sevida
ganzheitlich gelöst.

Datenschutz und ICT

von der Zitrone zum Limoncello

Ansprechpartner

sevida
ganzheitlich gelöst.

Inhalt

1. Verständnis zur Ausgangslage des revDSG schaffen
2. Was kommt auf die Institutionen zu
3. Umsetzungsmöglichkeiten und Vergleiche der Varianten

Andrea Crameri
Partner
Geschäftsführung & Beratung

Marco Brügger
Partner
Informatik, Security & Datenschutz

Begriffe

sevida
ganzheitlich gelöst.

Datenschutz	Schutz des Bürgers vor Beeinträchtigungen seiner Privatsphäre durch unbefugte Erhebung, Speicherung und Weitergabe von Daten, die seine Person betreffen. Erfüllung gesetzlicher Vorgaben
Datensicherheit	Sicherheit von Daten vor dem Zugriff Unbefugter. Beinhaltet technische und organisatorische Massnahmen

Datenschutz in Europa

sevida
ganzheitlich gelöst.

Datenschutzgrundverordnung (DSGVO, 2018)

Schutz der Privatsphäre für EU-Bürger:innen mittels verbindlicher Regeln für die

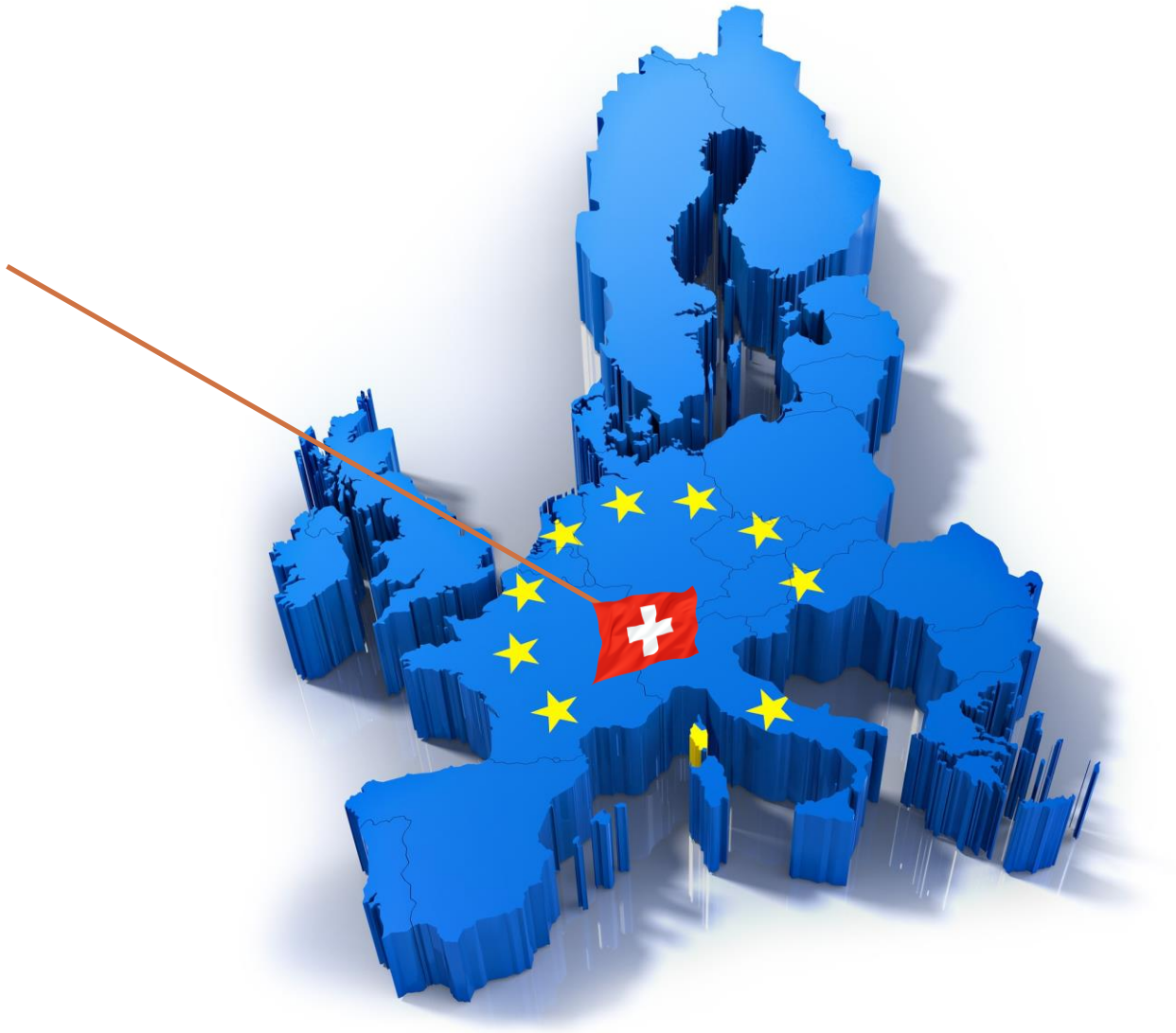
- Datenverarbeitung
- Datenspeicherung und
- Datenweiterleitung

