Allgemeine Dienstanweisung

betreffend die Inkraftsetzung der

ITSV DATENSCHUTZ– UND DATENSICHERHEITSVORSCHRIFT

Verteiler:
an alle Mitarbeiter (Angestellte, überlassene Dienstnehmer und Mitarbeiter externer Firmen)
Betriebsrat

Inhaltsverzeichnis

EINLEITUNG

Die ITSV-GmbH ist als Tochterunternehmen der Sozialversicherungsträger einer weiteren Öffentlichkeit ausgesetzt, als die meisten anderen privatwirtschaftlich tätigen Firmen. Auch ist anzunehmen, dass Mitarbeiter der ITSV-GmbH im Rahmen ihrer Tätigkeit in Hinkunft vermehrt Aufgaben durchzuführen haben, bei welchen Sie Zugriff auf Datenbestände des Hauptverbandes und der Sozialversicherungsträger, für die ein sehr hohes Schutzniveau zu gelten hat, bekommen. Aus diesen Gründen ist der sorgsame Umgang mit jeglichen Informationen (personenbezogenen und nicht personenbezogenen), welche sich ein Mitarbeiter im Rahmen seiner Tätigkeit für die ITSV, den Hauptverband oder einen Sozialversicherungsträger aneignet, unter ein sehr hohes Sorgfaltsniveau zu stellen.

Die vertrauliche Behandlung jeglicher Information gegenüber nicht nachweislich Berechtigten ist gerade deshalb so wichtig, da unter anderem mittels „Social Engineering Angriffen" ein Unbefugter sich von einer kleinen eher unscheinbaren Information bis hin zu einer für das Unternehmen überlebenswichtigen Information quasi „hinaufarbeiten" kann und das ohne technische Hilfsmittel einsetzen zu müssen. Dabei wird schrittweise vorgegangen indem möglichst viele verschiedene Leute im Unternehmen kontaktiert werden. Eine unscheinbare Information hilft dabei, noch eine weitere kleine Zusatzinformationen zu erlangen mit der dann ein Angreifer wiederum weitere Informationen, erlangen kann usw. Diese informationelle „Aufwärtsspirale" ist nur möglich, weil jeder Unternehmensmitarbeiter davon ausgeht, dass diese Informationen nur ein anderer Kollege bzw. eine zuständige Person haben kann und daher davon ausgeht, dass diesem die Zusatzinformation gefahrlos erteilt werden kann. Jede noch so kleine Information kann dabei von einem Angreifer zur Vertrauensbildung eingesetzt werden. Das beginnt bereits bei Gesprächen im Wirtshaus, in denen mitgehört werden kann, wie ein Mitarbeiter einem Kollegen darüber erzählt, an welchen Angeboten, Projekten etc. sie gerade arbeiten und reicht bis zur nicht fachgerechten Entsorgung von nicht mehr benötigten Unterlagen, aus welchen beispielsweise der Aufbau der im Unternehmen gebräuchlichen Benutzeridentifikationen herauslesbar ist.

Meist ist es auch leicht, direkt in das EDV-Netz eines Unternehmens einzudringen. Bisweilen reicht da ein Anruf beim Helpdesk, bei dem sich jemand als Mitarbeiter ausgibt und vorgibt sein Passwort vergessen zu haben. Als „vertrauensbildende Maßnahme" hat sich der Angreifer zuvor versichert, dass dieser Mitarbeiter auf Urlaub ist und kann meist auch weitere Namen bzw. Informationen in das Gespräch einfließen lassen, mit denen er das Vertrauen des Helpdeskmitarbeiters gewinnt (beispielsweise, dass es dringend ist, da ein Auftrag vom gemeinsamen Vorgesetzten mit dem Namen X kommt, wofür er sofort den Zugriff benötigt etc.). Derartige Telefonate sind, wenn Mitarbeiter zuvor zu leichtfertig mit Informationen über die Firma umgegangen sind, meist sehr gut vorbereitet und klingen absolut vertrauenswürdig. Noch leichter werden Benutzeridentifikationen und Passwörter von einem Angreifer erlangt, indem dieser nicht den Helpdesk sondern direkt ein Mitarbeiter kontaktiert und sich als IT-Mitarbeiter ausgibt, der sich mit seinem Detailwissen so gut „legitimieren" kann, dass diesem sogar das Passwörter und Benutzeridentifikation unmittelbar bekannt gegeben werden (Phishing - Attacken laufen nach dem selben Prinzip ab). Da die ITSV personell wächst und daher sich bei weitem nicht alle Mitarbeiter gegenseitig kennen, dürfen auch bei uns diese Gefahren nicht unterschätzt werden.

Einem besonderen Schutz unterliegt überdies der Umgang mit **personenbezogenen** Daten. Diesbezüglich sieht § 14 DSG 2000 auch ausdrücklich die Verpflichtung vor, Datensicherheitsvorschriften so zu erlassen und zur Verfügung zu halten, sodass sich die Mitarbeiter über die für sie geltenden Regelungen jederzeit informieren können.

Einer der wichtigsten Aspekte dieser Dienstanweisung ist auch der Schutz der Mitarbeiter, der leitenden Angestellten sowie der ITSV (als Verband iSd Verbandsverantwortlichkeitsgesetzes) vor strafrechtlicher Verfolgung. Die Einhaltung dieser Dienstanweisung gewährleistet, dass auch dieses Risiko für alle erheblich vermindert wird.

Aus diesen Gründen wird die folgende Dienstanweisung erlassen:

1. SPRACHGEBRAUCH

Bei den in dieser Dienstanweisung verwendeten personenbezogenen Bezeichnungen gilt die gewählte Form für beide Geschlechter.

2. GELTUNGSBEREICH

Diese Datensicherheitsvorschrift ergeht in Durchführung des §14 Datenschutzgesetz 2000 (DSG 2000), BGBl. I Nr. 165/1999 idgF, der Datenschutzverordnung der österreichischen Sozialversicherungsträger (SV-DSV 2001), des Gesundheitstelematikgesetzes (GTelG), BGBl. I Nr. 179/2004 idgF **sowie** weiterer Geheimhaltungsbestimmungen (z.B. Strafgesetzbuch, Verträge) ohne Bezug auf die Verwendung von „personenbezogenen" Daten.

Diese Sicherheitsvorschrift gilt für alle Mitarbeiter (siehe Pkt 3) der ITSV GmbH und gilt für die Verwendung von personenbezogenen und nicht personenbezogenen Daten gleichermaßen. Wo ausdrücklich der Terminus „personenbezogene Daten" verwendet wird, erstreckt sich die angeführte Bestimmung jedoch nur auf diese.

Insofern diese Dienstanweisung Rechte für Mitarbeiter der ITSV festlegt, können diese von Seiten der ITSV GmbH jederzeit widerrufen werden und können daher insbesondere auch keine rechtliche Basis für gewohnheitsrechtliche Ansprüche erzeugen.

3. BEGRIFFSBESTIMMUNGEN

Daten: Personenbezogene Daten sowie nicht personenbezogene Daten (z.B. Informationen über EDV-Systeme, Ausschreibungsbedingungen, Vertragsinhalte etc.) unabhängig davon, auf welchem Speichermedium sie aufbewahrt werden (Papier, CD, Festplatte, Speicherkarten, USB-Stick etc.). Anmerkung: Auch personenbezogene **TESTDATEN,** fallen unter die folgenden Bestimmungen (außer sie wurde vorher verfälscht).

Personenbezogene Daten: Angaben über Betroffene, deren Identität bestimmt (z.B. über die über den Betroffenen gesammelten Informationen oder den Namen) oder (wenn auch nur indirekt mittels zusätzlicher Verwendung von Datenbeständen anderer Auftraggeber) bestimmbar ist.

Betroffener: jede von der ITSV (=Auftraggeber) verschiedene natürliche oder juristische (GmbH, Verein, Sozialversicherungsträger etc.) Person oder Personengemeinschaft, deren Daten verwendet werden.

Verwendung von Daten: Das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen, Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten einer Datenanwendung.

Technische Einrichtungen: Hardware (Server, Laptops, PCs, Bildschirme etc.) und Software (Originaldateien, Kopien, etc.)

sensible Daten („besonders schutzwürdige Daten"): Personenbezogene Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, **Gesundheit** oder ihr Sexualleben.

Gesundheitsdaten: personenbezogene Daten über die physische oder psychische Befindlichkeit eines Menschen, einschließlich der im Zusammenhang mit der Erhebung der Ursachen für diese Befindlichkeit sowie der medizinischen Vorsorge oder Versorgung, der Pflege, der Verrechnung von Gesundheitsdienstleistungen oder der Versicherung von Gesundheitsrisiken erhobenen Daten. Dazu gehören insbesondere Daten die
a) die geistige Verfassung,
b) die Struktur, die Funktion oder den Zustand des Körpers oder Teile des Körpers,
c) die gesundheitsrelevanten Lebensgewohnheiten oder Umwelteinflüsse,
d) die verordneten oder bezogenen Arzneimittel, Heilbehelfe oder Hilfsmittel,
e) die Diagnose-, Therapie- oder Pflegemethoden oder
f) die Art, die Anzahl, die Dauer oder die Kosten von Gesundheitsdienstleistungen oder gesundheitsbezogene Versicherungsdienstleistungen betreffen.

Mitarbeiter: Personen die im Rahmen ihrer Tätigkeiten für die ITSV Einblick in Daten der ITSV oder im Rahmen von Aufträgen, welche die ITSV für die Sozialversicherung durchführt, erhalten. Es spielt keine Rolle, ob diese unmittelbar aufgrund eines Arbeitsvertrages oder aufgrund einer anderen Vertragsbeziehung (z.B. Arbeitskräfteüberlassung, externe Dienstleistung) tätig werden.

Datenträger: Jedes elektronische sowie nicht elektronische Medium, welches zur Aufbewahrung von Daten dienen kann (Papier, elektronische Datenträger aller Art etc.).

