Amtliche Verlautbarung der österreichischen Sozialversicherung im Internet: www.avsv.at

Hauptverband der österreichischen Sozialversicherungsträger

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

Datenschutzverordnung für die gesetzliche Sozialversicherung (SV-Datenschutzverordnung 2012 – SV-DSV 2012)

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 Austria Tabak
   b) Betriebskrankenkasse der Wiener Verkehrsbetriebe
   c) Betriebskrankenkasse Mondi
   d) Betriebskrankenkasse voestalpine Bahnsysteme
   e) Betriebskrankenkasse Zeltweg
   f) 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 Auftraggeber nach § 4 Z 4 DSG 2000 und Dienstleister nach § 4 Z 5 DSG 2000; für den Hauptverband auch als Betreiber eines Informationsverbundsystems nach § 4 Z 13 DSG 2000.

(2) Sie gilt sowohl für die Verwendung von Dateien im Sinn des DSG 2000 als auch für den Bereich des Grundrechts auf Datenschutz. Verweise auf Normen sind nach deren Stand am Tag der Kundmachung zu verstehen, soweit nicht ausdrücklich eine andere Fassung genannt ist.

Hauptverband als Dienstleister

§ 2. (1) Der Hauptverband der österreichischen Sozialversicherungsträger ist nach § 31 Abs. 11 ASVG Dienstleister für die Sozialversicherungsträger. Dies gilt insbesondere für

- die Vergabe einheitlicher Versicherungsnummern und deren Verknüpfung mit bereichsspezifischen Personenkennzeichen nach § 31 Abs. 4 Z 1 ASVG und § 9 E-GovG,
- die Einrichtung und Führung einer zentralen Anlage zur Aufbewahrung der für die Versicherung bedeutsamen Daten nach § 31 Abs. 4 Z 3 lit. a ASVG,
- die Auskunftserteilung nach § 31 Abs. 4 Z 3 lit. b ASVG,
- die Verwendung von Daten für Verrechnungszwecke auf Grund sozialversicherungsrechtlicher Bestimmungen,
- den Betrieb des elektronischen Verwaltungssystems ELSY nach § 31a Abs. 2 ASVG sowie

- seine Aufgaben als Zugangsstelle oder als Verbindungsstelle nach Art. 1 Abs. 2 lit. a oder lit. b der Durchführungsverordnung Nr. 987/2009 zur Verordnung (EG) Nr. 883/2004 und nach den §§ 4 f. des Sozialversicherungs-Ergänzungsgesetzes.

(2) Der Hauptverband der österreichischen Sozialversicherungsträger ist für die Sozialversicherungsträger im Rahmen des Informationsverbundsystems der österreichischen Sozialversicherung nach § 50 Abs. 1 DSG 2000 Betreiber dieses Systems. Die von ihm festgelegten Maßnahmen der Datensicherheit (§ 7) sind für die in diesem System tätigen Auftraggeber verbindlich (§ 31 Abs. 6 ASVG).

öffentlicher Bereich

§ 3. Die Datenanwendungen der Auftraggeber sind nach § 5 DSG 2000 dem öffentlichen Bereich zuzuordnen.

Aufgabengebiete

§ 4. Bei den Sozialversicherungsträgern und dem Hauptverband bestehen folgende Aufgabengebiete im Sinn des § 4 Z 12 DSG 2000:

1. Vollziehung des gesetzlichen Zuständigkeitsbereiches,
2. Wirtschaftsverwaltung einschließlich Finanz- und Beschaffungswesen sowie Kostenrechnung,
3. Personalverwaltung einschließlich Angelegenheiten der Versicherungsvertreter.

Grundsätze für die Verwendung von Daten

§ 5. (1) Daten dürfen vom Auftraggeber nur im Rahmen des § 6 DSG 2000 verwendet werden.

