Die etwas andere Anwaltskanzlei
dynamisch / prozessorientiert / systemdenkend / businessnah

Die Advokatur Sury AG

RVK – treffPUNKT KOMPAKT

Neues Datenschutzgesetz – Fokus Outsourcing

20. April 2023, online

info@dieadvokatur.ch
+41 41 227 58 58
Alpenquai 4
CH-6005 Luzern

DIE ADVOKATUR.CH

REFERENT: MLAW/MBA ANDRÉ HENRI KUHN

BALLY SWITZERLAND

forbo FLOORING SYSTEMS

Scuola universitaria professionale della Svizzera italiana

SUPSI

UNIVERSITY AT ALBANY State University of New York

UNIVERSITÄT LUZERN

CITROËN

RENAULT Passion for life

n|w Fachhochschule Nordwestschweiz Pädagogische Hochschule

DIE ADVOKATUR.CH

HSLU Hochschule Luzern

FFHS Fernfachhochschule Schweiz

Mitglied der SUPSI

Universität Basel

WELCHE FRAGEN BEANTWORTEN WIR HEUTE?

Teil 1 – Neues Datenschutzgesetz

Was bedeutet «Datenschutz»?

Was sind die Grundanliegen im neuen Datenschutzgesetz?

Was sind die wichtigsten Änderungen im Datenschutzrecht?

Was sind die Herausforderungen für Versicherer rund um Personendaten?

Wer trägt die Verantwortung?

WELCHE FRAGEN BEANTWORTEN WIR HEUTE?

Teil 2 – Auftragsbearbeitung / Outsourcing

Was ist eine Auftragsbearbeitung?

Wo liegt die Herausforderung in der Auftragsbearbeitung (Outsourcing)?

Was ist zu beachten beim Beizug von Auftragsbearbeitern?

Wie ist ein Auftragsbearbeiter-Vertrag zu gestalten?

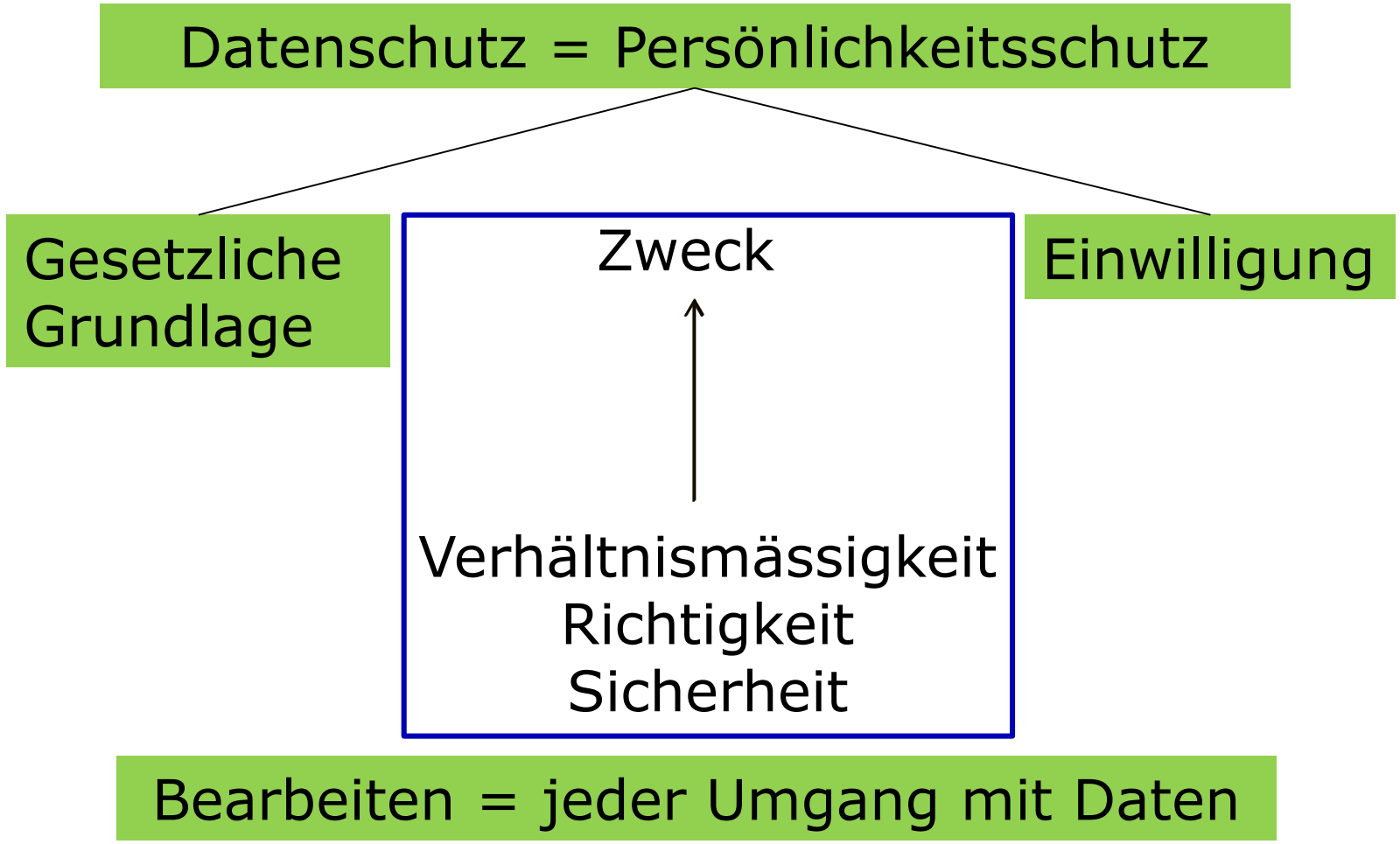
Wie kann der RVK Sie unterstützen?