Datenanwendung: Unter Datenanwendung sind nicht nur Programme zu verstehen, die Daten verarbeiten (z.B. Datenbanken, Personalverwaltungssoftware, selbstgestrickte Programme mit Access oder Excel etc.) sondern auch die Verarbeitung von personenbezogenen Daten welche bloß in - unter sachbezogenen Kriterien angelegten - Ordnern gespeichert/verarbeitet werden (und daher nicht von einer eigens erstellten Software).

Auch manuelle Verarbeitungen, welche nach mindestens einem Kriterium geordnet sind (z.B. Karteien) unterliegen teilweise den Bestimmungen des Datenschutzgesetzes.

Systembetreuer/Systemadministrator: Alle Personen die im Rahmen ihrer Tätigkeit (vereinzelt oder generell) anderen Personen Zugriff auf (nicht allgemein zugängliche) Informationen bzw. Arbeitsmittel einräumen können (z.B. PC, Exchangeserver, technische Protokolle aber auch auf bestimmte Benutzerkreise eingeschränkte Fileordner/Ablagesysteme wie beispielsweise Zugriffe auf Personal-, Buchhaltungsunterlagen, Outlook-Postfächer, Ordner etc).

Auftraggeber: natürliche oder juristische Personen, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten für einen bestimmten Zweck zu verarbeiten, und zwar unabhängig davon, ob sie die Verarbeitung selbst durchführen oder hiezu einen anderen heranziehen. Als Auftraggeber gelten die genannten Personen auch dann, wenn sie einem anderen Daten zur Herstellung eines von ihnen aufgetragenen Werkes überlassen und der Auftragnehmer die Entscheidung trifft, diese Daten zu verarbeiten.

4. ALLGEMEINE, ORGANISATORISCHE UND PERSONELLE MASSNAHMEN

4.1. Auftragsprinzip

Daten dürfen von den einzelnen Bereichen und von deren Mitarbeitern nur im Rahmen ihrer **Zuständigkeit** verwendet werden und sind immer vertraulich zu behandeln.

Die Verwendung von Daten des HVB sowie der Sozialversicherungsträger (SVT) im Rahmen eines von diesen erteilten Auftrages an die ITSV-GmbH unterliegen zusätzlich den vom HVB und dem jeweiligen Sozialversicherungsträger für den Einzelfall nachweislich kommunizierten Verwendungsbeschränkungen. Es besteht vor der Bearbeitung dieser Daten für jeden Mitarbeiter die Pflicht, sich über die Existenz und den Inhalt diese Vorschriften durch Nachfrage bei seinem Vorgesetzten zu informieren.

Die Zuständigkeit gründet sich auf gesetzliche Regelungen oder auf Aufträge der Geschäftsleitung. Sie können genereller Natur sein, z.B. sich aus der Geschäftseinteilung ergeben, oder für den Einzelfall erteilt werden. Die Erteilung von Aufträgen hat in der jeweils üblichen Form (z.B. Vordrucke, mündlich, Zuteilung von Schriftstücken, elektronisch) zu erfolgen.

Jeder (generell oder einzelfallbezogen erteilte) Auftrag, welcher auch die Verwendung von **personenbezogenen** Daten (mit)bedingt, muss zum Schutze des Mitarbeiters nachvollziehbar (keinesfalls daher ausschließlich mündlich) erteilt werden. Ein Auftrag hat daher insbesondere die zu verarbeitenden Daten, die zulässigen Verarbeitungsschritte sowie bei Übermittlungen von personenbezogenen Daten die berechtigten Empfängerkreise zu bezeichnen und ist vom Mitarbeiter zum Zwecke seiner Entlastung im Rahmen einer späteren Datenschutzüberprüfung (beispielsweise durch die Datenschutzkommission oder auch im Rahmen von internen Stichprobenüberprüfungen) aufzubewahren. Ein Mitarbeiter darf personenbezogenen Daten ohne nachvollziehbare (einzelfallbezogene **oder generelle**) Auftragserteilung nicht verwenden. Diese Inhalte können sich beispielsweise auch aus Beschlüssen des Auftraggebers (z.B. Verbandsvorstand, Trägerkonferenz) **oder auch generell** auf

Grundlage der Arbeitsplatzbeschreibung (z.B. Tätigkeit in der Buchhaltungsabteilung impliziert auch generell den Umgang mit Buchhaltungsdaten) ergeben.

Bei Verwendung von personenbezogenen Daten des HVB oder eines Sozialversicherungsträgers (bzw. von diesen verarbeiteten Daten) ist – so der Verwendungsumfang nicht bereits vorab durch entsprechende Beschlüsse der zuständigen Gremien ausrechend klar bestimmt wird – jeweils eine schriftliche Genehmigung des HVB bzw. des Sozialversicherungsträgers (z.B. per e-Mail) durch den Auftragsempfänger (Geschäftsleitung, Bereichsleiter oder im Einzellfall, soweit eine direkte Auftragserteilung zulässig ist, vom Mitarbeiter selbst) einzuholen.

Der schriftliche Nachweis über die Auftragserteilung ist den Auftrags-/Projektunterlagen beizulegen.

Personenbezogene Daten dürfen auch im Rahmen einer erteilten Genehmigung nur so eingeschränkt wie möglich verwendet werden und sind so bald sie nicht mehr benötigt werden, wieder zu löschen oder zu anonymisieren.

Bestehen Zweifel über die Verwendungsgenehmigung bzw. über deren Umfang, ist der zuständige Jurist der ITSV zu befassen.

4.2. Belehrungspflicht

Die ITSV-GmbH und deren Dienstleister haben in ihrem jeweiligen Wirkungsbereich alle involvierten Mitarbeiter in entsprechender Weise über ihre Pflichten gemäß dem Datenschutzgesetz 2000 (DSG 2000) und über ihre sonstigen Verschwiegenheitspflichten nachweislich gem. Anlage B zu belehren. Diese Belehrung ist durch den zuständigen Juristen der ITSV bei der Personalaufnahme bzw. bei externen Mitarbeitern durch den Leiter der (den Auftrag erteilenden) Organisationseinheit im Rahmen der Beauftragung durchzuführen. Die Abhaltung der Belehrung ist von jedem Mitarbeiter durch Unterfertigung des Merkblattes zu bestätigen. Diese Bestätigung ist den jeweiligen Personalunterlagen anzuschließen.

Sollte sich ein Mitarbeiter unsicher sein, ob eine dieser Bestimmungen sich allgemein auf die Verwendung von „Daten" oder speziell auf die Verwendung von „personenbezogenen Daten" bezieht, so hat dieser vor der Verwendung der personenbezogenen Daten Rücksprache mit dem zuständigen Juristen der ITSV zu halten. Grundsätzlich ist zu sagen, dass die meist strengeren Bestimmungen nur auf personenbezogene Daten anzuwenden sind und dann „personenbezogen" auch extra im Text angeführt ist. Diese strengeren Bestimmungen brauchen daher nicht auf „einfache" Daten angewendet werden.

Den Mitarbeitern ist es insbesondere untersagt:

- sich Daten unbefugt (d.h. ohne dass hiefür eine ausreichende rechtliche Grundlage für die Verarbeitung bzw. Übermittlung geltend gemacht werden kann) zu beschaffen,
- Daten zu einem anderen Zweck als für ihre eigene Arbeit zu verwenden
- unbefugten Personen oder unzuständigen Stellen Daten mitzuteilen,
- unbefugten Personen oder unzuständigen Stellen Daten zugänglich zu machen.

Die Mitarbeiter sind zur Einhaltung dieser Verbote auch nach Beendigung ihrer Mitarbeit bzw. ihrer Funktion verpflichtet.

Insofern Mitarbeiter längerfristig für die ITSV-GmbH tätig werden, haben diese an der jährlich stattfindenden Datenschutzschulung teilzunehmen.

Wenn Mitarbeiter Zweifel betreffend Ihre Berechtigung zur Verwendung von personenbezogenen Daten haben, ist von diesen der zuständige Jurist der ITSV zu befassen.

4.3. Datenverarbeitungsregister

Personenbezogene Daten dürfen im Rahmen von Datenanwendungen nur verwendet werden, wenn diese Datenanwendung bei der Datenschutzkommission (im Datenverarbeitungsregister) gem. § 17 DSG gemeldet wurde oder wenn die verwendeten Datenarten, der Zweck für den diese verarbeitet werden sowie die Übermittlungsempfänger an die diese übermittelt werden können unter eine der von der ITSV betriebenen Standardanwendungen (gem. Standard- und Musterverordnung, BGBl. II Nr. 312/2004) eingereiht werden können.

Die von der ITSV verwendeten Standardanwendungen sind im Anlage A als Bestandteil dieser Sicherheitsbestimmungen angehängt. Es ist zulässig, weniger als die in der Standardanwendung aufgeführten Datenarten bzw. Übermittlungsempfänger etc. zu verarbeiten. Sobald jedoch auch nur eine zusätzliche Datenart (d.h. ein zusätzliches „Datenfeld"; eine zusätzliche „Information") oder ein zusätzlicher Übermittlungsempfänger hinzukommt, bzw. sich der Zweck der Datenverarbeitung nicht mit dem in der Standardverordnung angeführten entspricht, hat vor Aufnahme der Datenverarbeitung eine Meldung der Datenanwendung gem. § 17 DSG durch den zuständigen Juristen der ITSV zu erfolgen.