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

1. Daten dürfen nur in der Art und dem Umfang verwendet werden, als dies für den Auftraggeber zur Wahrnehmung der ihm gesetzlich übertragenen Aufgaben eine wesentliche Voraussetzung ist. Die Verwendung nicht notwendiger Daten (Ballastwissen, Überschusswissen) ist unzulässig.
2. Übermittlungen 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 Datenverwendung begründet für sich allein noch keine Verpflichtung hiezu. Für eine Datenverwendung haben konkrete Gründe aus dem Vollziehungsbereich des jeweiligen Rechtsträgers im Sinn des § 6 DSG 2000 vorzuliegen.
4. Daten, die mit an Sicherheit grenzender Wahrscheinlichkeit nicht mehr benötigt werden, sind möglichst rasch zu löschen. Zu diesem Zweck sind Datenbestände regelmäßig auf die Notwendigkeit der darin enthaltenen Daten durchzusehen. Die bloße theoretische Möglichkeit, Datenbestände zur Vollziehung einer noch nicht absehbaren zukünftigen Regelung verwenden zu können, ist für sich allein kein ausreichender Grund, entsprechende Daten aufzubewahren.
5. Einem Ersuchen um Übermittlung darf ein Auftraggeber nur entsprechen, wenn folgende Voraussetzungen gemeinsam vorliegen:
   a) eine Rechtsgrundlage (Z 2) hiefür feststeht,
   b) bei Zweifeln an der Übermittlungszulässigkeit die ersuchende Stelle vor der Datenermittlung ihre Ermittlungsberechtigung glaubhaft gemacht hat,
   c) bei Online-Übermittlungsverfahren der Übermittlungsempfänger für die Dauer des Bestehens seiner Zugriffsberechtigung verpflichtet ist, regelmäßige Kontrollen durchzuführen, Kontrollmaßnahmen der übermittelnden Stelle zu unterstützen, dies auch tatsächlich geschieht und dies dem Auftraggeber gegenüber glaubhaft gemacht ist,
   d) sich Übermittlungsersuchen auf konkret umschriebene Daten oder Personen 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.
6. Das gelindeste zur Verfügung stehende Mittel im Sinn des § 7 Abs. 3 DSG 2000 wird dann nicht mehr eingesetzt, wenn Daten aus Beständen der Sozialversicherung für Zwecke verwendet werden sollen, zu deren Unterstützung andere Register eingerichtet sind (z. B. für Adressenermittlungen die Melderegister, für Einkommenserhebungen jene der Finanzverwaltung).
7. Die Verantwortlichkeit des Auftraggebers bzw. Dienstleisters für die weitere Verwendung der Daten endet mit der Übermittlung dieser 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 Daten zu trennen, die für diese Personen in deren Eigenschaft als Versicherte, Vertragspartner oder Dienstgeber (meldepflichtige Stellen) verwendet werden. 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.

Verwendung von sensiblen Daten

§ 6. (1) Die Verwendung von sensiblen Daten ist ausschließlich in den Fällen, die in § 9 DSG 2000 taxativ aufgezählt sind, zulässig.

(2) Ein „wichtiges öffentliches Interesse“ im Sinn des § 9 Z 3 DSG 2000 kann auch ein wichtiges wirtschaftliches öffentliches Interesse sein, wobei auch in solchen Zusammenhängen die Datenverwendung nur im tatsächlich notwendigen Ausmaß erfolgen darf (z. B. Evaluierung der Verwendung öffentlicher Mittel im Gesundheitswesen durch Aufsichtsbehörden und Rechnungshof, Zusammenwirken bei der Gesundheitsvorsorge nach § 459e Abs. 2 Z 4 und 5 ASVG).

(3) Medizinische Diagnostik im Sinn des § 9 Z 12 DSG 2000 umfasst auch Untersuchungen für Zwecke der Rehabilitation oder der Erbringung anderer Leistungen durch Sozialversicherungsträger einschließlich des Verfahrens in Sozialrechtssachen vor den Arbeits- und Sozialgerichten, wenn sie durch ärztliches Personal oder sonstige Personen vorgenommen werden, die einer entsprechenden Geheimhaltungspflicht unterliegen.

Datensicherheitsmaßnahmen

§ 7. (1) Auftraggeber und Dienstleister haben die Richtigkeit der Verarbeitungsergebnisse in regelmäßigen Abständen durch Stichproben oder Prüfprogramme zu überprüfen.

(2) Daten und Programme sind vor Entstellung, Zerstörung und Verlust sowie gegen unbefugte Verwendung und Weitergabe zu schützen.

(3) Der Auftraggeber (oder in dessen Auftrag der Dienstleister) hat für die Vernichtung unbrauchbarer oder nicht mehr benötigter Ausdrucke und sonstiger Datenträger Sorge zu tragen.

(4) Wird ein Fehler festgestellt, so haben der Auftraggeber und der Dienstleister alles zu unternehmen, um das Schadensausmaß gering zu halten, den Betroffenen unnötige Mühe zu ersparen, die Fehlerbehebung raschest einzuleiten und Folgefehler zu verhindern.

