Legal & Compliance

Datenschutz

ÖKK-Datenschutzweisung

Dokumenten-Nr.	03.0009_WS_Datenschutz
Autor	Dr. Alexander Lacher
Dokumenten-Eigner	Amann Angela (ÖKK)
Dokumenten-Bereich/Art	(03) Risk Management/Legal&Compliance/Governance/Weisung (WS)
Dokumenten-Status	(03) Freigegeben
Klassifizierung	ÖFFENTLICH (V1)
Geltungsbereich	ÖKK
Version	11.0
Gültig von	16.09.2013
Gültig bis (ohne Datum unbe-schränkt)	[Gültig bis]

Änderungs- und Freigabekontrolle (Versionsverlauf):

Version	Prüfstelle	Prüfdatum	Art der Änderung	Freigabestelle	Freigabe-datum
1.5	Dinner, Heinrich	16.09.2013	Anpassung Ref. Dok.	Dinner, Heinrich	16.09.2013
6.8	Dinner, Heinrich	15.04.2014	Review	Dinner, Heinrich	15.04.2014
7.3	Dinner, Heinrich	21.09.2016	Review & Anpassungen	Dinner, Heinrich	21.09.2016
8.0	Dinner, Heinrich	24.05.2018	Zusammenführung Weisung und Leitlinie Datenschutz sowie Review & Anpassung des neuen Dok	Dinner, Heinrich	24.05.2018
10.4	Heinz Patrick	24.10.2019	Review & Anpassungen	Heinz Patrick	24.10.2019

Verteiler:

Empfänger	Datum	Art der Mitteilung/Verteilung
Alle ÖKK-Mitarbeitenden	05.2018	Intranet
	04.2013	Intranet, physische Abgabe
	04.–12.2013	Schulungen, Rollout i.e.S.
Interessierte Öffentlichkeit	05.2018	Internet, BDSV (auf Anfrage)
	04.2013	Internet, BDSV (auf Anfrage)

Wo sich das vorliegende Reglement auf andere Weisungen oder Dokumente bezieht, sei zur besseren Übersicht das Verzeichnis aller Weisungen (Dokument 03.0000_WS_Weisungsverzeichnis) zu berücksichtigen.

Inhaltsverzeichnis

1 Einleitung

1.1 Ziel und Inhalt

Die vorliegende Weisung regelt die Grundsätze der Datenbearbeitung bei ÖKK. Sie definiert insbesondere die Organisation sowie die Aufgaben, Verantwortlichkeiten und Kompetenzen jener Personen, die für den Datenschutz bei ÖKK verantwortlich sind. Weiter soll mit dieser Weisung der Datenschutz betriebsintern in die Geschäftsabläufe eingebettet werden.

Der Datenschutz regelt die Sicherheit von Personendaten. Darunter versteht man alle Angaben (Daten), welche sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person beziehen bzw. dieser zugeordnet werden können. Es genügt, dass Personendaten, ohne einen Namen zu nennen, einer bestimmten Person zugeordnet werden können. Typische Beispiele für Personendaten bei einer Krankenversicherung sind Patientendaten wie etwa Name, Adresse, Nationalität, AHV-Nr., Geburtsdatum, Arbeitsort, Ausbildung, Beruf, Gesundheitsdaten oder die finanzielle Situation/Betreibungsinformationen.

ÖKK betrachtet den gesetzeskonformen und verantwortungsvollen Umgang mit Personendaten ihrer Versicherten/Kunden, Vertragspartner und Mitarbeitenden als Kernkompetenz.

Die Geschäftsleitung von ÖKK schafft mit dieser Weisung die Basis für den sorgsamen Umgang mit anvertrauten Gesundheits-, Versicherungs-, Personal- und administrativen Personendaten. Weiter werden insbesondere die zehn Grundsätze für die Bearbeitung personenbezogener Daten definiert.

Die ÖKK-Datenschutzweisung verdeutlicht die Werthaltung von ÖKK betreffend Datenschutz undsicherheit und konkretisiert die Anforderungen an die Datenschutzpolitik nach Art. 4 Abs. 2 Buchst. a der VDSZ.

1.2 Geltungsbereich

Diese Leitlinie gilt für ÖKK-Gruppe und all ihre Geschäftsbereiche. Sie ist für jede Datenbearbeitung verbindlich.

Das Bearbeiten von Personendaten umfasst jeden Umgang mit personenbezogenen Daten, wie das Beschaffen, Aufbewahren, Verändern, Verknüpfen, Bekanntgeben oder Vernichten. Dabei handelt es sich namentlich um das Bearbeiten von

- Gesundheits- und Versichertendaten
- Personaldaten von internen und externen Mitarbeitenden, inklusive Daten über Stellenbewerber und ehemalige Mitarbeitende
- Administrative Daten über Partner und Lieferanten, soweit Personendaten betroffen sind.

Der Schutz umfasst alle personenbezogenen Daten, die auf Papier oder in digitaler Form festgehalten sind oder mündlich geäussert werden.

Besonders strengen Vorschriften unterliegt die Bearbeitung von besonders schützenswerten Personendaten gemäss dem schweizerischen Datenschutzgesetz (DSG). Darunter versteht man Angaben, die den persönlichen Geheimbereich, insbesondere den seelischen, geistigen oder körperlichen Zustand eines Menschen betreffen. Auch so genannte Persönlichkeitsprofile sind besonders zu schützen. Sie ergeben sich aus einer Vielzahl von personenbezogenen Angaben, die sich zu einem Gesamtbild verdichten lassen, welches Rückschlüsse auf wesentliche Aspekte einer Persönlichkeit zulässt.

Für diese Leitlinie trägt der Betriebliche Datenschutzverantwortliche (BDSV) die Dokumentenverantwortung.

2 Die zehn Datenschutzgrundsätze von ÖKK

2.1 Achtung der Rechtsansprüche

ÖKK bearbeitet Gesundheits-, Patienten-/Versicherten-/Kunden-, Personal- und administrative Daten. Diese personenbezogenen Datenbearbeitungen bilden einen wesentlichen Aspekt unserer Versicherungstätigkeit. Da Personendaten naturgemäss sensibel sind, stehen sie unter besonderem gesetzlichen Schutz. Diesen Schutz gewährleistet ÖKK.

2.2 Sicherstellung der Persönlichkeitsrechte

Datenschutz bedeutet die Achtung der Privatsphäre und der Persönlichkeitsrechte aller Personen, von denen wir personenbezogene Daten erhalten, bearbeiten, weitergeben und aufbewahren. Die vorliegende Leitlinie bildet die Basis für alle Massnahmen und Aktivitäten im Bereich des Datenschutzes unter Achtung des Datenschutzgesetzes DSG.

2.3 Vertrauen verpflichtet

Versicherte/Kunden, Vertragspartner und Mitarbeitende schenken ÖKK ihr Vertrauen. Diesem Vertrauen fühlen wir uns verpflichtet und sorgen für Transparenz bei der Beschaffung und Bearbeitung personenbezogener Daten.

Die Daten unserer Versicherten umfassen neben administrativen Daten insbesondere medizinische Daten. Diese Daten bearbeiten wir nur insoweit und zu dem Zweck, als dass der Versicherte dazu sein Einverständnis gegeben hat oder das Gesetz dies vorschreibt oder erlaubt.

2.4 Datenschutzorganisation

Unser Betrieblicher Datenschutzverantwortlicher (BDSV) ist zuständig für den Datenschutz. Er erarbeitet Datenschutzvorschriften und kontrolliert deren Einhaltung. Er übt von Gesetzes wegen seine Funktion fachlich unabhängig aus, hat Zugang zu allen Datensammlungen und Datenbearbeitungen. Er führt eine Liste der Datensammlungen, welche der Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) auf Gesuch hin einsehen kann. Der BDSV überprüft die Bearbeitung der Personendaten und empfiehlt nötigenfalls Verbesserungsmassnahmen.