Die Mitarbeiter sind daher verpflichtet, dem zuständigen Juristen der ITSV die Aufnahme der Verarbeitung personenbezogener Daten (d.h. die Verwendung einer Software (einer Standardsoftware, einer Datenbank, eines selbstgestrickten Programms oder ähnlichem) oder einer manuellen Datenanwendung [z.B. von Karteikästen], die personenbezogene Daten verarbeitet) bereits im Projektstadium (vor der Aufnahme von Softwareentwicklungsarbeiten bzw. der Befüllung einer gekauften Applikation mit personenbezogenen Daten) **durch Übermittlung der in Anlage C angefügten „Applikationsbeschreibung aus datenschutzrechtlicher Sicht" bekannt zu geben. Bei jeder Änderung bzw. falls im Projektstadium noch nicht alle Felder der Applikationsbeschreibung befüllt werden konnten, ist – so rasch wie möglich - erneut eine vollständig ausgefüllte Applikationsbeschreibung an den zuständigen Juristen zu übermitteln. Es ist bei der Projektierung der Einführung einer neuen Datenverarbeitung (und der Änderung einer bestehenden Datenverarbeitung) zu bedenken, dass je nach Art der verarbeiteten Daten bzw. der Datenanwendung VOR Aufnahme der Verarbeitung bis zu 2 Monate dauern kann, bis von der Datenschutzkommission die Software (die Datenverarbeitung/-anwendung) zur Verwendung frei gegeben wird!!!**

5. ZUTRITTS-, ZUGRIFFSREGELUNG UND SICHERUNG GEGEN UNBEFUGTE INBETRIEBNAHME

Die technischen Einrichtungen sind in gesicherten Räumen (d.h. zumindest mit versperrbaren Türen) aufzustellen. Alle Türen dieser Räume müssen grundsätzlich versperrt werden.

Ein Raum, in dem technische Einrichtungen aufgestellt sind, darf während der Betriebszeit grundsätzlich nur von den Bediensteten der ITSV-GmbH betreten werden; andere Personen (z.B. Wartungstechniker, Besucher) dürfen sich nur im Beisein eines Mitarbeiters in solchen Räumen aufhalten. Unbeaufsichtigte Räume, in denen sich technische Einrichtungen befinden, sind stets versperrt zu halten.

Die Mitarbeiter der ITSV-GmbH haben die Pflicht, den Zutritt unbefugter Personen nach Möglichkeit zu verhindern.

Datensichtgeräte (Bildschirme, etc.) sind so aufzustellen, dass der mit ihnen wiedergegebene Inhalt nicht von Unbefugten mitgelesen werden kann.

Durch die Vergabe von Bedienerkennzeichen (Benutzeridentifikation und Passwort) ist sicherzustellen, dass mit dem Zutritt zum Raum noch kein Zugriff zu Datenanwendungen möglich ist.

Den Mitgliedern der Datenschutzkommission (DSK) ist nach Ausweisleistung der Zutritt zu solchen Räumen zu gestatten. Der jeweilige Leiter der überprüften Organisationseinheit, der zuständige Jurist sowie die

Geschäftsführung sind davon unverzüglich zu verständigen, damit diese die DSK entsprechend unterstützen können.

5.1. Zugriff auf Daten

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, Firewalls, gestaffelte Zugriffsberechtigungen, etc. Wenn Mitarbeiter auf ihren PCs lokale Administratorenrechte besitzen, ist diese Pflicht auch unmittelbar von diesen einzuhalten. Für Nicht-Techniker bedeutet das, dass Ausfälle dieser Schutzfunktionen (z.B. des Virenscanners) dem zuständigen Systemadministrator unverzüglich zu melden sind.

Der Zugriff auf gespeicherten Daten ist durch programmgesteuerte Zugriffsermächtigungen zu regeln. Die Differenzierung der Zugriffsermächtigung erfolgt über das Bedienerkennzeichen (Benutzeridentifikation) je nach Funktion sowie der Eingabe- und Abfrageberechtigung eines Mitarbeiters.

Nach jeder Änderung der Funktion eines Mitarbeiters sind seine Zugriffsermächtigungen erneut auf deren unbedingte Notwendigkeit zu evaluieren und neu zu vergeben. Erkennt der Mitarbeiter, dass ihm trotz Funktionsänderung nicht mehr unbedingt erforderliche Zugriffsberechtigungen weiterhin erteilt sind, so hat er dies unverzüglich der Systemadministration bekannt zu geben.

Zugriffsberechtigungen dürfen nur an Mitarbeiter erteilt werden, soweit sie diese für die Erfüllung ihrer Aufgaben unbedingt benötigen. Ein nur sehr sporadischer Bedarf an bestimmten Daten rechtfertigt nicht die Erteilung einer jederzeitigen Zugriffsberechtigung. In solchen Fällen sind die Daten von den berechtigten Mitarbeitern im Rahmen der Bestimmungen dieser Datensicherheitsvorschrift einzuholen.

Die Prinzipien zur Festlegung der Personen, die berechtigt sind, über technische Infrastruktur Einsicht in verarbeitete Daten zu nehmen bzw. Veränderungen an Daten vorzunehmen, richten sich nach den in der Punkten 4.1 angeführten Grundsätzen und sind gem. Punkt 5.2 umzusetzen.

Eine Speicherung von Daten hat nur in den jeweils hiefür vorgesehenen Ordnern zu erfolgen. Die Speicherung von personenbezogenen Daten (der Mitarbeiter oder anderer Betroffenen) in allgemein zugänglichen Ordnern ist – mit Ausnahme von Exzerpten aus allgemein zugänglichen Kontakt- bzw. Telefonlisten – ohne die Zustimmung der Betroffenen nicht zulässig.

Erteilte Zugriffsberechtigungen sind von der erteilenden Stelle auf nachvollziehbare Weise (inklusive des Berechtigungszeitraumes) zu dokumentieren.

Nutzen mehrere Personen regelmäßig (z.B. Praktikant(inn)en, studentische Hilfskräfte etc.) einen PC gemeinsam, ist sicherzustellen, dass die personenbezogenen Nutzer- und Anmeldeprofile sowie Datenbeständen ausschließlich den jeweils angemeldeten Nutzern zur Verfügung stehen. Dies gilt auch bei temporärer Nutzung von Mitarbeiter-PCs durch andere Mitarbeiter.

5.2. Sicherung gegen unbefugte Inbetriebnahme

Die Bedienung der Programme hat nur durch jene Mitarbeiter zu erfolgen, denen eine Benutzerkennzeichen/Benutzeridentifikation (BKZ) erteilt wurde.

Die Vergabe von BKZ erfolgt durch den Leiter des Bereichs Hardware bzw. von einem von diesem hiezu ermächtigten Mitarbeiter der ITSV. Dieser hat das zugewiesene BKZ dem jeweiligen Mitarbeiter ausschließlich mündlich mitzuteilen. Er hat dabei dem Mitarbeiter darauf aufmerksam zu machen, dass über das zugewiesene BKZ von ihm keine (d.h. auch keine elektronischen) Aufzeichnungen geführt werden dürfen.

Jeder Mitarbeiter wird bei der ersten Inbetriebnahme eines Endgerätes aufgefordert, ein persönliches Passwort zu vergeben, das dieser geheim zuhalten hat und über das keine Aufzeichnungen geführt werden dürfen. Jeder Mitarbeiter ist für die unter seinem BKZ getätigten Eingaben und Abfragen verantwortlich. Er hat daher die Wirksamkeit seines BKZ vor dem Verlassen des PCs oder bei Beendigung des Eingabe- oder Abfragebetriebes

aufzuheben (d.h. z.B. den PC zu sperren). Zusätzlich muss der Bildschirmschoner passwortgeschützt eingerichtet werden, sodass die Sperre automatisch nach wenigen Minuten Nicht-Benutzung automatisch aktiviert wird.

Ein Passwort hat aus einer Kombination aus Buchstaben und Ziffern oder Sonderzeichen zu bestehen und zumindest 6 Zeichen aufzuweisen. Zahlen/Buchstabenkombinationen, welche grundsätzlich auch anderen Personen bekannt sein können (z.B. Geburtsdatum, Namen, Wörter laut Wörterbuch) dürfen nicht verwendet werden, da diese leicht mit div. Passwortknackprogrammen herausgefunden werden können. Das Passwort ist von jedem Benutzer periodisch, mindestens jedoch einmal pro Jahr, zu ändern.

Bei Vergessen des Passwortes kann vom Leiter des Bereiches Hardware bzw. von einem von diesem hiezu ermächtigten Angestellten der ITSV ein neues Passwort vergeben werden, welches vom Mitarbeiter unverzüglich zu ändern ist; das Herausfinden des ehemals verwendeten Passwortes ist nicht möglich.

Wurde ein zugewiesenes Benutzerkennzeichen außer dem Mitarbeiter anderen Personen bekannt oder liegt eine diesbezügliche Vermutung vor, wurde ein Benutzerkennzeichen missbräuchlich verwendet oder besteht dahingehend ein Verdacht, so ist der Widerruf/die Änderung dieses BKZ umgehend zu veranlassen.

BKZ und Passwörter, welche für den technischen Systembetrieb erforderlich sind, sind für Zwecke der Vertretung im Rahmen der Systemadministration aufzuzeichnen und von der Geschäftsführung in einem Safe zu hinterlegen. Nach Gebrauch der Unterlagen sind diese BKZ und Passwörter zu ändern und erneut im Safe zu hinterlegen.