(5) Für die ordnungsgemäße und sichere Verwendung von Daten sind folgende Datensicherheitsmaßnahmen (§ 14 DSG 2000) zu setzen:

1. Es ist eine Vorgangsweise (Person, Organisationseinheit, Schulungen) für Datensicherheitsmaßnahmen und andere Datenschutzthemen festzulegen, in deren Rahmen die Unterlagen (Organisationsbeschreibungen, Datensicherheitsmaßnahmen etc.) des Versicherungsträgers und des Hauptverbandes gesammelt zur Verfügung stehen und die als interne Kontaktstelle für jene datenschutzrechtliche Fragen dient, die im Zusammenhang mit der Verwendung der Daten des Auskunftswerbers durch den jeweiligen Sozialversicherungsträger bzw. den Hauptverband stehen, insbesondere Auskunftsersuchen (§ 13) und Anfragen nach dem Auskunftspflichtrecht.
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. Bestehende Einrichtungen sind regelmäßig auf Verbesserungsmöglichkeiten zu untersuchen.
3. Zugriff auf Datenanwendungen darf nur eingeräumt werden, nachdem die Bestimmungen über das Datengeheimnis (§ 15 DSG 2000), die Datensicherheitsmaßnahmen und diese Verordnung zur Kenntnis gebracht wurden. Sammelzugriffsberechtigungen sind unzulässig. Ebenso unzulässig ist es, Datenbestände außerhalb ausdrücklicher gesetzlicher Bestimmungen gesammelt an zugriffsberechtigte Stellen zu übermitteln, um diesen bei Bedarf das Verwenden der Daten möglich zu machen.
4. Zugriffsberechtigungen außerhalb ausdrücklicher gesetzlicher Verpflichtungen sind möglichst 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. Datensichtgeräte (Bildschirme, etc.) sind so aufzustellen, dass der mit ihnen wiedergegebene Inhalt nicht von Unbefugten mitgelesen werden kann.
6. Von einem Verfahren der Datenschutzkommission nach § 30 DSG 2000 betreffend das Informationsverbundsystem der österreichischen Sozialversicherung, sind vom betroffenen Versicherungsträger jedenfalls der Hauptverband und jene Versicherungsträger zu verständigen (bzw. vom Hauptverband die betroffenen Versicherungsträger, § 321 ASVG, § 183 GSVG, § 171 BSVG, § 119 B-KUVG, § 87 NVG), welche Daten des Betroffenen verwenden.
7. Es sind alle dem jeweiligen Stand der Technik entsprechenden und wirtschaftlich zumutbaren Maßnahmen zu treffen, um eine Veränderung oder Vernichtung der Daten durch Programmstörungen zu verhindern, wie die Installation von Virenschutzprogrammen, fire-walls, Laufwerksperren, gestaffelte Zugriffsberechtigungen, etc.
8. Datenträger (Festplatten, Bänder, Disketten etc.) sind vor einer Veräußerung oder Entsorgung nach dem Stand der Technik physisch zu löschen oder sicher unlesbar zu machen. Die Beauftragung von Stellen, die bei solchen Arbeiten nicht an Weisungen eines Sozialversicherungsträgers oder des Hauptverbandes gebunden sind

und damit nicht unter direkter Kontrolle des Auftraggebers stehen, oder die nicht nach einschlägigen Standards zertifiziert sind, ist unzulässig.

