglichen, auf einfache Weise ein Auskunftsbegehren zu stellen oder die Korrektur bzw. Löschung von Daten zu verlangen (www.edoeb.admin.ch/datenschutz/00628/00638/index.html?lang=de).

Auch die Auskunft erfolgt schriftlich (auch in Form eines Ausdrucks oder einer Kopie), kostenlos und in allgemein verständlicher Form und innert 30 Tagen (Art. 126 Abs. 2 lit. a AVIV).

Ausnahmsweise dürfen die Kosten der Bekanntgabe und Publikation von Daten verrechnet werden (Art. 126a AVIV):

- Abs. 1: In den Fällen nach Artikel 97a Abs. 4 AVIG wird eine Gebühr erhoben, wenn die Datenbekanntgabe zahlreiche Kopien oder andere Vervielfältigungen oder besondere Nachforschungen erfordert. Die Höhe dieser Gebühr entspricht den in den Artikeln 14 und 16 der Verordnung vom 10. September 1969 über Kosten und Entschädigungen im Verwaltungsverfahren festgesetzten Beträgen.
- Abs. 2: Für Publikationen nach Artikel 97a Absatz 3 AVIG wird eine kostendeckende Gebühr erhoben.
- Abs. 3: Die Gebühr kann wegen Bedürftigkeit der gebührenpflichtigen Person oder aus anderen wichtigen Gründen ermässigt oder erlassen werden.

Zulässige Einschränkung

- 36** Das Auskunftsrecht darf unter Umständen nach den Vorgaben des anwendbaren Datenschutzrechts eingeschränkt, verweigert oder aufgeschoben werden (Art. 9 Abs. 4 DSG). Dies muss der auskunftsersuchenden Person in einem schriftlich begründeten Entscheid mitgeteilt werden.

Die Einschränkung muss verhältnismässig sein:

- Ein Gesetz im formellen Sinn sieht eine solche Einschränkung vor (Art. 9 Abs. 1 lit. a DSG);
- eine Verweigerung oder Einschränkung ist wegen überwiegenden Interessen Dritter erforderlich (Art. 9 Abs. 1 lit. b DSG);
- es bestehen überwiegende öffentlichen Interessen, insbesondere der inneren oder äusseren Sicherheit der Schweiz, und die Einschränkung oder Verweigerung des Auskunftsrechts ist zu ihrer Wahrung erforderlich (Art. 9 Abs. 2 lit. a DSG);
- die Auskunft oder die Information stellte den Zweck einer Strafuntersuchung oder eines anderen Untersuchungsverfahrens in Frage (Art. 9 Abs. 1 lit. b DSG).

INFORMATIONSSYSTEME DER AUSGLEICHSTELLE

Grundsatz

- 37** Die Ausgleichsstelle betreibt verschiedene Informationssysteme zur Erfüllung der gesetzlichen Aufgaben und für statistische Zwecke (Art. 83 Abs. 1 lit. i und o AVIG). Als Inhaberin der Datensätze, die in ihren Informationssystemen gespeichert werden, hat die Ausgleichsstelle ausschliessliche Kompetenz, über deren Inhalt und Zweck zu entscheiden.

In dieser Funktion hat sie ihre Systeme nach Art. 11a Abs. 2 DSG als Datensammlungen beim EDÖB angemeldet.

- 38** Die Ausgleichsstelle betreibt folgende Informationssysteme:

- AVAM: Es dient der öffentlichen Arbeitsvermittlung sowie den arbeitsmarktlichen Massnahmen und enthält alle relevanten Personendaten über die Versicherten nach AVIG und Stellensuchenden nach AVG (siehe AVAM-Verordnung);
- ASAL: Es ist ein den Arbeitslosenkassen zur Verfügung gestelltes Auszahlungssystem für Geldleistungen (siehe ASAL-Verordnung);
- LAMDA: Es ist eine zentrale Datenbank aus mehreren Quellen zu Statistik-, Reporting- und Analysezielen (Data-Warehouse), in welcher Daten aggregiert, neu zusammengestellt und Dritten zur Weiterbearbeitung zur Verfügung gestellt werden kann (siehe LAMDA-Verordnung).

Die spezifischen Verordnungen zu AVAM, ASAL und LAMDA regeln die Voraussetzungen zur Verwendung dieser Systeme. Dort sind auch die Zugriffsrechte und automatisierten Datenbekanntgaben an andere Systeme (Schnittstellen) geregelt. Dateninhaberin dieser Systeme ist die Ausgleichsstelle.

Das AVAM ist zugleich ein Informationssystem nach AVIG und nach AVG. Damit sind die Datenschutznormen sowohl des AVIG als auch des AVG auf diese Daten anwendbar.