6. SONSTIGE DATENSICHERHEITSREGELUNGEN

6.1. Aufbewahrung und Aufbewahrungsdauer

Es kann immer wieder beobachtet werden, dass die Altpapiercontainer von Firmen durchsucht werden (sicherlich nicht um Briefmarken zu sammeln). Umso wichtiger ist es jegliche Informationen vertraulich zu behandeln und gegen Einsichtnahme durch Unbefugte zu sichern. Dabei sind personenbezogene Daten und sensible Firmeninformationen mit einem besonders hohen Schutzniveau zu versehen. Um das zu erreichen ist insbesondere folgendes zu beachten:

- Die Aufbewahrung von Datenträger (auch Papier) hat nach Maßgabe deren Sensibilität und der technischen und organisatorischen Möglichkeiten versperrt durch die jeweiligen Bereiche zu erfolgen, z.B. versperrbare Schränke, Fächer, Karteikästen, Zimmer.
- Protokoll- und Dokumentationsdaten von personenbezogenen Daten sind gemäß § 14 Abs. 5 DSG 2000 maximal drei Jahre aufzubewahren, sofern gesetzlich nicht ausdrücklich anderes angeordnet ist.
- Ausdrucken von Dokumenten: Dokumente, welche personenbezogene Daten beinhalten oder sensible Firmeninformationen enthalten (z.B. Unterlagen von Bewerbern, jegliche Emails, diverse Vorstandsberichte, Listen mit Informationen von und über Personen, Zähllisten, Aufstellungen mit Geldwerten, Projektinformationen die alle Träger angehen usw.) sind – soweit sie nicht auf einen Drucker, der sich im selben Raum wie der Benutzer befindet, ausgedruckt werden - **ausschließlich** an einen der vorhandenen Netzwerkdrucker unter Aktivierung der Vertraulichkeitsfunktion zu schicken (Netzwerkdrucker auswählen - Eigenschaften – Papier – Druck an: „Druck vertraulich"). Dokumente, welche nicht unter diesen erhöhten Sorgfaltsmaßstab fallen (und daher deren Abruf durch die Vertraulichkeitsfunktion nicht möglich ist), sind nach deren Ausdruck sofort vom Drucker abzuholen, sodass Dritte diese nicht einsehen können. Die Nichtabholung der Ausdrucke stellt eine Dienstpflichtverletzung dar!
- Vernichtung von Ausdrucken: Dokumente, welche personenbezogene Daten beinhalten oder sensible Firmeninformationen enthalten sind **ausschließlich unter Verwendung des Aktenvernichters oder durch eine gesicherte Altpapierentsorgung zu vernichten.**
- Die Ablage von Daten ist grundsätzlich nur auf den Fileservern in den jeweils richtigen (und entsprechend geschützten) Ordnern gestattet. Durch die Offlinedateien (auf den Notebooks) können Daten, auch wenn diese in geschützten Bereichen gespeichert werden, leicht ausgelesen werden (Man kann durch das Booten mit alternativen Betriebssystemen (via CD oder Stick) das Windowsdateisystem leicht auslesen). Daher sind auf einem Notebook Daten nur solange zu speichern, wie diese benötigt werden. Gespeicherte sensible Firmeninformationen und personenbezogene Daten sind, sobald diese nicht mehr benötigt werden, umgehend nach Überspielung auf den Fileserver (zwecks zentraler Sicherung) wieder zu löschen. Der Sicherungsablauf ist so einzustellen, dass dieser weitgehend automatisch abläuft.
- Bei der Verarbeitung von vertraulichen Daten sind regelmäßig auch alle temporären Dateien zu löschen (z.B. beim Scannen entstehende Dateien).

Auf die Einhaltung der arbeitsverfassungsrechtlichenrechtlichen Vorschriften (insbesondere bestehender Betriebsvereinbarungen und Dienstanweisungen) ist zu achten.

6.2. Datensicherung

Nur durch konsequente Datensicherung ist es möglich, verloren gegangene bzw. zerstörte Datenbestände zu rekonstruieren. Datenverluste können durch Fehler in der Hardware (z.B. eine defekte Festplatte), fehlerhafte Software, Bedienungsfehler oder Stromausfälle verursacht werden. Manuelle Rekonstruktion von nicht gesicherten Daten ist nur selten oder nur unter hohem Kosten- und Zeitaufwand möglich. Der dadurch verursachte Schaden kann daher sehr hoch sein und kann auch von dem Mitarbeiter eingehoben werden, der den Schaden verursacht hat.

Um zerstörte Datenbestände wieder rekonstruieren zu können, sind daher in regelmäßigen Abständen im Generationsverfahren Sicherungskopien zu erzeugen und diese möglichst gesichert aufzubewahren (insbesondere an verschiedenen Orten). Dies wird, soweit die Daten auf den Servern der ITSV-GmbH gespeichert werden, im Rahmen der allgemeinen Sicherungsroutinen von den Systemadminstratoren der ITSV-GmbH durchgeführt.

Daten sind daher dauerhaft nicht auf der Festplatte des eigenen PCs/Notebooks sondern nur auf einem der Netzlaufwerke in dem korrekten Ordner zu speichern/zu verarbeiten.

Wenn länger als 2 Wochen keine Speicherung im entsprechenden Netzwerkordner erfolgen kann, sind unternehmenswichtige Daten auf externen Speichermedien zu sichern (Diskette, CD, DVD, Speicherkarte etc.) und sofort nach neuerlicher Anbindung an das ITSV-Netzwerk in die entsprechenden Netzwerkordner zu speichern. Die verwendeten Speichermedien sind danach zu löschen/zu vernichten.

Den Weisungen der Systemadministratoren in Bezug auf Datensicherung und Datensicherheit ist unmittelbar im selben Umfang wie einer Anweisung des eigenen Bereichsleiters Folge zu leisten!!

6.3. Verwendung von Daten zu Testzwecken

Für Testzwecke sind nach Möglichkeit synthetische Daten ohne Bezug zu einer realen Person zu verwenden. Die Verwendung von Echtdaten (Produktivdaten) zu Testzwecken ist vorab durch den zuständigen Juristen zu genehmigen.

6.4. Datenlöschung und Datenvernichtung

Richtigstellungen und Löschungen von personenbezogenen Daten gemäß § 27 DSG 2000 hat der jeweilige Auftraggeber (HVB, SVT, GF der ITSV) unter Anwendung des für das Aufgabengebiet vorgesehenen Änderungsdienstes (Regelungswerk für die Änderungen wie beispielsweise gesetzlich vorgesehene Löschungsfristen etc.) durchzuführen oder zu veranlassen.

Nicht mehr benötigte Daten, insbesondere abgelaufene Datenbestände, Fehlausdrucke oder Erfassungsformulare sowie nicht anonymisierte Testdaten, sind zu löschen bzw. so zu vernichten, dass eine Rekonstruktion nicht möglich ist. Wenn aus Gründen der Wirtschaftlichkeit die physische Löschung von Daten auf ausschließlich automationsunterstützt lesbaren Datenträgern nur zu bestimmten Zeitpunkten vorgenommen werden kann, sind diese Daten bis dahin logisch und sodann physisch zu löschen. Die entsprechenden Datenträger sind bis zur physischen Löschung versperrt aufzubewahren.

Laufend auszuscheidende Belege (Verarbeitungsaufträge, Aufzeichnungen über aufgezeichnete Daten, Ausdrucke) sind, sofern sie nicht zur ständigen Aufbewahrung bestimmt sind, einer gesicherten Vernichtung zuzuführen oder derart unkenntlich zu machen, dass eine Beziehung zu einer (natürlichen oder juristischen) Person mit höchstmöglicher Wahrscheinlichkeit nicht mehr hergestellt werden kann.

Für den Fall, dass technische Einrichtungen zu Servicezwecken aus dem Sicherheitsbereich entfernt (oder Altgeräte entsorgt) werden müssen, ist dafür Sorge zu tragen, dass eine unautorisierte Verwendung nicht stattfinden kann (z.B. dass nicht mit durch am Gerät noch vorhandene Voreinstellungen automatisiert in das SV-

Netz eingedrungen werden kann oder auf der technischen Einrichtung verarbeitete Daten eingesehen bzw. rekonstruiert werden können).

Bei einer Überführung eines Servers, PCs oder von einzelnen Datenträgern (z.B. Festplatten) zu einer Fremdfirma, sind auf der technischen Einrichtung verarbeitete Daten vom zuständigen Systemadministrator jedenfalls mit einem sicheren Verfahren (z.B. Mehrfachüberschreiben der Daten) zu löschen. Die Durchführung dieser Sicherheitsmaßnahmen ist nachvollziehbar zu dokumentieren. Nicht mehr benötigte Datenträger (CDs, Disketten, DVDs, Festplatten etc.) müssen ebenfalls an die Systemadministration zurückgegeben werden, von der sie fachgerecht zu entsorgen sind.

Die Entsorgung kann auch von dem o.a. Prozedere abweichen, wenn sie durch ein entsprechend zertifiziertes Fachunternehmen durchgeführt wird.

6.5. *Transport von Daten*

Beim Transport von Datenträgern sind diese gegen unbefugten Einblick bzw. Zugriff ausreichend zu sichern. Bei Versendung außer Haus ist grundsätzlich die Form der eingeschriebenen Sendung, allenfalls auch als Wertpaket, zu wählen.

Dateien mit vertraulichem Inhalt oder mit personenbezogenen Daten Dritter **dürfen, sobald eine bestimmte Methode von der ITSV als Service ermöglicht wird** (z.B. eine bestimmte Verschlüsselungsmethode, eine Web-Zugangsmöglichkeit mit Benutzeridentifikation und Passwort etc.), **an externe Stellen nur mit dieser zur Verfügung gestellten Methode** oder anderen sicheren Verschlüsselungsmethoden oder über sichere Netze **versendet werden**. Sichere Netze sind Netze, die eine Zugriffsmöglichkeit von Externen auf die übermittelten Daten auf Grund der verwendeten Technik soweit wie möglich ausschließt.

Bis dahin, ist eine Versendung von personenbezogenen Daten über nicht sichere Netze nur mit Zustimmung der Betroffenen zulässig (z.B. Verschlüsselung, VPN).).

Vor der Übermittlung von personenbezogenen Daten ist der zuständige Jurist der ITSV zu befassen, welcher zu bestätigen hat, dass die Übermittlung zulässig ist.

