Datenschutzvereinbarung

- zur Umsetzung der österreichischen sowie europäischen Schutzbestimmungen für personenbezogene Daten (insbesondere der Datenschutzgrundverordnung (DSGVO[1]), des österreichischen Datenschutzgesetzes (DSG) sowie der Datenschutzverordnung der Sozialversicherung (SV-DSV)[2] in den jeweils geltenden Fassungen sowie
- zur Geheimhaltung von nicht personenbezogenen Informationen zwischen

IT-Services der Sozialversicherung GmbH Johann-Böhm-Platz 1 1020 Wien	Adresse
(im folgenden (wirtschaftlicher) Auftraggeber)	(im folgenden Auftragsverarbeiter)
Erreichbarkeit des Datenschutzbeauftragten (DS-B) des Auftraggebers[3]: E-Mail: dsb@itsv.at Tel: 050 124 844 3854	Erreichbarkeit des Datenschutzbeauftragten des Auftragsverarbeiters[4] E-Mail:_____ Tel.: _____
	Gegebenenfalls Vertreter nach Art. 27 Abs. 1 DS-GVO in der Union[5]: Name: _____ Organisation: _____ Telefon: _____ E-Mail: _____

Wird in diesem Dokument eine Person oder Personengruppe nur in einer Geschlechtsform angesprochen, so sind immer die weibliche und die männliche Form gemeint. Das geschieht ausschließlich zum Zweck der leichteren Lesbarkeit.

Die **zeitliche und inhaltliche Geltung** dieser Vereinbarung umfasst nicht nur alle Tätigkeiten, welche vom Auftragsverarbeiter (nach Art. 4 Z 8 DSGVO) im Zuge der unten beschriebenen Verarbeitungstätigkeiten durchgeführt werden, bis zu deren Abschluss, sondern auch gleichartige Aufträge, soweit diese nicht wesentlich von den nachfolgend beschriebenen Verarbeitungstätigkeiten abweichen. Werden im Rahmen eines zukünftigen (Leistungs)auftrags bzw. einer Zusammenarbeit neue datenschutzrechtliche Bestimmungen (bei einem Leistungsauftrag beispielsweise in den mitabgeschlossenen AGBs) vereinbart, gelten diese für Auftrag bzw. Zusammenarbeit vorrangig.

[1] VERORDNUNG (EU) 2016/679 (Datenschutz-Grundverordnung): http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=DE
[2] https://www.ris.bka.gv.at/Avsv/, avsv Nr. 79/2918, Erläuterungen dazu unter: www.sozdok.at
[3] Die Kontaktdaten des Datenschutzbeauftragten sind im Detail auf www.itsv.at im Impressum angeführt
[4] Siehe Punkt IV.4
[5] Hat der Auftragsverarbeiter seinen Sitz außerhalb der Union, benennt er einen Vertreter (Art. 27(1) DSGVO

Inhaltsverzeichnis

I. Informationen gemäß Art. 13f DSGVO

Diese Informationen dienen zur Kenntnisnahme des Auftragsverarbeiters und sind von diesem den von ihm für die Leistungserbringung eingesetzten Personen (z.B.: seinen Mitarbeitern) - soweit datenschutzrechtlich erforderlich – zur Kenntnis zu bringen:

Der Auftraggeber ist als Tochter der österreichischen Sozialversicherungsträger sowie dem Hauptverband der österreichischen Sozialversicherungsträger (als Inhouse-GmbH) nahezu ausschließlich für diesen Kundenkreis unmittelbar tätig. Der Auftraggeber wird im Rahmen dieser Auftragserteilung daher im Normalfall selbst als Auftragsverarbeiter (und nicht als Verantwortlicher) tätig. Bei der Dienstleistung des Auftragsverarbeiters handelt es sich gegenständlich daher meist um eine „Subauftragsverarbeitung“. Vielfach auch um eine Sub-Subauftragsverarbeitung für den Hauptverband der österreichischen Sozialversicherungsträger in seiner Funktion als Auftragsverarbeiter für die Sozialversicherungsträger im Rahmen seiner gesetzlich übertragenen Aufgaben oder anderer öffentlicher Stellen gem. § 30 (5) Datenschutzgesetz (DSG). Der Auftraggeber tritt nur dann unmittelbar in seiner datenschutzrechtlichen Rolle als „Verantwortlicher“ auf, wenn der Auftragsverarbeiter Daten seiner Mitarbeiter oder von (insbesondere Projekt-, Leistungsabrechnungsdaten) Dienstleistern und Lieferanten des Auftraggebers verarbeitet.

Der Auftraggeber nimmt in Vertretung der ihn beauftragenden Verantwortlichen deren datenschutzrechtliche Pflichten und Rechte war. Die Pflichten des Auftragsverarbeiters gemäß dieser Vereinbarung bzw. der DSGVO gelten als erfüllt, wenn diese dem Auftraggeber gegenüber erfüllt werden bzw. wurden. Die Verantwortlichen aus dem Kreis der Sozialversicherung können diese Pflichten aber auch unmittelbar gegenüber dem Auftragsverarbeiter – gegen Ersatz dadurch allfällig für den Auftragsverarbeiter entstehenden Mehrkosten - wahrnehmen.

Die Datenverarbeitungen der Sozialversicherung sind gemäß § 26 (1) Z 1 DSG dem öffentlichen Bereich zuzuordnen.

Verantwortlich für (allfällig im Rahmen der dieser Vereinbarung zugrundeliegenden wirtschaftlichen Vertragsbeziehung) verarbeitete personenbezogene Daten der vom Auftragsverarbeiter für die Leistungserbringung eingesetzten Personen, ist die IT-Services der Sozialversicherung GmbH - ITSV (Verantwortliche gem. DSGVO). Informationen nach Art. 13 und 14 Datenschutz-Grundverordnung betreffend die Verarbeitung der personenbezogenen Daten der vom Auftragsverarbeiter eingesetzten Personen finden sich im Impressum auf der Homepage des Auftraggebers unter www.itsv.at. Der Auftragsverarbeiter hat seine Dienstnehmer auf diese Informationen hinzuweisen, sowie ihnen mitzuteilen, dass deren Zugriffe auf Daten(speicher) des Auftraggebers mitprotokolliert werden.

Eine Übermittlung von personenbezogenen Daten kann innerhalb der österreichischen Sozialversicherung (Hauptverband der österreichischen Sozialversicherungsträger, Sozialversicherungsträger, Töchter der Sozialversicherungsträger) erfolgen, soweit dies für die Erfüllung des Auftrages erforderlich ist (z.B.: Kontaktdaten eines Mitarbeiters des Auftragsverarbeiters im Rahmen einer Projektabwicklung). Personenbezogene Daten des Auftragsverarbeiters bzw. der von

ihm mit der Leistung beauftragten Personen werden nur soweit erforderlich und ausschließlich für Zwecke der Erfüllung dieses Vertrages verarbeitet.

II. Auftragsgegenstand

Folgende **durchzuführende Arbeiten bzw. Verarbeitungstätigkeiten** (datenschutzrelevanter Auftragsgegenstand) werden durchgeführt:

1. Verweis auf den wirtschaftlichen Auftrag (z.B.: Bestellantragsnummer)[6].

   _____
   _____

2. Gegenstand der Vereinbarung:

In **Beiblatt** sind vom Auftragsverarbeiter gemeinsam mit Unterstützung des DS-B des Auftraggebers die dort angeführten Angaben zu machen. Ändern sich im Rahmen seiner Tätigkeit diese Angaben, hat er dies dem Datenschutzbeauftragen des Auftraggebers (an: dsb@itsv.at) unverzüglich mitzuteilen.

III. Tätigkeit in den Räumlichkeiten des Auftraggebers unter unmittelbarer Anweisung von Mitarbeitern des Auftraggebers (Maßstab gem. § 4 Arbeitskräfteüberlassungsgesetz - AÜG)

Dieser Punkt findet nur auf Verarbeitungstätigkeiten Anwendung, für welche implizit vereinbart wurde, dass die vom Auftragsverarbeiter zur Leistungserbringung eingesetzten Personen in den Räumlichkeiten und unter Nutzung der Strukturen des Auftraggebers unter seiner unmittelbaren Aufsicht tätig werden (insbes. Personalleasing).

Die nachfolgenden Bestimmungen werden unmittelbar vom Auftraggeber im Rahmen des Eingliederungsprozesses eines externen „Beschäftigten“ angestoßen.