Datenschutz in der Schweiz

sevida
ganzheitlich gelöst.

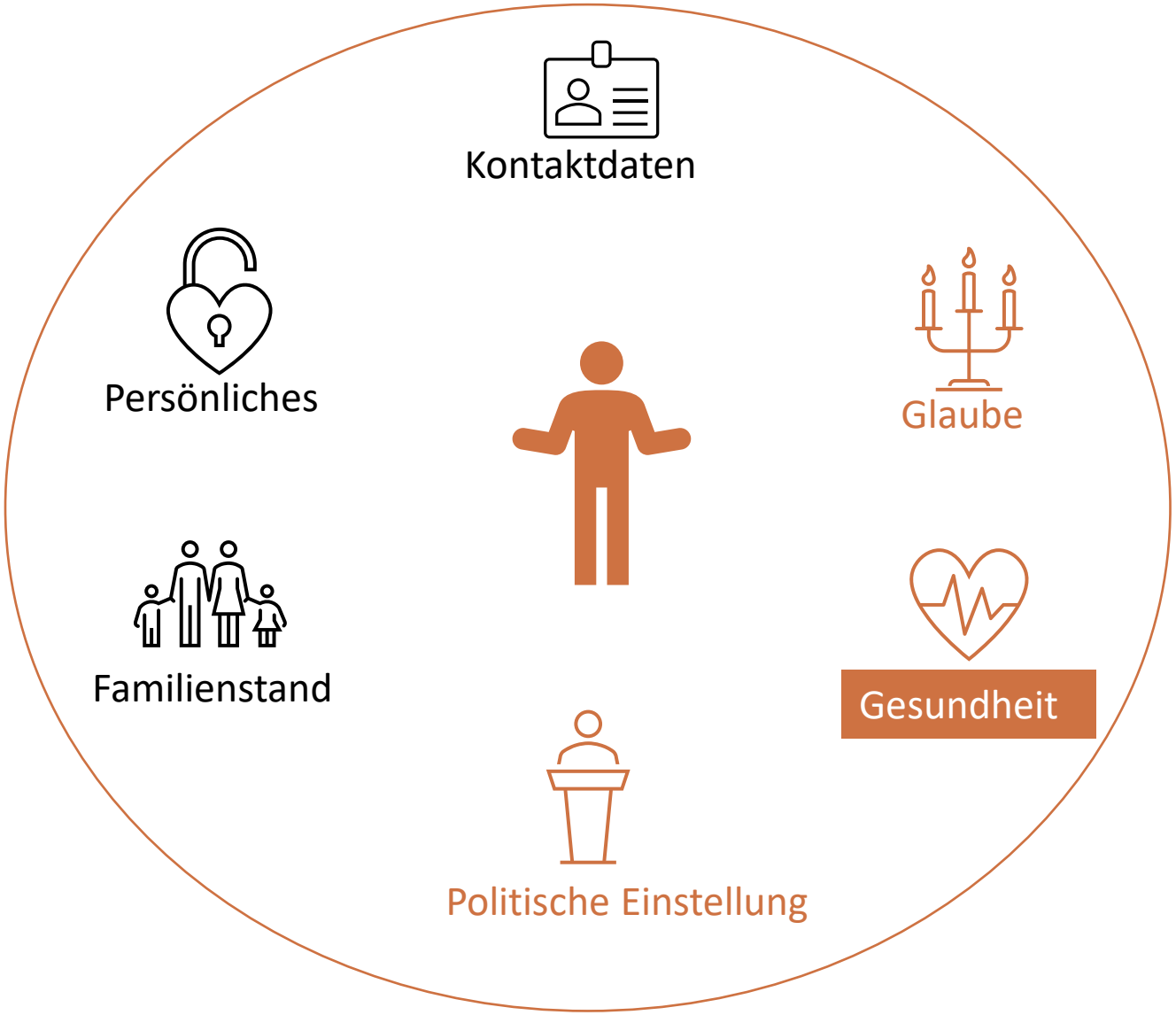
Angemessenheitsbeschluss

Revision des Schweizer Datenschutzgesetzes für die Anerkennung der Gleichwertigkeit des Schutzes der Bürger:innen (revDSG)



Datenschutz im Gesundheitswesen

sevida
ganzheitlich gelöst.



Besonders schützenswerte Daten (sensible Daten personenbezogen)

Datenschutz Status Quo

sevida
ganzheitlich gelöst.

25.09.2020
Revision des DSG abgeschlossen

Sept. 2020

Überprüfung
EU-Angemessenheitsbeschluss durch die Europäische Kommission

revDSG tritt in Kraft

01.09.2023

Keine Übergangsregelung, ausser für nicht mehr aktuelle Datenbearbeitungen.

Die Strafbestimmungen (CHF 250'000) gelten für Information, Auskunft, Exporte, Sicherheit, Outsourcing.

Aufgaben und Pflichten bezüglich Datenschutz

sevida
ganzheitlich gelöst.

Bearbeitungsverzeichnis

- Wo werden welche Daten in welcher Form bearbeitet
- Vorgaben gem. Gesetz
- ca. 60 Seiten Dokumentation

Informationspflichten

Datenschutzerklärungen und Einwilligungen für

- Bewohnende
- Angehörige, Beistände
- Interessenten
- Kunden
- Lieferanten
- Mitarbeitende
- Stellenbewerbende
- Webseitenbesuchende

Verträge und Vereinbarungen

- Softwarehersteller
- IT-Support
- Buchhaltung
- Lohnverarbeitung