Wie lautet die «Take-Home Message»?

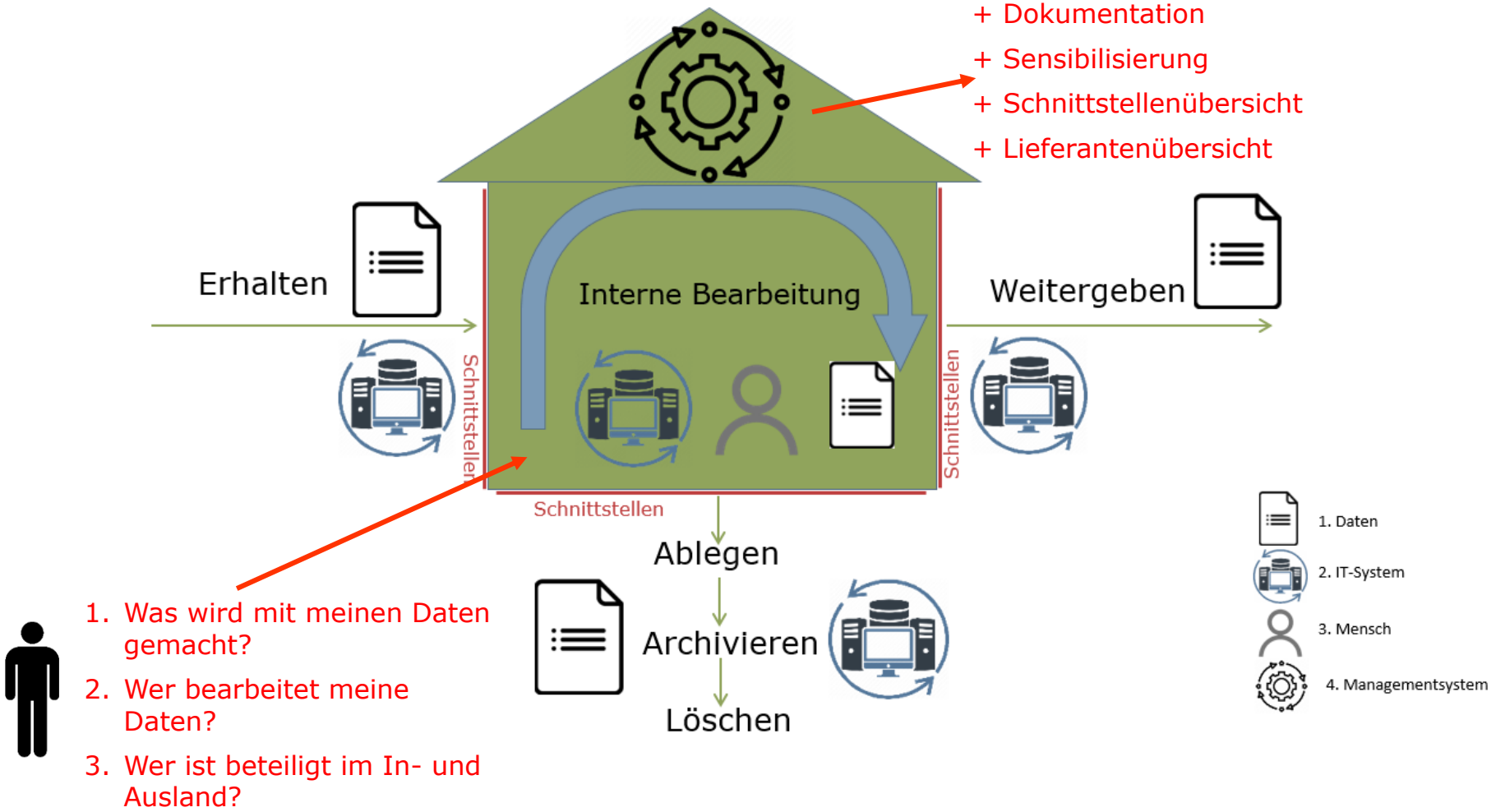
DIE ADVOKATUR.CH

Teil 1: Neues Datenschutzgesetz

WAS BEDEUTET DATENSCHUTZ?



WAS SIND DIE GRUNDANLIEGEN IM NEUEN DATENSCHUTZGESETZ?



WAS SIND DIE WICHTIGSTEN ÄNDERUNGEN IM DATENSCHUTZRECHT?

- Daten von juristischen Personen fallen nicht mehr in den Geltungsbereich des DSG: Art. 2 revDSG
- **Verschärfung der Informationspflichten bei der Datenerhebung: Art. 19 revDSG**
- **Ausbau der Rechte der betroffenen Person anhand von Auskunftsrecht: Art. 25 ff. revDSG**
- Datenschutz-Folgeabschätzung: Bei erhöhtem Risiko für Persönlichkeit der betroffenen Person: Art. 22 nDSG
- Informationspflichten bei einer automatisierten Einzelentscheidung: Art. 19 revDSG
- Privacy by design (Risiken vorbeugen):
  - Ab der Planung: Datenminimierung, Zugriffsberechtigungen, Löschungsmöglichkeit, Art. 7 Abs. 1 revDSG
- Privacy by default:
  - Standardmässige datenschutzfreundliche Einstellung (Bsp. Browser blockiert Cookies), Art. 7 Abs. 3 revDSG
- Unverzügliche Meldung bei Datenschutzverletzung an den EDÖB; Art. 24 revDSG
- Sanktionen (Art. 60 ff. revDSG)

WAS SIND DIE WICHTIGSTEN HERAUSFORDERUNGEN FÜR VERSICHERER RUND UM PERSONENDATEN?

Versicherer

- bearbeiten **grosse Mengen** an Daten über die Gesundheit von Versicherten, d.h. **besonders schützenswerte Personendaten** (vgl. Art. 5 Bst. c revDSG).
- unterstehen **zusätzlichen Anforderungen** an den Schutz von Daten / Geheimnissen (Art. 84 ff. KVG, Art. 36 f. KVAG, Art. 33 ATSG etc.; Richtlinien FINMA / BAG).
- benötigen für die Erfüllung wachsender Aufgaben spezifische Software und Kenntnisse, die extern, teils gemeinsam durch Pooling, beigezogen werden.

WER TRÄGT DIE VERANTWORTUNG?

Wer **Mittel und Zweck** der Datenbearbeitung **festlegt,** trägt die Verantwortung für die **rechtmässige** Datenbearbeitung.