Der Versand von Dateien via Email stellt eine Übermittlungsform dar, welche der einer Postkarte gleichkommt. Jedes Analyseprogramm im Datenstrom (z.B. Proxy, Emailserver, Firewall und auch diverse andere Geräte) ist in der Lage, diese Informationen (inkl. der Anhänge) zu lesen. Die Inhalte (inkl. aller Anhänge) werden oftmals zwischengespeichert und sind teilweise einer langjährigen Archivierung unterworfen. Oftmals enthalten die Office Dateien (Word, Excel, Powerpoint) auch Reste von vorherigen Entwurfstadien, sodass es ein Leichtes ist, die verschiedenen Versionen eines Dokumentes nachzuvollziehen. Ist die Versendung derartiger Dokumente (zwecks Weiterbearbeitung im Originalformat) daher nicht unbedingt erforderlich, ist die Umwandlung in ein PDF Dokument vorzunehmen, wobei in jedem Fall die Sicherheitsfeatures (zumindest ein Passwort zum Öffnen und eine Verschlüsselung) zu setzen sind. Informationen hiezu können von der Systemadministration erfragt werden. Werden die Dateien über ein sicheres Netz (verschlüsselte Dateiübertragung) versendet, ist eine Umwandlung in PDF jedoch nicht erforderlich.

6.6. *Kategorisierung von Daten und Aufgabengebieten*

Aus Gründen der Zweckmäßigkeit, Wirtschaftlichkeit und Sparsamkeit ist es sinnvoll, nicht für alle Daten- und Aufgabengebiete einen gleich hohen Aufwand (für die Datensicherheit) zu betreiben.

Insofern die Verarbeitung von personenbezogenen Daten betroffen ist, müssen diese Maßnahmen jedoch unter Berücksichtigung des Standes der Technik und der bei der Durchführung erwachsenden Kosten ein Schutzniveau gewährleisten, das den von der Verwendung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist. Unterstützung bei der Entscheidungsfindung kann jederzeit vom zuständigen Juristen der ITSV angefordert werden.

6.7. Auskunftserteilung gemäß § 26 DSG (an den Betroffenen betreffend die über ihn verarbeiteten Daten)

Zur Auskunftserteilung an den / die Betroffene/n gemäß § 26 DSG 2000 ist der jeweils zuständige Auftraggeber verpflichtet. Ein Auskunftsersuchen kann an die ITSV-GmbH hinsichtlich von „eigenen" Daten der ITSV oder Daten von Auftraggebern der ITSV-GmbH (wie beispielsweise des Hauptverbandes der VAEB und/oder anderer SVT, deren Daten für die die ITSV als Dienstleister Daten pflegt) betreffen.

Ein an die ITSV gestelltes Auskunftsbegehren gem. § 26 DSG über personenbezogene Daten des antragstellenden Betroffenen, welche durch die ITSV als Dienstleister für den HVB oder einen SVT verarbeitet werden, ist unverzüglich, möglichst noch am selben Tag – **über den zuständigen Juristen der ITSV-GmbH -** an die vom zuständigen Auftraggeber (HVB, SVT) namhaft gemachte Dienststelle, unter Beifügung der über den Antragsteller verarbeiteten Daten, weiterzuleiten.

Eine Auskunft gem. § 26 DSG über personenbezogene Daten des antragstellenden Betroffenen, welche durch die ITSV als Auftraggeber verarbeitet werden, ist - nach Auftragserteilung durch die Geschäftsführung - so rasch als möglich, jedenfalls jedoch innerhalb von 8 Wochen nach Einlangen des Auskunftsbegehrens (oder falls erforderlich nach Einzahlung des Kostenersatzes bzw. Konkretisierung des Auskunftsbegehrens) ausschließlich durch den zuständigen Juristen der ITSV nach folgenden Grundsätzen zu erteilen:

Eine Auskunft darf nur erteilt werden, wenn die Identität des Betroffenen in unbedenklicher Form festgestellt werden konnte. Auskünfte über Telefon, Telefax oder e-mail sind nur dann zulässig, wenn hiefür Sicherheitsvorkehrungen (Standleitungen, Rückruf, Verschlüsselungsverfahren, elektronische Signatur etc.) genützt werden. Die Auskunftserteilung ist hinsichtlich Form und Inhalt zu dokumentieren.

Auskünfte dürfen nur in folgenden Fällen gegeben werden:

- an den Betroffenen über die eigenen Daten
- an behördlich bestellte Vertreter auf Grund ausdrücklicher Bestellungsurkunden, Beschlüsse oder Aufträge,
- 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.

Die Auskunft ist so zu erteilen, dass bei durchschnittlichem Verständnis vom Betroffenen erwartet werden kann, er werde Inhalt und Aussage der Auskunft zweifelsfrei verstehen. Abkürzungen dürfen in der Auskunft verwendet werden, wenn erwartet werden kann, dass der Betroffene sie versteht oder wenn ihre Bedeutung dem Auskunftsschreiben zu entnehmen ist.

Wenn personenbezogene Daten auf Grund einer

- Standardanwendung (§ 17 Abs. 2 Z 6 DSG) oder
- Musterverordnung (§ 19 Abs. 2 DSG)

verwendet werden ist dem Betroffenen bei einer Anfrage nach § 26 DSG 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.

Das Auskunftsrecht umfasst auch Auskünfte aus Protokolldaten über Zugriffe auf Daten des Betroffenen, es sei denn es werden dadurch überwiegende Interessen des Auftraggebers oder eines Dritten bzw. öffentliche Interessen verletzt.

Eine Auskunft schließt auch Daten des Auskunftswerbers ein, die unter einem Ordnungsmerkmal eines Dritten (z. B. eines Dienstgebers, behandelnden Arztes) bzw. unter einem anderen Sachverhalt/Ordner gespeichert sind, soweit der Auskunftswerber einen geeigneten Hinweis zur Feststellung dieses Ordnungsmerkmales/Sachverhaltes gibt.

Von der Bearbeitung eines Auskunftsersuchens ist abzusehen, wenn der Betroffene nicht am Verfahren mitwirkt (d.h. beispielsweise die Datenverarbeitung nennt, in welcher möglicherweise Daten über ihn verarbeitet werden oder zumindest einen Sachverhalt schildert, aus dem geschlossen werden kann, in welcher Datenverarbeitung mit hoher Wahrscheinlichkeit Daten über den betroffenen Antragsteller verarbeitet werden). Auf diesen Umstand ist der Betroffene in einer Aufforderung zur Mitwirkung (Abs. 7, § 26 Abs. 4 DSG 2000) hinzuweisen. Als „Datenverarbeitung" sind in diesem Zusammenhang auch bloße Ordner zu verstehen in denen - sachbezogen – personenbezogene Daten verarbeitet werden.

Kostenersatz:
Auskünfte nach § 26 DSG 2000 sind unentgeltlich zu erteilen, wenn sie den aktuellen und direkt abfragbaren 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 19 € 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). Die Kosten sind vor Auskunftserteilung an den Betroffenen diesem durch das F/C der ITSV vorzuschreiben. Eine Barzahlung der Kosten ist nicht zulässig.

6.8. Übermittlungen / Auskunftserteilungen an Dritte

Eine Auskunftserteilung über personenbezogene Daten an Dritte außerhalb der ITSV-GmbH ist nur zulässig, wenn eindeutig die Berechtigung des Datenempfängers zum Empfang der Daten geklärt ist. Der Empfänger der Daten (eine natürliche Person) ist eindeutig zu identifizieren. Telefonische Auskünfte sind nur im Wege eines Rückrufes zu erteilen. Ausnahmsweise, wenn keine Bedenken hinsichtlich der Person des Anrufers und dessen Berechtigung, Auskünfte zu erhalten, bestehen, kann die Auskunft unmittelbar erfolgen. Die erfolgte Datenübermittlung (was, wann, warum und an wen) ist schriftlich oder automationsunterstützt festzuhalten und innerhalb der Löschungsfristen (=Skartierungsfristen) jederzeit abrufbar zu halten.

Officedokumente, welche personenbezogenen Daten enthalten, dürfen nur in Ausnahmefällen per eMail verschickt werden, wenn es die weitere Bearbeitung durch den Empfänger erforderlich macht. Sie sind in diesem Fall verschlüsselt zu übermitteln. Im Regelfall ist das Dokument vor dem Versand in Adobe PDF zu konvertieren, wobei in jedem Fall die Sicherheitsfeatures (zumindest ein Passwort zum Öffnen und eine Verschlüsselung) zu setzen ist. Werden die Dateien über ein sicheres Netz (verschlüsselte Dateiübertragung) versendet, ist eine Umwandlung in PDF jedoch nicht erforderlich. Müssen die Daten vom Empfänger weiterverarbeitet werden können, sind diese mit dem jeweiligen Programm (z.B. MS-Word) dokumentbezogen zu verschlüsseln.

6.9. Protokollierung von personenbezogenen Daten

Soweit dies unter Bedachtnahme auf § 14 Abs. 2 Schlusssatz erforderlich ist (Wirtschaftlichkeitsabwägung), sind gem. § 14 Abs. 2 Z 7 DSG 2000 vom Auftraggeber der Datenverwaltung (selbst oder über den beauftragten Dienstleister) Protokolle zu führen, um die tatsächlich durchgeführten Verwendungsvorgänge - wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollziehen zu können. Die Protokollierung ist so zu gestalten, dass auch Zugriffe der eigenen MitarbeiterInnen nachvollzogen werden können.

Eine Protokollierung von Übermittlungen solcher Daten, die im System verarbeitet werden, hat gem. § 14 Abs. 3 DSG so zu erfolgen, dass Anträge auf Auskunftserteilung gem. § 26 DSG entsprochen werden kann. Eine Protokollierung kann entfallen, wenn

- Daten auf Grund einer Standardanwendung (§ 17 Abs. 2 Z 6 DSG) oder Musterverordnung (§ 19 Abs. 2 DSG) verwendet werden (wie bei den Datenanwendungen, bei denen die ITSV-GmbH Auftraggeber ist (siehe Anlage A),
- Daten nach § 46 DSG für wissenschaftliche Forschung und Statistik verwendet werden oder
- Daten gesammelt als Grundlage gesetzlich vorgesehener konkreter weiterer Verwendungen (z.B. zur Vorbereitung von Wahlen nach § 45 Arbeiterkammergesetz) übermittelt werden.