Schulung Mitarbeitende

- Erstellung Schulungskonzept für Mitarbeitende
- Schulungsnachweise

Datensicherheit & Risikobewertung

- Bewertung der Verzeichnisse gemäss
  - Vertraulichkeit, Verfügbarkeit, Integrität
- Dokumentation Richtlinien
- Initiale und laufende Aufgaben festlegen und prüfen
- Erstellung Merkblätter für Mitarbeiter und exerne IT

Interne Aufwände für Umsetzung

sevida
ganzheitlich gelöst.

	Standard Hilfsmittel (Excel/Word)	DSG-Tool
Grundwissen aufbauen	Kurs oder CAS bei spezialisierten Anbietern/Schulen	In Workshop bei Tool-Einführung, zusätzlich spezifischer Fachkurs
Aufbau Bearbeitungsverzeichnis	Ca. 80 Std.	Ca. 4 Std. (Vorlagen/Vorschläge vorhanden)
Erstellen Informationspflichten	Ca. 50 Std.	In Tool vorhanden, prüfen ob für Institution passt Ca. 4 Std.
Erarbeiten Verträge und Vereinbarungen	Ca. 50 Std.	Vorlagen auf auf Institution anpassen Ca. 2 Std.
Analyse Datensicherheitsrichtlinien & Risikobewertung	Ca. 25 Std.	In Tool enthalten
Schulung Mitarbeitende (Initialisierung und Planung) Umsetzung der technischen Richtlinien und Arbeitsvorschriften	Ca. 16 Std. Ca. 16 – 24 Std.	Ca. 2 Std. Ca. 16 – 24 Std.
Total Initialaufwand	**Ca. 220 Std.**	**Ca. 50 Std.**
Jährlicher Aufwand	**Ca. 24 Tage**	**Ca. 2 Tage**

Hilfsmittel für die Umsetzung

sevida
ganzheitlich gelöst.