Im Rahmen der Aufnahme wird den für die Arbeitsleistung zur Verfügung gestellten Personen mitgeteilt, welche Dienstanweisungen diese einzuhalten haben. Der Auftragsverarbeiter wird seine Mitarbeiter dazu anweisen, die vom Auftraggeber kommunizierten (Datenschutz- bzw. Sicherheits-)Bestimmungen sowie die allenfalls fallspezifisch ergänzend auferlegten Anweisungen (z.B.: Hausordnung) einzuhalten, sowie die ihm im Rahmen des Aufnahmeprozesses vorgelegte Datenschutz-Verpflichtungserklärung zu unterfertigen. In dieser ist insbesondere auch angeführt, dass der externe Dienstnehmer keine der Vertraulichkeit unterliegenden Informationen (personenbezogene Daten, Betriebsgeheimnisse über andere Projekte des Auftraggebers etc.) an den Auftragsverarbeiter weitergeben darf. Des Weiteren erfährt der externe Mitarbeiter auch, welche Personen seine unmittelbaren Datenschutz-Ansprechpartner sind.

Der Auftraggeber betreibt eine „kritische Infrastruktur“ für die österreichische Sozialversicherung (gem. NIS-Richtlinie der Europäischen Union). Er hat daher erhöhte Sicherheitsbestimmungen umzusetzen, wozu auch die Berücksichtigung der Eignung der eingesetzten Personen gehört. Der Auftragsverarbeiter verpflichtet die von ihm zur Auftragserbringung eingesetzten Personen, dass diese - ausschließlich nach konkreter Aufforderung durch den Auftraggeber - einen Strafregisterauszug (Leumundszeugnis) abzugeben haben. Führt dieser zu Sicherheitsbedenken, kann der Auftraggeber die Tätigkeit dieser Person ablehnen und der Auftragsverarbeiter hat binnen 2 Wochen eine andere geeignete Person für die Leistungserbringung zur Verfügung zu stellen. Diese Verpflichtung kann durch eine schriftliche Bestätigung des Auftragsverarbeiters ersetzt werden, dass gegen die von ihm für die Leistungserbringung eingesetzten Person keinerlei strafrechtlich relevanten Verurteilungen vorliegen (z.B.: Vermögensdelikt, Vertraulichkeitsverstöße oder andere IT-Delikte). Diese Bestätigung ist vom Auftragsverarbeiter vor Auftragsdurchführung abzugeben. Erweist sich diese Bestätigung nachträglich als falsch, haftet der Auftragsverarbeiter verschuldensunabhängig für sämtliche Schäden, die dem Auftraggeber daraus entstehen. Des Weiteren wird er eine nicht der richterlichen Mäßigung unterliegenden Konventionalstrafe in der Höhe von € 50.000,- an den Auftraggeber entrichten.

IV. Allgemein anwendbare Bestimmungen zur Verarbeitung von personenbezogenen Daten

1. Soweit die Verarbeitungstätigkeit die Erhebung von Daten von oder über Betroffene (iSd Datenschutzgrundverordnung) als Haupt- oder implizit als Nebenleitung beinhaltet, verantwortet

[6] Falls es keine Bestellung gibt (z.B. Zusammenarbeit im Rahmen einer entgeltfreien Kooperation oder der wirtschaftliche Vertrag wurde von einem der Auftraggeber der ITSV abgeschlossen) ist eine entsprechende Projekt-/Auftragsbezeichnung bzw. -beschreibung zur Identifikation des, dieser Datenschutzvereinbarung zugrundeliegenden, Vorhabens anzuführen.

der Auftragsverarbeiter die korrekte Information der Betroffenen gem. der Art. 13f und erfüllt die in der DSGVO vorgesehenen Belehrungspflichten (z.B. Widerspruchsrecht, Beschwerderecht bei der DSB). Die Information bzw. Belehrung hat nachweislich und schriftlich zu erfolgen und ist dem Auftraggeber spätestens nach Abschluss der Vertragsbeziehung zu übergeben. Soweit zum Nachweis dieser Verpflichtungen gem. der DSGVO auch ein allgemeiner Nachweis ausreicht, ist dieser auch rein elektronisch zulässig.

2. Ist der Auftragsverarbeiter nicht (bzw. nicht mehr) in der Europäischen Union niedergelassen, bestellt er einen verantwortlichen Ansprechpartner in der Europäischen Union gemäß Art. 27 DSGVO und teilt dessen Kontaktdaten und allfällige Aktualisierungen dem Auftraggeber mit.

3. Der Auftragsverarbeiter verpflichtet sich, Daten bzw. Verarbeitungsergebnisse ausschließlich im Rahmen der Aufträge des Auftraggebers zu verarbeiten oder nur nach dessen schriftlichem Auftrag zu übermitteln. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragsverarbeiters eines derartigen schriftlichen Auftrages. Sofern der Auftragsverarbeiter gesetzlich zu einer über die dokumentierte Weisung des Auftraggebers nach Art. 28 Abs. 3 lit. a DSGVO hinausgehenden Verarbeitung der Daten des Auftraggebers verpflichtet ist oder wird, ist der Auftraggeber darüber vor der Verarbeitung nachweislich zu informieren.

4. Der Auftragsverarbeiter hat – wenn er zur Bestellung eines Datenschutzbeauftragten verpflichtet ist, oder diesen freiwillig implementiert hat – die Kontakt-Mailadresse des Datenschutzbeauftragten im Kopfteil dieser Vereinbarung als Ansprechstelle für datenschutzrechtliche Themen nach dieser Vereinbarung einzutragen. Der Datenschutzbeauftragte ist gegenüber dem Auftraggeber rechtsgültig bevollmächtigt, als Ansprechpartner für die Ausübung der datenschutzrelevanten Rechte und Pflichten nach dieser Vereinbarung zu fungieren. Ein Wechsel ist dem Auftraggeber an dsb@itsv.at mitzuteilen.

5. Der Auftragsverarbeiter sichert ausdrücklich zu, dass eine Verarbeitung (z.B. insbesondere auch ein Remotezugriff) der Daten - ohne vorherige handschriftliche (oder mittels elektronischer Signatur) unterfertigte Zustimmung des Auftraggebers - ausschließlich auf dem österreichischen Hoheitsgebiet oder Vertragsstaaten des Europäischen Wirtschaftsraumes stattfinden darf. Liegt eine ausdrückliche Zustimmung vor, verantwortet der Auftragsverarbeiter die Sicherstellung der datenschutzrechtlichen Zulässigkeit der Übermittlung durch Umsetzung entsprechender Maßnahmen (z.B. Einholung der Genehmigung der Datenschutzbehörde). Gleiches gilt, wenn dies im Rahmen des Einsatzes von Subauftragsverarbeitern geschieht. Die ergriffenen Maßnahmen sind dem Auftraggeber nachweislich zumindest 3 Werktage vor entsprechender Aufnahme der Verarbeitung an dsb@itsv.at zur Kenntnis zu bringen.

6. Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Wahrung des Datengeheimnisses im Sinne der österreichischen sowie europäischen Datenschutzbestimmungen (insbes. Art. 28, 29, 32 DSGVO) verpflichtet hat, sofern diese nicht ohnedies einer angemessenen gesetzlichen Verschwiegenheitspflicht im Sinne von Art. 28 Abs. 3 lit. b DSGVO und § 6 DSG (2018) unterliegen. Insbesondere müssen diese verpflichtet werden, dass deren Verschwiegenheitsverpflichtung nicht nur gegenüber dem Auftragsverarbeiter selbst, sondern auch nach Beendigung ihrer Tätigkeit für den Auftraggeber und dem Ausscheiden beim Auftragsverarbeiter aufrecht bleibt.

7. Der Auftragsverarbeiter wird, soweit dies nicht im Rahmen des Auftrages ersichtlich ist (nicht erforderlich daher z.B. bei Dienstleistung im Rahmen von Punkt III), die Namen der Mitarbeiter des Auftragsverarbeiters zur Verfügung stellen, die befugt sind auf die Informationen des Auftraggebers zuzugreifen oder das Recht besitzen, diese zu erhalten (z.B. welche natürliche Person im Rahmen eines Wartungsvertrages einen Remote-Zugang hat). Wenn das nicht möglich ist (z.B.: Remotezugriff über allgemeine Zugriffspunkte), sind im Beiblatt (im Punkt technische und organisatorische Maßnahmen) allgemein die Bedingungen bekannt zu geben, unter denen Mitarbeitern des Auftragsverarbeiters Zugriffsbefugnisse erteilt und entzogen werden.

8. Der Auftragsverarbeiter ist verpflichtet bzw. verpflichtet seine Mitarbeiter dazu, bei einem dem Auftragsverarbeiter oder einem seiner Mitarbeiter bekannt gewordenen (den Auftraggeber direkt oder indirekt betreffenden) Sicherheitsvorfall ohne Verzögerungen (jedenfalls binnen 12 Stunden) den Datenschutzbeauftragten des Auftraggebers (an: dsb@itsv.at sowie sur@itsv.at) zu informieren. Auch begründete Verdachtsfälle sind unverzüglich mitzuteilen. Die Verständigung hat zumindest folgende Informationen zu enthalten:

a) Eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Gruppe und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze.

b) Den Namen und die Kontaktdaten des Datenschutzbeauftragten des Auftragsverarbeiters oder einer sonstigen Anlaufstelle für weitere Informationen.

c) Eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten.

d) Eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen (Art. 33 Abs. 2 und 3 DSGVO).

