Amtliche Verlautbarung der österreichischen Sozialversicherung im Internet

Hauptverband der österreichischen Sozialversicherungsträger

Der Hauptverband der österreichischen Sozialversicherungsträger verlautbart gemäß § 31 Abs. 12 ASVG:

Datenschutzverordnung für die gesetzliche Sozialversicherung (SV-Datenschutzverordnung 2018 – SV-DSV 2018)

Geltungsbereich

§ 1. (1) Diese Verordnung gilt für

1. den Hauptverband der österreichischen Sozialversicherungsträger,
2. die Gebietskrankenkassen, und zwar die
   a) Wiener Gebietskrankenkasse
   b) Niederösterreichische Gebietskrankenkasse
   c) Burgenländische Gebietskrankenkasse
   d) Oberösterreichische Gebietskrankenkasse
   e) Steiermärkische Gebietskrankenkasse
   f) Kärntner Gebietskrankenkasse
   g) Salzburger Gebietskrankenkasse
   h) Tiroler Gebietskrankenkasse
   i) Vorarlberger Gebietskrankenkasse
3. die Betriebskrankenkassen, und zwar die
   a) Betriebskrankenkasse der Wiener Verkehrsbetriebe
   b) Betriebskrankenkasse Mondi
   c) Betriebskrankenkasse voestalpine Bahnsysteme
   d) Betriebskrankenkasse Zeltweg
   e) Betriebskrankenkasse Kapfenberg
4. die Versicherungsanstalten, und zwar die
   a) Versicherungsanstalt für Eisenbahnen und Bergbau
   b) Versicherungsanstalt öffentlich Bediensteter
   c) Sozialversicherungsanstalt der gewerblichen Wirtschaft
   d) Sozialversicherungsanstalt der Bauern
   e) Allgemeine Unfallversicherungsanstalt
   f) Pensionsversicherungsanstalt
   g) Versicherungsanstalt des österreichischen Notariates

als Verantwortliche gemäß Art. 4 Z 7 Datenschutz-Grundverordnung (DSGVO) und Auftragsverarbeiter gemäß Art. 4 Z 8 DSGVO. Soweit nicht anderes vorgesehen, ist der Hauptverband nach dieser Verordnung wie ein Sozialversicherungsträger zu behandeln.

(2) Die Sozialversicherungsträger sind verpflichtet, Unternehmen, über welche sie alleine oder gemeinsam mit anderen Sozialversicherungsträgern einen beherrschenden Einfluss ausüben, zur Anwendung dieser Verordnung zu verpflichten, soweit diese Unternehmen für Zwecke der Sozialversicherung (unter Verwendung von personenbezogenen Daten) tätig sind.

(3) Diese Verordnung bildet die Grundlage für eine einheitliche Vorgangsweise und Auslegung der DSGVO durch die Sozialversicherungsträger, solange keine kraft Anwendungsvorrang zu beachtenden anderslautenden Entscheidungen oder Änderungen der Rechtslage vorliegen. Diese Verordnung gilt sowohl für die Verarbeitung von personenbezogenen Daten in Dateisystemen nach Art. 4 Z 1 und 6 DSGVO bzw. nach dem Datenschutzgesetz (DSG) als auch für den Bereich des Grundrechts auf Datenschutz und auch in jenen Bereichen, in denen sich Datenverarbeitungen ganz oder teilweise auf Rechtsgrundlage außerhalb des Anwendungsbereiches des Vertrages über die Arbeitsweise der Europäischen Union stützen. Sie hat keine Rechtswirkungen darüber hinaus und begründet insbesondere keine Rechte und Pflichten von Versicherten, Beitragszahlern, Dienstgebern, Vertragspartnern oder meldepflichtigen Stellen.

(4) Verweise auf Normen sind nach deren Stand am Tag der Kundmachung dieser Verordnung zu verstehen, soweit nicht ausdrücklich eine andere Fassung genannt ist.

Öffentlicher Bereich

§ 2. Die Datenverarbeitungen der Verantwortlichen und der Auftragsverarbeiter der Sozialversicherung nach § 1 Abs. 2 sind, soweit nicht ausdrücklich anderes vorgesehen ist (§ 1 Abs. 3), nach § 26 Abs. 1 Z 1 DSG dem öffentlichen Bereich zuzuordnen.

Hauptverband als Auftragsverarbeiter

§ 3. (1) Soweit der Hauptverband der österreichischen Sozialversicherungsträger im Rahmen seiner gesetzlichen Zuständigkeit (z. B. nach § 31 Abs. 11 ASVG, § 84a Abs. 5 ASVG) tätig wird, ist er soweit nicht ausdrücklich anderes vorgesehen ist (§ 1 Abs. 3), als datenschutzrechtlicher Auftragsverarbeiter für die Sozialversicherungsträger zu behandeln.

(2) Diese Verordnung und die anderen Richtlinien und Beschlüsse des Hauptverbandes (REDV, SV-SR usw.) sind, soweit sie datenschutzrechtliche Bestimmungen enthalten und nicht ausdrücklich anderes vorgesehen ist (§ 1 Abs. 3), als „andere Rechtsinstrumente“ nach Art. 28 Abs. 3 DSGVO zu behandeln. Ihre Verbindlichkeit richtet sich nach § 31 Abs. 6 ASVG. Der Abschluss zusätzlicher Verträge über die Tätigkeit als Auftragsverarbeiter ist nicht notwendig. Die nach Art. 28 Abs. 3 DSGVO vorgesehenen Abläufe sind durch Vollziehung der jeweils anwendbaren Rechtsvorschriften, insbesondere dieser Verordnung und der § 31 Abs. 11, § 321, § 460a, § 460d, § 460e ASVG einzuhalten.

Sozialversicherungsträger als Auftragsverarbeiter

§ 4. (1) Sozialversicherungsträger sind, soweit nicht ausdrücklich anderes vorgesehen ist (§ 1 Abs. 3), Auftragsverarbeiter für die von ihnen verarbeiteten Daten auch dann, wenn diese Daten von anderen Sozialversicherungsträgern im Anwendungsbereich der Standardprodukte (vgl. Anhang der REDV 2006) oder anderen trägerübergreifenden Auftragsverarbeitungsvorgängen verarbeitet werden. § 3 Abs. 2 gilt sinngemäß.

(2) Dies gilt in gleicher Weise für die Gesellschaften, die von Sozialversicherungsträgern nach § 10 Z 7 BvergG 2006 wie eigene Dienststellen zu behandeln sind (sogenannte in-house-GmbHs wie die SVC, ITSV, SVD etc.). § 3 Abs. 2 gilt sinngemäß.

Gemeinsam für die Verarbeitung Verantwortliche

§ 5. (1) Datenverarbeitungen, bei denen Verantwortliche gemeinsam die Zwecke und die Mittel zur Verarbeitung festlegen, sind Verarbeitungen nach Art. 26 DSGVO, wenn folgende Kriterien gemeinsam erfüllt sind:

1. Gemeinsame Festlegung von Zwecken und Mitteln durch Sozialversicherungsträger. Diese liegt dann vor, wenn
   a) die Datenverarbeitung nur von Sozialversicherungsträgern geführt wird,
   b) nur Sozialversicherungsträger auf die Gestaltung dieser Datenverarbeitung, insbesondere auf die Einbeziehung anderer Stellen (z. B. Krankenfürsorgeanstalten, § 2 Abs. 1 Z 2 B-KUVG) entweder
      aa) alleinigen Einfluss haben oder
      bb) durch amtlich kundgemachte Rechtsvorschriften ein Einfluss anderer Stellen (z. B. Weisungsbindung im Rahmen eines übertragenen Wirkungsbereiches im Pflegegeld-Informationssystem, § 31 Abs. 4 Z 3 lit. a ASVG) vorgesehen ist.
   c) die beteiligten Sozialversicherungsträger einen Zuständigen aus ihrem Kreis bestellt haben, welchem die Koordination allfälliger administrativer Abläufe beim Betrieb der gemeinsamen Datenverarbeitung (z. B. nach § 13 Abs. 6) übertragen ist. Bei Datenverarbeitungen, die im Anhang der REDV 2006 genannt sind, ist dies der dort genannte Sozialversicherungsträger, bei mehreren genannten übernimmt, falls keine anderen Festlegungen getroffen sind, diese Aufgabe der Hauptverband bzw. dann, wenn dieser nicht genannt ist, der in der Liste nach § 4 Abs. 1 MKO 2016 erstgenannte Sozialversicherungsträger.
2. Der Zweck der Datenverarbeitung ist die Vollziehung der österreichischen Sozialversicherungsgesetze oder anderer amtlich kundgemachter Rechtsvorschriften, in denen ausdrücklich eine Mitarbeit von Sozialversicherungsträgern vorgesehen ist.
3. Die Mittel der Datenverarbeitung werden allein von Sozialversicherungsträgern aufgebracht oder es handelt sich um Mittel, deren Heranziehung im alleinigen Entscheidungsbereich der Sozialversicherungsträger liegt oder die durch amtlich kundgemachte Rechtsvorschriften dafür bereitzustellen sind.

(2) Die SV-DSV ist eine nach Art. 26 Abs. 1 DSGVO vorgesehene Rechtsvorschrift des Mitgliedstaates Österreich. Sie ersetzt die nach Art. 26 DSGVO ansonsten vorgesehenen Vereinbarungen. Es werden folgende Regeln getroffen:

1. Die Verpflichtungen nach der DSGVO, insbesondere die Informationspflichten nach Art. 13 und 14 DSGVO sowie die Erfüllung der Auskunftsverpflichtung nach Art. 15 DSGVO, sind (jeweils für die selbst verarbeiteten Daten) von jenen Sozialversicherungsträgern zu erfüllen, bei denen die betroffenen Personen versichert sind oder von denen sie (z. B. im Ruhestand) Leistungen erhalten, bei mehreren Sozialversicherungsträgern ist im Zweifel jener Sozialversicherungsträger als Anlaufstelle zuständig, an den die Meldung (§ 33 ff. ASVG usw.) zu richten war.
2. Liegt keine Versicherung vor, so ist jener Sozialversicherungsträger als Anlaufstelle zuständig, bei dem das letzte Versicherungsverhältnis bestand, im Zweifel jener Sozialversicherungsträger, an den die Meldung (§§ 33 ff. ASVG usw.) zu richten war.