ARTISET CURAVIVA INSOS YOUVITA senesuisse

#	Thema / Prüfpunkte	Resultat Beurteilung IST-Zustand	Vorschläge für Massnahmen	Termin	Verantwortlich
1	**Allgemeines / Ausgangslage**				
1.1	Wird Datenschutz in der Institution systematisch geplant und koordiniert?		▪ Grundsätze in Datenschutzkonzept festhalten ▪ Datenschutz ab Planung einer Datenbearbeitung berücksichtigen		
1.2	Wann und wie wird der Datenschutz thematisiert und Situation beurteilt in: ▪ Stiftungsrat/Vorstand? ▪ Geschäftsleitung?		▪ Erlass Datenschutzkonzept durch Stiftungsrat/Vorstand ▪ Datenschutz als Teil des Risikomanagements regelmässig auf Führungsebene behandeln		
1.3	Sind Grundsätze der Datenbearbeitung und Schutzmassnahmen bereits dokumentiert (Datenschutzkonzept, interne Reglemente und Weisungen etc.)?		▪ Datenschutzkonzept erstellen ▪ Datenschutzweisung erstellen		
1.4	Gab es bisher bereits besondere Vorfälle bzw. Probleme bzgl. Datenschutz?		Gemachte Erfahrungen berücksichtigen		
1.5	Untersteht die Institution		▪ Unterstellung klären		

- Checkliste
- Muster Datenschutzkonzept
- Muster Pflichtenheft DS-Beauftragte

Hilfsmittel verfügbar unter https://www.artiset.ch/Home/Pdsob/?ID=18842944-A18F-4F16-81FCBD53991C1FB7&method=render.news

Umsetzung mit Software-Tool

sevida
ganzheitlich gelöst.

#	Thema / Prüfpunkte gemäss ARTISET	IST-Zustand	Abgedeckt durch SIDAS	Im SIDAS-Template hinterlegt, im Workshop bearbeitet
1.	Allgemeines / Ausgangslage	**Kommentar**		Template/Workshop
1.1	Wird Datenschutz in der Institution systematisch geplant und koordiniert?	Datenschutzmanagement System mit Softwarelösung SIDAS im Einsatz, Verantwortlichkeiten und Stellvertretung benannt und im Konzept/in der Software unter den Stammdaten hinterlegt.	✓	✓
1.2	Wann und wie wird der Datenschutz thematisiert und Situation beurteilt in: ✦ Stiftungsrat/Vorstand? ✦ Geschäftsleitung?	Stiftungsrat/Vorstand/Geschäftsleitung fällte Entscheid für die Investition, Einführung und Umsetzung eines Datenschutzmanagement Systems mit der Softwarelösung SIDAS	✓	✓
1.3	Sind Grundsätze der Datenbearbeitung und Schutzmassnahmen bereits dokumentiert (Datenschutzkonzept, interne Reglemente und Weisungen etc.)?	Sicherheitsrichtlinien gemäss FMH/BSI/EPD umgesetzt und dokumentiert → Report • „Datensicherheit/Report detailliert" • „Merkblatt für Mitarbeiter" • „Merkblatt für IT-Verantwortliche"	✓	Im Workshop haben wir uns auf die organisatorischen Richtlinien konzentriert. Sind alle Richtlinien (auch die technischen) und Aufgaben auf Status erledigt?
1.4	Gab es bisher bereits besondere Vorfälle bzw. Probleme bzgl. Datenschutz?	Wenn ja, unter dem Punkt „Incidents" im SIDAS dokumentiert, Richtlinie 60-65 beinhalten Vorgaben für die Vorbereitung auf einen Vorfall, eine Checkliste im Falle eines Vorfalls und nach einem Vorfall	✓	• Richtlinien 60-65 erledigt? • Eventuelle Incidents dokumentiert?

- Bearbeitungsverzeichnis mit vorgegebenen Textcontainern und branchenspezifischen Inhaltsvorschlägen, inkl. aktuellen Rechtsgrundlagen
  --> automatisches Bearbeitungsverzeichnis
- Informationspflicht ggü. Bewohner/Angehörigen
  --> wird automatisch von Software erstellt
- Vertragsgrundlagen
  --> in Software vorhanden
- Hilfsmittel für Sicherstellen Datensicherheit
  --> in Software vorhanden, automatische Merkblätter für MA, EPD usw.