- 39** Damit die Ausgleichsstelle und die Durchführungsorgane der ALV (ALK, RAV, LAM, KAST) ihre Aufgaben wahrnehmen können, kommen zudem eine Vielzahl von zum Teil über Schnittstellen verbundene Informatiksysteme zum Einsatz:

- Für die Ausgleichsstelle: AVAM, ASAL, ASAL-ZDB, Personen-Register, BUR, LAMDA, B+VM, SAP ALV, MAVK, Test Director, TC-Net, Panoramica, ALV für Windows, JIRA.
- Für die ALK: ASAL, ASAL-ZDB, Personen-Register, BUR, LAMDA, SAP ALV, MAVK, Sunet UVAL, AUCO, TC-Net, Panoramica, ALV für Windows.
- Für die RAV, LAM, KAST: AVAM, ASAL-ZDB, Personen-Register, BUR, LAMDA, SAP ALV, MAVK, TC-Net, Panoramica, ALV für Windows, Jobroom.

Die Ausgleichsstelle als Inhaberin der Datensammlung

- 40** Als Dateninhaberin ist die Ausgleichsstelle dazu verpflichtet, umfassend für die Einhaltung der datenschutzrechtlichen Anforderungen zu sorgen, die Rechtmässigkeit der Datenbearbeitung zu überwachen und die Daten zu schützen (Art. 7 DSG). Die Bundesbehörde muss dafür sorgen, dass die Art und Weise des Bearbeitens die Betroffenen zu keinem Zeitpunkt in ihrer Persönlichkeit verletzt. Es müssen umfassend alle datenschutzrechtlichen Vorgaben beachtet und eingehalten werden.

Dieser Grundsatz gilt auch, wenn das Bundesorgan Dritte als Hilfspersonen bezieht oder die Datenbearbeitung vollständig ausgelagert wird (Outsourcing, Art. 10a DSGVO): Auch dann bleibt das zuständige Bundesorgan verantwortlich und muss sicherstellen, dass auch Dritte alles zur Wahrung der Persönlichkeitsrechte der Betroffenen tun, was es selbst tun müsste und alles unterlassen wird, was es selbst auch unterlassen müsste. Die Rechtsposition der Betroffenen darf sich durch die Auslagerung einer Datenbearbeitung nicht verschlechtern.

Eintrag von Daten in die Informationssysteme

- 41** Alle über die betroffene Person gesammelten Daten sind in den Informationssystemen der Ausgleichsstelle 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 Durchführungsorganen benötigt werden, um die ihnen gesetzlich übertragenen Aufgaben zu erfüllen (Art. 96b AVIG, Art. 33a AVG).

Informationen, für die das Informationssystem der Ausgleichsstelle kein Datenfeld vorsieht, dürfen e contrario nicht erhoben oder festgehalten werden.

Für ihre eigenen (kantonalen) Systeme dürfen die Durchführungsorgane bei der versicherten Person nur Daten erheben, wenn die ihnen von der Ausgleichsstelle zur Verfügung gestellten Informationssysteme zur Erfüllung ihrer gesetzlichen Aufgaben nicht genügen.

☞ Beispiel:

Ein RAV möchte weitere Versichertendaten zum Signalement (Hautfarbe, Kleidung) sowie Kreditkartenabrechnungen erheben und im DMS ablegen. Ist das erlaubt?

Nein, eine Datenerfassung, für die das Informationssystem der Ausgleichsstelle kein spezielles Datenfeld vorsieht, ist im DMS nicht erlaubt.

DATENMIGRATION

Grundsatz

- 42** Datenmigration, Datenexport und Datenimport sind besondere Formen der Datenbearbeitung. Deshalb sind immer auch die Voraussetzungen der Datenbearbeitung zu beachten.

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 Durchführungsorgane dürfen keine Daten erheben oder festhalten, für die in den Informationssystemen der Ausgleichsstelle keine Datenfelder vorgesehen sind. Erlaubt ist ihnen unter gewissen Voraussetzungen, die Daten aus den Informationssystemen in eigene Systeme zu importieren.

Voraussetzungen

- 43** Die Durchführungsorgane dürfen Daten aus den Informationssystemen der Ausgleichsstelle in eigene Systeme importieren, sofern folgende Voraussetzungen kumulativ erfüllt sind:
- Der Datenimport ist für den Vollzug des AVIG oder AVG notwendig (Verhältnismässigkeitsprüfung), da die von der Ausgleichsstelle zur Verfügung gestellten Systeme zur Erfüllung der vom AVIG oder AVG übertragenen Aufgaben nicht genügen;
 - im kantonalen Recht besteht eine Rechtsgrundlage für ein eigenes System sowie für die weitere Datenbearbeitung (gilt nur für kantonale Durchführungsorgane); und
 - die versicherte Person hat dem Datenimport zugestimmt.

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

Gesuch um Datenexport respektive Datenimport

- 44** Die Durchführungsorgane unterbreiten der Ausgleichsstelle (tcjd@seco.admin.ch) ein Gesuch, welches beinhaltet, in welchem Umfang sie Daten aus den Informationssystemen der Ausgleichsstelle exportieren und in eigene Systeme importieren und weiterverwenden möchten. Sie haben vorzulegen, wie sie den sicheren und datenschutzrechtskonformen Umgang mit den Daten garantieren können: In einem Reglement müssen insbesondere der Zugriff, die Löschung sowie der Nachweis regelmässiger Kontrollen geregelt werden.