9. Zugriff auf Datenverwendungen darf nur auf Grund persönlicher Benützerkennungen und Kennwörter (Passwörter) möglich sein. Die Kennwortvergabe hat vorzusehen, dass Kennwörter aus einer Mindestzahl von Zeichen und (wenn nicht schwer wiegende technische Gründe dagegen sprechen) einer Kombination aus Buchstaben, Ziffern (statt Ziffern auch Sonderzeichen) zu bestehen haben. Kennwörter sind geheim zu halten, ihre Änderung ist dem Zugriffsberechtigten innerhalb periodischer Zeiträume möglich zu machen. Das Kennwort muss von der Benutzerkennung verschieden sein.
10. Datenanwendungen 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, Überlassungen) 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.
11. Datenanwendungen sind technisch nach den Regeln des E-Governments des Bundes (E-Government-Gesetz, Signaturgesetz, Gesundheitstelematikgesetz) unter Berücksichtigung der bereichsspezifischen Personenkennzeichen (§ 31 Abs. 4 Z 1 ASVG) zu gestalten. Datenträger, die eine undokumentierte nachträgliche Veränderung oder ein nicht nachvollziehbares Löschen von Daten ermöglichen oder die auf einfache Weise durch ein anderes gleich aussehendes Exemplar ersetzt werden können (z. B. Disketten, Magnetbänder, USB-Sticks, CD-ROM, transportable Festplatten) dürfen für Übermittlungen oder Überlassungen nicht verwendet werden.
12. Datenanwendungen (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.
13. Zur Vermeidung, Abwehr und Nachverfolgung von Angriffen auf Datenbestände oder technische Einrichtungen der Datenverwendung ist mit den dafür bestehenden Einrichtungen für öffentliche Stellen zusammenzuarbeiten.
14. Die Sozialversicherungsträger und der Hauptverband haben sich an Einrichtungen zu beteiligen, durch welche eine elektronische Zustellung (§§ 28 ff. ZustG) möglich sind sowie selbst elektronische Posteingangsadressen anzubieten.

(6) Über alle Datensicherheitsmaßnahmen ist eine Dokumentation zu führen; diese ist mindestens elf Jahre aufzubewahren.

(7) Der Hauptverband als Betreiber nach § 50 Abs. 1 DSG 2000 hat gemeinsam mit den Versicherungsträgern durch Stichproben zu prüfen, ob die Verwendung der Daten den einschlägigen Bestimmungen entsprechend erfolgt und die erforderlichen Datensicherheitsmaßnahmen ergriffen worden sind.

(8) Bedient sich der Hauptverband oder ein Sozialversicherungsträger für den Datenverkehr eines Dienstleisters, so ist dieser zur Einhaltung aller datenschutzrechtlichen Bestimmungen und Ergreifung der in dieser Verordnung vorgesehenen Datensicherheitsmaßnahmen zu verpflichten.

Protokollierung

§ 8. (1) Protokolle sind regelmäßig zu prüfen und, soweit diese und andere Vorschriften keine anderen Aufbewahrungsfristen für Protokolle vorsehen, mindestens elf Jahre und höchstens 31 Jahre in automationsunterstützt lesbarer Form aufzubewahren.

(2) Protokollierungen (§ 14 Abs. 2 Z 7 DSG 2000) sind in leicht zugänglicher und für die zuständigen MitarbeiterInnen einfach lesbarer Weise vorzunehmen. Je nach Empfänger dürfen hinsichtlich Art der verwendeten Daten, Umfang und Zweck der Verwendung, Stand der technischen Möglichkeiten und Kosten unterschiedliche Protokollierungsmethoden verwendet werden, solange die Auskunftsverpflichtung dadurch nicht beeinträchtigt wird. Ob eine Protokollierung tatsächlich entfallen darf, ist für jede Datenanwendung im Einzelfall nach den Kriterien des § 14 DSG 2000 abzuwägen, die Protokollierung darf weiters nur in folgenden Zusammenhängen entfallen:

1. Wenn Daten auf Grund einer

   a) Standardanwendung (§ 17 Abs. 2 Z 6 DSG 2000) oder

   b) Musteranwendung (§ 19 Abs. 3 DSG 2000)

   verwendet werden. In diesem Fall ist dem Betroffenen bei einer Anfrage nach § 26 DSG 2000 mitzuteilen, dass bestimmte Datenarten des Betroffenenkreises, zu dem auch der Betroffene gehört, an einen bestimmten Empfängerkreis planmäßig übermittelt werden. Die hievon betroffenen Datenarten, Betroffenenkreise und Empfängerkreise sind in der Auskunft zu nennen.
2. Wenn Daten nach § 46 DSG 2000 für wissenschaftliche Forschung und Statistik verwendet werden.
3. Wenn Daten gesammelt als Grundlage gesetzlich vorgesehener konkreter weiterer Verwendungen (z. B. zur Vorbereitung von Wahlen nach § 45 AKG 1992) übermittelt werden.

4. Wenn die Programme, mit denen Daten verwendet werden, vor Inkrafttreten dieser Verordnung fertig gestellt wurden und der Einbau eines Programmteils zur Protokollierung wegen des in absehbarer Zeit erfolgenden Einsatzes neuer Programme unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit unzweckmäßig wäre.