In gleicher Weise gewährleistet der Vertrauensärztliche Dienst (VAD) den sorgfältigen, datenschutzkonformen Umgang mit den für unsere Vertrauensärzte bestimmten Daten.

Schliesslich ernennt ÖKK sog. „Daten-Eigner“, welche für einzelne Datensammlungen und deren Sicherheit verantwortlich sind. Unter „Datensammlung“ versteht man Bestände von Personendaten über mehr als eine Person, die so aufgebaut sind, dass die Daten nach betroffenen (natürlichen und juristischen) Personen erschliessbar sind, z.B. über Namen, Mitarbeiter- oder andere Ordnungsnummern. Beispiele von Datensammlungen sind: Karteien, Archive, Listen, Adressbestände usw.. Alle Mitarbeitenden sind verpflichtet, neue Datensammlungen vor Inbetriebnahme dem BDSV zu melden.

Sämtliche Datensammlungen werden seitens ÖKK inventarisiert. Das Inventar dient der Ordnungsmässigkeit und der Gewährleistung der Auskunftsbereitschaft.

2.5 Interne Prozesse

Personendaten dürfen nur im Rahmen definierter Prozesse bearbeitet und weitergegeben werden. Zusätzlich bestehen Prozesse, die den Datenschutz gewährleisten und fördern. Alle von ÖKK

bearbeiteten Datensammlungen werden vom zuständigen Daten-Eigner dem BDSV gemeldet. Dieser untersucht die Daten und die zu ihrem Schutz ergriffenen Massnahmen darauf, ob sie den gesetzlichen Bestimmungen zum Datenschutz entsprechen.

Unsere Mitarbeitenden erhalten hinsichtlich ihrer Tätigkeit und der damit verbunden Verantwortung für den Datenschutz die entsprechende Sensibilisierung und Ausbildung.

2.6 Überwachung des Datenschutzes

Unsere Kader stellen sicher, dass die Datensicherheit gewährleistet ist. ÖKK ermutigt alle Mitarbeitenden, Verbesserungsvorschläge für den Datenschutz einzubringen.

Der BDSV führt regelmässig interne Prüfungen (sog. Audits) durch, welche durch externe Kontrollen ergänzt werden. Damit stellen wir sicher, dass wir die Vorschriften und Massnahmen zum Datenschutz und zur Datensicherheit einhalten und laufend verbessern.

2.7 Rechte unserer Versicherten/Kunden

Unsere Versicherten/Kunden haben ein umfassendes Recht darauf, dass ihre personenbezogenen Daten korrekt, zweckmässig, verhältnismässig, transparent, sicher und auf Basis einer rechtlichen Grundlage bearbeitet werden. Zudem müssen personenbezogene Daten jederzeit aktuell und richtig sein.

Von Gesetzes wegen haben unsere Kunden/Versicherten ein Einsichtsrecht in ihre Daten und können ein entsprechendes Auskunftsgesuch stellen. Solche Anfragen und Auskunftsgesuche können schriftlich und mit einer kurzen Begründung an folgende Stelle eingereicht werden:

ÖKK
Betrieblicher Datenschutzverantwortlicher
Bahnhofstrasse 13
7302 Landquart
datenschutz@oekk.ch

2.8 Unsere Verantwortung

Wir unternehmen alles, um Ihre Daten zu schützen und den datenschutzrechtlichen Anforderungen zu entsprechen. ÖKK-Mitarbeitende können auf diejenigen personenbezogenen Daten zugreifen, welche sie für ihre Arbeit unbedingt benötigen. Eine Weitergabe dieser Daten erfolgt nur an Personen und Stellen, die einen Auftrag zur Bearbeitung dieser Daten zu erfüllen haben.

Alle Mitarbeitenden sind zu Stillschweigen und zur Geheimhaltung verpflichtet. Missbräuche und rechtswidriges Verhalten werden geahndet.

2.9 Datensicherheit

ÖKK trifft gemäss den datenschutzrechtlichen Bestimmungen alle Vorkehrungen zum Schutz von Personendaten. Wir schützen diese Daten während des gesamten Bearbeitungs- und Aufbewahrungsprozesses durch angemessene technische und organisatorische Massnahmen.

Die Datensicherheit gewährleistet die Vertraulichkeit, die Verfügbarkeit und die Integrität der Daten einerseits bei der manuellen wie auch bei der elektronischen Bearbeitung andererseits auch in der Sicherstellung der Informationssicherheit im Bereich des Projektmanagements sowie im Umgang mit Mobilgeräten und/oder bei der Telearbeit.

2.10 Zertifizierung

Die Bemühungen im Bereich des Datenschutzes werden durch eine unabhängige Stelle geprüft. Ein entsprechendes Gütesiegel belegt den Datenschutz- und -sicherheitsstand von ÖKK. Für die Datenannahmestelle (DAS) und weitere besonders sensible Geschäftsbereiche wie den Vertrauensärztlichen Dienst (VAD) besteht eine zertifizierte Datenschutzmanagementsysteme welche kontinuierlich verbessert wird.

3 Grundsätze zum Umgang mit Personendaten

3.1 Übersicht

Die Mitarbeitenden von ÖKK beachten bei der Datenbearbeitung folgende Grundsätze:

Rechtliche Anforderung	Grundsatz
Zweck	Personendaten werden nur zum vorgesehenen Zweck bearbeitet. • Für den Zugriff auf Personendaten gilt das Prinzip „Need to Know“ - Zugriff nur, wenn zur Aufgabenerfüllung notwendig. • Personendaten werden nur so lange bearbeitet, wie es die gesetzlichen Grundlagen erlauben.
Legitimation	Personendaten werden bei ÖKK zur Erfüllung von gesetzlichen Aufgaben bearbeitet. Die Ermächtigung zur Bearbeitung von Personendaten ist durch verschiedene Rechtsgrundlagen gegeben: • Rechtmässigkeit (Art. 4 Abs. 1 DSG) • Rechtfertigungsgründe (Art. 13 DSG) Anwendbares Recht: • Im Bereich der Sozialversicherungen (obligatorische Versicherungen) gilt ÖKK als Bundesorgan gemäss Art. 3 lit. h DSG; die Bearbeitung der Personendaten erfolgt auf der Grundlage des KVG. • Im Bereich der privaten Krankenversicherung (überobligatorische Versicherungen) gilt ÖKK im Sinne des DSG als private Person; die Bearbeitung der Personendaten bedarf gemäss VVG der Einwilligung der betroffenen Personen, so im Rahmen der AVB, des Versicherungsantrags oder im Einzelfall in Absprache mit den Betroffenen. Die Legitimation muss auch gegeben sein bei: • Grenzüberschreitender Bekanntgabe (Art. 6 Abs. 1 DSG) durch angemessenen Schutz (Art. 6 Abs. 2 DSG) • Datenbearbeitung durch Dritte (Art 10a Abs. 2 DSG)
Beschaffung	Die Beschaffung der Daten erfolgt stets unter Einhaltung der: • Rechtmässigkeit, • dem Prinzip von Treu und Glauben und • der Verhältnismässigkeit. Ist die gesetzliche Grundlage der Beschaffung nicht ersichtlich, ist der Zweck

	der Datenbearbeitung anzugeben.
Verhältnismässigkeit	Verhältnismässigkeit bedeutet: • Verhältnismässigkeit der Bearbeitung (Art. 4 Abs. 2 DSG) • Zweckbindung (Art. 4 Abs. 3 DSG) • Festlegung und Änderung des Zwecks (Art. 3 Bst. i DSG) • Nutzungsbeschränkung
Transparenz	Datensammlungen werden inventarisiert. Das Inventar dient der Ordnungsmässigkeit und der Gewährleistung der Auskunftsbereitschaft. Transparenz ergibt sich aus: • Treu und Glauben (Art. 4 Abs. 2 DSG) • Erkennbarkeit (Art. 4 Abs. 4 DSG) • Informationspflicht (Art. 7a Abs. 1 DSG) Transparenz muss für jede Datenbearbeitung gewährleistet werden: • Nach VVG ist die betroffene Person über die Beschaffung solcher Daten zu informieren. • Im Bereich der Sozialversicherungen besteht die Berechtigung von Gesetzes wegen.
Datenrichtigkeit	Der Dateneigner vergewissert sich, dass Personendaten richtig, vollständig und aktuell sind (Art. 5 Abs. 1 DSG). Jede betroffene Person kann verlangen, dass unrichtige Daten berichtigt werden (Art. 5 Abs. 2 DSG).
Datensicherheit	Personendaten müssen während des gesamten Bearbeitungs- und Aufbewahrungsprozesses geschützt und durch angemessene technische und organisatorische Massnahmen gesichert werden(Art. 7 DSG). Datensicherheit wird erreicht durch: • Datenvertraulichkeit • Datenverfügbarkeit • Datenintegrität
Ausbildung/Sensibilisierung	Mitarbeitende erhalten hinsichtlich ihrer Verantwortung für den Datenschutz und ihrer Tätigkeit die entsprechende Sensibilisierung und Ausbildung. Sie erhalten Zugriff auf Dokumente, Formulare, Meldungen und Informationen zum Thema Datenschutz über die entsprechende Intranet-Seite.