Zu beachten gilt, dass die Weiterverwendung der importierten Daten nur zum Zweck möglich ist, der bei der Sammlung der Daten bereits angegeben wurde.

Für kantonale Durchführungsorgane gilt: Dem Gesuch ist die vorab eingeholte Stellungnahme des kantonalen Kontrollorgans (kantonale/r Datenschützer/in) beizulegen.

Private Arbeitslosenkassen unterbreiten ihr Gesuch um Datenexport respektive Datenimport direkt dem SECO (tcjd@seco.admin.ch).

Folgen einer unbefugten Datenbeschaffung

- 45** Personen, die unbefugt besonders schützenswerte Personendaten oder Persönlichkeitsprofile aus den Informationssystemen der Ausgleichsstelle beschaffen, machen sich nach Art. 179^{novies} StGB strafbar.

Eine unbefugte Beschaffung stellen z. B. sogenannte «fishing expeditions» dar, bei denen der Zweck der Erhebung lediglich darin besteht, Daten ohne einen konkreten Verwendungsgrund auf Vorrat zu speichern.

Werden Daten aus den Informationssystemen mit der Absicht erhoben, eine Kopie zu erstellen, ist dies nicht legal. Auch dürfen keine Personendaten erhoben werden, nur um diese mit anderen Datenbeständen zu kombinieren (z. B. in kantonalen sozialversicherungsrechtlichen Datamarts).

DATENBEARBEITUNG DURCH DRITTE

Grundsatz

- 46 Die Personendatenbearbeitung durch Dritte ist eine besondere Form der Datenbearbeitung. Deshalb sind immer auch die Voraussetzungen der Datenbearbeitung zu beachten.

Das Bearbeiten von Personendaten kann durch Vereinbarung oder Gesetz Dritten übertragen werden (Art. 10a DSGVO). Werden Personendaten durch Dritte bearbeitet, spricht man auch von Datenbearbeitung im Auftrag, Auslagerung, Outsourcing oder Cloud-Computing.

Die Auslagerung nach Art. 10a DSGVO betrifft nur Personendaten. Anonymisierte oder pseudonymisierte Daten fallen nicht darunter.

Art. 10a DSGVO gilt sowohl für private Datenbearbeitende als auch für Bundesorgane (vgl. auch Art. 16 Abs. 1 DSGVO).

Hoheitliche Tätigkeiten können nicht ausgelagert werden.

Voraussetzungen

- 47 Das Bearbeiten von Personendaten kann durch Vereinbarung oder Gesetz Dritten übertragen werden, wenn (Art. 10a DSGVO):

- die Daten nur so bearbeitet werden, wie es der/die Auftraggeber/in tun dürfte; und
- keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet.

Der/die Auftraggeber/in muss sich zudem vergewissern, dass der/die Dritte die Datensicherheit gewährleistet.

Befindet sich der/die beauftragte Dritte im Ausland, gelten zusätzlich die Vorgaben von Art. 6 DSGVO.

Dritte können sich auf dieselben Rechtfertigungsgründe berufen wie der/die Auftraggeber/in selbst.

Auftraggeber/in bleibt verantwortlich

- 48 Die Datenbearbeitung durch Dritte beinhaltet keine Datenbekanntgabe, da die Datenherrschaft bei dem/der Auftraggeber/in verbleibt und die Verantwortung für die weitere Datenbearbeitung gerade nicht auf Dritte übertragen wird.

Für den/die Auftragnehmer/in gelten zwar die gleichen datenschutzrechtlichen Grundsätze wie für den/die Auftraggeber/in, aber diese/r bleibt bei der Datenbearbeitung durch Dritte vollumfänglich verantwortlich.

- 49 Der/die Auftraggeber/in 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 Beauftragten gelten die gleichen datenschutzrechtlichen Grundsätze wie für den/die Auftraggeber/in (Art. 10a DSGVO und Art. 22 Abs. 2 VDSG).

Dabei handelt es sich um eine Sorgfaltspflicht, die beinhaltet, dass z. B. die Ausgleichsstelle in einer nach den Umständen gebotenen Weise dafür sorgt, dass die Beauftragten

die Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten schützen (Art. 7 DSG).