(3) Die Protokollierung ist so zu gestalten, dass auch Zugriffe der eigenen MitarbeiterInnen nachvollzogen werden können.

(4) Die Registrierung einer einzelfallbezogenen Datenübermittlung an Stellen außerhalb des Aufsichtsbereiches der obersten Aufsichtsbehörde der Sozialversicherung (z. B. im Rahmen von Amtshilfe) befreit nicht von der Verpflichtung, diese Übermittlungen zu protokollieren. Auftraggeber einer Standardanwendung haben jedermann auf Anfrage mitzuteilen (§ 23 DSG 2000), welche Standardanwendungen sie tatsächlich vornehmen.

Datengeheimnis

§ 9. (1) Allen Bediensteten und sonstigen Personen, denen Daten aus Datenanwendungen auf Grund ihrer Beschäftigung oder Funktion bei einem Auftraggeber oder Dienstleister anvertraut oder zugänglich geworden sind, ist es unbeschadet sonstiger Verschwiegenheitspflichten untersagt,

1. sich Daten unbefugt zu beschaffen,
2. Daten zu einem anderen Zweck als für ihre eigene Arbeit zu verwenden,
3. unbefugten Personen oder unzuständigen Stellen Daten mitzuteilen,
4. unbefugten Personen oder unzuständigen Stellen Daten zugänglich zu machen.

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

Information der Bediensteten

§ 10. (1) Alle Bediensteten eines Auftraggebers oder Dienstleisters sind von diesem in geeigneter Form über die für sie wesentlichen Bestimmungen des Datenschutzgesetzes und dieser Verordnung in Kenntnis zu setzen.

(2) Die Bediensteten, die mit der Durchführung von Datenanwendungen befasst sind, sind in einem erhöhten Maße über datenschutzrechtliche Bestimmungen, insbesondere über das Datenschutzgesetz und diese Verordnung, zu informieren.

Datenverarbeitungsregister

§ 11. (1) Jede Datenanwendung ist nach der Datenverarbeitungsregister-Verordnung der Datenschutzkommission zur Eintragung in das Datenverarbeitungsregister zu melden, soweit nicht eine ausdrückliche Ausnahme nach § 17 oder § 50c Abs. 2 DSG 2000 besteht oder die Anwendung bereits auf Grund des Übergangsrechts (§ 61 DSG 2000) als gemeldet gilt.

(2) Bei Übermittlungen und Mitteilungen an Betroffene, die in schriftlicher Form ergehen, ist die Registernummer in deren Text anzugeben.

(3) Bei Übermittlungen und Mitteilungen an Betroffene mittels maschinell lesbarer Datenträger ist die Registernummer auf den Begleitpapieren oder auf den Datenträgern anzugeben.

Informationspflicht des Auftraggebers

§ 12. In welcher Form die Informationspflicht auszuüben ist, richtet sich nach § 24 DSG 2000. Diese Informationspflicht besteht unabhängig vom Einsichtsrecht in das Datenverarbeitungsregister.

Auskunftsrecht

§ 13. (1) Eine Auskunft darf unbeschadet der nachstehenden Bestimmungen nur erteilt werden, wenn die Identität des Betroffenen in unbedenklicher Form festgestellt werden kann.

(2) Auskünfte nach § 26 DSG 2000 dürfen nur in folgenden Fällen gegeben werden:

1. an den Betroffenen über die eigenen Daten (dies schließt die Anforderung einer Auskunft durch einen bevollmächtigten Dritten mit Zustellung an den Betroffenen nicht aus);
2. an behördlich bestellte Vertreter (Sachwalter, 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, nur dann, wenn vor der Auskunftserteilung bescheinigt ist, dass die Auskunftserteilung nicht gegen dessen Interessen verstößt. Diese Bescheinigung hat der Art der angeforderten Daten zu entsprechen und ist bei sensiblen Daten nachvollziehbar festzuhalten.

(3) Die Auskunft ist

1. vom Auftraggeber einer Datenanwendung nach § 26 DSG 2000,
2. vom Betreiber eines Informationsverbundsystems zumindest im Rahmen des § 50 Abs. 1 DSG 2000,
3. von Dienstleistern nach § 26 Abs. 10 DSG 2000

so zu erteilen, dass bei durchschnittlichem Verständnis von Betroffenen erwartet werden kann, sie würden Inhalt und Aussage der Auskunft zweifelsfrei verstehen. Abkürzungen dürfen in der Auskunft verwendet werden, wenn erwartet werden kann, dass die Betroffenen sie verstehen oder wenn ihre Bedeutung dem Auskunftsschreiben zu entnehmen ist.