Protokolle betreffend Datenanwendungen, deren Hauptzweck die Verarbeitung von personenbezogenen Daten darstellt, sind mindestens 11 Jahre und höchstens 31 Jahre in automationsunterstützt lesbaren Form aufzubewahren.

Protokoll- und Dokumentationsdaten dürfen nicht für Zwecke verwendet werden, die mit ihrem Ermittlungszweck – das ist die Kontrolle der Zulässigkeit der Verwendung des protokollierten oder dokumentierten Datenbestandes – unvereinbar sind. Unvereinbar ist insbesondere die Weiterverwendung zum Zweck der Kontrolle von Betroffenen, deren Daten im protokollierten Datenbestand enthalten sind, oder zum Zweck der Kontrolle jener Personen, die auf den protokollierten Datenbestand zugegriffen haben, aus einem anderen Grund als jenem der Prüfung ihrer Zugriffsberechtigung.

6.10. Benutzung von Endgeräten (PC, Notebooks, PDA, Mobiltelefone und ähnliches)

6.10.1. firmeneigene Endgeräte

Die Benutzung von Endgeräten für private Zwecke ist – ausgenommen es bestehen Einzelvereinbarungen (z.B. Dienstvertrag - Handynutzung) oder das Recht wird in gesonderten Dienstanweisungen erteilt, nicht gestattet. Insbesondere dürfen keine von dem Bereich Hardware nicht freigegebenen Anwendungen oder Programme installiert und betrieben werden.

Eine Ausnahme besteht nur für die private Nutung der gemäß dieser Dienstanweisung (korrekt bzw. entsprechend dieser Dienstanweisung) installierten Software auf den zur Verfügung gestellten Laptops für **rechtmäßige** Zwecke in der Freizeit. Dies allerdings nur unter der Voraussetzung, dass der Mitarbeiter den in dieser Dienstanweisung und allfälligen weiteren Dienstanweisungen und Betriebsvereinbarungen (bzgl. die Laptopverwendung) vorgesehenen Kontrollmaßnahmen ebenfalls akzeptiert. Die ITSV-GmbH hat jederzeit das Recht und die Pflicht den Laptop darauf zu überprüfen, ob dieser nur für rechtmäßige Zwecke benutzt wird. Nutzt der Mitarbeiter den Laptop daher auch für private Zwecke, nimmt er zu Kenntnis, dass er eine Überprüfung (auch allfällig angelegter privater Ordner/Dateien) nicht mit der Berufung auf das Datenschutzgesetz oder andere Persönlichkeitsrechte verweigern darf. Ist der Dienstnehmer mit der Überprüfung der privat genutzten Bereiche des Laptops nicht einverstanden, darf er den Laptop ausschließlich für berufliche und keinesfalls für private Zwecke nutzen.

Ausgenommen von den Einschränkungen dieser DA ist die Nutzung von Terminkalendersoftware im Rahmen der Büroautomatisierung (→Handy- SynchronisierungsSW).

Die Umgehung von Sicherheitseinstellungen (Virenschutz, Firewall usw.) ist (auch im Rahmen der erlaubten privaten Laptop Benutzung) keinesfalls gestattet und stellt eine grobe Dienstpflichtverletzung dar, welche auch ohne Abmahnung eine Entlassung rechtfertigt. Es wird auch ausdrücklich darauf hingewiesen, dass auf den Client-PCs im Netzwerk keine Serverdienste zu installieren und zu betreiben sind (z.B. Telnet-, FTP- oder WEB-Server).

Ein Handy darf nicht als Modem zum Zwecke der Umgehung der firmeneigenen Schutzeinrichtungen (z.B. Firewall) benutzt werden. Die Verwendung der firmeneigenen UMTS-Karte hat ausschließlich für dienstliche Zwecke zu erfolgen.

6.10.2. private Endgeräte

Die berufliche Verwendung von privaten Endgeräten (PC, Laptops) für Zwecke der ITSV-GmbH ist nicht gestattet.

6.11. Verwendung von nicht von der ITSV-GmbH zur Verfügung gestellter Software

Alle Programme auf den PCs unterliegen urheberrechtlichen Lizenzbestimmungen. Jedes Programm darf daher in der Regel mit einer Lizenz nur auf einem PC zur selben Zeit eingesetzt werden. Die Nutzung (d.h. auch das Kopieren bzw. die Vervielfältigung) von Programmen ohne zusätzliche Lizenz wird daher von Gesetzes wegen mit hohen Geld und mit Gefängnisstrafen geahndet.

Die Widerrechtliche Verwendung (Kopieren, aber auch bloßes Ablaufen lassen etc.) von Programmen kann der ITSV nicht nur einen nicht einzuschätzenden finanziellen sowie Image-Schaden zufügen, sondern seit in Kraft treten des Verbandsverantwortlichkeitsgesetzes mit 01.01.2006 auch zu einer strafrechtlichen Verurteilung der ITSV als juristischer Person führen. Eine strafrechtliche Verurteilung der ITSV kann wiederum zu einem Verbot an der Teilnahme von bestimmten Vergabeverfahren und auch – gerade wenn man den Aufgabenbereich der ITSV bedenkt - einen nicht wieder gutzumachenden Image-Schaden herbeiführen.

Neben der ITSV wird immer auch derjenige Mitarbeiter strafrechtlich (Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen) und auch zivilrechtlich (Abschöpfung von Bereicherungen, Lizenzzahlungen, Schadenersatz) verfolgt, der den Gesetzesverstoß verübt hat. Ebenso werden die verantwortlichen leitenden Angestellten der ITSV strafrechtlich verfolgt, wenn sie nicht ausreichende Maßnahmen ergriffen haben, um einen Verstoß von einem Bediensteten oder Beauftragten gegen immaterialgüterrechtliche Bestimmungen (d.h. „im Vorhinein") zu verhindern („Unterlassungsdelikt").

Das wissentliche Verwenden - das ist jede Art der Handhabung von Daten in einer Datenanwendung, also sowohl das Verarbeiten als auch das externe und interne Übermitteln von Daten - sowie das Installieren von Computerspielen und anderer nicht ausreichend lizenzierter bzw. technisch überprüfter Fremdsoftware, über E-Mail, Internet (WWW), Diskette, CD-ROM etc. ist daher ausdrücklich verboten.

Zur Vermeidung strafrechtlicher Konsequenzen werden daher stichprobenartig Überprüfungen der auf der firmeneigenen Hardware verwendeten Software/Lizenzen durchgeführt werden. Das Prüfungsergebnis ist mit der vom Systemadministrator zu führenden Liste (welcher Benutzer hat welche Lizenzberechtigungen) zu vergleichen.

Falls die dienstliche Notwendigkeit zur Installation von zusätzlicher Software besteht, so hat dies ausnahmslos nur über hiezu befugte Mitarbeiter der ITSV (oder mit deren ausdrücklicher Genehmigung) nach folgenden Richtlinien zu erfolgen.

Vor Installation ist die Software sowohl von rechtlicher (vom zuständigen Jurist) wie auch von technischer Seite (vom zuständigen Systemadministrator) freizugeben. Hiezu ist vom zuständigen Systemadministrator eine Liste der für die Verwendung auf den einzelnen Laptops genehmigten Softwarelizenzen zu führen. Auf dieser Liste ist auch die Genehmigung durch den zuständigen Juristen (samt dessen rechtlicher Begründung für die zulässige Verwendung der Lizenz) festzuhalten. Von der Systemadministration ist hiezu eine Aufstellung der auf der firmeneigenen Hardware (PCs der einzelnen Mitarbeiter und Server) installierten Software zu führen bzw. aktuell zu halten. Einzelne SW-Komponenten, wie z.B. Treiber, sind hievon nicht umfasst

Der Austausch von Lizenzen untereinander ist - ohne Genehmigung der Systemadministration (welche die entsprechenden Listen zu aktualisieren hat) - verboten.

Die Systemadministration ist berechtigt - generell oder einzelfallbezogen - technische Vorkehrungen zu treffen, die die Installation von nicht genehmigter Software verhindern.

Dem Benutzer ist nicht erlaubt, Geräte zu öffnen oder zu manipulieren. Das Öffnen des PC-Gehäuses und das Durchführen von Veränderungen an der PC-Hardware (z.B. Ein- bzw. Ausbau von Festplatten, Speicherbausteinen etc.) ist nur der Systemadministration erlaubt.

7. INTRA-/INTERNETAUFTRITT DER ITSV UND INFORMATIONSSERVER/-FOREN

Die ITSV betreibt einen zentralen Informations-Server bzw. diverse Foren, Gästebucher u.ä. und bietet die Möglichkeit, sich daran zu beteiligen und Form und Inhalt des Informationsraums eigenständig und eigenverantwortlich zu gestalten. Bei Etablierung eines derartigen Dienstes ist vom Leiter der inhaltlich zuständigen Organisationseinheit ein Foren/Gästebuch...- Verantwortlicher zu ernennen.

Die Inhalte des zentralen Informations-Servers haben mit dem gesetzlichen Aufgabenbereich der ITSV zu tun. Unzulässig ist jede Dateneinbringung, welche die öffentliche Ordnung und Sicherheit oder die Sittlichkeit gefährdet und daher geeignet ist, den Interessen der ITSV oder ihrem Ansehen in der Öffentlichkeit zu schaden oder die

gegen geltende Gesetze oder Verordnungen verstößt. Insbesondere betrifft dies auch die Beschimpfung und die Vernaderung/Verunglimpfung von anderen Personen. Im Fall von Verstößen hat der zuständige Foren/Gästebuch... - Verantwortliche der ITSV den Zugriff auf die betreffenden Inhalte mit sofortiger Wirkung sperren oder zu löschen. Hierüber ist auch der zuständige Jurist der ITSV zu informieren.