3.2 Umgang mit Personaldaten

Personaldaten dürfen nur soweit bearbeitet werden, als dies aus betrieblichen Gründen, namentlich im Hinblick auf die ordnungsgemässe Durchführung des Arbeitsvertrags, notwendig ist (Art. 328b OR). Im Personaldossier werden sämtliche im Zusammenhang mit dem Arbeitsverhältnis stehenden Dokumente aufbewahrt. Dort werden ebenfalls die schriftlichen Resultate von Mitarbeitergesprächen abgelegt.

ÖKK führt für jeden Mitarbeitenden ein Personaldossier, das entsprechend geschützt ist. Darauf Zugriff haben neben den mit der Führung des Dossiers beauftragten Personen (Personalbereich und Vorgesetzter) nur der BDSV.

Die betroffenen Personen selbst haben volles Einsichtsrecht. Das parallele Führen inoffizieller ("grauer") Personaldossiers, die den betroffenen Personen nicht zugänglich sind, ist untersagt.

3.3 Verpflichtung auf Datenschutz

Mitarbeitende werden im Rahmen des Arbeitsvertrags auf den Datenschutz verpflichtet. Vorgaben betreffend Datenschutz und Datensicherheit werden, abhängig von der Tätigkeit, in angemessener Weise in die Anstellungsverträge aufgenommen. Die Verpflichtung wird nachweisbar dokumentiert und im Personaldossier abgelegt.

3.4 Klassifizierung von Personendaten

Personendaten werden entsprechend den gesetzlichen Vorgaben und den Bedürfnissen von ÖKK klassifiziert. Die Klassifizierung erfolgt aufgrund des Schutzbedarfs der Daten durch den Dateneigner. Sie ist bei ÖKK in der Klassifizierungsweisung [03.0011] geregelt.

Der Schutz dieser Daten wird dabei auf den gesamten Prozess der Bearbeitung angewendet.

Der Mitarbeitende hat sich an die bestehenden Klassifizierungsstufen zu halten. Bei Unklarheiten kontaktiert er den Dateneigner oder den BDSV.

3.5 Inventarisierung

Datensammlungen werden durch den zuständigen Dateneigner inventarisiert. Zusätzlich identifiziert er die zur Bearbeitung der Daten benötigten Prozesse und Systeme. Alle diese datenschutzrelevanten Objekte dokumentiert er im Inventar und beschreibt sie wie folgt:

1. Bezeichnung der Objekte;
2. Zweck dieser Objekte;
3. Bezeichnung der Datenträger;
4. Kurz-Beschreibung der verwendeten Bearbeitungsmittel und -methoden;
5. Kurzbeschreibung zur Datensicherheit;
6. Kreis und ungefähre Anzahl der betroffenen Personen;
7. Kategorien der personenbezogenen Daten;
8. Kategorien derjenigen Stellen, die Daten eingeben oder verändern können;
9. Kategorien der Datenempfänger;
10. Datenherkunft;
11. Angaben zur Datenweitergabe;
12. Angaben zur Datenaufbewahrung und Löschung.

Anhand des Inventars erstellt der BDSV die Liste der Datensammlungen und Datenbearbeitungen. Er erhält damit einen Überblick, welche Daten wo bearbeitet werden und kann Bestand, Mutationen und Löschungen der Datensammlungen überwachen.

Die Inventarliste der Datensammlungen ist auf dem Intranet einsehbar. Externen wird diese bei begründetem Interesse zur Verfügung gestellt.

4 Datensammlung

4.1 Verantwortung

Für die einzelnen Datensammlungen werden Dateneigner ernannt. Dateneigner stellen die Einhaltung der datenschutzrechtlichen Anforderungen in technischer und organisatorischer Hinsicht sicher. Sie bestimmen die zum Bearbeiten der Daten befugten Personen und deren Zugriffrechte nach dem Need-to-know-Prinzip.

4.2 Bearbeiten von Datensammlungen

Grundsätzlich muss ein Mitarbeitender vom Dateneigner zur Bearbeitung einer Datensammlung autorisiert werden.

Bearbeitet ein Mitarbeitender eine Datensammlung, so muss er bei folgenden Tätigkeiten Rücksprache beim dafür verantwortlichen Dateneigner nehmen:

- Erstellung einer neuen Datensammlung, die aufgrund neuer Daten angelegt wird.
- Erstellung einer neuen Datensammlung, die aus der Kombination oder einer limitierten Sicht bestehender Daten entsteht.
- Übertragung einer bestehenden Datensammlung auf ein neues Medium (z.B. Übertragung einer sog. „Papierdatensammlung" auf einen PC).
- Vollständige und unwiederbringliche Zerstörung der Datensammlung.

Bei Zweckänderungen bestehender Datensammlungen ist zwingend der BDSV beizuziehen.

Eine vollständige und unveränderte Kopie einer bestehenden Datensammlung darf der Mitarbeitende anlegen, falls dies für seine Arbeitstätigkeit nötig ist.

4.3 Bearbeitungsreglemente

Für automatisierte Datensammlungen, die besonders schützenswerte Daten und Persönlichkeitsprofile enthalten, Dritten zugänglich gemacht werden oder mit anderen Datensammlungen verknüpft sind, ist ein Bearbeitungsreglement zu erstellen, wobei dieses auch als Handbuch oder Richtlinie ausgestaltet sein kann.

Das Bearbeitungsreglement dient als eigentliche Grundlage für den gesetzeskonformen Betrieb bzw. die gesetzeskonforme Nutzung einer Datensammlung. Das Reglement beinhaltet Angaben über die interne Organisation von ÖKK sowie über die Struktur, in der die Datensammlung oder das automatisierte Bearbeitungssystem eingebettet ist. Es beschreibt die Datenbearbeitungs- und Kontrollprozeduren und enthält alle Unterlagen über die Planung, Realisierung und den Betrieb der Datensammlung und der eingesetzten IT-Systeme. Es regelt namentlich Art und Umfang der Zugriffsberechtigung auf Personendaten.

Das Reglement muss regelmässig überprüft, angepasst und nachgeführt werden. Anpassungen sind dem BDSV zu melden und dem EDÖB in verständlicher Form jederzeit zur Verfügung stehen.

Ein Bearbeitungsreglement kann für mehrere Datensammlungen gültig sein, wenn es tatsächlich für die bezeichneten Datensammlungen zur Anwendung gelangt und für jede betreffende Datensammlung die notwendigen Anforderungen erfüllt.

Das Bearbeitungsreglement ist den interessierten Personen mittels Publikation auf dem Internet oder in anderer Form zugänglich zu machen.