(vgl. Art. 5 Bst. j revDSG)

Persönliche Verantwortung von Management und Mitarbeitenden

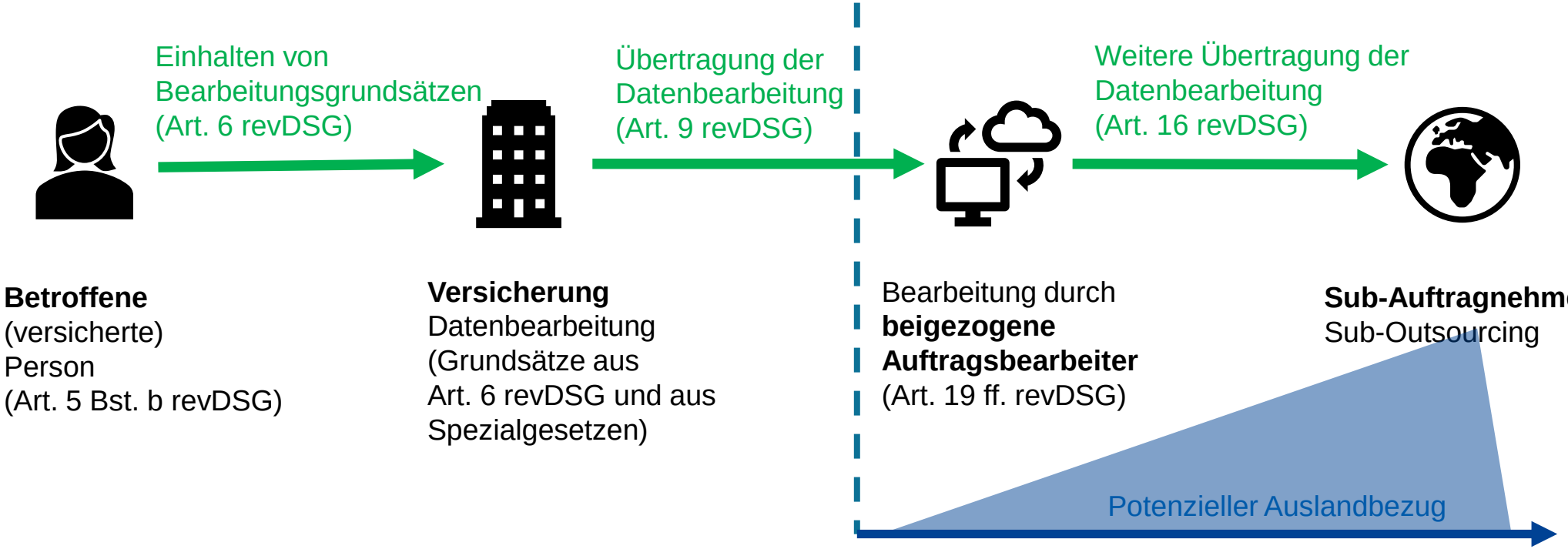
- Datenschutz ist die **Pflicht jedes/jeder Einzelnen**. Jeder ist verantwortlich, dass der Datenschutz in seinem Bereich eingehalten wird.

DIE ADVOKATUR.CH

Teil 2: Auftragsbearbeitung / Outsourcing

WAS IST EINE AUFTRAGSBEARBEITUNG? (I)

Outsourcing stellt ein mögliches Risiko dar für den Datenschutz, für die **Geheimhaltung/Schweigepflicht** (Art. 33 ATSG) sowie das **Amts-/Arztgeheimnis** (Art. 320 f. StGB).



WAS IST EINE AUFTRAGSBEARBEITUNG? (II)

- Ein Auftragsbearbeiter handelt im Auftrag des Verantwortlichen (Art. 5 Bst. k revDSG), um Daten zu bearbeiten (die Bezug zu Personen haben).
- Aus einer Auftragsbearbeitung entstehen Verpflichtungen,

  Daten nur so zu bearbeiten, wie es der Verantwortliche selbst tun dürfte, d.h., u.a.
  - Technische und organisatorische Massnahmen treffen (Art. 7 Abs. 2 revDSG)
  - Datensicherheit gewährleisten (Art. 9 revDSG)
  - Ev. weitere Geheimnisse zu schützen (Art. 320 ff. StGB, Art. 33 ATSG etc.)
  - Daten nur unter bestimmten Voraussetzungen ins Ausland zu übermitteln (Art. 16 revDSG)
  - Weitere Pflichten zu erfüllen (Art. 19 ff. revDSG)

WAS IST ZU BEACHTEN FÜR DEN BEIZUG VON AUFTRAGSBEARBEITERN? (I)

Art. 55 OR, analog:

Sorgfältige Auswahl	Sorgfältige Instruktion	Sorgfältige Kontrolle
Zertifikate verlangen	Präzise Formulierung der Aufgaben	Genaue Regelung der Kontrolle (Audits)
Referenzen einholen zur Prüfung der professionellen Fähigkeiten (auch) in der Gesundheitsbranche	Benennung der ausführenden Personen	Regelmässige Durchführung der Audits (vor Ort)
Sicherheitsstandards anfordern	Ausformulierung Security-Konzept	Zuständigkeiten fürs Audit regeln
Maturität im Management-System	Governance-Konzept liegt vor	Dokumentation der Audits klären
Vor-Ort-Überprüfung vornehmen	Bearbeitungsreglement vorlegen	Jährliches Management Commitment
Bonitäts- und Veritäts-Prüfung	Mitarbeitende schulen	Hinweis auf öffentliche Aufsicht
Anbieter vergleichen	Verpflichtungen der Mitarbeitenden zum Geheimnisschutz etc.	Kontrolle mit Checkliste (mindestens TOM’s aus dem Vertragsanhang)
	Modalitäten zur Vertragsanpassung	
	Regelung des Beizugs von Unter-Auftragnehmern	

WAS IST ZU BEACHTEN FÜR DEN BEIZUG VON AUFTRAGSBEARBEITERN? (II)

- **Dürfen die Daten an einen Auftragsbearbeiter weitergegeben werden?**
  (steht das im Gesetz oder besteht ein Vertrag mit Betroffenen?;
  vgl. Art. 9 Abs. 1 revDSG)
- **Ist der Auftragsbearbeiter in der Lage, die Datensicherheit zu gewährleisten?**
  (Art. 9 Abs. 2 revDSG)
- **Führt der Auftragsbearbeiter ein Verzeichnis der Bearbeitungstätigkeiten?**
  (Art. 12 Abs. 1 und 3 revDSG)
- **Gelangen Daten ins Ausland und ist die Gesetzgebung im Zielstaat angemessen?**
  (Art. 16 f. revDSG)

WAS IST ZU BEACHTEN FÜR DEN BEIZUG VON AUFTRAGSBEARBEITERN? (III)

- **Hat die betroffene Person in den Datentransfer ins Ausland eingewilligt und/oder bestehen ausreichende Garantien im Zielstaat** (Art. 19 Abs. 4 revDSG)?
- **Hält sich der Auftragsbearbeiter an gesetzliche und vertraglichen Auflagen?** (Art. 19 ff. revDSG)
- **Sind die Meldeprozesse bei Datenschutzvorfällen geregelt und effizient?** (vgl. Art. 24 revDSG)
- **Kann einer betroffenen Person Auskunft erteilt werden?** (Art. 25 ff. revDSG)
- **Ist sichergestellt, dass der Auftragsbearbeiter die Daten nicht ohne vorgängige Genehmigung des Verantwortlichen an Dritte weitergibt?** (Art. 9 Abs. 3 revDSG)

WAS IST ZU BEACHTEN FÜR DEN BEIZUG VON AUFTRAGSBEARBEITERN? (IV)

- Übermittlungen von sensiblen Daten und Informationen ausserhalb des räumlichen Einflussbereichs eines Versicherers müssen bereits im Projekt bekannt und dokumentiert sein.
- Die auszulagernden Tätigkeiten oder Geschäftsbereiche sind genau zu definieren (Art der Leistung, Ziel der Auslagerung, qualitative und quantitative Anforderungen an die Leistungen, Risikoprofil der Auslagerung).
- Es besteht ein Anforderungsprofil an einen künftigen Vertragspartner/eine künftige Vertragspartnerin sowie ein Due-Diligence Prozess für die sachgerechte Leistungserbringung.
- Schnittstellen und Datenflüsse nach Aussen werden dokumentiert und in einem Verzeichnis nachgeführt.
- Wo gesetzlich vorgeschrieben, informieren die Versicherungen die Betroffenen über ein Outsourcing ins Ausland.
- Besonders schützenswerte Personenangaben (z.B. über die Gesundheit) werden pseudonymisiert und verschlüsselt übermittelt.
- Eine fachkundige Person (z.B. ein Datenschutzberater) wird beigezogen.