8. BEAUFTRAGTER FÜR DATENSCHUTZ UND DATENSICHERHEIT

Die Überwachung der Einhaltung dieser Sicherheitsvorschrift obliegt dem zuständigen Juristen der ITSV GmbH (als Datenschutzbeauftragtem), **der berechtigt ist, bei Gefahr im Verzug Abweichungen von dieser Sicherheitsvorschrift anzuordnen.** Diesen Anordnungen ist unverzüglich nachzukommen. Über die angeordneten Abweichungen ist von diesem unverzüglich der Geschäftleitung Bericht zu erstatten. Die Anordnungen sind schriftlich festzuhalten. Bestehende Betriebsvereinbarungen sind zu befolgen.

Dem Datenschutzbeauftragten obliegen insbesondere die Sammlung und Aktualisierung sämtlicher Sicherheitsregelungen, Risikoanalyse, Vorschläge für die Sicherheitsmaßnahmen, Auskunftserteilung für alle Mitarbeiter sowie die Kontrolle der Einhaltung der Sicherheitsanordnungen durch Stichproben im Rahmen der bestehenden Betriebsvereinbarungen. Die Dokumentation über alle Datensicherheitsmassnahmen ist mindestens 11 Jahre aufzubewahren.

Er hat dafür Sorge zu tragen, dass in die aktuelle Fassung dieser Datensicherheitsvorschrift jederzeit Einsicht genommen werden kann.

Auf Anforderung durch die Datenschutzkommission sind ihr diese Unterlagen zur Kenntnis zu bringen.

Die Mitarbeiter aller Bereiche sind verpflichtet, sich untereinander sowie den zuständigen Organisationsleiter auf allfällige Sicherheitsmängel aufmerksam zu machen und Verstöße gegen die Sicherheitsbestimmungen zu melden. Der Organisationsleiter leitet diese Informationen an den zuständigen Juristen der ITSV weiter.

9. SYSTEMADMINISTRATION

Die für die Systemadministration/Systembetreuung tätigen Mitarbeiter haben Ihre Aufgaben unter größtmöglicher Schonung der Privatsphäre der Mitarbeiter sowie Dritter durchzuführen.

Die Einschau auf zulässigerweise privat verarbeitete Dateien ist unzulässig. Inhaltliche Überprüfungen (darunter ist auch die Einschau in private Ordner zu verstehen, ohne dass Dateien geöffnet werden) sind ausschließlich auf Grundlage und im Rahmen dieser Dienstanweisung sowie der allenfalls bestehenden Betriebsvereinbarungen zulässig.

Aufgrund des Umfanges der Zugriffsmöglichkeiten der Mitarbeiter der Systemadministration ist in diesem Zusammenhang nochmals auf die bestehenden arbeitsrechtlichen und gesetzlichen Geheimhaltungsverpflichtungen (insbesondere bestehende Betriebsvereinbarungen sowie § 15 Datenschutzgesetz) zu verweisen, denen die Systemadministratoren unterliegen. Die Einsicht in personenbezogene Daten ohne Auftrag oder die Weitergabe von im Rahmen ihrer Tätigkeit gesammelten Daten/Informationen durch Systemadministratoren an andere Mitarbeiter (auch an ihre Vorgesetzten außerhalb deren im (unten angeführt) zu erstellenden Berechtigungskonzept festgelegten Zuständigkeiten) oder externe Personen außerhalb ihrer Dienstpflichten und unter Umgehung der oben angeführten Zulässigkeitsvoraussetzungen, stellt eine **schwere Dienstpflichtverletzung** dar, die – ausgenommen es lag ein besonderer technischer Notfall vor – je nach schwere des Falles zur fristlosen Entlassung des Systemadministrators führen kann.

Neben personenbezogenen Daten ist in diesem Zusammenhang insbesondere auch zu betonen, dass Zugriffsberechtigungen auf Berichte der Gremien der ITSV und der Sozialversicherung (HVB, SV-Träger) besonders sensibel zu gestalten sind und daher nur im unbedingt nötigem Ausmaß weitergeben bzw. Dritten (auch innerhalb der ITSV und der Sozialversicherung) zugänglich gemacht werden dürfen (Aufsichtsratsberichte, Berichte des Verbandsvorstandes, der Trägerkonferenz, PLAs, Informationen über Interna der Träger etc.)

Erstellung und Überwachung von Berechtigungskonzepten:

Jeder Systemadministrator hat, soweit auf von ihm verwaltete Daten/Fileordner/Applikationen Zugriffe auch von Dritten möglich sind, für die von ihm verwalteten Zugriffsmöglichkeiten ein Berechtigungskonzept zu erstellen und diese Zugriffsberechtigungen – auf nachweisliche Art und Weise - zu verwalten. Dazu gehört insbesondere auch - im Rahmen des wirtschaftlich sinnvollen - die Einführung von Überwachungsmechanismen, die gewährleisten, dass bei einem Wechsel von Aufgaben eines im Rahmen des Berechtigungskonzeptes zugriffsberechtigten Mitarbeiters die von diesem nicht mehr benötigten Zugriffsberechtigungen **unverzüglich gelöscht werden**.

Ist der Systemadministrator nur für die technische Durchführung, nicht aber für die inhaltliche Festlegung der Zugriffsverantwortlichkeiten zuständig (**„technischer Systemadministrator"**), hat der inhaltlich Verantwortliche (**„inhaltliche Systemadministrator"**) das Berechtigungskonzept zu erstellen. Der technische Systemadministrator hat die Zugriffsberechtigungen - ausschließlich wie im Berechtigungskonzept durch den inhaltlich Verantwortlichen festgelegt - zu verwalten. Im Zweifelsfall hält er vor Vergabe von Berechtigungen Rücksprache mit dem inhaltlichen Systemadministrator. Auch ein Zugriff des Vorgesetzten eines (technischen und/oder inhaltlichen) Systemadministrators ist nur im Rahmen des Berechtigungskonzeptes zulässig. Der technische Systemadministrator ist nur im Rahmen seiner technischen Zuständigkeiten dafür verantwortlich, dass Zugriffe im Rahmen der im Berechtigungskonzept festgelegten Regeln erfolgen und für das Aufzeigen von bestehenden Zugriffsmöglichkeiten an seinen Vorgesetzten, der hiefür den inhaltlichen verantwortlichen Systemadministrator bestimmt. Für die Einhaltung der übrigen Bestimmungen ist ausschließlich der inhaltliche Systemverantwortliche verantwortlich.

Das Berechtigungskonzept und dessen Überwachungsmechanismen sind vom inhaltlichen Systemadministrator mit dem für Datenschutz zuständigen Juristen abzustimmen, da dieser als Datenschutzbeauftragter die von ihm zu führende Liste der Datensicherheitsmaßnahmen zu erstellen und laufend zu ergänzen hat.

Diese Bestimmungen richten sich unmittelbar an den inhaltlichen und den technischen Systemadministrator (kann auch nur eine Person sein) und nicht an deren Vorgesetzte. Der zuständige Jurist hat jedoch diese Berechtigungskonzepte – nach Absprache mit dem zuständigen Bereichsleiter und Einholung der Stellungnahmen der übrigen betroffenen Bereichsleiter im Management-JF - zur Genehmigung der Geschäftsführung vorzulegen. In Folge hat er die unter Punkt 12 geführte Liste der Systemadministratoren laufend zu ergänzen und an alle Mitarbeiter zu kommunizieren. In dieser Liste ist zwischen dem inhaltlich verantwortlichen und dem bloß technisch verantwortlichen (durchführenden) Systemadministrator zu unterscheiden.

10. EXTERNE DIENSTLEISTUNGEN

Sollten technische Einrichtungen von Fremdfirmen implementiert, gewartet oder bei Anwenderschulungen benützt werden, und Personal dieser Firmen hierbei Zugriff auf personenbezogene Daten erlangen, so ist darauf zu achten, dass bereits vor Tätigkeitsaufnahme für den jeweiligen Zweck der Dienstleistung mit der Fremdfirma ein Dienstleistervertrag gemäß den §§ 10ff DSG abgeschlossen worden ist (Muster siehe Anlage D) und die konkret eingesetzten Dienstnehmer jeweils Geheimhaltungsverpflichtungserklärungen unterschrieben haben.

11. AUSLEGUNG

Bei Fragen betreffend die Auslegung der Bestimmung dieser Dienstanweisung ist von den Mitarbeitern – insbesondere bei Fragen betreffend die Handhabung von personenbezogenen Daten - der zuständige Jurist der ITSV vor Ergreifung der jeweiligen Maßnahme zu befassen.

12. ANSPRECHPARTNER UND SYSTEMADMINISTRATOREN

Aufgabengebiet	Name	E-Mail	
Rechtliche Fragen (zuständiger Jurist)	Christoffer Stiger	christoffer.stiger@itsv.at	
Beauftragter für den Datenschutz und Datensicherheit	Christoffer Stiger	christoffer.stiger@itsv.at	
Systemadministratoren			**verant-wortlich für:**
Schiffamtsgasse	Thomas Prommer	thomas.prommer@itsv.at	Technik
Kundmanngasse:			
PC (Arbeitsplätze):	Brigitte Reichel Herbert Schmahl Martin Zentner	Brigitte.Reichel@itsv.at Herbert.Schmahl@itsv.at Martin.Zentner@itsv.at	Technik
Serverbetrieb (z.B. Oracle-DB für ZPV):	Andreas Göbl Günther Nowotny Roman Machate Fritz Weisser Andreas Behal Martin Klein Igor Vukajlovic	Andreas.Göbl@itsv.at Günther.Nowotny@itsv.at Roman.Machate@itsv.at Fritz.Weisser@itsv.at Andreas.Behal@itsv.at Martin.Klein@itsv.at Igor.Vukajlovic@itsv.at	Technik
Mainframe-Betrieb (Z.B.: Versicherungsdatei)	Josef Veigl Hubert Ziegerhofer Joachim Kornfeld Wolfgang Egert	Josef.Veigl@itsv.at Hubert.Ziegerhofer@itsv.at Joachim.Kornfeld@itsv.at Wolfgang.Egert@itsv.at	Technik
Karriere-Postfach (Outlook)	Peter Zahradnik	Peter.Zahradnik@itsv.at	Inhaltlich

13. SCHLUSSBESTIMMUNG

Sollten einzelne Bestimmungen dieser Dienstanweisung unwirksam oder undurchführbar sein oder werden, so bleiben die anderen Teile davon unberührt.