(4) Die Auskunft darf dadurch erteilt werden, dass dem Betroffenen ein Ausdruck seiner Daten (z. B. eine Bildschirmkopie) mit Erläuterungen übersandt wird. Eine mündliche Auskunftserteilung ist nur dann ausreichend, wenn der Betroffene damit einverstanden ist. Auskünfte über Telefon, Telefax oder E-Mail sind nur dann zulässig, wenn hiefür Sicherheitsvorkehrungen (Standleitungen, Rückruf, Verschlüsselungsverfahren, elektronische Signatur etc.) genützt werden.

(5) Das Auskunftsrecht umfasst Auskünfte aus Protokolldaten über Zugriffe auf Daten des Betroffenen, ebenso aus Datenverwendungen (Übermittlungen wie z. B. Auskünfte, Verarbeitungen), die von bzw. bei einem Dienstleister (z. B. dem Hauptverband nach § 31 Abs. 11 ASVG) erfolgten. Personenbezogene Daten Anderer (Benützerkennzeichen) oder Sicherheitsdaten der abfrageberechtigten Stellen (Passwörter etc.) dürfen bei Vorliegen überwiegender Interessen des Auftraggebers 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 des Betroffenen (Diagnosen, verrechnete Leistungen etc.) darf nicht unter Berufung auf ein Geheimhaltungsinteresse des Behandlers verweigert werden. Honorarbeträge gehören nicht zu den Behandlungsdaten.

(7) Ein Betroffener wirkt jedenfalls dann im Sinn des § 26 Abs. 3 DSG 2000 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 Betroffener sein kann und er bei umfangreichen Datenanwendungen auch den zeitlichen und inhaltlichen Zusammenhang der Verwendung seiner Daten nennt,
3. allenfalls durch die Vorlage von Unterlagen oder die Beschreibung von Lebensumständen glaubhaft macht, dass seine Daten irrtümlich oder missbräuchlich in Datenbeständen des Auftraggebers enthalten sind,
4. angibt, unter welchem Namen und Geburtsdaten (bzw. Namenschreibweisen) Daten über ihn aufgefunden werden könnten.

(8) Von der Bearbeitung eines Auskunftsersuchens ist abzusehen, wenn der Betroffene nicht am Verfahren mitwirkt. Auf diesen Umstand ist der Betroffene in einer Aufforderung zur Mitwirkung (Abs. 7, § 26 Abs. 4 DSG 2000) hinzuweisen.

(9) Auskünfte sind überdies nicht zu erteilen, wenn dies aus einem der in § 26 Abs. 2 DSG 2000 genannten weiteren Gründe unzulässig ist. Zu diesen Gründen zählen insbesondere jene Fälle der Datenübermittlung, in denen dem Betroffenen gegenüber (unbeschadet der ihm nach den maßgeblichen Verfahrensvorschriften zustehenden Rechte) nach Abwägung der Umstände des Einzelfalles wegen überwiegenden öffentlichen Interesses Daten geheim zu halten sind:

1. im Zuge eines gerichtlichen oder verwaltungsbehördlichen Strafverfahrens oder eines Disziplinarverfahrens sowie diesbezüglicher Vorerhebungen, solange das Verfahren noch nicht rechtskräftig abgeschlossen ist,
2. die Empfänger übermittelter Daten, sofern die Übermittlung für Zwecke eines gerichtlichen oder verwaltungsbehördlichen Strafverfahrens oder eines Disziplinarverfahrens durchgeführt wurde.

Pauschalierter Kostenersatz

§ 14. (1) Auskünfte nach § 26 DSG 2000 sind unentgeltlich zu erteilen, wenn sie den aktuellen Datenbestand einer Datenanwendung betreffen und wenn der Auskunftswerber im laufenden Kalenderjahr zum selben Aufgabengebiet noch kein Auskunftsersuchen an den Auftraggeber gestellt hat. In allen anderen Fällen kann ein pauschalierter Kostenersatz von 18,89 € verlangt werden. Ein höherer Kostenersatz darf nur dann verlangt werden, wenn tatsächlich höhere Kosten entstanden sind. Diese tatsächlichen Kosten sind an Hand der vollständigen Kosten der verbrauchten Arbeitszeit und konkreten Bezüge der hiefür eingesetzten Personen sowie des sonstigen Aufwandes (Material- und Sachaufwand etc.) zu errechnen (Vollkostenrechnung).