3. Liegt auch keine frühere Versicherung vor, ist jener Sozialversicherungsträger als Anlaufstelle zuständig, der zuletzt für die betroffene Person eine e-card ausgestellt hat.
4. Wurde auch keine e-card nach Z 3 ausgestellt, ist dann, wenn von der betroffenen Person nachgewiesen wird, dass personenbezogene Daten von einem Sozialversicherungsträger in Österreich verarbeitet wurden, jener Sozialversicherungsträger als Anlaufstelle zuständig, der für die betroffene Person nach internationalem Sozialversicherungsrecht zuständig wäre (§§ 7 SV-EG).
5. Anfragen, die sich auf die Informations- und/oder Auskunftsrechte nach der DSGVO stützen, aber bei einem unzuständigen Sozialversicherungsträger einlangen (Art. 26 Abs. 3 DSGVO), dürfen nicht zurückgewiesen werden, sondern sind an einen jeweils als zuständig ermittelten Verantwortlichen weiterzuleiten (§ 321 ASVG, § 183 GSVG, § 171 BSVG, § 119 B-KUVG, § 87 NVG usw.). Zu diesem Zweck dürfen personenbezogene Daten auch von einem unzuständigen Sozialversicherungsträger verarbeitet werden.
6. Allgemeine Auskünfte darüber, welche Sozialversicherungsträger als Anlaufstelle zur Wahrnehmung der Informationsrechte nach Art. 13 bis 15 DSGVO in Betracht kommen, sind von jedem Sozialversicherungsträger ungeachtet seiner Zuständigkeit, z. B. durch Übermittlung eines Versicherungsdatenauszuges, zu geben.

(3) Der Hauptverband hat der betroffenen Person auf Anfrage im Regelfall binnen eines Monats (Art. 12 DSGVO) Auskunft darüber zu geben, wer nach den bei ihm vorhandenen Daten dieser Person (§ 31 Abs. 4 Z 3 lit. a ASVG) für die Verarbeitung von Daten der betroffenen Person als möglicher Verantwortlicher in Betracht kommt oder mitzuteilen, dass kein möglicher Verantwortlicher betreffend der Daten der betroffenen Person gefunden werden konnte (Negativauskunft). Die Auskunft ist auf Grundlage der in der Anfrage genannten Daten (insb. Namens- und Geburtsdatumsschreibweisen) zu geben. Der Hauptverband hat für Anfragen im Internet eine allgemeine Auskunftsmöglichkeit (z. B. über „meineSV“ – Kontaktformular, Abfragemöglichkeit des Versicherungsdatenauszuges) anzubieten. Dafür sind zur Identitätsprüfung die Regeln des E-Government zu verwenden (Bürgerkarte, E-ID, §§ 4 ff. E-GovG).

(4) Die Vorgangsweise bei der Datenverarbeitung hat sich im Rahmen der durch diese Verordnung, die REDV 2006 und die Sicherheits-Richtlinien SV-SR gegebenen Regeln zu halten.

(5) Im Verzeichnis der Verarbeitungstätigkeiten ist von jedem Sozialversicherungsträger eine Liste jener Datenverarbeitungen zu veröffentlichen, in denen er Daten gemeinsam im Sinn des Art. 26 DSGVO verarbeitet und welche die Kriterien nach Abs. 1 erfüllen. Für Datenverarbeitungen, welche die Kriterien des Abs. 1 nicht erfüllen, ist jeder Sozialversicherungsträger alleiniger Verantwortlicher und damit auch alleinige Ansprechstelle für die Wahrnehmung der Informations- und Auskunftsrechte betreffend die darin verarbeiteten Daten.

Datenschutzbeauftragter

§ 6. (1) Jeder Sozialversicherungsträger hat gemäß § 5 DSG und nach Maßgabe des Art. 37 Abs. 5 DSGVO einen Datenschutzbeauftragten zu benennen. Mehrere Sozialversicherungsträger, die bei der Vollziehung der ihnen obliegenden Angelegenheiten in wesentlichen Bereichen zusammenarbeiten (z. B. nach den Richtlinien über die Zusammenarbeit zwischen Gebietskrankenkassen und Betriebskrankenkassen – avsv Nr. 134/2005), können auch gemeinsame Datenschutzbeauftragte bestellen.

(2) Der Datenschutzbeauftragte ist nach Art. 37 DSGVO auf der Grundlage seiner beruflichen Qualifikation, seines Fachwissens und seinen bisherigen Erfahrungen mit Datenverarbeitungen zu benennen; eine formalisierte Ausbildung ist nicht zu fordern. Dem Datenschutzbeauftragten ist Gelegenheit zu geben, seine Aufgaben nach Art. 39 DSGVO in zweckentsprechender Weise mit den dafür notwendigen räumlichen, zeitlichen und arbeitsmäßigen Kapazitäten, bei Bedarf durch Zuordnung entsprechender MitarbeiterInnen und technischen Ausstattungen zu erfüllen. Als Datenschutzbeauftragte können auch natürliche Personen vorgesehen werden, die nicht Dienstnehmer des Sozialversicherungsträgers sind, wobei in diesem Fall gegebenenfalls eine Zeichnungsbefugnis vorgesehen werden sollte, da der Datenschutzbeauftragte u. a. auch mit der Aufsichtsbehörde zusammen zu arbeiten hat. Der Datenschutzbeauftragte muss aber nicht als Vertreter des Sozialversicherungsträgers zur Unterfertigung schriftlicher Ausfertigungen berechtigt werden, wenn auf andere Weise eine rasche Ausführung seiner Agenden (insbesondere bei Data Breach-Notification) sichergestellt ist.

(3) Persönliche Erreichbarkeit von Ansprechpersonen in Datenschutzangelegenheiten (nicht jedoch ständige persönliche Erreichbarkeit des Datenschutzbeauftragten selbst) ist im Rahmen der beim Sozialversicherungsträger üblichen Kundendienstzeiten sicher zu stellen.

(4) Die Kontaktdaten des Datenschutzbeauftragten sind im Internet auf der jeweiligen Website des Sozialversicherungsträgers zu veröffentlichen und der Datenschutzbehörde mitzuteilen.

(5) Jeder Verantwortliche hat nach Anhörung des Datenschutzbeauftragten (Art. 39 Abs. 1 lit. b DSGVO) eine Vorgangsweise (Person, Organisationseinheit, Schulungen) für Datensicherheitsmaßnahmen und andere Datenschutzthemen festzulegen. Im Rahmen dieser Vorgangsweise sind einschlägige Unterlagen (Organisationsbeschreibungen, Datensicherheitsmaßnahmen etc., z. B. über das Intranet) gesammelt zugänglich zu machen. Es ist weiters eine Stelle festzulegen, die als interne Kontaktstelle für jene datenschutzrechtlichen Fragen dient, die im Zusammenhang mit der Verarbeitung der Daten eines Auskunfts- oder Antragstellers in technischer und rechtlicher Hinsicht entstehen. Dies gilt auch, soweit datenschutzrechtliche Gesichtspunkte nicht völlig ausgeschlossen werden können, für Auskunftsersuchen und Anfragen nach dem Auskunftspflichtrecht.

(6) Der Datenschutzbeauftragte und die für ihn tätigen Personen sind unbeschadet sonstiger Verschwiegenheitspflichten bei der Erfüllung der Aufgaben und auch nach Ende ihrer Tätigkeit zur Geheimhaltung verpflichtet (§ 460a ASVG).

(7) Der Datenschutzbeauftragte ist bezüglich der Ausübung seiner Aufgaben weisungsfrei.

(8) Der Datenschutzbeauftragte hat gegenüber dem Verantwortlichen beratende Funktion. Verbindliche Anordnungen sind von den geschäftsführenden Organen des Sozialversicherungsträgers zu treffen. Der Datenschutzbeauftragte kann nicht als verantwortlicher Beauftragter nach § 9 Verwaltungsstrafgesetz bestellt werden.

(9) Verantwortliche und Auftragsverarbeiter haben den Datenschutzbeauftragten im Sinne des Art. 38 DSGVO zu unterstützen.

Datengeheimnis

§ 7. (1) Alle Bediensteten und sonstige Personen (z. B. Versicherungsvertreter) sind zur Geheimhaltung von personenbezogenen Daten verpflichtet, die ihnen bei einem Verantwortlichen oder Auftragsverarbeiter aufgrund ihrer Beschäftigung oder Funktion anvertraut oder zugänglich wurden. Dies unbeschadet sonstiger allfälliger Verschwiegenheitspflichten (§ 460a AVSG). Darüber hinaus ist es diesen Personen insbesondere untersagt,

1. sich personenbezogene Daten unbefugt zu beschaffen;
2. personenbezogene Daten zu einem anderen Zweck als für ihre eigene Arbeit zu verarbeiten;
3. unbefugten Personen oder offensichtlich unzuständigen Stellen personenbezogene Daten zugänglich zu machen.

(2) Die im Abs. 1 genannten Personen sind zur Einhaltung dieser Verbote sowie zur Verschwiegenheit auch nach Beendigung ihres Dienstverhältnisses oder ihrer Funktion verpflichtet.

Grundsätze für die Verarbeitung von personenbezogenen Daten

§ 8. (1) Personenbezogene Daten dürfen nur im Rahmen des Art. 5 Abs. 1 DSGVO verarbeitet werden. Zur Auslegung der DSGVO sind auch deren Erwägungsgründe heranzuziehen.

(2) Grundsätze für die Verarbeitung von personenbezogenen Daten in der Sozialversicherung sind:

1. Personenbezogene Daten dürfen nur in der Art und dem Umfang verwendet werden, als dies für den Verantwortlichen oder den Auftragsverarbeiter zur Wahrnehmung der ihm gesetzlich übertragenen Aufgaben bzw. der Erfüllung der in diesem Zusammenhang geschlossenen Verträge (Privatwirtschaftsverwaltung) eine wesentliche Voraussetzung ist. Dazu gehört auch die Überprüfung, ob eine Maßnahme sinnvoll war (z. B. Kontrollen, Evaluierungen, Prüfungen des Erfolges von Rehabilitationsmaßnahmen, Prüfung eines Ausbildungserfolges). Die Verarbeitung nicht notwendiger personenbezogener Daten (Ballastwissen, Überschusswissen) ist unzulässig. Aufzeichnungen über technische Vorgänge (Programm-zu-Programm-Verbindungen, Abläufe des Portalverbundprotokolls), die der technischen Sicherheit, Nachvollziehbarkeit und Kontrolle von Datenverarbeitungen dienen, bilden kein Überschusswissen, auch wenn sie nicht für eine konkrete Datenverarbeitung fachlicher Art verarbeitet werden. Aufzeichnungen, die für Aufgaben der Innenrevision, für Einschaurechte einer Aufsichtsbehörde nach den §§ 448 ff. ASVG, Untersuchungen der Aufsichtsbehörde nach Art. 58 DSGVO oder Prüfungen durch den Rechnungshof nach Art. 126c B-VG verwendet werden sollen, bilden kein Überschusswissen. Bei ihrer Aufbewahrung ist jedoch auf möglichste Schonung personenbezogener Aspekte Rücksicht zu nehmen (keine Speicherung im Rahmen allgemein zugänglicher Arbeitsabläufe).
2. Datenverarbeitungen dürfen nur auf Grund einer ausdrücklichen Rechtsgrundlage durchgeführt werden und nicht schon dann, wenn eine solche Berechtigung im Wege einer Interpretation einer Bestimmung erschlossen werden könnte.
3. Die datenschutzrechtliche Zulässigkeit einer Datenverarbeitung begründet für sich allein noch keine Verpflichtung hiezu. Für eine Datenverarbeitung haben konkrete Gründe aus dem Vollziehungsbereich des jeweiligen Rechtsträgers im Sinn des Art. 5 Abs. 1 DSGVO vorzuliegen.
4. Personenbezogene Daten, die nicht mehr benötigt werden, sind vorbehaltlich allfälliger Aufbewahrungsfristen (§ 16) zu löschen oder zu archivieren. Zu diesem Zweck sind Dateisysteme nach Art. 4 Z 6 DSGVO regelmäßig auf die Notwendigkeit der darin enthaltenen personenbezogenen Daten durchzusehen. Die bloße theoretische Möglichkeit, Datenbestände zur Vollziehung einer noch nicht absehbaren zukünftigen Regelung verarbeiten zu können, ist für sich allein kein ausreichender Grund, entsprechende personenbezogene Daten aufzubewahren.
5. Einem Ersuchen eines Dritten um Übermittlung darf ein Verantwortlicher oder Auftragsverarbeiter nur entsprechen, wenn folgende Voraussetzungen gemeinsam vorliegen:
   a) eine Rechtsgrundlage (Z 2) hiefür feststeht und die Sicherheit des Datenaustausches gewährleistet ist;
   b) bei Zweifeln an der Übermittlungszulässigkeit die ersuchende Stelle vor der Datenermittlung ihre Ermittlungsberechtigung glaubhaft gemacht hat;
   c) bei automationsunterstützten Übermittlungsverfahren der Übermittlungsempfänger für die Dauer des Bestehens seiner Zugriffsberechtigung verpflichtet ist, regelmäßige Kontrollen durchzuführen, Kontrollmaßnahmen der übermittelnden Stelle zu unterstützen und die tatsächliche Umsetzung dieser Pflichten dem Verantwortlichen oder Auftragsverarbeiter gegenüber glaubhaft gemacht ist;