4.4 Meldepflichten

4.4.1 Interne Meldepflichten

Der interne Mitarbeitende hat neue Datensammlungen vor deren Eröffnung dem BDSV zu melden.Von dieser internen Meldepflicht ausgenommen sind Datensammlungen, die auf eine Zeit von weniger als sechs Monaten und allein zum Zwecke angelegt werden, später einmal in eine endgültige Datensammlung integriert zu werden (bspw. eine Gästeliste für einen Apéro, die später in die Datensammlung „Gönner" integriert wird).

Systematische Veränderungen an der Datensammlung oder bei der Datenbearbeitung, bspw. Bearbeitung zusätzlicher Datenkategorien, Änderungen des Bearbeitungszwecks oder auch das Löschen von Datensammlungen, hat der Mitarbeitende dem BDSV zu melden.

4.4.2 Externe Meldepflichten

Die externe Meldepflicht fällt weg, da der BDSV beim EDÖB gemeldet ist.

4.5 Anonymisierung

Personendaten gelten als anonymisiert, wenn diejenigen Daten entfernt wurden, welche die Identifizierung der betroffenen Person ermöglicht hätten.

Dürfen Personendaten einer bestimmten oder bestimmbaren natürlichen Person nicht mehr zugeordnet werden können (bspw. zu Testzwecken oder zum Führen von Statistiken), so hat der Mitarbeitende diese zu anonymisieren.

4.6 Pseudonymisierung

Bei der Pseudonymisierung handelt es sich um das Verändern von personenbezogenen Daten durch eine Zuordnungsvorschrift (z.B. die Verwendung von Pseudonymen). Dadurch können die Einzelangaben über persönliche oder sachliche Verhältnisse ohne Kenntnis oder Nutzen der Zuordnungsvorschrift nicht mehr einer bestimmten natürlichen Person zugeordnet werden.

Nur, wenn die Möglichkeit zur Identifizierung beibehalten werden muss, sind diese zu pseudonymisieren. Welche Identifikationsmerkmale der Mitarbeitende zu entfernen bzw. zu verändern hat, um die Bestimmbarkeit des Betroffenen auszuschliessen, hängt vom Einzelfall ab und ist in Zusammenarbeit mit dem Dateneigner oder dem BDSV festzulegen.

ÖKK muss die Personalien der Versicherten zur Aufbewahrung der diagnosebezogenen Daten pseudonymisieren. Die Aufhebung der Pseudonymisierung darf nur durch die Vertrauensärztin oder den Vertrauensarzt erfolgen (Art. 59 Abs. 1ter KVV).

Personenbezogene Daten, die so verändert werden, dass sie nicht mehr oder nur mit einem unverhältnismässig grossen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren Person zugeordnet werden können, unterliegen den Anforderungen des Datenschutzes nicht mehr.

4.7 Aufbewahrung und Archivierung

Generell müssen Personendaten so aufbewahrt und archiviert werden, dass Unbefugten keine Einsicht möglich ist. Dies wird durch geeignete Vorkehrungen realisiert. So muss bspw. das Aufbewahren von Personendaten in Papierform in abschliessbaren Räumen und Behältnissen erfolgen.

Der Dateneigner legt die Dauer der Aufbewahrung nach der Art der Personendaten fest. Bei der Festlegung der Aufbewahrungsdauer richtet er sich nach den gesetzlichen Vorgaben, die in der DSMS-Weisung [03.0015] sowie insbesondere in der Weisung Legal & Compliance dokumentiert sind.

4.8 Vernichtung

Papierunterlagen mit personenbezogenen Daten hat der Mitarbeitende mittels Aktenvernichtern zu entsorgen. Wo dies nicht möglich ist, sind diese Papierdokumente in geschlossenen, zugangskontrollierten Räumen zu lagern, bis die endgültige Vernichtung erfolgen kann.

Die endgültige Vernichtung des geshredderten Schriftguts sowie der zwischengelagerten Papierdokumente erfolgt durch die Logistik unter Aufsicht in der Verbrennungsanlage.

Der kompletten Löschung eines Versicherten-Dossier kann nur erfolgen, wenn die betroffene Person über mögliche rechtliche Konsequenzen, vorab der daraus resultierenden Beweislosigkeit in einem möglichen Streitfall, aufmerksam gemacht wurde. Die Löschung erfolgt nur auf ausdrücklichen Wunsch der betroffenen Person und nur im gesetzlich zulässigen Rahmen. Massgebend ist primär die schweizerische Gesetzgebung. Besteht weiterhin ein Versicherungsverhältnis, so müssen die Stammdaten sowie sämtliche notwendige Angaben pendenter Leistungsverarbeitungen zwecks Abwicklung des Versicherungsgeschäftes sowie Angaben des Rechnungswesen und/oder der Inkassoabteilung bestehen bleiben.

5 Datenbearbeitung durch Dritte (Outsourcing)

Gemäss Art. 84 KVG ist die ÖKK als mit der Durchführung der sozialen Krankenversicherung betrautes Organ befugt, Personendaten, einschliesslich besonders schützenswerter Daten und Persönlichkeitsprofile, durch Dritte bearbeiten zu lassen. Generell besteht die Möglichkeit des Outsourcings, solange keine vertraglichen oder gesetzlichen Geheimnispflichten dem entgegenstehen.

Bei der Bearbeitung von Personendaten durch Dritte, die sogenannten Outsourcingnehmer, sind stets die massgeblichen Anforderungen des DSG, insbesondere Art. 10a DSG, zu berücksichtigen. Art. 10a DSG statuiert, dass der Outsourcingnehmer die Daten nur so bearbeiten darf, wie es die ÖKK selbst es tun dürfte und dass sich die ÖKK zu vergewissern hat, dass der Outsourcingnehmer die Datensicherheit gewährleistet.

Daraus ergeben sich folgende verbindlichen Vorgaben für eine Beauftragung eines Dritten seitens ÖKK:

- Generell darf der Dritte Daten nur so bearbeiten, wie es ÖKK selber dürfte und keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet. Eine Datenbearbeitung, die unrechtmässig ist, bleibt auch dann unrechtmässig, wenn sie durch Dritte vorgenommen wird.
- ÖKK bleibt Inhaberin der Datensammlung und trägt weiterhin die volle datenschutzrechtliche

  Verantwortung für die ausgelagerte Datenbearbeitung.
- Auch bei Outsourcing von Datenbearbeitungen bleibt die gesetzliche Auskunftspflicht von ÖKK als Inhaberin der Datensammlung gegenüber betroffenen Personen bestehen. Es ist sicherzustellen, dass die ÖKK trotz Auslagerung ihrer Auskunftspflicht jederzeit nachkommen kann.
- ÖKK ist dafür verantwortlich, dass der Outsourcingnehmer die Datensicherheit gewährleistet.
- ÖKK lässt grosse Sorgfalt walten bei der Auswahl, der Instruktion und der Überwachung eines Outsourcingnehmers. Die ausgelagerte Funktion ist zudem in das interne Kontrollsystem von ÖKK zu integrieren.
- Die Datenbearbeitung durch Dritte muss stets in einem schriftlichen Vertrag (Outsourcing-Vertrag)

  geregelt sein. Schnittstellen, Verantwortlichkeiten, Zuständigkeiten und Haftungsfragen sind vertraglich zu regeln.
- Im Outsourcing-Vertrag und mit internen Massnahmen ist sicherzustellen, dass bei einem unerwarte-

ten Ausfall des Outsourcingnehmers (z. Bsp. aufgrund ausserordentlicher Kündigung oder Einstellung der Geschäftstätigkeit) einerseits die Datensicherheit gewährleistet bleibt und andererseits der ÖKK und ihren Kunden keine übermässigen Schäden entstehen.