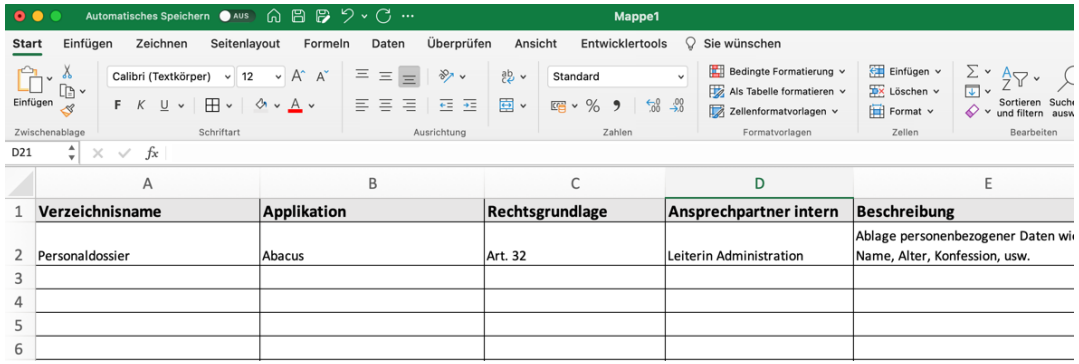
Abdeckung Punkte aus Artiset-Checkliste: https://www.siriusag.com/files/pdf/checkliste-artiset_kommentar-sirius.pdf

Umsetzung Verzeichnis

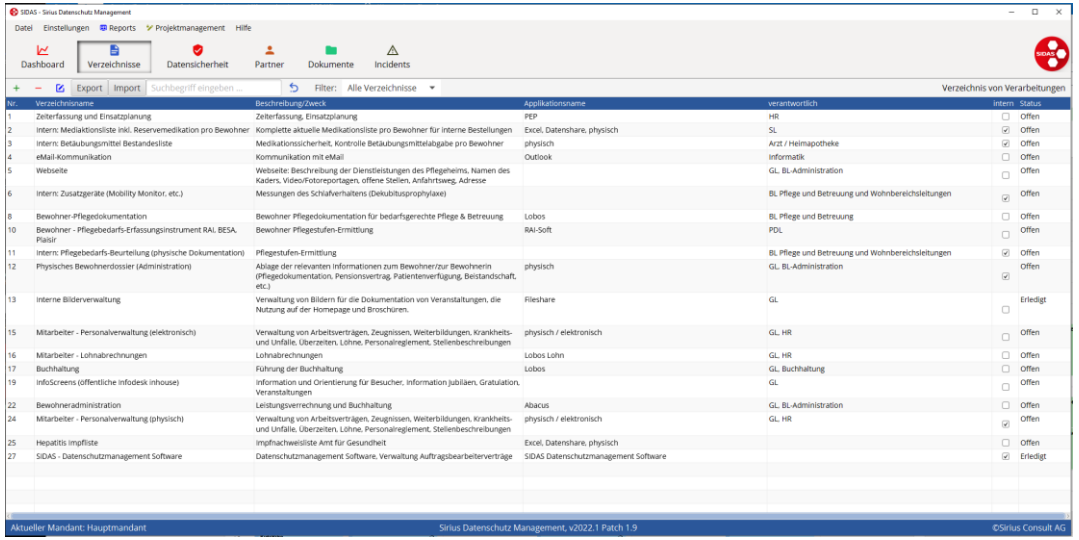
sevida
ganzheitlich gelöst.