d) sich Übermittlungsersuchen auf konkret umschriebene personenbezogene Daten beziehen, wobei die Übermittlung nur allgemein beschriebener Datenbestände jedenfalls unzulässig ist;

e) andere Möglichkeiten, ein überwiegendes und demnach berechtigtes Interesse zu wahren, nicht vorliegen oder nicht zumutbar sind.

Dies gilt in gleicher Weise auch für einen Auftragsverarbeiter, wenn er im Rahmen seiner Auftragserfüllung Übermittlungsersuchen zu erledigen hat.

6. Das gelindeste zur Verfügung stehende Mittel im Sinn des § 1 Abs. 2 letzter Satz DSG wird dann nicht mehr eingesetzt, wenn personenbezogene Daten aus Beständen der Sozialversicherung für Zwecke verarbeitet werden sollen, zu deren Unterstützung andere Register eingerichtet sind (z. B. für Adressenermittlungen die Melderegister, für Einkommenserhebungen jene der Finanzverwaltung).
7. Die Verantwortung des Verantwortlichen bzw. des Auftragsverarbeiters für die weitere Verwendung der personenbezogenen Daten endet mit der Übermittlung dieser personenbezogenen Daten an Dritte.
8. Daten eines Sozialversicherungsträgers oder des Hauptverbandes über die Beschäftigung von eigenen Bediensteten (Personaldaten), über Vertragspartner (§§ 338 ff. ASVG) oder sonstige Geschäftspartner, Lieferanten usw. sind organisatorisch (z. B. durch getrennte Zugriffsrechte) von jenen personenbezogenen Daten zu trennen, die für diese Personen in deren Eigenschaft als Versicherte, Vertragspartner oder Dienstgeber (meldepflichtige Stellen) verarbeitet werden. Eine gleichzeitige Verarbeitung solcher Daten in mehreren Zusammenhängen ist auf das unbedingt notwendige Ausmaß (z. B. Wohn- und/oder Betriebsadressen) einzuschränken. Die zur Verwendung von Dienstnehmerdaten berechtigten Personen dürfen aus den Versicherungsdaten nur jene Auskünfte erhalten, die nach den jeweiligen gesetzlichen Bestimmungen auch einem Dienstgeber außerhalb der Sozialversicherung oder einer sonstigen hiezu berechtigten Stelle gegeben werden dürfen.
9. Daten eines Sozialversicherungsträgers oder des Hauptverbandes dürfen für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke weiter verarbeitet werden, wenn die Weiterverarbeitung gemäß Art. 89 Abs. 1 DSGVO erfolgt.
10. Neu eingerichtete Datenverarbeitungen sind jedenfalls, vorhandene Datenverarbeitungen möglichst so zu gestalten, dass das jeweilige bereichsspezifische Personenkennzeichen bPK nach § 9 E-GovG verwendet werden und das GTelG sowie die Abläufe des E-GovG (inkl. Portalverbundorganisation des Bundes) eingehalten werden kann. Dies kann nur für solche Datenverarbeitungen entfallen, die nicht für Zwecke außerhalb des jeweiligen Rechtsträgers vorgesehen sind und bei denen eine zukünftige Zusammenarbeit mit ähnlichen Datenverarbeitungen anderer Rechtsträger ausgeschlossen werden kann.
11. Bei der Verarbeitung von pseudonymisierten oder anonymisierten Daten ist darauf zu achten, dass ausgeschlossen wird, durch Kombination mehrere Angaben dennoch auf einen Personenbezug rückschließen zu können. Zu diesem Zweck dürfen Datenbestände, die auf Gruppen von weniger als zehn Sachverhalten beruhen, durch Target Record Swapping oder ähnliche Verfahren so verändert werden, dass zwar nicht die grundsätzliche Aussage beeinträchtigt wird, wohl aber Rückschlüsse auf Einzelpersonen unmöglich werden. Allgemein ist eine möglichst hohe k-Anonymität anzustreben.

Verarbeitung besonderer Kategorien personenbezogener Daten

§ 9. (1) Die Verarbeitung von besonderen Kategorien personenbezogener Daten ist ausschließlich in den Fällen, die in Art 9 DSGVO taxativ aufgezählt sind, zulässig.

(2) Ein wichtiges öffentliches Interesse im Sinn des Art. 9 Abs. 2 lit. i DSGVO kann auch ein wichtiges wirtschaftliches öffentliches Interesse an internem Controlling sowie externer Revision und Aufsichtstätigkeit sein, wobei auch in solchen Zusammenhängen die Datenverarbeitung nur im tatsächlich notwendigen Ausmaß erfolgen darf (z. B. Evaluierung der Verwendung öffentlicher Mittel im Gesundheitswesen durch Aufsichtsbehörden und Rechnungshof, Ergebnisprüfung für den Einsatz von Heilmethoden, Beobachtung volkswirtschaftlicher Entwicklungen nach § 31 Abs. 3 Z 2 ASVG, Zusammenwirken bei der Gesundheitsvorsorge nach § 459e Abs. 2 Z 4 und 5 ASVG).

(3) Wichtiges öffentliches Interesse im Sinn dieser Verordnung besteht auch, wenn die Verarbeitung im öffentlichen Interesse liegenden Archivzwecken, wissenschaftlichen oder historischen Forschungszwecken oder statistischen Zwecken dient.

Einwilligung für die Verarbeitung von personenbezogenen Daten

§ 10. (1) Eine datenschutzrechtlich gültige Einwilligung iSd Art. 4 Z 11 DSGVO ist insbesondere dann gegeben, wenn sie von der betroffenen Person

1. freiwillig;
2. für einen konkreten Sachverhalt („den bestimmten Fall“);
3. nach ausreichender Information („in informierter Weise“);

entweder ausdrücklich (explizit) und schriftlich erfolgt, d. h. durch die Erklärung, dass zugestimmt wird, oder schlüssig (konkludent) durch eine aktive Handlung abgegeben wurde (z. B. das Anklicken einer Checkbox), die nur so verstanden werden kann, dass die betroffene Person mit der Verarbeitung ihrer Daten einverstanden ist.

(2) Wird die Einwilligung nach Abs. 1 widerrufen, bewirkt dies die Rechtswidrigkeit künftiger Datenverwendung, d. h. Rechtswidrigkeit der Verarbeitung der Daten des Widerrufenden ab dem Einlangen des Widerrufs beim Verant-

wortlichen, sofern nicht eine weitere, von der widerrufenen Einwilligung unabhängige Rechtsgrundlage für die Verarbeitung gemäß Art. 6 oder 9 DSGVO besteht.

(3) Gesetzlich vorgesehene Aufgaben (z. B. im Rahmen der Satzung oder Krankenordnung eines Sozialversicherungsträgers) beruhen nicht auf einer Einwilligung zur Verarbeitung der davon betroffenen personenbezogenen Daten. Eine Einwilligung im Sinn der DSGVO ist daher für Datenverarbeitungen im Rahmen solcher Aufgaben nicht notwendig.

Datensicherheitsmaßnahmen

§ 11. (1) Verantwortliche und Auftragsverarbeiter haben bereits im Stadium der Konzeption und Entwicklung von Datenverarbeitungen die Grundsätze des Art. 25 DSGVO zu berücksichtigen.

(2) Verantwortliche und Auftragsverarbeiter haben die Richtigkeit der Verarbeitungen in regelmäßigen Abständen durch Stichproben oder Prüfprogramme zu überprüfen. Die ergriffenen Datensicherheitsmaßnahmen sind gemäß Art. 32 Abs. 1 lit. d DSGVO zur Feststellung ihrer Wirksamkeit und Aktualität regelmäßig zu testen. Die Ergebnisse der Tests sowie die daraus abzuleitenden (Verbesserungs-)Maßnahmen sind zu dokumentieren (ISO-Zertifizierungen etc.). Die Ergebnisse dieser Prüfung sind drei Jahre ab dem Jahr, in dem die Prüfung stattgefunden hat, aufzubewahren. Der jeweils aktuelle Stand dieser Dokumentationen ist auf Wunsch der Datenschutzbehörde in deren Funktion als Aufsichtsbehörde zur Verfügung zu stellen.

(3) Personenbezogene Daten und Programme sind unter Berücksichtigung des Standes der Technik und der Implementierungskosten vor Veränderung, Vernichtung und Verlust sowie gegen unbefugte Verwendung und Weitergabe zu schützen.

(4) Der Verantwortliche (oder in dessen Auftrag der Auftragsverarbeiter) hat für die Vernichtung unbrauchbarer oder nicht mehr benötigter Ausdrucke und sonstiger Datenträger bzw. das sichere Löschen nicht mehr benötigter Daten nach dem jeweiligen Stand der Technik Sorge zu tragen.