Sicherstellung einer angemessenen Datensicherheit

- 50** Untersteht der/die Dritte nicht direkt dem DSG (z. B. ein RAV oder eine öffentliche ALK), vergewissert sich das verantwortliche Organ (z. B. die Ausgleichsstelle), dass andere gesetzliche Bestimmungen (z. B. das kantonale Datenschutzrecht) einen gleichwertigen Datenschutz gewährleisten, andernfalls stellt es diesen auf vertraglichem Wege sicher (Art. 22 Abs. 3 VDSG).
- 51** Sachgerechte Massnahmen zur Sicherstellung einer angemessenen Datensicherheit sind etwa:
- Sorgfältige Auswahl der Beauftragten;
 - gründliche Instruktion der Beauftragten sowie ausreichende Information über die Sensitivität der Daten;
 - Beendigung des Auftragsverhältnisses im Falle, dass die Beauftragten trotz entsprechender Abmahnung nicht die nötige Sicherheit bieten;
 - vertragliche Zusicherung der Beauftragten, dass sie über angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten verfügen;
 - Verpflichtung der Beauftragten, 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 Beauftragten durch stichprobeweise Kontrollen (Vermeidung eines Verschuldens der Ausgleichsstelle, sollte es aufgrund erkennbar mangelhafter Datensicherheit seitens der Beauftragten zu einer unrechtmässigen Persönlichkeitsverletzung kommen).

Datenschutzvereinbarung

- 52** Eine spezifische Mustervereinbarung für die Datenbearbeitung durch Dritte nach Art. 10a DSG steht seitens des EDÖB nicht zur Verfügung (die nur auf Englisch verfügbare Mustervereinbarung für die Datenübermittlung ins Ausland ist dennoch dienlich: www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/unternehmen/anmeldung-einer-datensammlung/mustervertrag-fuer-das-outsourcing-von-datenbearbeitungen-ins-au.html).

In der Verordnung zum DSG sind insbesondere folgende Artikel relevant für die Bezeichnung der Rechte und Pflichten in einer Datenschutzvereinbarung:

- Art. 1 Abs. 6 VDSG (i.V.m. Art. 8 Abs. 4 DSG) beinhaltet die den/die Dateninhaber/in (=Auftraggeber/in) treffende Weiterleitungspflicht, wenn ein Auskunftsbegehren Daten betrifft, die im Auftrag von Dritten bearbeitet werden. Dies allerdings nur, sofern er/sie nicht selbst in der Lage ist, Auskunft zu erteilen. Art. 8 Abs. 4 DSG lautet explizit: «Lässt der Inhaber der Datensammlung Personendaten durch einen Dritten bearbeiten, so bleibt er auskunftspflichtig. Der Dritte ist auskunftspflichtig, wenn er den Inhaber nicht bekannt gibt oder dieser keinen Wohnsitz in der Schweiz hat.»
- Art. 3 Abs. 1 lit. g VDSG legt fest, dass Datensammlungen (Art. 11a Abs. 3 DSG) vor Eröffnung beim EDÖB anzumelden sind. Die Anmeldung enthält auch Angaben bezüglich Dritter, die in die Datensammlung Daten eingeben und Änderungen an den

Daten vornehmen dürfen. Dies gilt gemäss Art. 16 Abs. 1 lit. g VDSG auch für verantwortliche Bundesorgane.

- Das Bundesorgan bleibt gemäss Art. 22 Abs. 2 VDSG bei der Datenbearbeitung im Auftrag verantwortlich: «Das Bundesorgan, das Personendaten durch Dritte bearbeiten lässt, bleibt für den Datenschutz verantwortlich. Es sorgt dafür, dass die Daten auftragsgemäss bearbeitet werden, insbesondere was deren Verwendung und Bekanntgabe betrifft».

Und Abs. 3 lautet: «Untersteht der Dritte dem DSG nicht, vergewissert sich das verantwortliche Organ, dass andere gesetzliche Bestimmungen einen gleichwertigen Datenschutz gewährleisten, andernfalls stellt es diesen auf vertraglichem Wege sicher».

53 Das öffentliche Organ, das Personendaten durch Dritte bearbeiten lässt, bleibt für den Datenschutz verantwortlich. Es sorgt dafür, dass die Daten auftragsgemäss bearbeitet werden, insbesondere was deren Verwendung und Bekanntgabe betrifft.

54 Die datenschutzrechtlichen Vorgaben und Vereinbarungen (=Rechte und Pflichten) sind vertraglich festzulegen, z. B.:

- Ausgangslage;
- Gegenstand und Umfang der Datenbearbeitung;
- Verantwortlichkeiten;
- Informationssicherheit;
- Kontrolle (Berichts- und Informationspflichten);
- Zweckbindung der Daten;
- Zugriff, Verwendungszweck und Bekanntgabe von Daten;
- 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 Datenbearbeitung;
- spezifische Massnahmen;
- Haftung (Konventionalstrafen);
- Verhältnis zu anderen AGB;
- Vertragsdauer und Vertragsauflösung;
- Anonymisierung, Pseudonymisierung und Löschung der Daten;
- Anwendbares Recht und Gerichtsstand.

Von den Durchführungsorganen für ihre eigenen Systeme erhobenen Daten

- 55 Den Durchführungsorganen ist es nicht gestattet, Daten aus den Informationssystemen der Ausgleichsstelle an Dritte zur Bearbeitung weiterzugeben. Dies bedeutet, dass sie Daten, die sie z. B. aus dem AVAM oder ASAL in eigene (kantonale) Systeme mit dem Einverständnis des SECO importiert haben, nicht zur Weiterbearbeitung (z. B. Auswertung) an Dritte weitergeben dürfen.