(2) Von der Einhebung eines Kostenersatzes ist abzusehen, wenn der Aufwand für die Vorschreibung und Einhebung des Kostenersatzes unverhältnismäßig höher liegen würde als der Aufwand für die Auskunftserteilung; hievon kann hinsichtlich aller von einem Auskunftsersuchen betroffenen Datenverarbeitungen oder einzelner dieser Datenverarbeitungen Gebrauch gemacht werden.

(3) Für die Beurteilung, ob ein Auskunftswerber im laufenden Kalenderjahr schon ein Auskunftsersuchen gestellt hat, ist das Eingangsdatum der Auskunftsersuchen beim Auftraggeber maßgebend.

(4) Unter aktuellen Daten im Sinn des Abs. 1 sind jene Daten zu verstehen, die zum Zeitpunkt der Antragstellung in den laufenden, automationsunterstützt oder manuell geführten Dateien des Auftraggebers unter einem Ordnungsmerkmal des Betroffenen gespeichert sind und auf die direkt zugegriffen werden kann.

Mitteilung des Kostenersatzes

§ 15. (1) Das Verlangen nach Kostenersatz ist dem Auskunftswerber unverzüglich nach Einlangen des – gegebenenfalls konkreter gefassten (§ 13 Abs. 7) – Auskunftsbegehrens mitzuteilen. Erfolgt diese Mitteilung schriftlich, ist auch eine Kontoverbindung anzugeben. Das Verlangen nach Bareinzahlung bei einer eigenen Stelle des Auftraggebers ist unzulässig.

(2) Von der Bearbeitung eines Auskunftsantrages ist abzusehen, wenn der nach Abs. 1 mitgeteilte Kostenersatz nicht entrichtet wurde.

Auskunftsfrist

§ 16. (1) Die in § 26 Abs. 4 DSG 2000 enthaltene Frist von 8 Wochen für die Erteilung von Auskünften beginnt bei unentgeltlich zu erfüllenden Auskunftsbegehren mit dem Einlangen des Auskunftsbegehrens beim Auftraggeber.

(2) Wurde ein Kostenersatz verlangt, so beginnt die Frist für die Auskunftserteilung mit Einlangen des Kostenersatzes bei der auskunftsverpflichteten Stelle (Auftraggeber bzw. Dienstleister, wenn dieser zur Auskunft verpflichtet ist).

(3) 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

§ 17. (1) § 26 DSG 2000 ist 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 des Betroffenen sowie außerhalb gesetzlicher oder vertraglicher Beziehungen (§ 42 ASVG, § 338 Abs. 4 ASVG u. a.) nach dem DSG 2000 und dieser Verordnung zu erteilen, soweit sich der Auskunftsberechtigte nicht ausdrücklich auf eine andere Rechtsgrundlage beruft (z. B. auf das Auskunftspflichtgesetz).

Richtigstellung oder Löschung

§ 18. (1) Eine logische Richtigstellung oder Löschung (§ 27 DSG 2000) von Daten hat durch solche Maßnahmen zu erfolgen, die bei einer Abfrage die Unrichtigkeit der verarbeiteten Daten angeben und auf die richtigen Daten verweisen oder den Umstand der Löschung anzeigen. Das Recht auf Richtigstellung oder Löschung umfasst keinesfalls ein Recht auf Veränderungen in Programmabläufen. Daten sind physisch zu löschen, ausgenommen die Löschung oder Richtigstellung von Daten kann auf ausschließlich automationsunterstützt lesbaren Datenträgern aus Gründen der Wirtschaftlichkeit nur zu bestimmten Zeitpunkten vorgenommen werden; in diesem Fall sind die zu löschenden Daten für den Zugriff zu sperren.

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

(3) Daten, die für Zwecke der Dokumentation (z. B. Versicherungszeiten, Meldungsdaten nach den §§ 33 ff ASVG) oder der internen Kontrolle aufbewahrt werden müssen, dürfen nur durch einen zweckentsprechenden Vermerk richtig gestellt werden. Solche Daten dürfen vor Ablauf der für sie geltenden Aufbewahrungsfrist nur dann physisch richtig gestellt oder gelöscht werden, wenn sie für ihre ursprünglichen Dokumentations- und Kontrollzwecke nicht mehr benötigt werden.