Das Vertragsverhältnis mit dem Dritten (Outsourcing-Vertrag) ist so zu gestalten, dass die Einhaltung der oben dargestellten Grundsätze sichergestellt ist. Im Einzelnen soll ein Outsourcing-Vertrag folgende Punkte eindeutig, vollständig und unmissverständlich regeln:

- Bezeichnung der Vertragspartner (Name, Rechtsform, Anschrift, Vertreter).
- Gegenstand des Datenbearbeitungsauftrages.
- Genaue Umschreibung des Zwecks und der Aufgaben (Datenbearbeitungen), die der Outsourcingnehmer zu erfüllen hat. Der Outsourcingnehmer muss verpflichtet werden, die Daten ausschliesslich zweck- und weisungsgebunden zu verwenden, womit die Verwendung der Daten für eigene Zwecke des Outsourcingnehmers oder fremde Zwecke ausgeschlossen wird.
- Statuierung, dass ÖKK alleiniger „Eigentümer"/Berechtigter an den zur Verfügung gestellten und

  bearbeiteten Daten bleibt und Klärung der Eigentums- und Nutzungsverhältnisse bezüglich der eingesetzten Hard- und Software.
- Ort der zu erbringenden Leistung (insbesondere eindeutige Abgrenzung zur Datenbearbeitung im Ausland).
- Fixierung der Sicherheitsstandards für den Datenaustausch und die Sicherheitsanforderungen, die der Outsourcingnehmer bei der Datenbearbeitung zu erfüllen hat.
- Genaue Beschreibung der Datenschutzmassnahmen, die der Outsourcingnehmer umzusetzen hat, und wie er dies sicherstellen und nachweisen wird. Der Outsourcingnehmer muss jederzeit gewährleisten und nachweisen können, dass er die im Auftrag der ÖKK bearbeiteten Daten und die dafür eingesetzten Systeme mittels technischer, personeller und organisatorischer Massnahmen angemessen gegen unbefugten Zugriff, unbefugtes Bearbeiten und Verlust schützt
- Statuierung, dass der Outsourcingnehmer sich strikt an die Weisungen von ÖKK zur Datenbearbeitung zu halten hat. Dies beinhaltet insbesondere auch das Recht von ÖKK zur Weisung, die Daten an die ÖKK herauszugeben oder die Daten unwiederherstellbar zu vernichten.
- Die weisungsberechtigten Personen von ÖKK und die Kontaktpersonen seitens des Outsourcingnehmers sind zu bestimmen.
- Berichterstattungspflicht des Outsourcingnehmers: einerseits periodisch, anderseits unverzüglich bei Unregelmässigkeiten, Störungen, besonderen Vorfällen und Verdacht auf Datenschutzverletzungen.
- Pflicht der ÖKK, sich zu vergewissern, dass der Outsourcingnehmer die notwendigen Sicherheitsstandards einhält und tatsächlich anwendet, und daraus abgeleitet das Recht der ÖKK, beim Outsourcingnehmer jederzeit Überprüfungen durchzuführen und Einsicht zu nehmen, um die Einhaltung der gesetzlichen Datenschutzvorschriften und der vertraglichen Regelungen zu überprüfen („Right-to-Audit Clause"). Beschreibung der Tiefe und Breite solcher Überprüfungen, ihrer Kostenfolgen und der Modalitäten ihrer Durchführung.
- Verbot des Anfertigens von Kopien durch den Outsourcingnehmer, ausser zum Zweck der Datensicherung im vertraglich vereinbarten Umfang.
- Schriftliche Verpflichtung der Mitarbeitenden des Outsourcingnehmers zur Geheimhaltung sowie zur Einhaltung der gesetzlichen Datenschutzvorschriften.
- Modalitäten der Änderung von wesentlichen Vertragsbestandteilen, z.B. Vorgehen bei Tests und

Freigabe von Änderungen der Datenbearbeitungsverfahren, technischer und organisatorischer Datenschutzmassnahmen.

- Gegebenenfalls Laufzeiten und Kündigungsfristen der Datenbearbeitung, Voraussetzungen und Vorgehensweise zu ordentlicher und fristloser Kündigung. Es ist vertraglich festzuhalten, dass die Verletzung datenschutzrechtlicher Pflichten durch den Outsourcingnehmer die ÖKK zu einer ausserordentlichen Vertragskündigung berechtigt.
- Verpflichtung von ÖKK und Outsourcingnehmer zu einer kontrollierten Rückabwicklung und

  Beendigung der Datenbearbeitungen durch den Outsourcingnehmer (vor und nach Vertragsende), auch im Falle einer ausserordentlichen Kündigung.
- Ausschluss des Einsatzes von Unterauftragnehmern des Outsourcingnehmers. Soll der Einsatz von Unterauftragnehmern zugelassen werden, so sind die obigen Punkte auch für jeden einzelnen Unterauftragnehmer eindeutig, vollständig und unmissverständlich zu regeln.

ÖKK ist verpflichtet, die Versicherten über das Outsourcing bzw. den Beizug Dritter bei der Datenbearbeitung hinreichend zu informieren.

6 Datenbearbeitung für Dritte (Insourcing)

ÖKK bearbeitet Personendaten im Rahmen der Abwicklung der obligatorischen Krankversicherung für andere Krankenversicherer (Partnerversicherungen) in Anwendung von Art. 84 KVG, welche diese Bearbeitungen vertraglich an ÖKK übertragen haben. Zudem bearbeitet ÖKK Leistungsabrechnungen im Auftragsverhältnis auch für Versicherungsunternehmen ausserhalb des Bereiches der obligatorischen Krankenversicherungen. In diesen vertraglich geregelten Fällen von Datenbearbeitung für Dritte ist somit ÖKK in der Position des Outsourcingnehmers.

Sowohl bei der Beauftragung durch eine Tochtergesellschaft der ÖKK Holding AG als auch bei einer Beauftragung durch ein aussenstehendes Unternehmen sind die für die Datenbearbeitung durch Dritte geltenden Anforderungen zu erfüllen. Die im vorhergehenden Abschnitt „Datenbearbeitung durch Dritte (Outsourcing)“ statuierten Pflichten des Outsourcingnehmers finden sinngemäss Anwendung.

Alle Verträge, in welchen ÖKK als Outsourcingnehmer auftritt, sind aus Beweis- und Dokumentationsgründen schriftlich zu abzuschliessen. Dabei kann auf diese Weisung verwiesen werden.

Für die an sie übertragenen Bearbeitungen von Personendaten ist ÖKK für die Einhaltung der Informationspflicht gemäss Art. 14 DSG verantwortlich.

Sämtliche Pflichten, die in dieser Datenschutzweisung Mitarbeitenden der ÖKK auferlegt werden, gelten sinngemäss auch, wenn die betreffenden Mitarbeitenden im vertraglichen Rahmen Datenbearbeitungs-Dienstleistungen für Partnerversicherungen erbringen.

7 Auskünfte

7.1 Auskunftspflicht

Die von der Datenbearbeitung betroffenen Personen haben das Recht, über alle ihre Daten Auskunft zu verlangen. Die versicherte Person hat – unabhängig von einem Interessensnachweis – jederzeit das Recht, eine Kopie des gesamten Dossiers von ÖKK zu erhalten. Zudem kann sie eine Berichtigung unrichtiger Daten verlangen.

ÖKK muss deshalb allen betroffenen Personen Auskunft bzw. Einsicht in deren Daten entsprechend den gesetzlichen Vorgaben erteilen können. Der BDSV muss die termingerechte und korrekte Beantwortung von Auskunftsbegehren sicherstellen.

7.2 Auskunftsgesuche

Auskunftsgesuche erfolgen grundsätzlich schriftlich.

Elektronische Auskunftsgesuche sind zulässig, wenn die Identität der fragenden Person zweifelsfrei festgestellt werden kann.

7.3 Auskunftspflichtige Stellen

Je nach auskunftsbegehrender Person erteilen folgende Stellen Auskunft:

1. Versicherte und Externe wenden sich an den BDSV.
2. Mitarbeitende: Anfragen von Mitarbeitenden sind an die Personalabteilung zu richten.

7.4 Auskunftserteilung i.e.S.

Die auskunftspflichtige Stelle prüft das Begehren kontaktiert den zuständigen Dateneigner.

Auskünfte über Daten von Verstorbenen dürfen nur erteilt werden, wenn der Gesuchsteller sich mittels Erbenschein identifizieren kann.