Hingegen dürfen sie „eigene“ Daten an Dritte zur Bearbeitung weitergeben, diesfalls richtet sich der Datenschutz nach kantonalem Datenschutzrecht.

BEARBEITEN FÜR FORSCHUNG, PLANUNG UND STATISTIK (FORSCHUNGSPRIVILEG)

Grundsatz

- 56 Das Forschungsprivileg ist eine besondere Form der Datenbearbeitung. Deshalb sind immer auch die Voraussetzungen der Datenbearbeitung zu beachten.

Art. 20 DSG 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.

Ausgleichsstelle und private Arbeitslosenkassen

- 57 Soweit eine gesetzliche Grundlage besteht (z. B. in AVIG, AVIV, AVG, AVV, V-AVAM, V-ASAL, V-LAMDA), können die Ausgleichsstelle und die privaten Arbeitslosenkassen Personendaten für nicht personenbezogene Zwecke nach den erleichternden Bedingungen von Art. 22 DSG bearbeiten bzw. zur Bearbeitung weitergeben (z. B. für Forschung, Planung, Statistik, Gutachten oder Expertisen). Dafür können sie von gewissen gesetzlichen Vorgaben abweichen:

- Die Personendaten dürfen auch für Zwecke bearbeitet werden, die bei der Erhebung nicht angegeben wurden oder für die betroffene Person nicht erkennbar waren (Art. 4 Abs. 3 DSG). Nicht erlaubt ist es hingegen, die für nicht personenbezogene Zwecke erhobenen Daten (z. B. statistische Daten) zu personenbezogenen Zwecken weiterzubearbeiten;
- für die Bearbeitung der Personendaten genügt eine gesetzliche Grundlage nach Art. 17 Abs. 1 DSG. Die besonders strengen Anforderungen an die Rechtsgrundlage bei besonders schützenswerten Personendaten nach Abs. 2 müssen nicht erfüllt sein;
- die Bekanntgabe von Personendaten (als besondere Datenbearbeitung) darf auch erfolgen, wenn dafür keine Rechtsgrundlage nach Art. 17 DSG besteht. Dann ist jedoch eine Einwilligung der teilnehmenden Personen in die vorgesehenen Forschungsprojekte und Studien notwendig. Bei Widerruf der Einwilligung müssen die Daten der betroffenen Person vernichtet werden.

- 58 Damit vom Forschungsprivileg Gebrauch gemacht werden darf, müssen gemäss Art. 22 Abs. 1 lit. a bis c DSG folgende Voraussetzungen kumulativ erfüllt sein:

- Die Daten müssen anonymisiert werden, sobald der Zweck des Bearbeitens dies erlaubt;
- die datenempfangenden Stellen (z. B. Universität, privates Forschungsinstitut) darf die Daten nur mit Zustimmung der Ausgleichsstelle oder der privaten Arbeitslosenkassen an Dritte weitergeben; und
- die Ergebnisse dürfen nur in einer Form veröffentlicht werden, in der die Personen, deren Daten verwendet wurden, nicht bestimmbar sind.

Kantonale Durchführungsorgane

- 59 Die kantonalen Datenschutzgesetze sehen teilweise ähnlich konzipierte Forschungsprivilegien vor. Die genauen Bedingungen und Privilegierungen sind dort zu finden.

Beauftragte Private

- 60 Beauftragte Private können das Forschungsprivileg von Art. 22 DSG nicht anwenden. Sie dürfen die Daten für Forschung, Planung, Statistik, Gutachten, Expertisen usw. aber aufgrund der Rechtfertigung von Art. 13 Abs. 2 lit. e DSG bearbeiten.

INTERINSTITUTIONELLE ZUSAMMENARBEIT (IIZ)

Grundsatz

- 61 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.

Ziele

- 62 Die Zielsetzungen der einzelnen Institutionen, insbesondere die Ausbildungs- und Arbeitsintegration, sollen mit Hilfe der IIZ unterstützt werden. Zu diesem Zweck können den Wiedereingliederungsstellen Kompetenzen der kantonalen Amtsstelle oder den erwähnten Institutionen die Fallverantwortung während einer gewissen Zeit übertragen werden. Art. 85f Abs. 2-4 AVIG stellt hierzu in Abweichung von Art. 32 und 33 ATSG die gesetzlichen Grundlagen bereit für die Amts- und Verwaltungshilfe und den Austausch von Akten und Informationen mit Zugriff auf Datenträger, namentlich mit der IV (Abs. 3). Erfolgt der Datenaustausch mit der IV ohne Zustimmung der betroffenen Person, ist diese anschliessend darüber und über dessen Inhalt zu informieren (Abs. 4).