(5) Für die ordnungsgemäße und sichere Verarbeitung von personenbezogenen Daten sind insbesondere folgende Datensicherheitsmaßnahmen zu setzen:

1. Die technische Datensicherheit ist auf Grundlage der SV-Sicherheitsrichtlinien SV-SR, avsv Nr. 95/2017, zu gewährleisten.
2. Für die Programmverwaltung sind Zuständigkeiten und Regeln festzulegen. Zugriffsschutz zu personenbezogenen Daten und Datensicherheitsmaßnahmen sind nach Maßgabe des jeweiligen Standes der Technik zu organisieren; erteilte Zugriffsberechtigungen sind einfach lesbar auf nachvollziehbare Weise (inklusive des Berechtigungszeitraumes) zu dokumentieren. Der Umfang der Zugriffsberechtigungen ist auf das für die Aufgabenerfüllung Erforderliche zu beschränken. Bestehende Einrichtungen sind regelmäßig auf Verbesserungsmöglichkeiten zu untersuchen.
3. Zugriff auf Datenverarbeitungen darf nur eingeräumt werden, nachdem die Bestimmungen über das Datengeheimnis, die Datensicherheitsmaßnahmen und diese Verordnung zur Kenntnis gebracht wurden. Ein Zugriff muss in letzter (Protokoll-)Instanz immer auf eine identifizierbare natürliche Person rückführbar sein. Sammelzugriffsberechtigungen, über die Zugriffe mehrerer Personen dokumentiert werden, sind unzulässig. Ebenso unzulässig ist es, Datenbestände außerhalb ausdrücklicher gesetzlicher Bestimmungen oder eindeutiger Vereinbarungen über eine Auftragsdatenverarbeitung gesammelt an zugriffsberechtigte Stellen zu übermitteln, um diesen bei Bedarf das Verarbeiten der personenbezogenen Daten möglich zu machen.
4. Zugriffsberechtigungen außerhalb ausdrücklicher gesetzlicher Verpflichtungen (z. B. im Rahmen von Projekten nach § 459e ASVG) sind nur befristet einzuräumen und jedenfalls zu beenden, wenn sie
   a) zur weiteren Arbeit nicht mehr benötigt werden oder
   b) vom Berechtigten Verstöße gegen Datensicherheitsvorschriften gesetzt wurden.
5. Bei der Neueinrichtung von Datenverarbeitungen ist gemäß Art. 32 Abs. 1 lit. a DSGVO zu prüfen, ob die Verwendung personenbezogener Daten in diesen Verarbeitungen durch vorgezogene Pseudonymisierung gesichert werden kann (bei der Personendaten nur an einer Stelle des gesamten Ablaufes verwendet werden und der restliche Ablauf über technisch nicht personenbezogene Identitätskennzeichen verläuft). Die Verwendung bereichsspezifischer Personenkennzeichen bPK nach § 9 E-GovG (§ 31 Abs. 4 Z 1 ASVG) ist in neuen Datenverarbeitungen jedenfalls vorzusehen.
6. Datenträger, unabhängig davon ob diese unverschlüsselt oder verschlüsselt sind, welche eine undokumentierte nachträgliche Veränderung oder ein nicht nachvollziehbares Löschen von personenbezogenen Daten ermöglichen oder die auf einfache Weise durch ein anderes gleich aussehendes Exemplar ersetzt werden können (z. B. USB-Sticks, CD-ROMs, transportable Festplatten, etc.) dürfen für Übermittlungen nicht verwendet werden.
7. Datenverarbeitungen (insbesondere Übermittlungen), für die Anwendungen im Rahmen des elektronischen Verwaltungssystems der österreichischen Sozialversicherung ELSY (§§ 31a ff. ASVG) oder hinsichtlich der Datensicherheit gleichwertige Datenübermittlungssysteme zur Verfügung stehen, dürfen nicht über andere Wege (Programme, Applikationen usw.) vorgenommen werden.
8. Datenverarbeitungen sind, so dies im Sinne einer wirtschaftlichen, zweckmäßigen und sparsamen Erfüllung der gesetzlichen Aufgaben der Sozialversicherungsträger möglich ist, in getrennter Form so zu organisieren, dass Datenweitergaben (Übermittlungen) nur an wenigen Schnittstellen erfolgen und die gemeinsame Nutzung von

Datenbeständen für verschiedene Zwecke, aber auch die parallele Führung von Datenbeständen für gleiche Zwecke vermieden wird.

9. Zur Vermeidung, Abwehr und Nachverfolgung von Angriffen auf Datenbestände oder technische Einrichtungen der Datenverarbeitung ist mit den dafür bestehenden Einrichtungen für öffentliche Stellen zusammenzuarbeiten (z. B. Gov-CERT).
10. Die Sozialversicherungsträger und der Hauptverband haben sich an Einrichtungen anzubinden, durch welche eine sichere elektronische Zustellung (§§ 28 ff. ZustG) möglich ist sowie selbst elektronische Posteingangsadressen für Zustelldienste anzubieten.
11. Von einem Verfahren der Datenschutzbehörde nach § 24 DSG ist vom betroffenen Versicherungsträger jedenfalls der Hauptverband in Grundzügen des Sachverhaltes zu verständigen (§ 321 ASVG, § 183 GSVG, § 171 BSVG, § 119 B-KUVG, § 87 NVG). Der Hauptverband hat andere Sozialversicherungsträger, welche personenbezogene Daten der gleichen Kategorie usw. der betroffenen Person verarbeiten, über die rechtlichen Grundlagen des Verfahrens zu informieren.

Die Anordnung dieser Datensicherheitsmaßnahmen umfasst auch die Einrichtung redundanter Systeme, auf welche die Daten der Primärsysteme in regelmäßigen Abständen übertragen werden („Spiegelung“) und die bei Ausfall der Primärsysteme deren Aufgaben übernehmen.

(6) Vor dem Einsatz von Datenverarbeitungen sind diese unabhängig von der Art ihrer Erstellung (Eigenentwicklung, Fremdbeschaffung) auf Funktionalität und Einhaltung der datensicherheitstechnischen Voraussetzungen zu prüfen. Für die Prüfung sind entweder ausschließlich synthetische Daten heranzuziehen oder vor Beginn der Prüfung alle Voraussetzungen nach der DSGVO, dem DSG sowie dieser Verordnung – welche ein Produktivsystem zu erfüllen hat – umzusetzen. Prüfungen (nicht aber Tests mit originären Echtdaten) können auch bereits vor Inkrafttreten der gesetzlichen Grundlage für die Datenverarbeitung durchgeführt werden, damit der gesetzliche vorgesehene Produktivsetzungszeitpunkt eingehalten werden kann.

(7) Über alle Datensicherheitsmaßnahmen ist eine Dokumentation zu führen; diese ist laufend – oder ansonsten zumindest einmal jährlich – zu aktualisieren und mindestens drei Jahre bis nach Beendigung der Datenverarbeitung aufzubewahren. Alternativ kann die Dokumentation in einem laufend aktuell gehaltenen elektronischen System (z. B. IT-MAP) geführt werden. Die Dokumentation der Sicherheitsmaßnahmen dient gleichzeitig auch als Basis für eine gemäß § 13 erforderliche Folgenabschätzung.

(8) Die zu ergreifenden Datensicherheitsmaßnahmen sind sozialversicherungsübergreifend im Sinne der SV-SR zu standardisieren. Sie sind in das EDV-Handbuch (§ 16 REDV 2006) zu übernehmen und gelten, soweit nicht konkrete Ausnahmen zulässig erklärt wurden, für alle Sozialversicherungsträger.

(9) Die Datensicherheitsmaßnahmen sind zur Feststellung deren Wirksamkeit und Aktualität gemäß Art. 32 Abs. 1 lit. d DSGVO regelmäßig zu überprüfen. Die daraus resultierenden Ergebnisse der Überprüfung sowie die daraus abzuleitenden (Verbesserungs-)Maßnahmen sind zu dokumentieren, unverzüglich einer Risikobewertung zu unterziehen und entsprechend dem Ergebnis der Risikobewertung priorisiert umzusetzen.

(10) Bedient sich der Hauptverband oder ein Sozialversicherungsträger für eine Datenverarbeitung eines Auftragsverarbeiters, so ist dieser zur Einhaltung aller datenschutzrechtlichen Bestimmungen und Ergreifung der in dieser Verordnung vorgesehenen Datensicherheitsmaßnahmen zu verpflichten.

Meldung von Verletzungen des Schutzes personenbezogener Daten (Data Breach Notification)

§ 12. (1) Ein Verantwortlicher hat im Falle einer Verletzung des Schutzes personenbezogener Daten eine Meldung nach Maßgabe des Art. 33 DSGVO an die Datenschutzbehörde zu erstatten, wenn dadurch voraussichtlich ein Risiko für die Rechte und Freiheiten der betroffenen Personen besteht. Ein solches Risiko ist dann anzunehmen, wenn auf Dauer leistungsrechtliche Anwartschaften oder Leistungsansprüche der betroffenen Personen oder deren Identitätsdaten (z. B. durch Veränderung) gefährdet wurden. Ein Risiko ist im Regelfall nicht anzunehmen, wenn durch sofortige Maßnahmen eine Verletzung des Schutzes personenbezogener Daten verhindert werden kann (Sperre von Geräten, Maßnahmen nach dem Signatur- und VertrauensdiensteG wie Zertifikatssperren) und nicht aus anderen Gründen (z. B. wenn ein weiter verbreiteter Software- oder Hardwarefehler angenommen werden muss) eine Information notwendig erscheint. Der eigene Datenschutzbeauftragte ist unabhängig davon jedenfalls zu informieren.

(2) Wenn einem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, hat er diese zu dokumentieren und unverzüglich dem Verantwortlichen zu melden. Ist eine Meldung nach Abs. 1 zu erstatten, so hat der Verantwortliche zeitgleich auch den Chief Security Officer (CSO) des Hauptverbandes in Grundzügen (ohne personenbezogene Daten) darüber zu informieren.

(3) Im Rahmen einer Verletzung des Schutzes personenbezogener Daten haben der Verantwortliche und der Auftragsverarbeiter alles zu unternehmen, um das Schadensausmaß gering zu halten, den betroffenen Personen unnötige Mühe zu ersparen, die Fehlerbehebung raschest einzuleiten und Folgefehler zu verhindern.

(4) Ob die betroffenen Personen von einer Verletzung der personenbezogenen Daten zu benachrichtigen sind, richtet sich nach Art. 34 DSGVO. Ein unverhältnismäßiger Aufwand (Art. 34 Abs. 3 lit. c DSGVO) ist dann anzunehmen, wenn der Kreis der betroffenen Personen nicht eingegrenzt werden kann. Bei Schutzverletzungen, die daraus entstanden sind, dass einem Patienten in medizinischen Zusammenhängen (Erste Hilfe) rasch geholfen werden sollte, ist im Zweifel nicht anzunehmen, dass daraus ein hohes Risiko im Sinn des Art. 34 DSGVO entstanden ist.

Verzeichnis von Verarbeitungstätigkeiten (VVT)

§ 13. (1) Die Verantwortlichen und die Auftragsverarbeiter haben für jede Datenverarbeitung ein schriftliches Verzeichnis der dafür vorhandenen Verarbeitungstätigkeiten gemäß Art. 30 DSGVO zu führen. Der Hauptverband hat dafür im Rahmen seiner Zuständigkeit zur Schaffung einheitlicher Formulare (§ 31 Abs. 4 Z 6 ASVG) Muster aufzulegen.