WIE IST EIN AUFTRAGSBEARBEITER-VERTRAG ZU GESTALTEN? (I)

Mindestinhalt von Outsourcing- bzw. Auftragsbearbeiter-Verträgen sind:

- Genaue Beschreibung der Tätigkeiten;
- Beschreibung der Einbindung in die Datenflüsse der Versicherer;
- Dienstleistungsbereitschaft und Erreichbarkeit des Auftragsbearbeiters;
- Verbindliche Projektorganisation und konkrete Ansprechpersonen (mindestens nach Kompetenzprofil definiert);
- Anforderungen an die Datenbearbeitung, die Informationssicherheit und die Geheimhaltung;
- Kündigungsmodalitäten mit der Verpflichtung zur Zusammenarbeit bei einer Übertragung von Daten und Informationen an die Versicherer oder an von den Versicherern benannte Dritte;
- Bereitstellung aktueller Daten und Gewährleistung für ein Backup nach Bearbeitung;
- Allfällige Wartungs- und Service-Zeiten sowie maximale Ausfallzeiten;
- Verpflichtung zum Geheimnisschutz und zur Verschwiegenheit über das Ende der Vertragsbeziehung hinaus.

WIE IST EIN AUFTRAGSBEARBEITER-VERTRAG ZU GESTALTEN? (II)

Auftragsbearbeiterinnen/Auftragsbearbeiter verpflichten sich mindestens zu hinreichenden Garantien betreffend Datenschutz und Informationssicherheit.

Dies besteht unter anderem darin,

- Daten nur so zu verwenden, wie es den Versicherern selbst erlaubt ist.
- Die Datensicherheit jederzeit zu gewährleisten.
- Daten aufzubewahren, wie und wo es die Versicherer vorschreiben. Insbesondere werden ohne schriftliche Zusage der Versicherer keine Daten oder Informationen in Drittstaaten übermittelt.
- Mitarbeitende und Hilfspersonen zu Geheimnisschutz, Verschwiegenheit und Vertraulichkeit auch über deren Vertragsverhältnis hinaus zu verpflichten.
- Allfällige Ungewöhnlichkeiten oder Mängel in Abläufen sind umgehend den Versicherern mitzuteilen

WIE KANN DER RVK SIE UNTERSTÜTZEN?

RA Geisser

– Separate Präsentation

WIE LAUTET DIE TAKE-HOME MESSAGE?

- Das neue Datenschutzgesetz tritt am 1. September 2023 in Kraft.
- Das Gesetz sieht verschärfte Regeln im Umgang mit Personendaten vor.
- Die Krankenkassen tragen die Verantwortung für sorgfältigen Umgang mit Personenangaben, insb. wenn Informationen über die Gesundheit vorliegen.
- Die Verantwortlichen bestimmen, wer Personendaten wie und wo bearbeitet.
- Durch Outsourcing und Pooling können Bearbeitungsschritte effizienter gelöst werden, dies bedingt gemeinsame vertragliche Grundlagen.
- Durch Auftragsbearbeiter Verträge und Anhänge (u.a. TOM's Listen) können die Regeln überprüfbar dargelegt werden.

FRAGEN?