(4) Das Recht auf Richtigstellung betrifft nur solche Daten, deren Richtigkeit für den Zweck der Datenanwendung von Bedeutung ist; eine bloße Unvollständigkeit, die angesichts des Verwendungszwecks der Daten keine inhaltliche Änderung hervorrufen würde, bewirkt noch keinen Berichtigungsanspruch; insbesondere begründet ein Verlangen nach Ergänzung von Titeln oder akademischen Graden außerhalb der für die Führung dieser Bezeichnungen geltenden Rechtsvorschriften keinen Richtigstellungsanspruch.

(5) Der Beweis der Richtigkeit der Daten im Sinn des § 27 Abs. 2 DSG 2000 hat sich darauf zu beziehen, dass sie bei ihrer Ermittlung richtig waren oder ihre Richtigkeit (z. B. auf Grund einer unbestrittenen Dienstgebermeldung oder sonst unbedenklicher Urkunden) anzunehmen war. In solchen Fällen sind Richtigstellungen nur durch zusätzliche Anmerkungen, nicht jedoch durch Änderung der ursprünglichen Daten vorzunehmen.

(6) Mitteilungen und andere Erledigungen im Rahmen eines Richtigstellungs- oder Löschungsverfahrens sind keine Bescheide im Sinn des § 410 ASVG, auf die datenschutzrechtliche Grundlage ist im Text solcher Erledigungen ausdrücklich hinzuweisen.

(7) Ein Bestreitungsvermerk der Richtigkeit der Daten durch den Betroffenen ist nur dann beizufügen, wenn der Betroffene dies schriftlich verlangt hat.

Schlussbestimmung

§ 19. (1) Diese Verordnung tritt mit 1. Juni 2012 in Kraft.

(2) § 7 Abs. 5 Z 11 zweiter Satz über die Nichtverwendung bestimmter Datenträger für Übermittlungen und Überlassungen tritt abweichend von Abs. 1 erst am 31. Dezember 2012 in Kraft.

*

Diese Verordnung wurde vom Verbandsvorstand des Hauptverbandes der österreichischen Sozialversicherungsträger am 22. Mai 2012 beschlossen.

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

Für den Hauptverband der österreichischen Sozialversicherungsträger:

Schelling **Kandlhofer**

Signaturwert	AE6PfNYdtG3un61hT9ZSuJ5kyqEhbHXN2JyryesEu2CKbncRCtWOkusUtTlsHTSh iVI1 a5oGT9ViqTAM47cVRxbAuJfl8ThFiHj6R22TLK4j3uEiI28q5spPbbOueU/r QOZm/joo p4jcoXbqAO8L1badnspOypQxB+AUaLj0RXM	
	Unterzeichner	Michaela Gmoser, Dr. Hauptverband der österreichischen Sozialversicherungsträger ab 2008
	Datum/Zeit-UTC	2012-05-30T12:15:04Z
	Aussteller-Zertifikat	CN=a-sign-corporate-light-02, OU=a-sign-corporate-light-02, O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH, C=AT
	Serien-Nr	222039
	Methode	urn:dsig:RSAwithSHA1
Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: https://www.avsv.at/avi/signatur.html Da die technische Rückführung dieses Dokuments nicht möglich ist, wird gemäß § 20 E-GovG eine Verifizierung angeboten. Informationen zur Verifikation finden Sie unter https://www.avsv.at/avi/verifikation.html.	
Hinweis	Dieses Dokument wurde amtssigniert. Auch ein Ausdruck dieses Dokuments hat gemäß § 20 E-Government-Gesetz die Beweiskraft einer öffentlichen Urkunde.	

	**Unterzeichner**	Hauptverband der oesterreichischen SV-Traeger
	Datum/Zeit-UTC	2015-12-04T17:53:01+01:00
	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. Diese Kundmachung wurde mit der Übernahme ins RIS neuerlich elektronisch signiert, dies dient der Sicherheit der Kundmachung und wurde aus technischen Gründen vorgenommen. Diese neuerliche Signatur hat auf den Inhalt der Kundmachung keinen Einfluss, insbesondere hat das Datum der Signatur für das Inkrafttreten keine Bedeutung. An der Rechtsverbindlichkeit der früheren Kundmachung ändert sich dabei nichts.	