Der BDSV lässt die Dateneigner alle Daten identifizieren, die über die betroffene Person vorhanden sind. Hierzu wird eine Kopie des gesamten Dossiers und/oder ein Ausdruck der entsprechenden Daten erstellt und an die betroffene Stelle gesandt.

Die Personalabteilung muss jede Auskunft dem BDSV nach dem folgenden Schema mitteilen: Wer hat welche Daten wem, wann (Datum) und in welcher Form (schriftlich, telefonisch etc.) herausgegeben? Der BDSV sammelt diese und seine eigenen Meldungen und bewahrt sie auf.

Die Auskunft oder der begründete Entscheid über die Beschränkung des Auskunftsrechts erfolgt innert 30 Tagen. Falls diese Frist nicht eingehalten werden kann, wird dem Gesuchsteller die Frist mitgeteilt, bis wann er die Auskunft erhält.

Grundsätzlich erteilt ÖKK Auskünfte in Schriftform (Ausdrucke, Fotokopien). ÖKK kann die betroffene Person ihre Daten auch an Ort und Stelle einsehen lassen. Elektronische Auskunftserteilungen sind zulässig, wenn die persönlichen Daten der betroffenen Person vor dem Zugriff unberechtigter Dritter geschützt sind. Die Auskunft kann auch mündlich (namentlich telefonisch) erteilt werden, wenn die betroffene Person eingewilligt hat und durch den Auskunftserteilenden eindeutig identifiziert worden ist.

Grundsätzlich ist die Auskunftserteilung kostenlos. Über Ausnahmen entscheidet der BDSV.

7.5 Auskunftserteilung gegenüber EDÖB

Dem EDÖB muss der BDSV auf Anfrage Auskunft über diejenigen Datensammlungen geben, in denen regelmässig besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeitet oder aus denen regelmässig Personendaten an Dritte bekannt gegeben werden.

8 Weitergabe von Personendaten

8.1 Innerhalb von ÖKK

Innerhalb derselben juristischen Person dürfen Mitarbeitende Personendaten einander bekanntgeben, falls dies zur Erfüllung der beruflichen Aufgabe notwendig ist.

Die Datenbekanntgabe unter Gesellschaften der ÖKK-Gruppe richtet sich nach Ziff. 4 dieser Weisung (Datenbearbeitung durch Dritte [Outsourcing]).

8.2 An Dritte im Inland

Die Weiterleitung und Weitergabe von Personendaten an Dritte erfolgt in der Regel durch automatisierte und genehmigte Prozesse.

Bei nicht-standardisierten Prozessen muss der jeweilige Datenbearbeiter vor der Weitergabe von Personendaten an Dritte (wie Behörden, Versicherungen, Polizei, Staatsanwaltschaften) beim BDSV eine Bewilligung einholen.

Der BDSV prüft, ob die Weitergabe zulässig ist und ob die Datensicherheit bei der Übermittlung ausreichend ist. Im Zweifelsfall muss die betroffene Person ihre Einwilligung erteilen.

8.3 An Dritte im Ausland

Die Übermittlung von einzelnen Personendaten oder Datensammlungen ins Ausland unterliegt besonders strengen gesetzlichen Auflagen. Besteht die Notwendigkeit einer Datenübermittlung ins Ausland, ist vorgängig der BDSV beizuziehen. Auskunftsbegehren und Akteneinsichten werden gemäss Weisung Legal & Compliance gehandhabt.

Grundsätzlich wird festgehalten, dass keine Daten ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Person schwerwiegend gefährdet wird. Massgebend sind primär die Voraussetzungen nach Art. 6 DSG. Daten werden generell nur in sichere Staaten abgegeben. ÖKK orientiert sich dabei an der Liste des EDÖB resp. nach dem Swiss-US Privacy Shield.

8.4 Anforderungen an Auskunft und Weitergabe

Der BDSV bestimmt bei Unklarheiten die Art (schriftlich, mündlich, elektronisch, automatisiert) sowie den Umfang der Auskunftserteilung der Weitergabe von Personendaten sowie die zu treffenden Schutzmechanismen.

9 Massnahmen zur Datensicherheit

Zum Schutz von Personendaten ergreift ÖKK die notwendigen technischen und organisatorischen Massnahmen. Jeder Mitarbeitende hat die geltenden Massnahmen zu beachten, darf diese nicht umgehen und hat deren Wirksamkeit im Rahmen seiner Tätigkeit zu kontrollieren. Unwirksame oder fehlende Massnahmen sind dem Vorgesetzten oder dem BDSV zu melden.

Die Massnahmen zur Wahrung der Datensicherheit sind in der Weisung Informationssicherheit dargestellt.

10 Überwachung und Überprüfung

Die Erfüllung der gesetzlichen und intern festgelegten Datenschutzbestimmungen wird durch Systemüberwachungen, Sicherheitskontrollen sowie durch regelmässige interne und externe Audits überprüft.

10.1 Überwachung

ÖKK definiert Verfahren und Schutzmassnahmen, um die Einhaltung des Datenschutzes und der Datensicherheit überwachen. In erster Linie werden technische Schutzmassnahmen gegen Missbrauch und Schaden eingesetzt.

Diese (technischen) Überwachungsmassnahmen sind in der Weisung Informationssicherheit geregelt. ÖKK passt ihre Massnahmen regelmässig dem aktuellen Stand der Technik an.

10.2 Interne und externe Audits

Audits sind nach einem definierten Prozess gemäss Auditplan durchzuführen. Dabei müssen Objektivität und Unabhängigkeit der Auditoren gewährleistet sein.

Folgende Prüfziele werden verfolgt:

- Konformität zu den datenschutzrechtlichen und regulatorischen Rahmenbedingungen;
- Erfüllung der definierten Anforderungen an die Datensicherheit;
- Kontrolle der Implementierung und der Wartung des Datenschutzmanagementsystems;
- Prüfung und Planung von Korrektur- und Vorsorgemassnahmen.

Das für den geprüften Bereich zuständige Management muss sicherstellen, dass Massnahmen aus dem Audit umgesetzt werden. Die Umsetzung der Massnahmen wird kontrolliert.

10.2.1 Audit des Datenschutzmanagementsystems

ÖKK muss ihr Datenschutzmanagementsystem regelmässigen Audits unterziehen, um dessen Wirksamkeit zu überprüfen. Dazu prüft der BDSV, ob die Anforderungen an das Datenschutzmanagementsystem und der Inhalt dieser Weisung ordnungsgemäss umgesetzt sind.

Für das Audit wird ein Verfahren definiert, das ein methodisches Vorgehen erlaubt, für den Wirksamkeitsnachweis geeignet ist und die Verantwortlichkeiten für die Durchführung von Audits und die Berichterstattung regelt.

10.2.2 Berichterstattung gegenüber der Geschäftsleitung

Der BDSV orientiert die Geschäftsleitung jährlich mit einem Bericht und einem Vortrag über seine Tätigkeit. Ausserordentliche Vorkommnisse meldet er der Geschäftsleitung unverzüglich.

10.3 Nichtkonformität

10.3.1 Überblick

Bei möglichen Verstössen gegen gesetzliche und/oder reglementarische Bestimmungen (sog.

„Nichtkonformität“) erfolgt eine sog. „Konformitätsanalyse“. Dabei wird die mögliche Nichtkonformität analysiert, beurteilt und ggf. Massnahmen zur Beseitigung derselben eingeleitet. Alternativ kann eine Nichtkonformität auch vermieden werden, indem beispielsweise auf die betreffende Bearbeitung verzichtet wird. Eine Nichtkonformität darf hingegen weder akzeptiert noch wiederholt oder übertragen werden.