Im Rahmen der IIZ werden Daten bekanntgegeben, ausgetauscht oder bearbeitet. Dabei interessiert insbesondere, ob bei einer Aufgabendelegation an eine andere Behörde, Institution oder an eine gemeinsame Wiedereingliederungsstelle Besonderheiten gelten und wie bezogen auf diese Beziehungen die Anforderungen des Datenschutzes zu konkretisieren sind. Ausgangspunkt bildet damit die Frage, inwieweit die Aufgabenerfüllung durch solche Behörden, Institutionen und Stellen zulässig ist.

Erleichterter Datenaustausch

- 63** 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. Vorausgesetzt ist jedoch, dass eine Datenbekanntgabe auf Gesuch hin und nur im Einzelfall (= 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:

- Die betroffene Person bezieht Leistungen von einer in Art. 85f Abs. 1 lit. a bis h AVIG erwähnten Stelle;
- sie stimmt der Datenbekanntgabe zu; und
- die genannten Stellen gewähren den Durchführungsorganen der ALV Gegenrecht.

Einwilligung in die Datenbekanntgabe

- 64** Ist für die Bearbeitung von Personendaten die Einwilligung der betroffenen Person erforderlich, so ist sie gemäss Art. 4 Abs. 5 DSGVO nur gültig, wenn sie nach angemessener Information freiwillig erfolgte. Bei der Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen muss die Einwilligung zudem ausdrücklich erfolgen.

Unfreiwilligkeit liegt vor, wenn bei einer Verweigerung Nachteile drohen, die mit dem Bearbeitungszweck in keinem sachlichen Zusammenhang stehen oder aus anderen Gründen unverhältnismässig sind.

Zudem muss die Einverständniserklärung jederzeit widerrufen werden können. Auf die Widerrufbarkeit kann nicht verzichtet werden. Wird eine Sanktionsfolge angedroht, verliert die Einwilligung an Gültigkeit und ein IIZ-Datenaustausch ist unzulässig.

- 65** 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. 19 Abs. 1 lit. d DSGVO erfüllt sind.

Informationspflicht

- 66** 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.

Fehlendes Gegenrecht: Einzelfallregelung

- 67** 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 lit. a lit. h 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 für Fälle ohne Notwendigkeit der Einwilligung. Diese Möglichkeit bezieht sich auf die Sozialhilfebehörden.

Datenbekanntgabe an die IV

- 68** 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.

Transparenz

- 69** 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.

Sichtung der AVAM-Daten

- 70** Die Sichtung der AVAM-Daten durch die in Art. 85f Abs. 1 lit. a - h AVIG 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).

Schweigepflicht und Geheimnisschutz

71 Was die Geheimhaltung von Informationen in der IIZ anbelangt, ist vorab der strafrechtliche Geheimnisschutz massgebend (Art. 320 und 321 StGB sowie Art. 35 DSGVO). 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.

Übersicht Datenaustausch

72 Die nachfolgende Tabelle aus dem Gutachten Kieser gibt Auskunft darüber, bei welcher Stelle (es kann sich auch um eine gemeinsam betriebene Wiedereingliederungsstelle handeln) unter welchen Voraussetzungen die Durchführungsorgane der ALV Daten beschaffen und welche Stellen diesen Durchführungsorganen Daten bekanntgeben dürfen.

	Art. 85f Abs. 2 AVIG	Art. 85f Abs. 3 und 4 AVIG	Art. 97a Abs. 1 lit. b sowie lit. f Ziff. 1 AVIG	Art. 97a Abs. 4 lit. b AVIG	Art. 19 Abs. 1 lit. a bis e DSGVO
Berufsberatungsstelle	Ja (Einverständnis der Person und Gegenrecht; Einzelfall)	Nein	Nein	Ja (schriftliches Einverständnis bestehend oder vorausgesetzt; Einzelfall)	Ja (auch ohne Einwilligung unter bestimmten Voraussetzungen; Einzelfall; keine praktische Bedeutung)
Sozialdienst	Ja (Einverständnis der Person und Gegenrecht; Einzelfall)	Nein	Art. 97a Abs. 1 lit. f Ziff. 1 AVIG: Ja (auch ohne Einwilligung; schriftliches Gesuch; Einzelfall)	Ja (schriftliche Einverständnis bestehend oder vorausgesetzt; Einzelfall)	Ja (auch ohne Einwilligung unter bestimmten Voraussetzungen; Einzelfall; keine praktische Bedeutung)
Durchführungsorgan der kantonalen Arbeitslosenhilfegesetze	Ja (Einverständnis der Person und Gegenrecht; Einzelfall)	Nein	Nein	Ja (schriftliche Einverständnis bestehend oder vorausgesetzt; Einzelfall)	Ja (auch ohne Einwilligung unter bestimmten Voraussetzungen; Einzelfall; keine praktische Bedeutung)
Durchführungsorgan der IV	Ja (Einverständnis der Person und Gegenrecht; Einzelfall)	Ja (kein überwiegendes Privatinteresse; Auskünfte und Unterlagen dienen der Klärung von	Art. 97a Abs. 1 lit. b AVIG: Ja (wenn sich Pflicht aus Bundesgesetz ergibt)	Ja (schriftliche Einverständnis bestehend oder vorausgesetzt; Einzelfall)	Ja (auch ohne Einwilligung unter bestimmten Voraussetzungen; Einzelfall; keine praktische Bedeutung)