Der Auftragsverarbeiter verpflichtet sich, jeden Sicherheitsvorfall zu untersuchen und erforderlichenfalls gemeinsam mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten, sowie zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen zu ergreifen. Der Auftragsverarbeiter sichert in diesem Zusammenhang zu, den Auftraggeber bei Erfüllung der Pflichten nach Art. 33 und 34 DSGVO im erforderlichen Umfang zu unterstützen.

9. Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er in seinem Zuständigkeitsbereich durch, dem Stand der Technik entsprechende, technische und organisatorische Maßnahmen (zur Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme/Software) ein im Sinne des Art. 32 DSGVO angemessenes Schutzniveau für die Daten des Auftraggebers hergestellt hat. Er erklärt auch, dass er die Grundsätze für die Verarbeitung von personenbezogenen Daten gemäß Art. 5 DSGVO einhält. Personenbezogene Daten sind insbesondere vor auftragswidriger Veränderung, Vernichtung und Verlust sowie gegen unbefugte Verwendung und Weitergabe zu schützen. Ein angemessenes Schutzniveau berücksichtigt die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken (Risikoabwägung Art. 32, 35 DSGVO) und ermöglicht eine sofortige Feststellung von relevanten Verletzungsereignissen. Die ergriffenen Datensicherheitsmaßnahmen sind jährlich zu überprüfen und auf den jeweils aktuellen technischen Stand zu aktualisieren. Der Nachweis einer für die jeweilige Verarbeitungstätigkeit einschlägigen Zertifizierung reicht hierzu aus (z.B.: ISO-Zertifizierungen, siehe dazu Punkt 15). Die Dokumentation ist drei Jahre (ab dem Jahr in dem die Datenverarbeitung beendet wurde) aufzubewahren. Die Dokumentationspflicht kann auch durch Übergabe der Nachweise mit Vertragsbeendigung vorzeitig erfüllt werden. Die vom Auftragsverarbeiter getroffenen Maßnahmen sind allgemein in Beiblatt anzuführen.

   Der Auftragsverarbeiter unterstützt den Auftraggeber in diesem Zusammenhang bei der Erstellung von Datenschutz-Sicherheits- oder Folgenabschätzungen bzw. im Rahmen von vorherigen Konsultationen mit der Aufsichtsbehörde gem. den Art. 24, 32, 35 und 36 DSGVO.

10. Eine Sub-Beauftragung an weitere (Subauftrags-)verarbeiter bzw. deren Auswechselung - ohne vorherige handschriftliche (oder mittels elektronischer Signatur) unterfertigte Zustimmung des Auftraggebers - ist unzulässig. Soweit vom Auftragsverarbeiter allfällig bereits bestehende Sub-Auftragsverarbeiter im Beiblatt angeführt werden, gilt der Einsatz dieser Subauftragsverarbeiter - mit Unterfertigung dieses Vertrages durch den Auftraggeber - im Sinne dieses Punktes als genehmigt.

    Als Subauftragsverhältnisse im Sinne dieser Regelung sind nur solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen und im Rahmen der Sub-Dienstleistung Zugriffe auf personenbezogene Daten möglich (d.h. nicht ausgeschlossen) sind. Nicht hierzu gehören Nebenleistungen[7], welche nur mittelbaren Einfluss auf die Gesamtvertragsleistung beziehungsweise das gewünschte Ergebnis haben.

    Im Fall der ausdrücklichen Genehmigung eines Subauftragsverarbeiters, aber auch beim Heranziehen eines nur für Nebenleistungen beigezogenen Subauftragsverarbeiters, muss ein Vertrag zwischen dem Auftragsverarbeiter und dem Subauftragsverarbeiter geschlossen werden, in dem der Auftragsverarbeiter sicherzustellen hat, dass der Subauftragsverarbeiter – bezogen auf

[7] z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice, sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen

den Auftragsgegenstand - dieselben Verpflichtungen eingeht, die den Auftragsverarbeiter auf Grund dieser Vereinbarung treffen. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge (betreffend die darin enthaltenen Datenschutzbestimmungen) zwischen dem Auftragsverarbeiter und Sub-Auftragsverarbeiter. Der Auftragsverarbeiter haftet für die vom Sub-Auftragsverarbeiter verursachten Verstöße bzw. Schäden solidarisch mit diesem.

Die Annahme von personenbezogenen Daten durch den Auftragsverarbeiter bzw. die Gewährung eines Zugriffes auf personenbezogenen Daten des Auftraggebers an den Subauftragsverarbeiter sind erst nach Vorliegen der oben angeführten Voraussetzungen gestattet.

11. Der Auftragsverarbeiter trägt für die technischen und organisatorischen Voraussetzungen Vorsorge, dass der Auftraggeber die Bestimmungen der DSGVO hinsichtlich der Artikel 13 bis 15 (Informations- und Auskunftsrecht), und der Artikel 16,17 und 18 (Recht auf Berichtigung, Einschränkung sowie Löschung) gegenüber Betroffenen innerhalb der gesetzlichen Fristen jederzeit erfüllen kann, und überlässt dem Auftraggeber alle dafür notwendigen Informationen.

    Zusätzlich verpflichtet sich der Auftragsverarbeiter zur aktiven Unterstützung hinsichtlich der Erfüllung dieser Pflichten. Er ist nicht befugt die Rechte der Betroffenen ohne Auftrag des Auftraggebers selbst zu beantworten bzw. zu behandeln. Insbesondere auch Auskünfte an betroffene Personen, sowie an sonstige Dritte, darf der Auftragsverarbeiter nicht erteilen. Direkt an ihn gerichtete Anfragen bzw. Begehren, soweit diese Bezüge zur Auftragsverarbeitung aufweisen, wird er unverzüglich an den Auftraggeber (an dsb@itsv.at) weiterleiten.

    Zu den Verpflichtungen des Auftragsverarbeiters gehört es auch, Datenübermittlungen bzw. Zugriffe seiner Mitarbeiter (bzw. aller Erfüllungsgehilfen) auf Daten des Auftraggebers zu protokollieren, wenn er diese Daten auf seinen eigenen Anlagen verarbeitet. Die Protokollierung ist so zu gestalten, dass Zugriffe der eigenen Mitarbeiter bzw. Erfüllungsgehilfen des Auftragsverarbeiters samt Datum und Uhrzeit der Verarbeitung nachvollzogen werden können. Insbesondere sind daher Sammelzugriffsberechtigungen auf im Auftrag des Auftraggebers verarbeitete personenbezogene Daten (über die Zugriffe mehrerer Personen dokumentiert werden) unzulässig. Protokolle müssen vor Manipulation und unbefugtem Zugriff geschützt sein. Soweit eine andere Rechtsgrundlage keine anderen Aufbewahrungsfristen für Protokolle vorsieht, sind diese drei Jahre in automationsunterstützter (lesbarer) Form aufzubewahren. Danach sind die Protokolldaten zu löschen. Diese Bestimmung kann auch durch Übergabe der Protokolldaten im Rahmen der Auftragsbeendigung an den Auftraggeber erfüllt werden.

12. Für den Fall, dass Mitarbeitern des Auftragsverarbeiters durch den Auftraggeber Remotezugriffe auf Server oder Clients des Auftraggebers eingeräumt werden, hat der Auftragsverarbeiter einen Wechsel seiner Dienstnehmer dem Auftraggeber unverzüglich per E-Mail an dsb@itsv.at mitzuteilen, sodass die Zugriffsberechtigung von Seiten des Auftraggebers deaktiviert werden kann. Soweit der Auftragsverarbeiter selbst Zugriffsberechtigungen seiner Mitarbeiter auf Systeme des Auftraggebers verwaltet, hat er eine Aktualisierung der Berechtigungen selbst ohne Verzögerungen durchzuführen und auf Nachfrage des Auftraggebers dies auch nachzuweisen bzw. zu bestätigen. Zugriffsberechtigungen sind nur befristet einzuräumen und jedenfalls zu beenden, wenn sie zur weiteren Arbeit nicht mehr benötigt werden oder von den Berechtigten Verstößen gegen Datensicherheitsvorschriften gesetzt wurden.

    Der Auftragsverarbeiter hat seine Dienstnehmer darauf hinzuweisen, dass deren Zugriffe auf Daten(speicher) des Auftraggebers mitprotokolliert werden.