10.3.2 Konformitätsanalyse

Falls eine Bearbeitung von Personendaten von den rechtlichen Vorgaben abweicht, muss der BDSV eine Konformitätsprüfung vornehmen. Zusammen mit dem jeweiligen Dateneigner identifiziert der BDSV zuerst die Ursachen der Nichtkonformität. Sodann beurteilt der BDSV die Bearbeitung entweder als „konform“ oder „leicht“ bzw. „erheblich“ nicht-konform. Neben der Datenbearbeitung

i.e.S. beurteilt ÖKK auch alle ihre datenschutzrelevanten Objekte (Datensammlungen, Systeme und Prozesse) auf ihre Konformität in Bezug auf die massgeblichen externen (gesetzlichen, vertraglichen, branchenspezifischen) Vorgaben.

Damit ergänzt die Konformitätsanalyse die herkömmliche Risikoanalyse, wobei jede Nichtkonformität auszuschliessen bzw. zu beseitigen ist.

10.3.3 Vorgehen bei Nichtkonformität

Bei Nichtkonformität untersagt der BSDV entweder künftige Datenbearbeitungen oder er trifft angemessene Massnahmen zur Beseitigung der Nichtkonformität. Dabei werden die bestehenden Massnahmen auf ihre Einhaltung und Wirksamkeit. Bei Unwirksamkeit definiert der BDSV neue oder zusätzliche Massnahmen, stellt deren Umsetzung sicher und dokumentiert sie. Dazu entwickelt er einen Plan zur Überprüfung/Nachprüfung der Rechtsverletzung sowie die Korrektur- oder vorsorgliche Massnahmen zur Verbesserung des Datenschutzmanagementsystems enthält.

10.4 Datenschutzverletzungen durch Mitarbeitende

Die Mitarbeitenden und Kader aller Stufen haben mögliche oder tatsächliche Datenschutzverletzungen dem BDSV unverzüglich und direkt mitzuteilen („whistle-blowing“). Der BDSV führt sodann Kontrollen und Abklärungen durch oder gibt solche in Auftrag.

Bei bestätigtem Verdacht auf Datenschutzverletzungen entscheidet das jeweils zuständige GL- Mitglied in Abstimmung mit HR und auf Antrag des BDSV über arbeitsrechtliche Sanktionen. Je nach Schweregrad (Art, Häufigkeit etc.) können disziplinarische Massnahmen, Kündigungen, Freistellungen oder fristlose Entlassungen beschlossen werden. ÖKK verfügt über eine Weisung Sanktionenrecht, welche die Verfahrensschritte regelt.

Über den Beizug der Strafverfolgungsbehörden entscheidet die GL in Abstimmung mit HR und auf Antrag des BDSV.

11 Organisation des Datenschutzes

11.1 Geschäftsleitung

Die GL definiert mit der Leitlinie Datenschutz [03.0019] die übergeordneten Grundsätze für die Gewährleistung des Datenschutzes und der Datensicherheit bei ÖKK. Sie legt damit die Basis für den sorgsamen Umgang mit den ÖKK anvertrauten Personendaten.

Um den Datenschutz innerhalb von ÖKK nach einem definierten Verfahren planen, implementieren, überprüfen und verbessern zu können, etabliert die GL das Datenschutzmanagementsystem. Die GL stellt die hierfür erforderlichen Ressourcen zur Verfügung. Insbesondere ermöglicht sie interne und externe Überprüfungen, deren Ergebnisse in die Konformitätsanalyse einfliessen. Damit soll das Datenschutzmanagementsystem kontinuierlich verbessert werden.

Ressourcen und -Massnahmen werden aber, wenn immer möglich, optimal den wirtschaftlichen Möglichkeiten und den betrieblichen Gegebenheiten von ÖKK angepasst werden.

11.2 Vorgesetzte

Die Vorgesetzten aller Stufen sind in ihren Verantwortungsbereichen für die Durchsetzung und Einhaltung des Datenschutzes und der Datensicherheit verantwortlich, insbesondere im Rahmen der Geschäftsprozesse. Sie sorgen in Zusammenarbeit mit dem BDSV für die Schulung und Sensibilisierung der Mitarbeitenden. Sie nehmen eine Vorbildfunktion wahr und fördern die Motivation der Mitarbeitenden, Massnahmen zum Datenschutz und zur Datensicherheit einzuhalten.

11.3 Betrieblicher Datenschutzverantwortlicher

Der BDSV ist die Ansprechstelle für den Datenschutz. Seine Verantwortlichkeiten können dem Pflichtenheft Betrieblicher Datenschutzverantwortlicher (BDSV) [03.0010] entnommen werden. Sie beinhalten insbesondere folgende Aufgaben:

- Die Überwachung der Anwendung der Vorschriften zum Datenschutz, sowohl bei der internen Datenbearbeitung, bei der Datenbearbeitung durch Dritte (Outsourcing) wie bei der Datenbearbeitung zugunsten Dritter (Insourcing)
- Behandlung von Meldungen betreffend der Missachtung von Vorschriften
- Beratung von Mitarbeitenden und Kadern bei der Anwendung von Massnahmen
- Prüfung und Umsetzung neuer datenschutzrechtlicher Bestimmungen
- Führen der Liste der Datensammlungen mit Personendaten
- Vornahme unabhängiger Kontrollen
- Abgabe von Empfehlungen zur Verbesserung des Datenschutzes
- Durchführung von Konformitätsprüfungen (auch durch Externe)
- Jährliche Information der GL über seine Tätigkeit und den Stand des Datenschutzes bei ÖKK

11.4 Dateneigner

Im Innenverhältnis sind sog. „Dateneigner“ für die ÖKK - Datensammlungen verantwortlich. Die Dateneigner haben folgende Aufgaben und Verantwortlichkeiten:

- Gewährleistung von Datenschutz und Datensicherheit bei den ihm zugewiesenen Datensammlungen sowie deren Überwachung
- Sicherstellung der Qualität, Datenintegrität und Richtigkeit der Daten
- Klassifizierung und Inventarisierung der Datensammlungen und der zu ihrer Bearbeitung benötigten Prozesse und Systeme sowie deren Beschreibung Erlass und Überwachung der Einhaltung von Bearbeitungsreglementen, sofern solche nötig sind
- Meldung neuer Datensammlungen vor deren Eröffnung an den BDSV
- Meldung von Löschungen und Änderungen von Datensammlungen an den BDSV
- Meldung der Notwendigkeit einer Bekanntgabe von Personendaten sowie der Übermittlung von Datensammlungen ins Ausland an den BDSV
- Unterstützung bei Auskunftserteilungen
- Bestimmung der zum Bearbeiten der Daten befugten Personen und deren Zugriffrechte

11.5 Vertrauensärzte und Vertrauensärztlicher Dienst

Die Aufgaben der Vertrauensärzte werden in Art. 57 Abs. 4 und 5 KVG umschrieben.

Sie wahren die Persönlichkeitsrechte der Versicherten, indem sie unabhängig sind und den zuständigen Stellen von ÖKK nur bestimmte Angaben weitergeben.

Diese gesetzlich vorgeschriebene Unabhängigkeit muss auch für die Organisation des Vertrauensärztlichen Dienstes (VAD) gegeben sein. Dies erfordert namentlich eigene Bearbeitungsreglemente. Weiter muss jederzeit sichergestellt sein, dass besonders schützenswerte Personendaten den VAD nicht verlassen können. Die vom VAD erstellten Dokumente dürfen nur auf eigenen Speichermedien archiviert werden, die nur den Mitarbeitenden des VAD zugänglich sind.

11.6 Personalbereich

Die Personalleitung und die im Personalbereich tätigen Mitarbeitenden sind für die sorgfältige und datenschutzkonforme Bearbeitung der Personaldaten verantwortlich.

11.7 Leiter Betrieb Informatik

Der Leiter Betrieb Informatik trägt die Verantwortung, dass die Datensicherheit und datenschutzrechtliche Massnahmen technisch umgesetzt werden. Dabei unterstützen ihn insbesondere die Applikations- und Systemverantwortlichen. Er arbeitet eng mit dem BDSV zusammen, um die Konformität der Massnahmen zu prüfen. So beurteilt er Risiken, Vorfälle und Beinahe-Vorfälle, welche den Datenschutz gefährden können.