		Ansprüchen; Einzelfall)			
Durchführungsorgan der Krankenversicherung	Ja (Einverständnis der Person und Gegenrecht; Einzelfall)	Nein	Art. 97a Abs. 1 lit. b AVIG: Ja (wenn sich Pflicht aus Bundesgesetz ergibt)	Ja (schriftliche Einverständnis bestehend oder vorausgesetzt; Einzelfall)	Ja (auch ohne Einwilligung unter bestimmten Voraussetzungen; Einzelfall; keine praktische Bedeutung)
Durchführungsorgan der Asylgesetzgebung	Ja (Einverständnis der Person und Gegenrecht; Einzelfall)	Nein	Nein	Ja (schriftliche Einverständnis bestehend oder vorausgesetzt; Einzelfall)	Ja (auch ohne Einwilligung unter bestimmten Voraussetzungen; Einzelfall; keine praktische Bedeutung)
Kantonale Berufsbildungsbehörde	Ja (Einverständnis der Person und Gegenrecht; Einzelfall)	Nein	Nein	Ja (schriftliche Einverständnis bestehend oder vorausgesetzt; Einzelfall)	Ja (auch ohne Einwilligung unter bestimmten Voraussetzungen; Einzelfall; keine praktische Bedeutung)
Suva	Ja (Einverständnis der Person und Gegenrecht; Einzelfall)	Nein	Art. 97a Abs. 1 lit. b AVIG: Ja (wenn sich Pflicht aus Bundesgesetz ergibt)	Ja (schriftliche Einverständnis bestehend oder vorausgesetzt; Einzelfall)	Ja (auch ohne Einwilligung unter bestimmten Voraussetzungen; Einzelfall; keine praktische Bedeutung)
Andere private und öffentliche Institutionen	Ja (Einverständnis der Person und Gegenrecht; Einzelfall)	Nein	Nein	Ja (schriftliche Einverständnis bestehend oder vorausgesetzt; Einzelfall)	Ja (auch ohne Einwilligung unter bestimmten Voraussetzungen; Einzelfall; keine praktische Bedeutung)

DATENSICHERHEIT

Grundsatz

- 73** Die datenbearbeitenden Durchführungsorgane müssen für die Vertraulichkeit, Verfügbarkeit und Integrität der Personendaten, die sie bearbeiten, garantieren. Sie sind verpflichtet, die Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten zu schützen (Art. 7 DSG).

Für weiterführende Informationen verweisen wir auf den «Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes» des EDÖB (www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/leitfaeden/technische-und-organisatorische-massnahmen-des-datenschutzes.html).

Technische Massnahmen

- 74 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;
 - E-Mails, welche Personendaten enthalten, sind nach Möglichkeit verschlüsselt, mittels Public Key oder anderen anerkannten Verschlüsselungsverfahren zu übermitteln (state of the art); und
 - 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. Das SECO stellt den Durchführungsorganen ein geeignetes technisches Verfahren zur Verfügung.

Organisatorische Massnahmen

- 75 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 (vgl. etwa AVAM oder AVAM-DMS);
 - 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 (INKL. PAPIERAKTEN)

Grundsatz

- 76** Art. 21 DSGVO verlangt, dass Personendaten, die nicht mehr benötigt werden, der Archivierung zuzuführen, zu vernichten oder zu anonymisieren sind. Ziel der Bestimmung ist es, Personendaten nach einer gewissen Zeit dem datenbearbeitenden Bundesorgan zu entziehen und entweder der historischen Überlieferung zuzuführen oder zu vernichten.

Aufbewahrung

- 77** 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.
- 78** Das DSGVO (Art. 21 DSGVO) sieht keine bestimmte Aufbewahrungsfrist vor. 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 10 Jahren anonymisiert oder vernichtet werden (so z. B. für Arbeitslosenkassen bei Akten und Aufzeichnungen auf Bild- oder Datenträgern gemäss Art. 125 Abs. 5 AVIV).
- 79** Anonymisierte Daten dürfen gemäss Art. 21 Abs. 2 lit. a DSGVO 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.
- 80** Art. 125 AVIV widmet sich der Aktenaufbewahrung durch die Arbeitslosenkassen:
- Die Aufbewahrungspflicht für die Bücher und Buchungsbelege beträgt zehn Jahre. Die Akten über die Versicherungsfälle müssen nach Abschluss der Rahmenfrist für den Leistungsbezug mindestens noch fünf Jahre aufbewahrt werden (Abs. 1);
 - Abgeschlossene Akten dürfen als Aufzeichnungen auf Bild oder Datenträgern aufbewahrt werden, die Aufzeichnungen müssen die Dokumente jedoch originalgetreu wiedergeben (Abs. 2);
 - Die für die Aufbewahrung auf Bild- oder Datenträgern betrauten Organe müssen sicherstellen, dass die Personendaten gegen Verlust, unbefugte Bearbeitung oder Kenntnisnahme und gegen unbefugte Aneignung angemessen geschützt sind. Die Aufzeichnungen müssen jederzeit lesbar gemacht werden können (Abs. 3);