(2) Das Verzeichnis der Verarbeitungstätigkeiten hat jedenfalls folgende Angaben zu enthalten:

1. den Namen und die Kontaktdaten des Verantwortlichen (sowie – falls vorhanden – die verfahrensverantwortliche Abteilung), und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, gegebenenfalls des Vertreters des Verantwortlichen, sowie des Datenschutzbeauftragten (Art. 30 Abs. 1 lit. a DSGVO);
2. die Zwecke der Verarbeitung (z. B. Versicherungsdatenverwaltung, Beitragseinhebung, Leistungserbringung, Leistungsverrechnung, Forderungseinbringung, Personalverwaltung, Verwaltungskörperorganisation, Gesundheitsförderungsprojekte nach § 459e ASVG, Vollziehung von Strukturplänen nach § 84a Abs. 1 ASVG);
3. bei Verantwortlichen eine Zusammenstellung jener Datenverarbeitungen die gemeinsam mit anderen Verantwortlichen erfolgt (Art. 26 DSGVO);
4. bei Verantwortlichen die Beschreibung der Datenkategorien betroffener Personenkreise und der Kategorien personenbezogener Daten (= Datenarten), bei Auftragsverarbeitern die Kategorien von Verarbeitungen, die im Auftrag des Verantwortlichen durchgeführt werden;
5. bei Verantwortlichen die Kategorien von Empfängern (einschließlich Empfänger in Drittländern oder internationalen Organisationen), bei Auftragsverarbeitern nur – falls überhaupt gegeben – Empfänger in Drittländern oder internationalen Organisationen; für Datenübermittlungen im Rahmen von Amtshilfe (Art. 22 B-VG) ist auf die allgemeine Amtshilfeverpflichtung, nicht jedoch auf die Namen aller Amtshilfeberechtigten Institutionen zu verweisen. Die betroffene Person selbst sowie eigene MitarbeiterInnen sind nicht namentlich als Empfänger anzuführen.
6. bei Verantwortlichen wenn möglich: die Löschungsfristen der verschiedenen Datenkategorien und
7. wenn möglich: die Beschreibung technischer und organisatorischer Maßnahmen gemäß Art. 32 DSGVO.

(3) Die Verantwortlichen und die Auftragsverarbeiter haben das Verzeichnis der Verarbeitungstätigkeiten nach Abs. 2 im Internet auf der jeweiligen Website zu veröffentlichen. Diese Verpflichtung dient der Erfüllung der Informationspflichten des Verantwortlichen gegenüber den betroffenen Personen.

(4) Änderungen und Löschungen von Datenverarbeitungen im Verzeichnis der Verarbeitungstätigkeiten, die im Rahmen eines Standardproduktes (§ 2 Z 6 REDV 2006) vorzunehmen sind, sind durch den Standardprodukt-Dienstleister (§ 5 Abs. 2 Z 1 und 5 REDV 2006) als Auftragsverarbeiter durchzuführen, bzw. für den Fall, dass dieser nicht Verantwortlicher einzelner Datenarten sein sollte, auch als Muster zu erstellen. In jenen Fällen, in denen der Standardprodukt-Dienstleister nicht für die Entwicklung der jeweiligen Datenverarbeitung verantwortlich ist, hat der jeweilige Produktverantwortliche das VVT-Muster zu erstellen. Das geänderte Verzeichnis bzw. das Muster ist von den Standardprodukt-Dienstleistern als Vorlage an die betroffenen Sozialversicherungsträger weiterzuleiten. Von sonstigen Änderungen (sowie auch Löschungen) von Datenverarbeitungen im Verzeichnis der Verarbeitungstätigkeiten hat der Verantwortliche – soweit dafür Auftragsverarbeiter vorhanden sind – die Auftragsverarbeiter unverzüglich zu verständigen.

(5) Bei gemeinsamen Datenverarbeitungen hat der jeweilige Zuständige (§ 5Abs. 1 Z 1 lit. c) das Verzeichnis zu der betreffenden Verarbeitungstätigkeit zu erstellen sowie Änderungsmeldungen und Löschungen darin vorzunehmen bzw. vorzubereiten. Dieses Verzeichnis hat auch die jeweiligen (unmittelbar beauftragten) Auftragsverarbeiter zu umfassen und dieses ist von ihm auf dem in Abs. 5 genannten Weg an die betroffenen Sozialversicherungsträger bzw. Auftragsverarbeiter weiterzuleiten.

(6) Das Verzeichnis von Verarbeitungstätigkeiten ist nach der erstmaligen Erstellung auf Basis einer umfassenden Datenerhebung laufend – oder zumindest einmal jährlich – zu aktualisieren. Als Grundlage und weitere Detaillierung des Verzeichnisses der Verarbeitungstätigkeiten ist im Rahmen der Aufzeichnungen der jeweiligen IT-Organisation/Abteilung eine Übersicht über die jeweiligen Verarbeitungen (z. B. IT-MAP) zu führen. Diese Unterlagen sind laufend auf Aktualität zu prüfen und entsprechend aktuell zu halten.

(7) Jeder Verantwortliche, seine Auftragsverarbeiter oder gegebenenfalls deren Vertreter haben der Datenschutzbehörde auf deren Anfrage das Verzeichnis der Verarbeitungstätigkeiten zur Verfügung zu stellen.

Datenschutz-Folgenabschätzung

§ 14. (1) Wenn bei einer Datenverarbeitung die Voraussetzungen des Art. 35 Abs. 1 DSGVO gegeben sind, so ist vom Verantwortlichen vorab eine Datenschutz-Folgenabschätzung durchzuführen. Wenn mehrere Verantwortliche gemeinsam mehrere ähnliche Verarbeitungsvorgänge betreiben, so kann dafür eine einzige Abschätzung vorgenommen werden. Die Mindestangaben nach Art. 35 Abs. 7 DSGVO und die Verhaltensregeln dieser Verordnung sind dabei einzuhalten. Der Hauptverband hat für die Datenschutz-Folgenabschätzung im Rahmen seiner Zuständigkeit zur Schaffung einheitlicher Formulare (§ 31 Abs. 4 Z 6 ASVG) Muster aufzulegen.

(2) Wenn bei einer Datenverarbeitung, welche im Rahmen eines Standardproduktes (§ 2 Z 6 REDV 2006) durchgeführt wird, die Voraussetzungen des Art. 35 Abs. 1 DSGVO vorliegen, ist die Folgenabschätzung durch den Standardprodukt-Dienstleister (§ 5 Abs. 2 Z 1 und 5 REDV 2006) bzw. bei gemeinsamen Verarbeitungstätigkeiten vom

jeweiligen Zuständigen (§ 5 Abs. 1 lit. c) durchzuführen. Das Ergebnis ist allen betroffenen Verantwortlichen zu übermitteln.

(3) Keine Datenschutz-Folgenabschätzung ist nötig, wenn

1. für bereits existierende Verarbeitungsvorgänge (Datenanwendungen) diese Verarbeitungsvorgänge durch die Datenschutzbehörde bereits zu einem früheren Zeitpunkt im Zuge einer DVR-Registrierung im Rahmen eines Vorabkontrollverfahrens gemäß § 18 Datenschutzgesetz 2000 (DSG 2000) genehmigt wurden.
2. die Aufsichtsbehörde (Datenschutzbehörde) eine Liste von Datenverarbeitungen veröffentlicht hat (Art. 35 Abs. 5 DSGVO), wonach dies für bestimmte Verarbeitungen nicht erforderlich ist;
3. ein Ausnahmetatbestand des Art. 35 Abs. 10 DSGVO vorliegt (insbesondere bereits im Rahmen eines Gesetzgebungsverfahrens eine allgemeine Datenschutz-Folgenabschätzung durchgeführt worden ist).

(4) Bei der Entscheidung, ob eine Datenschutz-Folgenabschätzung nötig ist oder nicht, hat der Verantwortliche den Rat des Datenschutzbeauftragten einzuholen.

Protokollierung

§ 15. (1) Protokollierungen sind in leicht zugänglicher und einfach lesbarer bzw. weiter verarbeitbarer Weise vorzunehmen. Die Führung eines Verzeichnisses von Verarbeitungstätigkeiten einer einzelfallbezogenen Datenübermittlung an Stellen außerhalb des Aufsichtsbereiches der Aufsichtsbehörde der Sozialversicherung (z. B. im Rahmen von Amtshilfe) befreit nicht von der Verpflichtung, diese Übermittlungen zu protokollieren (es reicht hiezu allerdings eine Dokumentation im Akt). Alle Zugriffe auf personenbezogene Daten im Rahmen von Standardprodukten sind nach einheitlichen Regeln zu protokollieren.

(2) Als Angabe über den Grund für eine Abfrage reicht es zur Dokumentation aus, wenn der Arbeitsbereich der jeweils protokollierten zugreifenden MitarbeiterInnen auch rückwirkend eindeutig ermittelt werden kann. Dies kann durch Aufzeichnungen erfolgen, die automatisch im Zuge der Abfrage entstehen oder durch zusätzliche Unterlagen (z. B. laufend nummerierte Formulare mit weiteren Angaben, die durch Angaben im Protokolldatensatz auffindbar bleiben).

(3) Ob eine Protokollierung tatsächlich entfallen darf, ist für jede Datenverarbeitung im Einzelfall nach Maßgabe des Art. 24 DSGVO abzuwägen. Datenübermittlungen an Stellen außerhalb eines Sozialversicherungsträgers (z. B. im Rahmen von Amtshilfe nach Art. 22 B-VG und darauf beruhenden einfachgesetzlichen Bestimmungen) sind jedenfalls zu protokollieren. Datenverarbeitungen durch automatisiert ohne zusätzliche Eingriffe ablaufende Programm-zu-Programm-Verbindungen, die der Aktualisierung der jeweiligen Datenverarbeitungen dienen, müssen nicht protokolliert werden, wenn nicht aus Gründen der Fehlereingrenzung bzw. Fehlerverfolgung dennoch eine Protokollierung notwendig ist, um feststellen zu können, ob eine Übermittlung korrekt stattgefunden hat oder nicht. Die Protokollierung darf darüber hinaus nur entfallen, wenn

1. personenbezogene Daten nach § 7 DSG für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke verarbeitet werden;
2. personenbezogene Daten gesammelt als Grundlage gesetzlich vorgesehener konkreter weiterer Verwendungen (z. B. zur Vorbereitung von Wahlen nach § 45 AKG 1992) übermittelt werden.

(4) Die Protokollierung ist bis spätestens Anfang 2020 so zu gestalten, dass zur Sicherung interner Prüfungen (Innenrevision) auch Zugriffe der eigenen MitarbeiterInnen samt Datum und Uhrzeit der Verarbeitung nachvollzogen werden können. Soweit dies aus technischen Gründen (alte Host-Lösungen) nicht möglich ist, sind die Gründe hiefür zu dokumentieren und zumindest ein Konzept über die Ablöse solcher Lösungen zu erstellen. Die Daten dieser MitarbeiterInnen sind jedoch nicht Gegenstand des Auskunftsrechts. Die MitarbeiterInnen sind nachweislich darüber zu informieren, dass sämtliche ihrer Zugriffe auf Datenverarbeitungen der Protokollierung unterliegen und dokumentiert werden.