13. Für den Fall, dass der Auftragsverarbeiter an einem der Rechenzentrumsbetriebsstandorte des Auftraggebers tätig wird, hat der Auftragsverarbeiter vor dem Beginn der Tätigkeiten die Vertraulichkeitserklärung des Eigentümers bzw. Vermieters dieser Räumlichkeiten auf desen Verlangen zu unterfertigen. Eine solche Vertraulichkeitserklärung ist auch von den einzelnen am jeweiligen Rechenzentrumsstandort vom Auftragsverarbeiter eingesetzten Personen zu unterfertigen, wenn dies der jeweilige (vom Auftraggeber verschiedene) Rechenzentrumsstandortbetreiber verlangt.

14. Für den Fall, dass im Rahmen einer beauftragten Dienstleistung Datenträger des Auftraggebers repariert, instandgesetzt, erneuert bzw. ausgetauscht oder entsorgt werden, sind entsprechende technische und organisatorische Maßnahmen zur Sicherheit der auf den Datenträgern allenfalls noch gespeicherten Daten(spuren) zu treffen. Kann der Datenträger nicht repariert werden oder wird er nach Reparatur nicht an den Auftraggeber zurückgegeben, sind die Daten bzw. die Datenträger gemäß dem Standard ÖNORM S 2109-4 oder einem sicherheitstechnisch

gleichwertigem Standard bzw. Zertifizierung entweder so zu löschen, dass eine Wiederherstellung ausgeschlossen werden kann oder der Datenträger ist so zu entsorgen, dass die Daten unwiederbringlich zerstört werden.

15. Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm übermittelten Daten das Recht der Einsichtnahme und Kontrolle der Datenverarbeitungseinrichtungen des Auftragsverarbeiters eingeräumt. Der Auftragsverarbeiter verpflichtet sich, dem Auftraggeber – sowie allenfalls von diesem beauftragten Dritten – jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind. Hierzu gehört insbesondere auch die Berechtigung in Protokolle gemäß Punkt IV.11 und andere – die Daten des Auftraggebers betreffende – (Sicherheits-)Dokumentationen Einsicht zu nehmen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.

    Der Nachweis allgemeiner Sicherheitsmaßnahmen (nicht jedoch von konkreten Maßnahmen, wie beispielsweise die Einsicht in Protokollauszüge) kann auch erfolgen durch

    - die nachgewiesene Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
    - die aufrechte Zertifizierung nach einem genehmigten Zertifizierungsverfahren gem. Art. 42 DS-GVO;
    - aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, externe Datenschutzauditoren, Qualitätsauditoren);
    - eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudits (z.B. nach BSI-Grundschutz, ISO 27001).

    Soweit hierzu nachweislich

    - ein Auftrag einer Aufsichtsbehörde, welcher der Auftraggeber unterliegt (z.B. Datenschutzbehörde, Rechnungshof, Bundesministerium) oder
    - eines Gesellschafters des Auftraggebers (Hauptverband der österr. Sozialversicherungsträger oder Sozialversicherungsträger) oder
    - ein konkreter Verdachtsmoment auf einen Verstoß gegen eine die konkrete Auftragsverarbeitung berührende Sicherheitsbestimmung bzw. -vorkehrung vorliegt,

    kann (eingeschränkt auf die konkrete Auftragsverarbeitung) unabhängig vom Vorliegen einer der oben angeführten Nachweise vom Auftraggeber auch eine konkrete Prüfung der vom Auftragsverarbeiter gesetzten technischen und organisatorischen Maßnahmen erfolgen.

    Derartige Kontrollen beim Auftragsverarbeiter haben tunlichst ohne vermeidbare Störungen des Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung (zumindest eine Woche) und zu Geschäftszeiten des Auftragsverarbeiters statt. Auf Wunsch und Kosten des Auftragsverarbeiters kann dieser verlangen, dass die Überprüfung von einem neutralen Dritten, auf den sich die Parteien einvernehmlich einigen, durchgeführt wird.

    Für die anlassbezogene Durchführung von Kontrollen bzw. Stichproben durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch für seine eigenen Personalaufwendungen geltend machen, der in seiner Höhe mit dem konkreten, anlassbezogenen Kontrollaufwand beschränkt ist. Die grundsätzliche Etablierung von Maßnahmen, die eine Kontrolle erst ermöglichen bzw. in Umsetzung der Verpflichtungen des Auftragsverarbeiters nach der DSGVO erfolgen, wird dagegen nicht eigens entgolten.

16. Der Auftraggeber ist unverzüglich über Kontrollhandlungen und Maßnahmen der Datenschutzbehörde oder einer anderen Behörde zu informieren, soweit der Auftraggeber direkt oder indirekt betroffen ist. Dies gilt insbesondere auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten beim Auftragsverarbeiter ermittelt.

17. Soweit der Auftraggeber seinerseits einer Kontrolle durch eine (Datenschutz)behörde, den Rechnungshof, ein Verwaltungs- oder Strafverfahren, den (Haftungs)anspruch einer betroffenen Person oder eines Dritten oder einen anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragsverarbeiter ausgesetzt ist, hat dieser ihn nach besten Kräften zu unterstützen.

18. Kopien der Software oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung im Rahmen des Auftrages erforderlich sind.
19. Der Auftragsverarbeiter hat für die Vernichtung unbrauchbarer oder nicht mehr benötigter Ausdrucke und sonstiger Datenträger nach dem jeweiligen Stand der Technik Sorge zu tragen.
20. Der Auftragsverarbeiter ist nach Beendigung der Dienstleistung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, unabhängig davon, ob diese personenbezogene Daten enthalten oder nicht (inkl. die die Verarbeitungen des Auftraggebers betreffende Protokolldaten), ausschließlich dem Auftraggeber zu übergeben bzw. in dessen Auftrag für ihn weiter vor unbefugter Einsicht gesichert aufzubewahren. Der Auftragsverarbeiter darf die Daten nicht eigenmächtig, sondern nur nach dokumentierter schriftlicher Auftragserteilung durch den Auftraggeber (oder einer zuständigen Behörde) berichtigen, löschen oder deren Verarbeitung einschränken.

V. Geheimhaltung nicht personenbezogener Informationen

Darüber hinaus hat der Auftragsverarbeiter auch sonstige Umstände und Informationen, die ihm im Rahmen der Abwicklung bekannt werden, geheim zu halten und nicht an Dritte weiterzugeben. Diese Pflicht ist auch seinen Mitarbeitern und allfälligen Subauftragsverarbeitern zu überbinden und gilt auch – soweit die Informationsweitergabe nicht für die unmittelbare Auftragserfüllung erforderlich ist – im Verhältnis der Mitarbeiter gegenüber den eigenen Arbeitgebern bzw. dem Auftragsverarbeiter selbst. Sämtliche Informationen dürfen nur für, von dieser Vereinbarung umfasste Zwecke, verarbeitet werden. Die Weitergabe von Informationen an Dritte sowie die Veröffentlichung dieser Informationen ist unzulässig. Diese Informationen sind als Geschäfts- und Betriebsgeheimnisse des Auftraggebers zu behandeln.

VI. Außerordentliche Kündigung

1. Der Auftraggeber kann Verträge mit dem Auftragsverarbeiter jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn in Bezug auf den oben in Punkt I.1 referenzierten Vertrag ein schwerwiegender Verstoß des Auftragsverarbeiters oder dessen Sub-Auftragsverarbeiter gegen Datenschutzvorschriften oder die Bestimmungen dieses Datenschutzvertrages vorliegt oder der Auftragsverarbeiter bzw. dessen Sub-Auftragsverarbeiter Kontrollrechte des Auftraggebers vertragswidrig verweigert. Dieses Kündigungsrecht bezieht sich nicht nur auf diese Datenschutzvereinbarung sondern auch auf allfällig dieser Vereinbarung zugrundeliegende wirtschaftliche Auftragsverträge/-beziehungen.
2. Ein schwerwiegender Verstoß liegt insbesondere dann vor, wenn der Auftragsverarbeiter im Falle einer Auftragsverarbeitung gemäß Punkt III keine geeigneten Personen nominiert bzw. nicht in der erforderlichen Zeit nachnominiert.
3. Ein schwerwiegender Verstoß liegt insbesondere auch dann vor, wenn der Auftragsverarbeiter oder dessen Sub-Auftragsverarbeiter, die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen, in erheblichem Maße nicht erfüllen oder nicht erfüllt haben. Im Zweifelsfall ist vom Vorliegen eines bloß „sonstigen Verstoßes“ auszugehen.
4. Bei sonstigen Verstößen gegen diesen Datenschutzvertrag setzt der Auftraggeber dem Auftragsverarbeiter eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung im Sinne von Abs. 1 berechtigt.
5. Der Auftragsverarbeiter hat dem Auftraggeber alle Kosten zu erstatten, die diesem durch die vorzeitige Beendigung dieses Datenschutzvertrages bzw. dem diesem Vertrag zugrundeliegenden wirtschaftlichen Auftragsvertrag in Folge der berechtigten Wahrnehmung dieses Sonderkündigungsrechts entstehen.