11.8 Mitarbeitende

Alle Mitarbeitenden sind für Datenschutz und Datensicherheit in ihrem Aufgabenbereich verantwortlich und verpflichtet, Personendaten nach den gesetzlichen und internen Bestimmungen zu bearbeiten. Kritische Aufmerksamkeit und eigenverantwortliches Verhalten werden vorausgesetzt. Mitarbeitende können sich bei Unklarheiten oder für Auskünfte jederzeit an ihren Vorgesetzten oder an den BDSV wenden.

Mitarbeitende werden mit Aufnahme ihrer Tätigkeit im Rahmen des Arbeitsvertrags auf den Datenschutz und auf die Datensicherheit verpflichtet. Die Verpflichtung wird nachweisbar im Personaldossier dokumentiert.

Im Rahmen der Leumunds- und Bonitätsprüfung kann das Human Resources während des Arbeitsverhältnisses Auszuge aus dem Straf- und oder Betreibungsregister verlangen, wenn ein begründeter Verdacht auf eine strafbare Handlung besteht oder bei internen Funktionswechseln in besonders vertrauensvolle Funktionen oder Führungspositionen, bei denen ein guter Leumund in objektiver Hinsicht unabdingbar ist (z.B. aufgrund der Vorbildfunktion gegenüber den anderen Mitarbeitenden oder wegen Repräsentationsaufgaben gegenüber der Öffentlichkeit).

Mitarbeitende werden hinsichtlich ihrer Verantwortung für den Datenschutz sensibilisiert und ausgebildet. Dokumente, Formulare, Meldungen und Informationen zum Thema Datenschutz werden den Mitarbeitenden zentral über die entsprechende Intranet-Seite zur Verfügung gestellt.

12 Datenschutzmanagementsystem

Um den Datenschutz nachhaltig und wirkungsvoll zu gewährleisten, wird ein Datenschutzmanagementsystem aufgebaut und betrieben. Durch entsprechende Verfahren wird es laufend überprüft und verbessert.

12.1 Umfang

Das Datenschutzmanagementsystem umfasst gemäss Art. 4 Abs. 2 VDSZ namentlich:

- Die Leitlinie Datenschutz (im Sinne einer Datenschutzpolitik) [03.0019]
- Die Dokumentation von Zielen und Massnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit
- Die organisatorischen und technischen Vorkehrungen zur Verwirklichung der festgelegten Datenschutzziele und -massnahmen, insbesondere die Vorkehrungen zur Behebung festgestellter Mängel.

12.2 Anforderungen

Damit ein Datenschutzmanagementsystem den gesetzlichen Mindestanforderungen und denjenigen der Zertifizierung genügt, sind die Anforderungen der Norm ISO 27001 betreffend das Informationssicherheitsmanagementsystem (ISMS) zu übernehmen und entsprechend auszulegen, wobei anstelle des Begriffs Informationssicherheit (IS) der Begriff Datenschutz (DS) einzusetzen ist und die Kontrollziele und Kontrollen gemäss Anhang A der Norm ISO 27001 durch folgende Ziele und Massnahmen zu ersetzen bzw. zu ergänzen und abzuändern sind (vgl. DSMS-Richtlinien).

12.3 Ziele und Massnahmen

Bei der Erstellung des Datenschutzmanagementsystems müssen folgende Ziele und Massnahmen hinsichtlich der Datenbearbeitung erfüllt sein:

- **Rechtmässigkeit** (Art. 4 Abs. 1 DSG):
  1. Rechtfertigungsgründe (Art. 13 DSG)
  2. Gesetzliche Grundlage (Art. 17 und 19 f. DSG)
  3. Datenbearbeitung durch Dritte (Art. 10a Abs. 1 DSG)
- **Transparenz:**
  1. Treu und Glauben (Art. 4 Abs. 2 DSG)
  2. Erkennbarkeit (Art. 4 Abs. 4 DSG)
  3. Informationspflicht (Art. 7a Abs. 1 DSG)
- **Verhältnismässigkeit**:
  1. Verhältnismässige Bearbeitung (Art. 4 Abs. 2 DSG)
- **Zweckbindung** (Art. 4 Abs. 3 DSG):
  1. Zweckbestimmung bzw. -änderung
  2. Nutzungsbeschränkung
- **Datenrichtigkeit**:
  1. Datenrichtigkeit (Art. 5 Abs. 1 DSG)
  2. Berichtigung von Daten (Art. 5 Abs. 2 DSG)
- **Grenzüberschreitende Datenbekanntgabe** (Art. 6 Abs. 1 DSG):
  1. Angemessener Schutz (Art. 6 Abs. 2 DSG)
- **Datensicherheit** (Art. 7 DSG):

1. Datenvertraulichkeit
2. Datenintegrität
3. Datenverfügbarkeit
4. Datenbearbeitung durch Dritte (Art 10a Abs. 2 DSG)

- **Registrierung der Datensammlungen** (Art. 11a Abs. 1 DSG und Art. 12b Abs. 1 VDSG):
  1. Anmeldepflicht (Art. 11a Abs. 2 und 3; Ausnahmen Art. 11a Abs. 5 Bst. e und f DSG)
  2. Liste der nicht angemeldeten Datensammlungen (Art. 12b Abs. 1 Bst. b VDSG)
- **Auskunftsrecht und Verfahren**:
  1. Auskunftsrecht betreffend eigene Daten (Art. 8 Abs. 1 DSG)
  2. Rechtsansprüche und Verfahren (Art. 15 und 25 DSG)

Die neun ausgewählten Ziele entstammen direkt dem DSG, die zwanzig dazugehörigen Massnahmen sind analog zur Norm ISO 27002 strukturiert.

12.4 Externe Rahmenbedingungen

Legal & Compliance überwacht laufend die für ÖKK relevanten rechtlichen und politischen Entwicklungen und erstattet der GL periodisch oder ad hoc Bericht hierüber. Gegenstand des Monitorings sind damit auch datenschutzrechtliche Normen (insbesondere DSG, VDSG, ATSG, KVG, VVG, VDSZ, DSMS-Richtlinien (mit dem Anhang und den Erläuterungen)) sowie etwaige Standesregeln von Branchen- oder Berufsverbänden. ÖKK orientiert sich primär an der schweizerischen Gesetzgebung. In begründeten Fällen kann die Anwendung und Berücksichtigung der EU-DSGVO geboten resp. notwendig sein.

Der BDSV ist verantwortlich für die zeit- und lagegerechte Antizipation/Umsetzung datenschutzrechtlicher Neuerungen.

12.5 Review des Datenschutzmanagementsystems

Im Auftrag der GL bewertet der BDSV das Datenschutzmanagementsystem periodisch, um dessen Eignung, Angemessenheit und Wirksamkeit sicherzustellen. Dazu müssen die notwendigen Informationen erhoben und bewertet werden.

Der BDSV legt das Bewertungsverfahren fest und dokumentiert die Bewertungen sowie allfällige Verbesserungsmassnahmen am Datenschutzmanagementsystem.

12.6 Schulungen und Kompetenzen

Das Datenschutzmanagementsystem fordert die laufende und bedarfsgerechte Aus- und Weiterbildung aller involvierten Personen, Stellen und Funktionen. Der BDSV prüft entsprechende Massnahmen leitet diese nötigenfalls ein. Die Effektivität der jeweiligen Ausbildungen, die Fähigkeiten, Erfahrungen und Qualifikationen der Mitarbeitenden müssen nachgewiesen werden können (Ausbildungskontrolle).

Weiter stellt der BDSV sicher, dass die Mitarbeitenden ihre datenschutzrechtlichen Pflichten erfüllen können. Namentlich müssen sie die notwendigen Kompetenzen erhalten.

Genehmigung

Das vorliegende Dokument ist am 16.09.2013 von der Geschäftsleitung erstmals genehmigt worden.

Landquart, _____

ÖKK

Stefan Schena Vorsitzender der Geschäftsleitung	Patrick Heinz Bereichsleiter Leistungen