Diese Dienstanweisung ist jederzeit im Outlook unter „Öffentliche Ordner - Alle Öffentlichen Ordner" im Unterverzeichnis "BV und Dienstanweisungen" in ihrer aktuellen Fassung einsehbar.

Diese Dienstanweisung tritt mit sofortiger Wirkung in Kraft.

(Hubert Wackerle) (Erwin Fleischhacker)

(Für die Geschäftsführung)

Anlagen:
A von der ITSV geführte Standardanwendung gem. Standard- u. Musterverordnung, BGBl. II Nr. 312/2004
B – Verpflichtungserklärung
C – Applikationsbeschreibung aus datenschutzrechtlicher Sicht
D – Muster für einen datenschutzrechtlichen Dienstleistervertrag:

Anlage A – von der ITSV geführte Standardanwendung gem. Standard- u. Musterverordnung, BGBl. II Nr. 312/2004

Die gesamte Personalverwaltung wird derzeit von der KPMG Niederösterreich durchgeführt. Eine Standard-Personalverwaltung und Buchhaltung/Rechnungswesen werden in SAP geführt und bedarf keiner Meldung an die DSK, da die Grenzen der entsprechenden DS-Standardanwendungen nicht überschritten werden. Folgende Standardanwendungen werden geführt:

SA001 Rechnungswesen und Logistik

SA002 Personalverwaltung für privatrechtliche Dienstverhältnisse

Anlage B – Verpflichtungserklärung

Verpflichtungserklärung für Dienstnehmer zur Einhaltung des Datengeheimnisses gemäß § 15 Datenschutzgesetz 2000 und zur Verschwiegenheit bezüglich sonstiger bekannt gewordener Daten sowie Dienst- und Amtsvorgänge (Punkt 8 des Dienstvertrages)

Diese Verpflichtungserklärung betrifft:

Familienname: _____ (in BLOCKSCHRIFT)

Vornamen: _____ (in BLOCKSCHRIFT)

1) VERPFLICHTUNGSERKLÄRUNG

Im Zuge Ihres Dienstverhältnisses erhalten Sie voraussichtlich Kenntnis über personenbezogene Daten (Personen und personenbezogene Umstände) und nicht personenbezogene Daten (Dienst- und Amtsvorgänge - insbesondere technische Daten betreffend interne und externe Hardware-/Softwarestrukturen sowie Rechtsbeziehungen mit Dritten).

Alle diese Daten sind absolut vertraulich zu behandeln und unterliegen den Vorschriften des österreichischen Datenschutzgesetzes sowie anderer rechtlicher Bestimmungen über die Geheimhaltungspflicht (Dienstvertrag, Strafgesetzbuch, Telekommunikationsgesetz, Amtsverschwiegenheit, Organhaftpflichtgesetz, § 460a ASVG bzw. § 231 GSVG bzw. § 219 BSVG etc.).

Aus einer Verweigerung der Ausführung eines Auftrages, der gegen das Datengeheimnis verstoßen würde, darf Ihnen kein Nachteil erwachsen (§ 15 Abs. 4 DSG).

Mit Ihrer Unterschrift verpflichten Sie sich daher:

- das Datengeheimnis gemäß den Bestimmungen des Datenschutzgesetzes i.d.g.F., insbesondere § 15 DSG (Datengeheimnis) zu wahren.
- zu absoluter Verschwiegenheit über alle, Ihnen anlässlich Ihrer Tätigkeit bekannt gewordenen, nicht von den zuständigen Organwaltern ausdrücklich als unbedenklich bezeichneten Daten (Dienst- und Amtsvorgänge).
- zur Einhaltung der Bestimmungen der Datenschutzverordnung des Hauptverbandes der österreichischen Sozialversicherung in der jeweils geltenden Fassung (http://www.sozdok.at/bin/sozserv/haupt?SID=1682240546)

Mit Ihrer Unterschrift verpflichten Sie sich weiters:

- unbefugten Personen oder unzuständigen Stellen die Kenntnisnahme von Daten, die Ihnen in Ausübung Ihres Dienstes bekannt geworden sind, nicht zu ermöglichen, sowie solche Daten nicht zu einem anderen als dem zum jeweiligen rechtmäßigen Aufgabenvollzug gehörenden Zweck zu verwenden.
- Automationsunterstützt oder manuell verarbeitete Daten, die Ihnen auf Grund Ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger Verschwiegenheitspflichten, nur auf Grund einer ausdrücklichen mündlichen oder schriftlichen Zustimmung eines der vertretungsbefugten Organe der ITSV GmbH oder einer von diesen bevollmächtigten Person zu verwenden.
- diese Verpflichtung auch nach Beendigung Ihres Mitarbeiterverhältnisses und dem Ausscheiden aus der Firma einzuhalten.

Sie nehmen durch Ihre Unterschrift zur Kenntnis,

- dass weiterreichende andere Bestimmungen über die Geheimhaltungspflicht von der oben angeführten Verpflichtung unberührt bleiben, sofern sie nicht mit dem Datenschutzgesetz im Widerspruch stehen,
- dass als Dienst- und Amtsvorgänge insbesondere jene zur Kenntnis gelangten Vorgänge zu verstehen sind, die dienstinterner Natur sind, oder die Rechte Dritter berühren;
- dass unter Daten nicht nur personenbezogene Daten, sondern auch nicht personenbezogene Daten - insbesondere über die technische Infrastruktur und den strukturellen Aufbau von Datenanwendungen – zu verstehen sind;

- dass Verstöße gegen die oben angeführte Verpflichtung zu entsprechender strafrechtlicher Verfolgung führen können, schadenersatzpflichtig machen und auch arbeitsrechtliche Folgen haben können (z.B. Entlassung gemäß § 27 Angestelltengesetz; Organhaftpflichtgesetz).

Wien, am

Unterschrift des Verpflichteten

Anlage C – Applikationsbeschreibung aus datenschutzrechtlicher Sicht

bsp_PL_ab1_200610 31_v0.1.doc	bsp_JU_ah1_200610 31_v0.1.doc	bsp_JU_ab3_200610 31_v0.1.doc	bsp_JU_ab2_200610 31_v0.1.doc

Diese Dokumente sind auch jederzeit im Outlook unter „Öffentliche Ordner - Alle Öffentlichen Ordner" im Unterverzeichnis "BV und Dienstanweisungen" in ihrer aktuellen Fassung einsehbar.

Anlage D – Muster für einen datenschutzrechtlichen Dienstleistervertrag:

Bestimmungen betreffend die Überlassung von Daten zum Zweck der Verarbeitung als Dienstleistung gemäß § 10 des Datenschutzgesetzes 2000, BGBl. I Nr. 165/1999 (DSG 2000):

[Beschreibung des Inhaltes der Dienstanweisung:
.....
.....
.....
.....*]*

Der Dienstleister verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der Aufträge des Auftraggebers zu verwenden und ausschließlich dem Auftraggeber zurückzugeben oder nur nach dessen schriftlichem Auftrag zu übermitteln. Desgleichen bedarf eine Verwendung der überlassenen Daten für eigene Zwecke des Dienstleisters eines derartigen schriftlichen Auftrages.

Der Dienstleister erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Wahrung des Datengeheimnisses im Sinne des § 15 DSG 2000 verpflichtet hat. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit dem Datenverkehr beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Dienstleister aufrecht. Die Verpflichtung zur Verschwiegenheit ist auch für Daten von juristischen Personen und handelsrechtlichen Personengesellschaften einzuhalten.
Der Dienstleister erklärt rechtsverbindlich, dass er ausreichende Sicherheitsmaßnahmen im Sinne des § 14 DSG 2000 ergriffen hat, um zu verhindern, dass Daten ordnungswidrig verwendet oder Dritten unbefugt zugänglich werden.

Der Dienstleister kann ein anderes Unternehmen nur nach Zustimmung des Auftraggebers zur Durchführung von Verarbeitungen heranziehen. Er hat den Auftraggeber von der beabsichtigten Heranziehung eines Subverarbeiters rechtzeitig zu verständigen. Außerdem muss ein Vertrag zwischen dem Dienstleister und dem Subverarbeiter im Sinne des § 10 DSG 2000 geschlossen werden. In diesem Vertrag hat der Dienstleister sicherzustellen, dass der Subverarbeiter dieselben Verpflichtungen eingeht, die dem Dienstleister auf Grund dieser Vereinbarung obliegen.

Der Dienstleister trägt für die technischen und organisatorischen Voraussetzungen Vorsorge, dass der Auftraggeber die Bestimmungen der § 26 (Auskunftsrecht) und § 27 (Recht auf Richtigstellung oder Löschung) DSG 2000 gegenüber dem Betroffenen innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen.

Der Dienstleister ist nach Beendigung der Dienstleistung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben bzw. in dessen Auftrag für ihn weiter vor unbefugter Einsicht gesichert aufzubewahren oder auftragsgemäß zu vernichten.

Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle der Datenverarbeitungseinrichtungen eingeräumt. Der Dienstleister verpflichtet sich, dem Auftraggeber jene Informationen zur

Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

Wien, am .....

Wien, am .....

für die ITSV-GmbH als Auftraggeber
die Geschäftsführung

für die ..... als Dienstleister

.....
(Name in Blockschrift)