VII. Sonstige Bestimmungen und Informationen

1. Die Geheimhaltungspflicht wird durch das Ende des Vertragsverhältnisses nicht berührt und bleibt zeitlich unbegrenzt aufrecht.
2. Die in diesem Vertrag verwendeten Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung (DSGVO) zu verstehen. Die Bestimmungen dieser Vereinbarung sind von Auftraggeber und Auftragsverarbeiter im Sinne der Entscheidungen des Europäischen Gerichtshofes (EuGH), der Europäischen Kommission (EK), der Datenschutzbehörde (DSB) oder

des Datenschutzrates (DSR) zu interpretieren. Wenn rechtlich erforderlich, sind Änderungen der rahmenrechtlichen Grundlagen (DSGVO, DSG) durch einvernehmliche Anpassung dieser Vereinbarung zu vollziehen. Dadurch auftretende Aufwände sind durch den jeweils zuständigen Rolleninhaber (Auftragsverarbeiter oder Verantwortlichen/Auftraggeber) zu tragen.

Für die Geschäftsführung der IT-Services der Sozialversicherung GmbH (Auftraggeber)	Für den Auftragsverarbeiter
Wien, am _____	_____, am _____

VIII. BEIBLATT

Die Punkte a-c sind vom Auftraggeber, die Punkte d – f vom Auftragsverarbeiter auszufüllen. In Punkt d sind vom

a. Verarbeitete Datenkategorien und Datenherkunft (§ 13 (2) Z 4 SV-DSV):

Datenkategorien	
allgemeine technische Kommunikations- und Diensteabwicklungsdaten (z.B.: IP-Adresse, e-Mailadresse) ohne weitere ergänzende personenbezogene Informationen.	
Identitätsdaten (wie Namen, akad. Grade, Geburtsdaten, Geburtsort, Sterbedatum, Geschlecht, Familienstand, Staatsbürgerschaft, etc.).	
Organisations-/Unternehmensdaten (wie Sitz, Betriebsort, Rechtsform, Geschäftszweig, Fachsektionen, Wirtschaftsklassen, Berufsgruppen, Gründungs- und Auflösungsdaten, Scheinunternehmensdaten, Kammermitgliedschaften, etc.).	
Erreichbarkeitsdaten (wie Adressen, inkl. Abgabestellen, elektr. Postfächer, Tel.Nr., Mail-Adressen, IP-Adressen, Fax-Nr., etc.).	
arbeitsrechtliche Personalverwaltungsdaten (wie Tätigkeitsbereiche, Funktionsumfang, Ausbildung, Dienst-/Versicherungszeiten, Berechnungs-/Beitragsgrundlagen, etwaiger Behindertenstatus, Bezüge, Kurienzugehörigkeit, Gewerkschaftszugehörigkeit bei Direktverrechnung, Mitarbeitervorsorge- und Pensionskassendaten, zuständiger Sozialversicherungsträger, Bewerberdaten etc.).	
Abrechnungsdaten (wie Bankdaten, Geldadress- & Abbuchungsvereinbarungen, Zeichnungsberechtigungen, Beitragskontonummern, Insolvenzdaten, Leistungsabrechnungen, Honorare, Tarife).	
Angehörigen- & Vertretungs-(Vollmachts-) & Partnerbeziehungen (wie Erwachsenenvertreter, Kuratoren, Konzerne, Pächter, Erben, Gesellschafter, etc.	
Personenkennzeichen (wie SVNR, EKVK-Nummer, UID-, Steuer-, Kammer-, Firmenbuch-, LKF-Code, Steuernummer, bPK, in- und ausländische Betreuungsnummern, etc.).	
Meldende Stellen.	
Regressdaten (z.B. Angaben zu Schädiger, Schaden, Schadenshöhe, zuständige Haftpflicht-Versicherung, etc.).	
Vertragsdaten (z.B. Zeitraum, Fachgebiet, Befähigungen, Angebote, Nachlässe etc.).	
Patientendaten (z. B. behandelnde Einrichtung, Sterbedaten (diese sind oben unter Identifikationsdaten enthalten), Anamnesedaten, Gesundheitszustand, Indikation, etc.).	

Datenherkunft?	
aus bestehenden Systemen des Auftraggebers/Verantwortlichen?	
aus bestehenden Systemen des Auftragsverarbeiters?	
aktive Erhebung von personenbezogenen Daten des Betroffenen? Falls ja: Wurde der Betroffene gem. Art. 13f belehrt (Erhebungsformular)?	
vom Betroffenen bekannt gegeben (z.B. im Rahmen eines Antrages; einer Bewerbung)?	
Sonstiges:	

b. Verarbeitete Kategorien betroffener Personen (§ 13 (2) Z 4 SV-DSV):

A	Angaben über Bewerber, Dienstnehmer und Funktionsträger (Verwaltungskörper und Beiräte), Sitzungsteilnehmer der Aufsichtsbehörden bzw. des Bundesministeriums für Finanzen (Personaldaten)	
B	Mitarbeiter/Kontaktpersonen der Kunden oder Lieferanten des Auftragsverarbeiters (Empfänger und Erbringer von Lieferungen oder Leistungen)	
C	Versicherte, Leistungsempfänger	

D	Dienstgeber, Vertreter	
E	Patienten	

c. Zweck der Datenverarbeitung

Kundenverwaltung, Rechnungswesen, Logistik, Buchführung, Projektmanagement.	
Personalverwaltungsdaten: Angaben über Dienstnehmer und Funktionsträger (Verwaltungskörper und Beiräte), Sitzungsteilnehmer der Aufsichtsbehörden bzw. des Bundesministeriums für Finanzen.	
Stationäre Bildverarbeitung und die damit verbundene Akustikverarbeitung zu Überwachungszwecken (Videoüberwachung).	
Zugriffsverwaltung für EDV-Systeme sowie Zutrittsberechtigungen in die Räumlichkeiten des Auftraggebers.	
Allenfalls zusätzlich für Sozialversicherungsverarbeitungen:	
Verwaltung von Angaben über das Bestehen einer Versicherung (Versicherungsdaten).	
Verwaltung von Angaben über die Erbringung von Leistungen (Leistungsdaten).	
Mitwirkung im Gesundheitsbereich (Gesundheitsversorgungsdaten).	

d. Kategorien von Verarbeitungen, die von (Sub-)Auftragsverarbeitern durchgeführt werden

Verarbeitungstätigkeit		Name und Kontaktdaten des AV	Datenschutzbeauftragter (Mail/Tel)	AGB-DSGVO? Art. 28 DSGVO[i]?[8] **GZ/Datum:**
Rechenzentrums-Betriebstätigkeiten				
Netzwerk-Betriebstätigkeiten				
Softwareentwicklung				
Softwarewartung				
technische Servicedeskleistungen				
Call-Center Leistungen				
Erhebung von Daten von oder über Betroffene				

e. Datenübermittlungen an ein Drittland/eine internationale Organisation?

(z.B.: Remotezugang oder Hotline/Service-Desk im Drittland)

Ja		Nein	

FALLS JA: WOHIN/AN WEN?
AUF WELCHER RECHTLICHEN BASIS WIRD DIE ÜBERMITTLUNG VORGENOMMEN UND WELCHE ENTSPRECHEND GEEIGNETEN GARANTIEN LIEGEN VOR (ART. 45-49 DSGVO)?

[8] gem. § 4 SV-DSV nicht innerhalb der SV erforderlich; § 11 (10) SV-DSV :

f. Allgemeine Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen (TOMs) des Auftragsverarbeiters

Die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO wird nachgewiesen: Welche:	
Eine Zertifizierung nach einem genehmigten Zertifizierungsverfahren gem. Art. 42 DS-GVO liegt vor. Welche:	
Aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen nach gängigen Standards liegen vor (z.B. Wirtschaftsprüfer, externe Datenschutzauditoren, Qualitätsauditoren) Welche:	
Eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudits (z.B. nach BSI-Grundschutz, ISO 27001) liegt vor. Welche:	
Link auf WebSite mit Aufschlüsselung getroffener Sicherheitsmaßnahmen: LINK:	
Falls keiner der oben angeführten allgemeinen Nachweise vorliegt sind die nachfolgenden Fragen auszufüllen:	

1. Zutrittskontrolle (physisch)

Es ist sicherzustellen, dass unberechtigten Personen der Zutritt zu den IKT-Einrichtungen verwehrt ist, in denen personenbezogene Daten verarbeitet und genutzt werden. d.h. der physische Zutritt zu den IKT-Einrichtungen ist zu regeln.