(5) Protokolle müssen vor Manipulation und unbefugtem Zugriff geschützt sein. Protokolle sind regelmäßig zu prüfen und, soweit diese und andere Vorschriften keine anderen Aufbewahrungsfristen für Protokolle vorsehen, drei Jahre in automationsunterstützt lesbarer Form aufzubewahren. Danach sind die Protokolldaten zu löschen. Die Dreijahresfrist beginnt nach Ablauf jenes Kalenderjahres, in dem der protokollierte Zugriff stattgefunden hat.

Aufbewahrungsfristen

§ 16. (1) Die Mindestaufbewahrungsfristen richten sich nach den hiefür geltenden Regeln (z. B. § 10 KAKuG für Krankengeschichten, § 58 der Rechnungsvorschriften gemäß § 444 ASVG, usw.).

(2) Nach Ablauf dieser Fristen sind Daten, die nicht zur dauernden Aufbewahrung (einschließlich Sicherung, Aktualisierung von Signaturen etc.) einem Archiv übergeben werden, zu löschen, wenn sichergestellt ist, dass dabei keine Aufzeichnungen betroffen sein können, die aufgrund der zivil- und strafrechtlichen Verjährungsfristen noch rechtlich relevant werden können. Für den Fall, dass dies nicht ausgeschlossen werden kann, dürfen Daten auch über die Mindestaufbewahrungsfristen hinaus außerhalb eines Archives, längstens (soweit nicht nach anderen Rechtsvorschriften längere Fristen zulässig sind), jedoch für zweiundvierzig Jahre in personenbezogener Form aufbewahrt werden. Es ist auch in diesem Fall sicherzustellen, dass Zugriffe aus dem laufenden Bürobetrieb auf Daten, die nach dieser Bestimmung aufbewahrt werden, nicht ohne zusätzliche Kontrollen erfolgen können.

(3) Bestimmungen über Auskünfte, Aufbewahrungsfristen, Archivierung gelten nicht für Daten, die aus einer allenfalls zulässigen Nutzung durch ArbeitnehmerInnen und FunktionsträgerInnen eines Sozialversicherungsträgers für

private Zwecke (z. B. E-mail) entstehen. In den internen Organisationsvorschriften ist dafür insoweit Vorsorge zu treffen, als die Anlegung getrennter Mailordner bzw. Verzeichnisse für solche Daten vorzusehen ist. Solche Daten (Mailordner, Verzeichnisse) sind nach Beendigung des Arbeitsverhältnisses zu löschen bzw. ist den Betroffenen Gelegenheit zu geben, dies selbst zu tun. Dokumentation, Protokollierungen und technische Maßnahmen (Zugriffssperren) zur Klärung allenfalls rechtswidriger Handlungen bleiben davon unberührt und sind weiterhin zulässig.

Archivierung

§ 17. (1) Ob und durch wen ein Archiv geführt wird, obliegt der Entscheidung des geschäftsführenden Organs des Sozialversicherungsträgers bzw. des Hauptverbandes.

(2) Ein Archiv ist im Rahmen des Datenschutzrechts so zu führen, dass archivwürdige Daten für wissenschaftliche oder historische Forschungszwecke weiterhin zur Verfügung stehen (Art. 17 Abs. 3 lit. d DSGVO, z. B. Unterlagen geschäftsführender Organe, Aufzeichnungen über Versicherungsdaten). Dabei ist dafür zu sorgen, dass

1. Zugriffe aus dem laufenden Bürobetrieb nicht möglich sind und
2. Zugriffe nur nach Angabe rechtmäßiger Gründe für eindeutig identifizierte Personen möglich sind (z. B. wissenschaftliche Untersuchungen, Erforschung von Zeitreihen der Bevölkerungsentwicklung, Morbiditätsstatistiken des Gesundheitswesens oder sonstiger historischer Zusammenhänge; Feststellung länger zurückliegender beitrags- oder leistungsrechtlicher Ansprüche, z. B. nach § 68a ASVG, Aufklärung von länger zurückliegenden Straftaten) sowie
3. für Zugriffe eindeutige, von den üblichen Zugriffsberechtigungen des laufenden Betriebes getrennte Aufzeichnungen geführt werden und
4. Archivregelungen (Benützungsbedingungen) nach dem Vorbild der Archive des Bundes und der Länder erstellt werden.

(3) Personenbezogene Daten, die für wissenschaftliche Untersuchungen benützt werden sollen, sind zu pseudonymisieren. Eine vollständige Pseudonymisierung der Archivbestände darf jedoch, um Forschungen volkswirtschaftlicher Art nicht zu verhindern, nur im Rahmen einer für den Vollziehungsbereich des Bundes allgemein geltenden Vorgangsweise erfolgen. Bis zur Schaffung einer für die Vollziehung des Bundes bereichsübergreifend geltenden Pseudonymisierungsmöglichkeit dürfen Daten personenbezogen archiviert werden. In diesem Zusammenhang ist es unerheblich, auf welchen Datenträgern die betroffenen Daten ursprünglich verzeichnet waren (z. B. Stammkarten auf Papier, Kunststoffkarteiblättern, Mikrofilmen).

(4) Aus einem Archiv ist betroffenen Personen auf Antrag Auskunft (§ 19) über die sie betreffenden personenbezogenen Daten zu erteilen, soweit

1. das Archivgut erschlossen ist,
2. die betroffenen Personen Angaben machen, die das Auffinden der personenbezogenen Daten ermöglichen, und
3. der für die Erteilung der Auskunft erforderliche Aufwand im Verhältnis zu dem geltend gemachten Informationsinteresse steht.

(5) Machen betroffene Personen glaubhaft, dass das Archivgut eine falsche Tatsachenbehauptung enthält, die sie erheblich in ihren Rechten beeinträchtigt, so können sie verlangen, dass dem betreffenden Archivgut eine von der betroffenen Person verfasste Gegendarstellung beigefügt wird.

Informationspflicht des Verantwortlichen

§ 18. In welcher Form die Informationspflicht auszuüben ist, richtet sich nach Art. 13 und 14 DSGVO.

Auskunftsrecht

§ 19. (1) Eine Auskunft (Art. 15 DSGVO) darf nur erteilt werden, wenn die Identität der betroffenen Person in unbedenklicher Form festgestellt werden kann. Eine Kopie der verarbeiteten Dateninhalte muss so gestaltet sein, dass die Datenschutzrechte anderer Personen nicht verletzt werden.

(2) Auskünfte nach Art. 15 DSGVO dürfen nur in folgenden Fällen gegeben werden:

1. an die betroffene Person über die eigenen Daten. Dies schließt die Beantwortung einer Anfrage an einen bevollmächtigten Dritten nicht aus, soweit der Umfang der Bevollmächtigung nach den jeweiligen Umständen des Einzelfalles eindeutig nachvollziehbar ist;
2. an behördlich bestellte Vertreter (Erwachsenenvertreter, Kuratoren etc.) auf Grund ausdrücklicher Bestellungsurkunden, Beschlüsse oder Aufträge;
3. an gesetzliche Vertreter (Erziehungsberechtigte), jedoch in den Fällen, in denen ein Kind das 14. Lebensjahr bereits vollendet hat (§ 361 Abs. 2 ASVG), nur dann, wenn vor der Auskunftserteilung bescheinigt ist, dass die Auskunftserteilung nicht gegen dessen Interessen verstößt. Diese Bescheinigung hat der Art der angeforderten personenbezogenen Daten zu entsprechen und ist bei besonderen Kategorien personenbezogener Daten nachvollziehbar festzuhalten.

In diesen Fällen muss allenfalls auch eine Negativauskunft ausgestellt werden.

(3) Bei Anfragen an einen Auftragsverarbeiter ist auf den zuständigen Verantwortlichen zu verweisen. Auskünfte sind so zu erteilen, dass bei durchschnittlichem Verständnis von der betroffenen Person erwartet werden kann, dass sie Inhalt und Aussage der Auskunft zweifelsfrei versteht. Ein Auftragsverarbeiter hat von erteilten Auskünften den jewei-

ligen Verantwortlichen zu informieren. Das Auskunftsrecht betreffend Empfänger (oder Kategorien von Empfängern) umfasst nicht personenbezogene Daten anderer Personen (z. B. Name, Benutzerkennzeichen von MitarbeiterInnen) oder Sicherheitsdaten der abfrageberechtigten Stellen (z. B. Passwörter). Abkürzungen dürfen in der Auskunft verwendet werden, wenn erwartet werden kann, dass die betroffene Person sie versteht, oder wenn ihre Bedeutung dem Auskunftsschreiben zu entnehmen ist.

(4) Die Auskunft darf auch dadurch erteilt werden, dass der betroffenen Person ein Link oder die Internetadresse übermittelt wird, an der die entsprechende Auskunft jederzeit ohne weitere Suche mit persönlicher Identifikation (E-ID, Handysignatur) abrufbar ist oder ein Ausdruck ihrer Daten (z. B. eine Bildschirmkopie) mit Erläuterungen übersandt wird. Eine mündliche Auskunftserteilung ist nur dann ausreichend, wenn die betroffene Person damit einverstanden ist. Auskünfte über Telefon sind nur dann zulässig, wenn hiefür Sicherheitsvorkehrungen (Rückruf, Rückfragen, etc.) genützt werden. Auskünfte über Telefax dürfen nur ausnahmsweise erteilt werden, und nur dann, wenn insbesondere die gespeicherten Rufnummern regelmäßig und nachweislich auf ihre Aktualität geprüft werden. Ab 2020 ist eine Auskunftserteilung über Telefax nicht mehr zulässig, soweit dafür keine besonderen gesetzlichen Bestimmungen bestehen (§ 27 Abs. 12 GTelG 2012, BVergG 2017). Auskünfte über E-Mail (ohne Verschlüsselungsverfahren, elektronische Signatur, etc.) sind nur in Einzelfällen zulässig, wenn der Empfänger nachweislich durch Rückfragen etc. eindeutig identifiziert worden ist. Für Auskünfte in elektronischer Form ist vorrangig die Organisation des SV-Postfaches zu verwenden. Per Telefon, Telefax oder E-Mail dürfen besondere Kategorien von personenbezogenen Daten nur dann übermittelt werden, wenn vor der Übermittlung nachweislich und nachvollziehbar festgestellt werden konnte (z. B. durch einzelfallbezogene, auch telefonische, Anfragen von Versicherten zu ihrem Akt/Fall im Verwaltungsverfahren), dass die betroffene Person aufgrund der vorhandenen Informationen eindeutig identifiziert werden konnte und mit dieser Übermittlung einverstanden ist. Auch in solchen Fällen ist auf die Möglichkeit der Nutzung des SV-Postfaches hinzuweisen.