- Bei Auflösung der Arbeitslosenkasse ist deren Träger für die ordnungsgemässe Aufbewahrung verantwortlich. Gibt es keinen Träger, so bezeichnet die Arbeitslosenkasse mit dem Liquidationsbeschluss eine Person oder Stelle, die für die ordnungsgemässe Aufbewahrung verantwortlich ist (Abs. 4);
- Akten und Aufzeichnungen auf Bild- oder Datenträgern, die personenbezogene Daten enthalten, müssen spätestens nach zehn Jahren vernichtet werden. Vorbehalten bleibt die Pflicht zur Ablieferung von Akten an die staatlichen Archive (Abs. 5);
- Die Arbeitslosenkassen sind für die Aufzeichnung der aufzubewahrenden Akten auf Bild- oder Datenträger verantwortlich. Wenn sie diese Aufgabe einem zentralen Dienst übertragen, ist eine Arbeitslosenkasse zu bezeichnen, die insgesamt die Verantwortung trägt. Diese erlässt ein Bearbeitungsreglement, welches die vorgeschriebenen Bestimmungen der eidgenössischen Gesetzgebung über den Datenschutz enthält (Abs. 6); und
- Die Aufsichtsbehörde überwacht die Durchführung (Abs. 7).

81 Zu beachten gilt es zudem die Vorschriften über Mindestaufbewahrungsfristen. Diese konkretisieren die Zweckbestimmung, Dossiers nachzuverfolgen und allfällige Haftungen geltend machen zu können (vgl. z. B. Art. 125 Abs. 1 AVIV oder Art. 7 Abs. 2 V-AVAM).

Archivierung

82 Archivieren ist die Aktivität, wodurch die Daten – in Abgrenzung zur Aufbewahrung – losgelöst vom Bearbeitungskontext verfügbar gehalten werden (Art. 21 DSG).

Vernichtung

83 Vernichten ist die Aktivität, wodurch Daten unwiederbringlich zerstört oder unlesbar gemacht werden (z. B. physische Zerstörung des Datenträgers Papier, CD usw.) (Art. 21 DSG). Gemäss Art. 21 Abs. 2 DSG gilt der Grundsatz, dass Personendaten, die nicht archivwürdig sind, grundsätzlich vernichtet werden müssen.

Von der Vernichtung ausgenommen sind:

- anonymisierte Daten (lit. a);
- Daten, die zu Beweis- oder Sicherheitszwecken aufbewahrt werden (lit. b); oder
- Aufbewahrung zur Wahrung der schutzwürdigen Interessen der betroffenen Person (lit. b).

84 Spätestens nach Ablauf der zehnjährigen Aufbewahrungspflicht müssen Personendaten vernichtet oder anonymisiert werden.

Für die Löschung der Daten der Informationssysteme der Ausgleichsstelle ist das SECO, respektive allenfalls das Bundesarchiv für die anonymisierte Archivierung zuständig. Für die Vernichtung aller übrigen Daten und Akten sind die Durchführungsorgane selber verantwortlich.

Art. 126 Abs. 3 AVIV sieht zudem vor, dass die betroffene Person verlangen kann, dass eine Berichtigung, Ergänzung oder Vernichtung ihrer Daten auch denjenigen Stellen mitgeteilt werden muss, an welche die Daten weitergegeben wurden.

Gesuch um Vernichtung

85 Einem Gesuch um Personendatenvernichtung nach Art. 25 Abs. 3 lit. a DSGVO kann nur stattgegeben werden, wenn die fraglichen Personendaten vom verantwortlichen Bundesorgan überhaupt nicht (mehr) bearbeitet werden dürfen. Anspruch auf Vernichtung besteht insbesondere bei:

- einer Datenbearbeitung ohne gesetzliche Grundlage nach Art. 17 DSGVO;
- einem Wegfall des Datenbearbeitungszwecks;
- einer Datenbearbeitung, welche zur Aufgabenerfüllung gar nicht erforderlich ist;
- einer Bearbeitung von unrichtigen Daten, welche eine Persönlichkeitsverletzung darstellt und zu deren Beseitigung eine Berichtigung nicht ausreicht; oder
- einer Bearbeitung von Daten, welche widerrechtlich beschafft wurden.

Transparenz und Nachvollziehbarkeit

86 Die Anonymisierung oder Vernichtung (Art. 21 Abs. 2 DSGVO) der Daten muss transparent und nachvollziehbar sein. Die Durchführungsorgane tragen die Verantwortung für die fachgerechte Anonymisierung oder Vernichtung der Daten, welche in ihren jeweiligen Datensystemen oder Akten erfasst sind. Sie haben dafür zu garantieren, 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.

Vgl. Die entsprechenden Regelungen in V-AVAM, V-ASAL, V-LAMDA.