Die folgenden technischen und organisatorischen Maßnahmen sind für die im Grundvertrag vereinbarte Erfassung, Verarbeitung und Nutzung von personenbezogenen Daten durch den Auftragsverarbeiter zu implementieren:

Nr.	JA	NEIN	nicht notwendig	Mindest-Sicherheitsniveau erfüllt durch: (ACHTUNG: Wenn „NEIN“ und „nicht notwendig“ ausgefüllt wird, ist eine Begründung anzugeben.)
1.1	☐	☐	☐	Maßnahmen für eine Alarmierung in kritischen Bereichen sind vorhanden
	Begründung:			
1.2	☐	☐	☐	Maßnahmen für manuelle Schließanlage mit Regelungen für die Schlüsselverwaltung (Schlüsselregistrierung, Schlüsselverteilungssystem) sind vorhanden
	Begründung:			
1.3	☐	☐	☐	Maßnahmen für Besucherregistrierung sind vorhanden
	Begründung:			
1.4	☐	☐	☐	Maßnahmen für ein elektronische Schließsystem mit Chipkarte/Transponder sind für sensible Bereiche vorhanden
	Begründung:			

1.5	☐	☐	☐	Maßnahmen für die Sorgfältige Auswahl und Unterweisung der Reinigungskräfte, Haustechnikkräfte, … sind vorhanden
	Begründung:			

2. Zugangskontrolle (logisch)

Jede Verwendung von Datenverarbeitungssystemen durch unbefugte Personen ist zu verhindern, d.h. der logische Zugang zu diesen IKT-Systemen ist zu regeln.

Die folgenden technischen und organisatorischen Maßnahmen sind für die vertragliche Erfassung, Verarbeitung und Nutzung von persönlichen Daten durch den Auftragsverarbeiter zu implementieren:

Nr.	JA	NEIN	nicht not-wendig	Mindest-Sicherheitsniveau erfüllt durch: (ACHTUNG: Wenn „NEIN“ und „nicht notwendig“ ausgefüllt wird, ist eine Begründung anzugeben.)
2.1	☐	☐	☐	Maßnahmen für die Authentifizierung mit Benutzername / Passwort (Passwortvergabe basiert auf gültigen Passwortregelungen) sind vorhanden
	Begründung:			
2.2	☐	☐	☐	Maßnahmen für die Verwendung von aktueller Antiviren-Software sind vorhanden
	Begründung:			
2.3	☐	☐	☐	Maßnahmen für die Verwendung einer aktuellen Firewall-Version am Perimeter oder/und zwischen anderen Netzwerken sind vorhanden (Regelsatz: es ist alles verboten, was nicht erlaubt ist)
	Begründung:			
2.4	☐	☐	☐	Maßnahmen zum Erstellen von Benutzerprofilen sind vorhanden
	Begründung:			
2.5	☐	☐	☐	Maßnahmen für die Verschlüsselung von mobilen Datenträgern sind vorhanden
	Begründung:			
2.6	☐	☐	☐	Maßnahmen für die Verschlüsselung von Datenträgern in Laptops / Notebooks sind vorhanden
	Begründung:			
2.7	☐	☐	☐	Maßnahmen für eine zentrale Smartphone-Verwaltungssoftware (z.B. für externes Löschen von Daten) sind vorhanden
	Begründung:			

3. Zugriffskontrolle

Es ist sicherzustellen, dass die zur Nutzung eines Datenverarbeitungssystems befugte Person nur auf die Informationen in ihrem jeweiligen Zugriffsbereich zugreifen kann und dass keine personenbezogenen Daten ohne entsprechende Berechtigung während der Verarbeitung oder Nutzung sowie nach der Speicherung gelesen, kopiert, geändert oder entfernt werden können; d.h. Berechtigungssysteme und Informationssicherheitsmaßnahmen sind zu entwickeln.

Die folgenden technischen und organisatorischen Maßnahmen sind für die vertragliche Erfassung, Verarbeitung und Nutzung von persönlichen Daten durch den Auftragsverarbeiter zu implementieren:

Nr.	JA	NEIN	nicht not-wendig	Mindest-Sicherheitsniveau erfüllt durch: (ACHTUNG: Wenn „NEIN“ und „nicht notwendig“ ausgefüllt wird, ist eine Begründung anzugeben.)
3.1	☐	☐	☐	Maßnahmen für den Einsatz von Rollen und Berechtigungen nach dem "Need-to-know-Grundsatz" sind vorhanden
	Begründung:			
3.2	☐	☐	☐	Maßnahmen zur Minimierung der Anzahl der Administratoren (beschränkt sich auf das "absolut notwendige Minimum") sind vorhanden
	Begründung:			
3.3	☐	☐	☐	Maßnahmen zur Protokollierung der Zugriffe auf Anwendungen, Eingabe, Änderung und Löschen von Daten sind vorhanden
	Begründung:			
3.4	☐	☐	☐	Maßnahmen zum sicheren Löschen von Datenträgern vor ihrer neuerlichen Verwendung sind vorhanden
	Begründung:			
3.5	☐	☐	☐	Maßnahmen zur Physischen Vernichtung (z.B.: nach DIN 66399) oder Beauftragung eines entsprechenden Dienstleisters sind vorhanden
	Begründung:			
3.6	☐	☐	☐	Maßnahmen zur Verwaltung von Rechten durch vorgegebene Systemadministratoren oder/und einen Identitätsmanagement-System über einen definierten Prozess sind vorhanden
	Begründung:			
3.7	☐	☐	☐	Maßnahmen für eine Passwort-Richtlinie, die die Komplexität, die Länge sowie die Gültigkeitsdauer des Passworts bzw. die Authentifizierung über 2 Faktor und/oder biometrische Methoden definiert, sind vorhanden
	Begründung:			
3.8	☐	☐	☐	Maßnahmen zur sicheren Aufbewahrung (verschließbare Schränke und Schubladen, Datensafe, …) von Datenträgern nach der Kritikalität der gespeicherten Daten sind vorhanden

	Begründung:			
3.9	☐	☐	☐	Maßnahmen zur Speicherung der Daten an einem sicheren Ort entsprechend der Klassifizierung der Daten und/oder deren Verschlüsselung sind vorhanden
	Begründung:			

4. Überlassungskontrolle

Es ist sicherzustellen, dass keine personenbezogenen Daten während der elektronischen Übermittlung oder der Speicherung auf Datenträger von unbefugten Personen gelesen, kopiert, geändert oder entfernt werden können, und dass überprüft und festgelegt werden kann, wohin personenbezogene Daten zu übermittelt sind, d.h. die Modalität der Datenübermittlung ist zu regeln.

Die folgenden technischen und organisatorischen Maßnahmen sind für die vertragliche Erfassung, Verarbeitung und Nutzung von persönlichen Daten durch den Auftragsverarbeiter zu implementieren:

Nr.	JA	NEIN	nicht not-wendig	Mindest-Sicherheitsniveau erfüllt durch: (ACHTUNG: Wenn „NEIN“ und „nicht notwendig“ ausgefüllt wird, ist eine Begründung anzugeben.)
4.1	☐	☐	☐	Maßnahmen für die Verschlüsselung bei Datenübertragung im Internet oder Netzwerken, die sich nicht in der alleinigen Verfügungshoheit befinden (z.B. TLS, …) mittels sicherer kryptographischer Verfahren (lt. Stand der Technik) sind vorhanden
	Begründung:			
4.2	☐	☐	☐	Maßnahmen zur halb- oder vollautomatischen Identifikation der Datenempfänger, zur halb- oder vollautomatischen Überprüfung der Zeiträume der geplanten Übermittlungen und zur Umsetzung der halb- oder vollautomatischen vereinbarten Löschfristen sind vorhanden
	Begründung:			

5. Eingabekontrolle

Es ist sicherzustellen, dass im Nachhinein geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in die Datenverarbeitungssysteme eingegeben, geändert oder entfernt wurden (z.B. durch das Führen von Aufzeichnungen).

Die folgenden technischen und organisatorischen Maßnahmen sind vertraglich für die Erfassung, Verarbeitung und Nutzung von persönlichen Daten durch den Auftragsverarbeiter zu implementieren:

Nr.	JA	NEIN	nicht not-wendig	Mindest-Sicherheitsniveau erfüllt durch: (ACHTUNG: Wenn „NEIN“ und „nicht notwendig“ ausgefüllt wird, ist eine Begründung anzugeben.)
5.1	☐	☐	☐	Maßnahmen zur Protokollierung von Eingaben, Änderungen oder Löschen von Daten sind vorhanden
	Begründung:			

5.2	☐	☐	☐	Maßnahmen zur Nachverfolgbarkeit von Eingaben, Änderungen oder Löschen von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) sind vorhanden
	Begründung:			
5.3	☐	☐	☐	Maßnahmen zur Vergabe von Rechten für das Eingeben, Ändern oder Löschen von Daten auf der Grundlage eines Berechtigungskonzepts sind vorhanden
	Begründung:			
5.4	☐	☐	☐	Maßnahmen für das Führen einer Übersichtsliste, unter Angabe mit welchen Applikationen welche Daten eingegeben, geändert oder gelöscht werden können, sind vorhanden
	Begründung:			

6. Verfügbarkeitskontrolle

Es ist sicherzustellen, dass personenbezogene Daten vor unabsichtlicher Zerstörung oder Verlust geschützt werden.