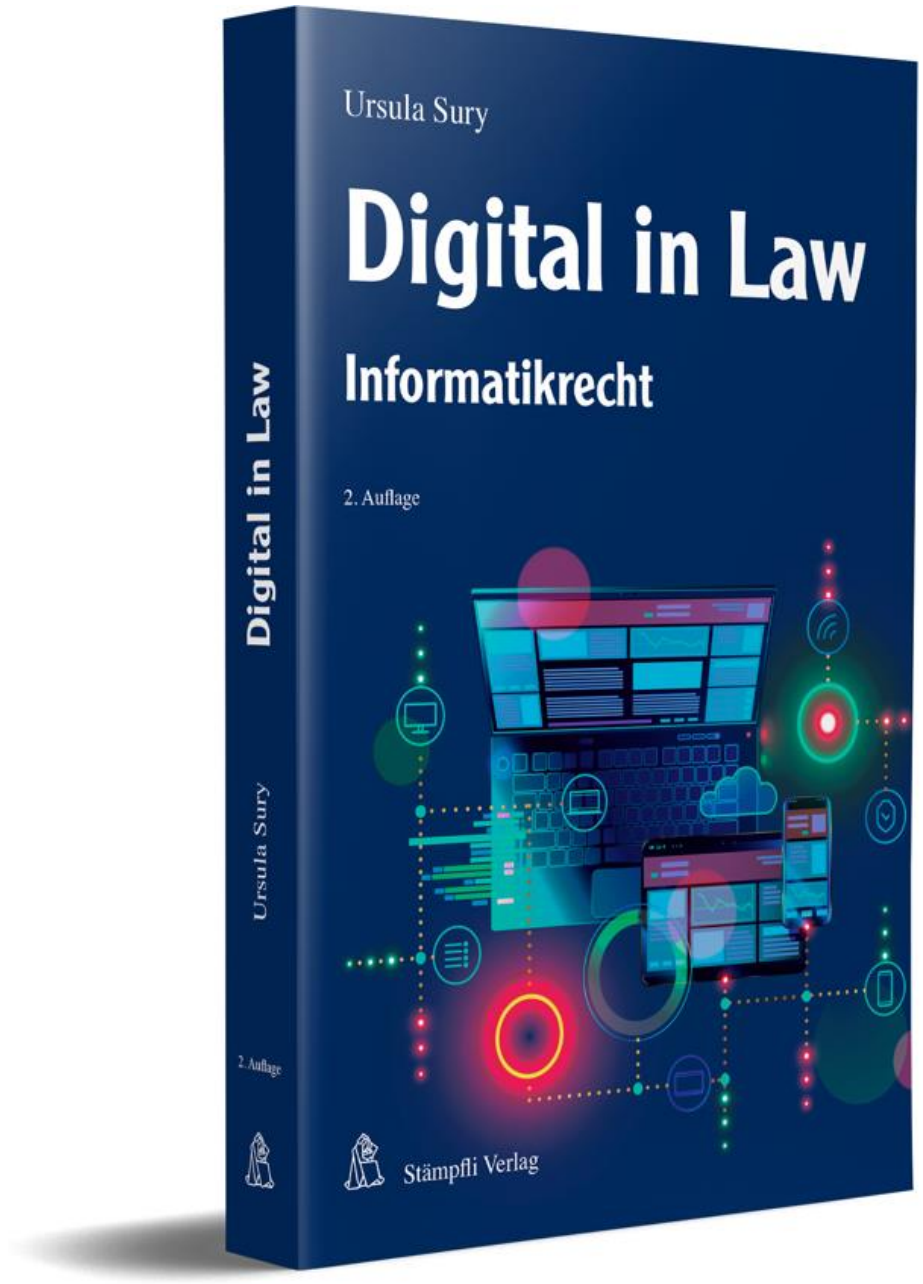
Kontakt: info@dieadvokatur.ch

LITERATUR

- BAERISWYL/PÄRLI/BLONSKI (Hrsg.), Datenschutzgesetz, 2. Auflage, Bern 2023
- HUSI-STÄMPFLI/MORAND/SURY, Datenschutzrecht, Zürich 2023 (im Juni)
- ROSENTHAL DAVID, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020
- SURY URSULA, Digital in Law, Bern 2021
- SURY URSULA, Neues Datenschutzgesetz und Dokumentation von Unternehmen, in: SJZ 9/2021, S. 458 ff.

MATERIALIEN

- FINMA Rundschreiben 2018/3 Outsourcing: www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2018-03-01012021_de.pdf?la=de
- BAG Kreisschreiben 7.9 Outsourcing an BAG-Versicherer vom 30. Mai 2022: siehe unter https://www.bag.admin.ch/bag/de/home/versicherungen/krankenversicherung/krankenversicherung-versicherer-aufsicht/kreis-und-informationsschreiben/kreisschreiben-schweiz.html
- EDÖB: Erläuterungen zu Cloud Computing: www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/cloud-computing/erlaeuterungen-zu-cloud-computing.html



DIE ADVOKATUR.CH

› Gibt einen umfassenden Überblick über die Rechtsaspekte in der digitalen Welt

WIR BEDANKEN UNS FÜR IHRE ZEIT!

DIE ADVOKATUR.CH

Effizient, unternehmerisch und qualitativ -
eine Kanzlei ganz alternativ!

info@dieadvokatur.ch
+41 41 227 58 58

Alpenquai 4
CH-6005 Luzern