(5) Bei der schlüssig dargelegten Behauptung, dass ein Missbrauchsfall einer Abfrage vorliegt, umfasst das Auskunftsrecht auch Auskünfte aus Protokolldaten über externe Zugriffe auf Daten der betroffenen Person, ebenso aus Datenverarbeitungen (auch Übermittlungen wie z. B. Auskünfte, Verarbeitungen), die von bzw. bei einem Auftragsverarbeiter (z. B. dem Hauptverband nach § 31 Abs. 11 ASVG) erfolgten. Personenbezogene Daten anderer Personen (z. B. Benutzerkennzeichen oder Namen von MitarbeiterInnen) oder Sicherheitsdaten der abfrageberechtigten Stellen (z. B. Passwörter) dürfen bei Vorliegen überwiegender Interessen des Verantwortlichen oder eines Dritten bzw. überwiegender öffentlicher Interessen nicht preisgegeben werden.

(6) Eine Auskunft schließt auch Daten des Auskunftswerbers ein, die unter einem Ordnungsmerkmal eines Dritten (z. B. eines Dienstgebers, behandelnden Arztes) gespeichert sind, soweit der Auskunftswerber einen geeigneten Hinweis zur Feststellung dieses Ordnungsmerkmales gibt. Auskunft über eigene Behandlungsdaten der betroffenen Person (Diagnosen, verrechnete Leistungen etc.) darf nicht unter Berufung auf ein Geheimhaltungsinteresse des Behandlers verweigert werden. Angaben über Honorarzahlungen durch eine Versicherung gehören nicht zu den Behandlungsdaten von Patienten.

(7) Bei der Beantwortung eines Auskunftsbegehrens ist die betroffene Person unaufgefordert über die Rechte zu informieren, die ihr zustehen. Dies beinhaltet insbesondere das Recht auf:

1. Berichtigung (Art. 16 DSGVO);
2. Löschung (Art. 17 DSGVO);
3. Einschränkung (Art. 18 DSGVO);
4. Widerspruch gegen die Verarbeitung (Art. 21 DSGVO);
5. Beschwerde bei der Datenschutzbehörde (Art. 79 DSGVO).

Die Beantwortung eines Auskunftsbegehrens und andere Erledigungen im Rahmen eines Auskunftsverfahrens sind keine Bescheide im Sinn des § 410 ASVG, auf die datenschutzrechtliche Grundlage ist im Text solcher Erledigungen ausdrücklich hinzuweisen.

(8) Ein Auskunftswerber hat am Auskunftsverfahren in dem ihm zumutbaren Ausmaß mitzuwirken, um ungerechtfertigten und unverhältnismäßigen Aufwand beim Verantwortlichen zu vermeiden. Von der Bearbeitung eines Auskunftsersuchens ist abzusehen, wenn die betroffene Person nach entsprechender Aufforderung nicht in zumutbarer Weise am Verfahren mitwirkt. Auf diesen Umstand ist die betroffene Person in einer Aufforderung zur Mitwirkung hinzuweisen. Ein Auskunftswerber wirkt jedenfalls dann am Verfahren mit, wenn er

1. in jenen Fällen, in denen Anhaltspunkte dafür vorliegen, dass mehrere Personen mit gleichen oder sehr ähnlichen Daten vorhanden sind, die notwendigen konkreten Hinweise zur Unterscheidung seiner Person von diesen anderen Personen gibt;
2. die Datenverarbeitungen bezeichnet, bezüglich derer er betroffene Person sein kann und er bei umfangreichen Datenverarbeitungen auch den zeitlichen und inhaltlichen Zusammenhang der Verarbeitung seiner Daten nennt;
3. allenfalls durch die Vorlage von Unterlagen oder die Beschreibung von Lebensumständen glaubhaft macht, dass seine personenbezogenen Daten irrtümlich oder missbräuchlich in Datenbeständen des Verantwortlichen enthalten sind;
4. angibt, unter welchem Namen (bzw. Namenschreibweisen) und Geburtsdaten Daten über ihn aufgefunden werden könnten.

(9) Auskünfte sind überdies nicht zu erteilen, soweit überwiegende berechtigte Interessen des Verantwortlichen oder eines Dritten, insbesondere auch überwiegende öffentliche Interessen, der Auskunftserteilung entgegenstehen. Fälle, in denen der betroffenen Person gegenüber wegen überwiegenden öffentlichen Interesses Daten geheim zu halten sind (unbeschadet der ihr nach den maßgeblichen Verfahrensvorschriften zustehenden Rechte – nach Abwägung der Umstände des Einzelfalles), sind insbesondere Datenübermittlungen:

1. im Zuge eines gerichtlichen oder verwaltungsbehördlichen Strafverfahrens oder eines Disziplinarverfahrens sowie diesbezüglicher Vorerhebungen, solange das Verfahren noch nicht rechtskräftig abgeschlossen ist;
2. bei denen die Empfänger diesen Stellen angehören, sofern die Übermittlung für Zwecke eines gerichtlichen oder verwaltungsbehördlichen Strafverfahrens oder eines Disziplinarverfahrens durchgeführt wurde.

(10) Für Auskunftsanträge gelten die Fristen gemäß Art. 12 DSGVO. Die in Art. 12 Abs. 3 DSGVO enthaltene Frist von einem Monat für die Erteilung von Auskünften beginnt mit dem Einlangen des Auskunftsbegehrens beim Verantwortlichen. Wurde der Auskunftswerber aufgefordert, sein Auskunftsbegehren zu konkretisieren, so beginnt die Frist für die Auskunftserteilung mit dem Einlangen des konkretisierten Auskunftsbegehrens bei der auskunftsverpflichteten Stelle.

Andere Auskunftsvorschriften

§ 20. (1) Die Auskunftsbestimmungen des DSG und der DSGVO sind nicht anzuwenden, wenn Auskunftsbegehren auf einer anderen Grundlage als dem Datenschutzgesetz beruhen. Insbesondere werden die Vorschriften über Aufklärung und Information (§§ 81, 81a ASVG, §§ 27, 27a B-KUVG, §§ 43, 43a GSVG, § 41, 41a BSVG, §§ 17, 17a NVG) nicht berührt.

(2) Auskünfte über personenbezogene Daten sind außerhalb des Versicherungsverhältnisses der betroffenen Person sowie außerhalb gesetzlicher oder vertraglicher Beziehungen (§ 42 ASVG, § 338 Abs. 4 ASVG u. a.) nach der DSGVO, dem DSG und dieser Verordnung zu erteilen, soweit sich der Auskunftsberechtigte nicht ausdrücklich auf eine andere Rechtsgrundlage beruft.

Recht auf Berichtigung

§ 21. (1) Das Recht auf Berichtigung von personenbezogenen Daten nach Art. 16 DSGVO in den Stammdaten der Datenverarbeitungen der Sozialversicherung besteht nur insoweit, als nicht andere gesetzliche Vorschriften entgegenstehen (wie z. B. § 358 ASVG betreffend die Feststellung des Geburtsdatums). Das Recht auf Berichtigung umfasst keinesfalls ein Recht auf Veränderungen in Programmabläufen.

(2) Akademische Titel/Grade sind in den Datenverarbeitungen der Sozialversicherung (inklusive e-card) nach den Verzeichnissen des Bundesministeriums für Wissenschaft, Forschung und Wirtschaft über die Führung und Abkürzung akademischer Grade einzutragen (NARIC-Verzeichnis und deren Eintragungsrichtlinien). Namen und Titel dürfen stärker als es für die Anführung auf einer e-card notwendig ist, abgekürzt werden, wenn es die Bestimmungen über die Europäische Krankenversicherungskarte EKVK oder andere international zu beachtende Regeln oder kurzfristig nicht änderbare Feldlängen notwendig machen. Andere (Berufs- und Ehren-)Titel oder Bezeichnungen sind nur dann zu verwenden, wenn die jeweilige Bezeichnung nach dem Personalstatut (§ 9 IPRG) des Betroffenen ein Bestandteil des Namens ist.

(3) Die Speicherung von Namens- und Geburtsdatenvarianten, früheren Namen oder Adressvarianten ist zulässig, wenn sie zur besseren Feststellung der Identität beitragen kann.

(4) Ein Berichtigungswerber hat am Berichtigungsverfahren in dem ihm zumutbaren Ausmaß mitzuwirken, um ungerechtfertigten und unverhältnismäßigen Aufwand beim Verantwortlichen zu vermeiden. Von der Bearbeitung eines Berichtigungsantrags ist abzusehen, wenn die betroffene Person nicht am Verfahren mitwirkt. Auf diesen Umstand ist die betroffene Person in einer Aufforderung zur Mitwirkung hinzuweisen. Ein Berichtigungswerber wirkt jedenfalls dann am Verfahren mit, wenn er

1. in jenen Fällen, in denen Anhaltspunkte dafür vorliegen, dass mehrere Personen mit gleichen oder sehr ähnlichen Daten vorhanden sind, die notwendigen konkreten Hinweise zur Unterscheidung seiner Person von diesen anderen Personen gibt;
2. die Datenverarbeitungen bezeichnet, bezüglich derer er betroffene Person sein kann und er bei umfangreichen Datenverarbeitungen auch den zeitlichen und inhaltlichen Zusammenhang der Verarbeitung seiner Daten nennt;
3. allenfalls durch die Vorlage von Unterlagen glaubhaft macht, dass seine personenbezogenen Daten unrichtig oder unvollständig in Datenbeständen des Verantwortlichen enthalten sind;
4. angibt, unter welchem Namen (bzw. Namenschreibweisen) und Geburtsdaten Daten über ihn aufgefunden werden könnten.

(5) Für Berichtigungsanträge gelten die Fristen gemäß Art. 12 DSGVO. Die in Art. 12 Abs. 3 DSGVO enthaltene Frist von einem Monat für die Entscheidung über den Berichtigungsantrag beginnt mit dem Einlangen des Berichtigungsbegehrens beim Verantwortlichen. Wurde der Berichtigungswerber aufgefordert, sein Berichtigungsbegehren zu konkretisieren bzw. Unterlagen dazu vorzulegen, so beginnt die Frist für dieses mit dem Einlangen des konkretisierten Berichtigungsbegehrens bei der zuständigen Stelle zu laufen.

(6) Mitteilungen über eine Berichtigung, eine Ablehnung derselben und andere Erledigungen im Rahmen eines Berichtigungsverfahrens sind keine Bescheide im Sinn des § 410 ASVG, auf die datenschutzrechtliche Grundlage ist im

Text solcher Erledigungen ausdrücklich hinzuweisen und diese sind neben der Begründung der Entscheidung mit einer Rechtsbehelfsbelehrung über die Möglichkeit einer Beschwerde bei der Datenschutzbehörde zu versehen.

Recht auf Löschung

§ 22. (1) Vor jeder Löschung von Daten ist zu prüfen, ob diese Daten tatsächlich von allen in Frage kommenden Verarbeitungen nicht mehr benötigt werden. Löschungen vor Ablauf der Aufbewahrungsfristen (§ 16) sind unzulässig. Eine Löschung ist weiters unzulässig, solange eine andere Datenverarbeitung diese Daten benötigt (zur Einschränkung der Verarbeitung siehe § 23). Daten, die zur Vollziehung gesetzlicher Vorschriften heranzuziehen sind, dürfen nicht gelöscht werden. Das Recht auf Löschung von personenbezogenen Daten nach Art. 17 DSGVO umfasst keinesfalls ein Recht auf Veränderungen in Programmabläufen.