Die folgenden technischen und organisatorischen Maßnahmen sind für die vertragliche Erfassung, Verarbeitung und Nutzung von persönlichen Daten durch den Auftragsverarbeiter zu implementieren:

Nr.	JA	NEIN	nicht not-wendig	Mindest-Sicherheitsniveau erfüllt durch: (ACHTUNG: Wenn „NEIN“ und „nicht notwendig“ ausgefüllt wird, ist eine Begründung anzugeben.)
6.1	☐	☐	☐	Maßnahmen für die Klimatisierung in Serverräumen sind vorhanden
	Begründung:			
6.2	☐	☐	☐	Maßnahmen für Geräte zur Überwachung der Temperatur, Luftfeuchtigkeit oder anderer Messwerte in Serverräumen sind vorhanden
	Begründung:			
6.3	☐	☐	☐	Maßnahmen für den vorbeugenden Brandschutz (Brandmeldeanlage) in Serverräumen sind vorhanden
	Begründung:			
6.4	☐	☐	☐	Maßnahmen für geeignete Feuerlöscher oder Löschanlage in Serverräumen sind vorhanden
	Begründung:			
6.5	☐	☐	☐	Maßnahmen für ein Sicherungs- und Wiederherstellungskonzeptes sind vorhanden
	Begründung:			

6.6	☐	☐	☐	Maßnahmen für die Überprüfung der Wiederherstellung der Daten in der definierten Zeit sind vorhanden
	Begründung:			
6.7	☐	☐	☐	geeignete organisatorische Maßnahmen für ein PATCH-Management sind vorhanden
	Begründung:			
6.8	☐	☐	☐	Maßnahmen für die Speicherung der gesicherten Daten in einem anderen Brandabschnitt oder an einem sicheren, externen Ort
	Begründung:			
6.9	☐	☐	☐	Maßnahmen zum Schutz von Serverräume in Hochwassergebieten sind vorhanden
	Begründung:			

7. Separierungsregel

Es ist sicherzustellen, dass die für verschiedene Zwecke gesammelten unterschiedlichen Daten getrennt verarbeitet werden, d.h. wenn der Grund zur Datenverarbeitung nicht mehr besteht, können und müssen die entsprechenden Daten auch gelöscht werden.

Die folgenden technischen und organisatorischen Maßnahmen sind für die vertragliche Erfassung, Verarbeitung und Nutzung von persönlichen Daten durch den Auftragsverarbeiter zu implementieren:

Nr.	JA	NEIN	nicht notwendig	Mindest-Sicherheitsniveau erfüllt durch: (ACHTUNG: Wenn „NEIN“ und „nicht notwendig“ ausgefüllt wird, ist eine Begründung anzugeben.)
7.1	☐	☐	☐	Maßnahmen für die Festlegung der Datenbankrechte sind vorhanden
	Begründung:			
7.2	☐	☐	☐	Maßnahmen für die Trennung der Zugriffsrechte auf verschiedene Mandanten sind vorhanden
	Begründung:			
7.3	☐	☐	☐	Maßnahmen für die Trennung von Produktiv-, Qualität- und/oder Test-System sind vorhanden
	Begründung:			

8. Notfallmanagement

Es ist sicherzustellen, dass für die auftretenden Datenschutzverletzungen geeignete Managementprozesse vorhanden sind.

Die folgenden technischen und organisatorischen Maßnahmen sind für die vertragliche Erfassung, Verarbeitung und Nutzung von persönlichen Daten durch den Auftragsverarbeiter zu implementieren:

Nr.	JA	NEIN	nicht notwendig	Mindest-Sicherheitsniveau erfüllt durch: (ACHTUNG: Wenn „NEIN“ und „nicht notwendig“ ausgefüllt wird, ist eine Begründung anzugeben.)
8.1	☐	☐	☐	Maßnahmen zur Erkennung, Bewertung und Behebung von Datenschutzverletzungen sind vorhanden
	Begründung:			
8.2	☐	☐	☐	Maßnahmen für die Überprüfung (z.B.: Audit, Simulation, …) des Notfall-Prozess sind vorhanden
	Begründung:			

Nur für den internen Gebrauch (DS-Applikationsbeschreibung)

(dient als Teil der internen Dokumentation nicht der Weiterleitung an den Auftragsverarbeiter)

A) Verantwortliche bzw. Auftraggeber, für die die Verarbeitung aktuell oder zukünftig voraussichtlich durchgeführt wird (Zwecks Erfassung der Verantwortlichen in der Vertragsverwaltung der ITSV)[9]

Die jeweiligen Datenschutzbeauftragten der Verantwortlichen sind erreichbar über deren Homepage sowie unmittelbar per E-Mail unter dsb@*Trägerkürzel*.at (z.B.: dsb@wgkk.at)	
Verantwortliche/r	(ankreuzen)
Hauptverband der österreichischen Sozialversicherungsträger und alle Sozialversicherungsträger	
alle KV-Träger (Sparte)	
alle Unfallversicherungsträger (Sparte)	
IT-Services der Sozialversicherung GmbH Johann Böhm Platz 1 1020 Wien E-Mail: office@itsv.at Telefon: 050124-	
Hauptverband der österreichischen Sozialversicherungsträger Ergänzungsregister-Nummer: 9110010357474 Haidingergasse 1 1030 Wien Postfach 600 Telefon: +43 / 1 / 71132 - 0 E-Mail: posteingang.allgemein@sozialversicherung.at Internet: www.hauptverband.at, www.sozialversicherung.at Datenschutzbeauftragter (dsb@sozialversicherung.at)	
Wiener Gebietskrankenkasse (WGKK) Ergänzungsregister-Nummer: 9110003816834 Wienerbergstraße 15-19 1100 Wien Postfach 6000 Telefon: +43 / 1 / 60122 - 0 E-Mail: office@wgkk.at Internet: www.wgkk.at	
Niederösterreichische Gebietskrankenkasse (NÖGKK) Ergänzungsregister-Nummer: 9110002126828 Kremser Landstraße 3 3100 St. Pölten Postfach 164 Telefon: +43 / 0 / 50 899 - 6100 (Versicherte); +43 / 0 / 50 899 - 7100 (Dienstgeber) E-Mail: info@noegkk.at Internet: www.noegkk.at	
Burgenländische Gebietskrankenkasse (BGKK) Ergänzungsregister-Nummer: 9110020118461 Siegfried Marcus Straße 5 7000 Eisenstadt Telefon: +43 / 2682 / 608 - 0 E-Mail: bgkk@bgkk.at Internet: www.bgkk.at	
Oberösterreichische Gebietskrankenkasse (OÖGKK) Ergänzungsregister-Nummer: 9110010512859 Gruberstraße 77 4020 Linz Postfach 61 Telefon: +43 / 0 / 5 78 07 - 0 E-Mail: ooegkk@ooegkk.at Internet: www.ooegkk.at	

[9] Die Angabe ist vom bzw. unter Befragung des Produktverantwortlichen auszufüllen.

Steiermärkische Gebietskrankenkasse (StGKK) Ergänzungsregister-Nummer: 9110008901610 Josef-Pongratz-Platz 1 8010 Graz Postfach 900 Telefon: +43 / 316 / 8035 - 0 E-Mail: service@stgkk.at Internet: www.stgkk.at	
Kärntner Gebietskrankenkasse (KGKK) Ergänzungsregister-Nummer: 9110003511395 Kempfstraße 8 9020 Klagenfurt Telefon: +43 / 0 / 50 58 55 - 0 E-Mail: kaerntner.gkk@kgkk.at Internet: www.kgkk.at	
Salzburger Gebietskrankenkasse (SGKK) Ergänzungsregister-Nummer: 9110006520837 Engelbert-Weiß-Weg 10 5020 Salzburg Postfach 2020 Telefon: +43 / 662 / 8889 - 0 E-Mail: sgkk@sgkk.at Internet: www.sgkk.at	
Tiroler Gebietskrankenkasse (TGKK) Ergänzungsregister-Nummer: 9110002515189 Klara-Pölt-Weg 2 6020 Innsbruck Telefon: +43 / 0 / 59160 E-Mail: tgkk@tgkk.at Internet: www.tgkk.at	
Vorarlberger Gebietskrankenkasse (VGKK) Ergänzungsregister-Nummer: 9110002392575 Jahngasse 4 6850 Dornbirn Telefon: +43 / 0 / 50 8455 - 0 E-Mail: vgkk@vgkk.at Internet: www.vgkk.at	
Betriebskrankenkasse der Wiener Verkehrsbetriebe (BKKWVB) Ergänzungsregister-Nummer: 9110001545699 Erdbergstraße 202/E7a 1030 Wien Telefon: +43 / 1 / 79 09 - 23999 E-Mail: office@bkkwvb.at Internet: www.bkkwvb.at	
Betriebskrankenkasse Mondi (BKKMondi) Ergänzungsregister-Nummer: 9110002037568 Theresienthalstraße 50 3363 Ulmerfeld-Hausmening Telefon: +43 / 7475 / 500 E-Mail: service@bkkmondi.at Internet: www.bkkmondi.at	
Betriebskrankenkasse voestalpine Bahnsysteme (BKK-Bahnsysteme) Ergänzungsregister-Nummer: 9110006170261 Kerpelystraße 201 8700 Leoben Telefon: +43 / 0 / 50 304 25 - 3138 E-Mail: bkkbahnsysteme@bkkva.sozvers.at Internet: www.bkk-bahnsysteme.at	
Betriebskrankenkasse Zeltweg (BKKZeltweg) Ergänzungsregister-Nummer: 9110008577235 Alpinestraße 1 8740 Zeltweg Telefon: +43 / 0 / 50 30428 DW 171 bis 177 E-Mail: bkk.zeltweg@bkkzw.sozvers.at Internet: www.bkkzeltweg.at	
Betriebskrankenkasse Kapfenberg (BKK-KA) Ergänzungsregister-Nummer: 9110006265837 Friedrich-Böhler-Straße 11 8605 Kapfenberg	

Postfach 94 Telefon: +43 / 3862 / 20 - 36648 E-Mail: direktion@bkkka.sozvers.at Internet: www.bkk-ka.sozvers.at	
Versicherungsanstalt für Eisenbahnen und Bergbau (VAEB) Ergänzungsregister-Nummer: 9110004199363 Linke Wienzeile 48 – 52 1060 Wien Telefon: +43 / 0 / 50 2350 - 0 E-Mail: office@vaeb.at Internet: www.vaeb.at	
Versicherungsanstalt öffentlich Bediensteter (BVA) Ergänzungsregister-Nummer: 9110006685673 Josefstädter Straße 80 1080 Wien Postfach 500 Telefon: +43 / 1 / 050405 E-Mail: postoffice@bva.at Internet: www.bva.at	
Sozialversicherungsanstalt der gewerblichen Wirtschaft (SVA) Ergänzungsregister-Nummer: 9110008661972 Wiedner Hauptstraße 84-86 1051 Wien Telefon: +43 / 0 / 5 08 08 -0 E-Mail: svagw@svagw.at Internet: www.svagw.at	
Sozialversicherungsanstalt der Bauern (SVB) Ergänzungsregister-Nummer: 9110009850696 Ghegastrasse 1 1030 Wien Telefon: +43 / 1 / 797 06 - 0 E-Mail: hauptstelle@svb.at, info@svb.at Internet: www.svb.at	
Allgemeine Unfallversicherungsanstalt (AUVA) Ergänzungsregister-Nummer: 9110011258268 Adalbert-Stifter-Straße 65-67 1200 Wien Telefon: +43 / 1 / 33111 - 0 E-Mail: HAV@auva.at Internet: www.auva.at	
Pensionsversicherungsanstalt (PVA) Ergänzungsregister-Nummer: 9110011163128 Friedrich-Hillegeist-Straße 1 1021 Wien Telefon: +43 / 0 / 503 03 E-Mail: pva@pensionsversicherung.at Internet: www.pensionsversicherung.at	
Versicherungsanstalt des österreichischen Notariates (VAN) Ergänzungsregister-Nummer: 9110011297991 Florianigasse 2 1080 Wien Postfach 15 Telefon: +43 / 1 / 405 13 81 - 0 E-Mail: office@van.co.at Internet: www.notar.at	
Bundesministerium für Finanzen (BMF) Ergänzungsregister-Nummer: 9110005102096 Johannesgasse 5 1010 Wien Telefon: +43 / 1 / 51433 - 0 Internet: www.bmf.gv.at	
Bundesministerium für Arbeit, Soziales, Gesundheit und Konsumentenschutz (BMASGK) Ergänzungsregister-Nummer: 9110019891221 Stubenring 1 1010 Wien Telefon: +43 / 1 / 71100 – 0 E-Mail: post@sozialministerium.at Internet: www.sozialministerium.at	

Bundesministerium für Inneres (BMI) Ergänzungsregister-Nummer: 9110006619920 Herrengasse 7 1010 Wien Telefon: +43 / 1 / 53126 – 0 E-Mail: post@bmi.gv.at Internet: www.bmi.gv.at	

B) Datenempfänger und Rechtsgrundlage (Zwecks Aufnahme in das VVT)

1	interne EDV-Organisation (z. B. für Wartung der Daten) gem. Betriebsvereinbarungen, Dienstvertrag, Arbeitsanweisungen.	X
2	Datenschutzbehörde, soweit für die Ausübung des Aufsichtsrechts und die Führung konkreter Verfahren im Einzelfall nötig (§§ 32 Abs. 1 Z 4 und Z 5 DSG).	X
3	Bundesministerium für Finanzen und Bundesministerium für Arbeit, Soziales, Gesundheit und Konsumentenschutz, soweit für die Ausübung des Aufsichtsrechts im Einzelfall nötig (§§ 448 ff ASVG).	X
4	Interne Revision / Kontrolle / Organe der ITSV GmbH / Rechnungshof (Rechnungshofgesetz, UGB, GmbHG, Satzungen).	X
5	Gesellschafter, Konzernbereich (ASVG, UGB, GmbHG, Satzungen, SV-DSV, REDV).	
6	Behörden, welche aufgrund der bestehenden Rechtsgrundlage gemäß Art. 4 Z 9 DSGVO Daten zu erhalten haben (wie Sozialversicherungsträger, Arbeitsmarktservice, Finanzbehörden, Gerichte, Mitarbeitervorsorgekasse, etc.).	
7	Vertrags- oder Geschäftspartner, die an der Lieferung oder Leistung mitwirken bzw. mitwirken sollen.	
8	Banken zur Abwicklung des Zahlungsverkehrs.	
9	Rechtsvertreter im Geschäftsfall.	
10	Wirtschaftsprüfer für Zwecke eines Audits.	
11	Inkassounternehmen zur Schuldeneintreibung.	
12	Fremdfinanzierer wie Leasing- oder Factoringunternehmen und Zessionare, sofern die Lieferung oder Leistung auf diese Weise fremdfinanziert wird.	
13	Versicherungsunternehmen aus Anlass des Abschlusses eines Versicherungsvertrages über die Lieferung/Leistung oder des Eintritts des Versicherungsfalles.	
14	Bundesanstalt „Statistik Österreich“ für die Erstellung der gesetzlich vorgeschriebenen (amtlichen) Statistiken (Bundesstatistikgesetz 2000).	
15	Kunden (Empfänger von Leistungen).	
16	SachbearbeiterInnen / Akten-Bearbeitung (z.B. Personalabteilung, Finanzen und Controlling)	
17	Mitarbeitervorsorgekassen nach dem Betrieblichen Mitarbeiter- und Selbständigenvorsorgegesetz - BMSVG	
	zusätzlich spezifische sozialversicherungsrelevante-Verarbeitungen:	
18	Hauptverband der österreichischen Sozialversicherungsträger	
18	Sozialversicherungsträger	
20	Kranken- & Unfallfürsorgeanstalten (§ 2 Abs. 1 Z 2 B-KUVG)	
21	Pensionsinstitut der Linz AG	
22	Arbeitsmarktservice	
23	Entscheidungsträger gemäß § 22 Abs. 1 BPGG (Bundespflegegeldgesetz)	
24	Finanzbehörden	
25	Länder	
26	Kammern für Arbeiter und Angestellte, Landarbeiterkammern	

27	Wohnbauförderungsfonds	
28	Stammzahlenregisterbehörde im Rahmen ihrer Befugnisse nach dem E-Government-Gesetz	
29	Behörden des Bundes einschließlich der Gerichte und der Gerichtshöfe öffentlichen Rechts sowie Behörden der Länder im Rahmen von Amtshilfe	
30	Versicherungsunternehmen (soweit sie zur Klärung der Entstehung eines regressierbaren Schadenersatzanspruches (§§ 332 ff ASVG) und zu dessen Ausgleich notwendig sind.)	
	SONSTIGE:	
31		
32		

[i] Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags (bzw. datenschutzrechtlicher Bestimmungen in einem Vertrag bzw. soweit zulässig auch in AGBs).