(2) Anträge auf Löschung sind nach der Sach- und Rechtslage im Zeitpunkt ihres Einlangens zu behandeln, sie müssen nicht solange aufgehoben werden, bis die Daten tatsächlich nicht mehr benötigt werden. Ausnahmen von der Löschpflicht bestehen im Rahmen des Art. 17 Abs. 3 DSGVO.

(3) Daten, die gespeichert werden, um Verwechslungen von Personen mit gleichen oder sehr ähnlichen Namen und Geburtsdaten zu erschweren, dürfen nicht gelöscht werden.

(4) Bei personenbezogenen Daten, die für Sicherungszwecke (Sicherungskopien ohne zusätzlichen Verwendungszweck) aufbewahrt werden, ist durch geeignete Maßnahmen sicherzustellen, dass im Falle eines Rückgriffes auf diese Daten allfällige Löschungen wirksam bleiben.

(5) Ein Löschungswerber hat am Löschungsverfahren in dem ihm zumutbaren Ausmaß mitzuwirken, um ungerechtfertigten und unverhältnismäßigen Aufwand beim Verantwortlichen zu vermeiden. Von der Bearbeitung eines Löschungsantrags ist abzusehen, wenn die betroffene Person nicht am Verfahren mitwirkt. Auf diesen Umstand ist die betroffene Person in einer Aufforderung zur Mitwirkung hinzuweisen. Ein Löschungswerber wirkt jedenfalls dann am Verfahren mit, wenn er

1. ein erkennbares Löschungsbegehren abgibt;
2. die Datenverarbeitungen bzw. den Löschungsgegenstand bezeichnet, bezüglich derer er betroffene Person sein kann und er bei umfangreichen Datenverarbeitungen auch den zeitlichen und inhaltlichen Zusammenhang der Verarbeitung seiner Daten nennt;
3. einen Löschungsgrund angibt;
4. in jenen Fällen, in denen Anhaltspunkte dafür vorliegen, dass mehrere Personen mit gleichen oder sehr ähnlichen Daten vorhanden sind, die notwendigen konkreten Hinweise zur Unterscheidung seiner Person von diesen anderen Personen gibt;
5. allenfalls durch die Vorlage von Unterlagen glaubhaft macht, dass seine personenbezogenen Daten in den Datenbeständen des Verantwortlichen zu löschen sind;
6. angibt, unter welchem Namen (bzw. Namenschreibweisen) und Geburtsdaten Daten über ihn aufgefunden werden könnten.

(6) Ein zulässiger Löschungsantrag kann nur die eigenen personenbezogenen Daten betreffen. In diesem Rahmen kann der Löschungswerber den Umfang des Löschungsrechts selbst bestimmen.

(7) Für Löschungsanträge gelten die Fristen gemäß Art. 12 DSGVO. Die in Art. 12 Abs. 3 DSGVO enthaltene Frist von einem Monat für die Entscheidung über den Löschungsantrag beginnt mit dem Einlangen des Löschungsbegehrens beim Verantwortlichen. Wurde der Löschungswerber aufgefordert, sein Löschungsbegehren zu konkretisieren bzw. Unterlagen dazu vorzulegen, so beginnt die Frist für dieses mit dem Einlangen des konkretisierten Löschungsbegehrens bei der zuständigen Stelle zu laufen.

(8) Mitteilungen über eine Löschung, eine Ablehnung derselben und andere Erledigungen im Rahmen eines Löschungsverfahrens sind keine Bescheide im Sinn des § 410 ASVG, auf die datenschutzrechtliche Grundlage ist im Text solcher Erledigungen ausdrücklich hinzuweisen und diese sind neben der Begründung der Entscheidung mit einer Rechtsbehelfsbelehrung über die Möglichkeit einer Beschwerde bei der Datenschutzbehörde zu versehen.

Recht auf Einschränkung der Verarbeitung

§ 23. (1) Das Recht auf Einschränkung der Verarbeitung von personenbezogenen Daten nach Art. 18 DSGVO umfasst keinesfalls ein Recht auf Veränderungen in Programmabläufen.

(2) Das Recht auf Einschränkung der Verarbeitung ist ein zeitlich beschränktes bzw. bedingtes Recht. Es handelt sich um einen vorübergehenden Schutzzustand, damit der betroffenen Person aus der Datenverarbeitung bzw. durch die Beendigung der Datenverarbeitung keine Nachteile entstehen. Die Einschränkung der Verarbeitung ist soweit dies nicht anders möglich ist, durch Zugriffssperre und/oder Pseudonymisierung und/oder von der Datenverarbeitung abgesonderte Sicherung der Daten herzustellen.

(3) In den Fällen des Art. 18 Abs. 1 lit. a (Berichtigung) und d (Widerspruch) DSGVO ist die Einschränkung auf die Dauer der Prüfung des Hauptanspruches beschränkt.

(4) Ein Einschränkungswerber hat am Einschränkungsverfahren in dem ihm zumutbaren Ausmaß mitzuwirken, um ungerechtfertigten und unverhältnismäßigen Aufwand beim Verantwortlichen zu vermeiden. Von der Bearbeitung eines Einschränkungsantrags ist abzusehen, wenn die betroffene Person nicht am Verfahren mitwirkt. Auf diesen Umstand ist

die betroffene Person in einer Aufforderung zur Mitwirkung hinzuweisen. Ein Einschränkungswerber wirkt jedenfalls dann am Verfahren mit, wenn er

1. eine erkennbare und explizite Einschränkung der Nutzung beantragt;
2. die Datenverarbeitungen bzw. den Einschränkungsgegenstand bezeichnet, bezüglich derer er betroffene Person sein kann und er bei umfangreichen Datenverarbeitungen auch den zeitlichen und inhaltlichen Zusammenhang der Verarbeitung seiner Daten nennt;
3. in jenen Fällen, in denen Anhaltspunkte dafür vorliegen, dass mehrere Personen mit gleichen oder sehr ähnlichen Daten vorhanden sind, die notwendigen konkreten Hinweise zur Unterscheidung seiner Person von diesen anderen Personen gibt;
4. allenfalls durch die Vorlage von Unterlagen glaubhaft macht, dass seine personenbezogenen Daten in den Datenbeständen des Verantwortlichen einzuschränken sind;
5. angibt, unter welchem Namen (bzw. Namenschreibweisen) und Geburtsdaten Daten über ihn aufgefunden werden könnten.

(5) Wird die Richtigkeit personenbezogener Daten bestritten und lässt sich weder die Richtigkeit noch die Unrichtigkeit der Daten feststellen, besteht für die betroffene Person kein Recht auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO.

(6) Personenbezogene Daten, hinsichtlich derer das Recht auf Einschränkung der Datenverarbeitung ausgeübt worden ist, dürfen nur mehr mit Einwilligung der betroffenen Person, zur Geltendmachung von Rechtsansprüchen, zum Schutz der Rechte anderer oder aus wichtigen öffentlichen Interessen verarbeitet werden.

(7) Für Einschränkungsanträge gelten die Fristen gemäß Art. 12 DSGVO. Die in Art. 12 Abs. 3 DSGVO enthaltene Frist von einem Monat für die Entscheidung über den Einschränkungsantrag beginnt mit dem Einlangen des Einschränkungsbegehrens beim Verantwortlichen. Wurde der Einschränkungswerber aufgefordert, sein Einschränkungsbegehren zu konkretisieren bzw. Unterlagen dazu vorzulegen, so beginnt die Frist für dieses mit dem Einlangen des konkretisierten Einschränkungsbegehrens bei der zuständigen Stelle zu laufen.

(8) Die betroffene Person muss vom Verantwortlichen vor Aufhebung der Einschränkung informiert werden.

(9) Mitteilungen über eine Einschränkung, eine Aufhebung oder Ablehnung derselben und andere Erledigungen im Rahmen eines Einschränkungsverfahrens sind keine Bescheide im Sinn des § 410 ASVG, auf die datenschutzrechtliche Grundlage ist im Text solcher Erledigungen ausdrücklich hinzuweisen und diese sind neben der Begründung der Entscheidung mit einer Rechtsbehelfsbelehrung über die Möglichkeit einer Beschwerde bei der Datenschutzbehörde zu versehen.

Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung

§ 24. In welcher Form die Mitteilungspflicht auszuüben ist, richtet sich nach Art. 19 DSGVO.

Widerspruchsrecht

§ 25. Das Recht auf Widerspruch richtet sich nach Art. 21 DSGVO. Das Recht auf Widerspruch gemäß Art. 21 Abs. 1 DSGVO besteht nicht, soweit an der Verarbeitung ein zwingendes öffentliches Interesse, das die Interessen der betroffenen Person überwiegt, oder eine gesetzliche Verpflichtung (inklusive deren Durchführungsregeln, wie Satzungen, Krankenordnungen, etc.) zur Verarbeitung besteht.

Information der Bediensteten

§ 26. (1) Alle Bediensteten eines Verantwortlichen oder Auftragsverarbeiters sind von diesem in geeigneter Form über die für sie wesentlichen Bestimmungen des DSG, der DSGVO und dieser Verordnung in Kenntnis zu setzen.

(2) Die Bediensteten, die mit der Durchführung von Datenverarbeitungen befasst sind, sind in einem erhöhten Maße über datenschutzrechtliche Bestimmungen zu informieren.

Inkrafttreten

§ 27. (1) Diese Verordnung tritt mit 25. Mai 2018 in Kraft. Gleichzeitig tritt die SV-Datenschutzverordnung 2012 (SV-DSV 2012), avsv Nr. 63/2012, geändert durch avsv Nr. 54/2016 und avsv Nr. 181/2016, außer Kraft.

*

Diese Datenschutzverordnung für die gesetzliche Sozialversicherung (SV-DSV) wurde vom Verbandsvorstand des Hauptverbandes der österreichischen Sozialversicherungsträger am 17. April 2018 beschlossen.

Die Erläuterungen dieser Verordnung sind unter www.sozdok.at kostenlos zugänglich.

Für den Hauptverband der österreichischen Sozialversicherungsträger:

Biach **Probst**

	**Unterzeichner**	Hauptverband der oesterreichischen SV-Traeger
	Datum/Zeit-UTC	2018-04-19T10:50:17+02:00
	Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter https://www.sozialversicherung.at/signaturpruefung/ bzw. https://www.signaturpruefung.gv.at. Informationen zur Prüfung des Ausdrucks finden Sie unter https://www.sozialversicherung.at/verifikation/
Hinweis	Dieses Dokument wurde amtssigniert. Auch ein Ausdruck dieses Dokuments hat gemäß § 20 E-Government-Gesetz die Beweiskraft einer öffentlichen Urkunde.	