Führen des Verzeichnisses (Software und physische/elektronische Ablage)

- Details zum Verzeichnis
- Rechtsgrundlage
- Interne Ansprechpartner:innen
- Beschreibung des Verzeichnisses, Zweck, Interesse, Speicher/Löschfrist usw.
- Angaben (Einschätzung) zu
  - Vertraulichkeit
  - Verfügbarkeit
  - Integrität



	A	B	C	D	E
1	**Verzeichnisname**	**Applikation**	**Rechtsgrundlage**	**Ansprechpartner intern**	**Beschreibung**
2	Personaldossier	Abacus	Art. 32	Leiterin Administration	Ablage personenbezogener Daten wi Name, Alter, Konfession, usw.
3					
4					
5					
6					



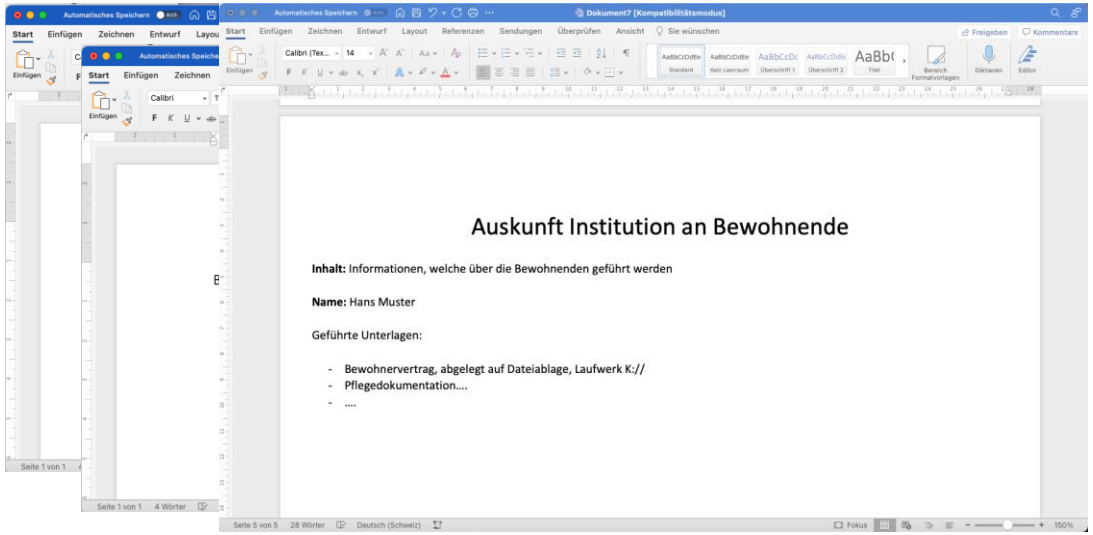
Informationspflichten

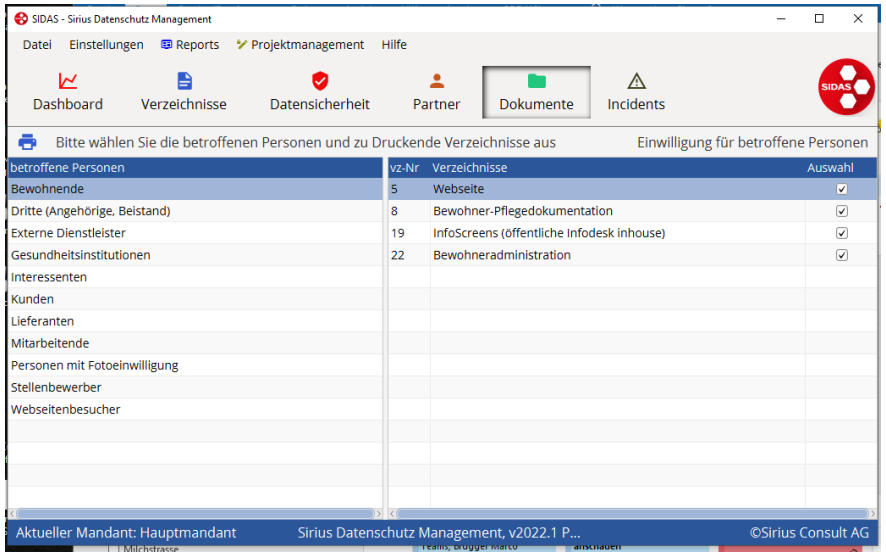
sevida
ganzheitlich gelöst.

Informationen an Bewohner:innen, Angehörige, Lieferanten usw.

- Automatische Verfügbarkeit von Datenschutzerklärungen und Dokumenten für die Bescheinigung von Einwilligungen

- Nachvollziehbarkeit, wer wann welche Einwilligung benötigt





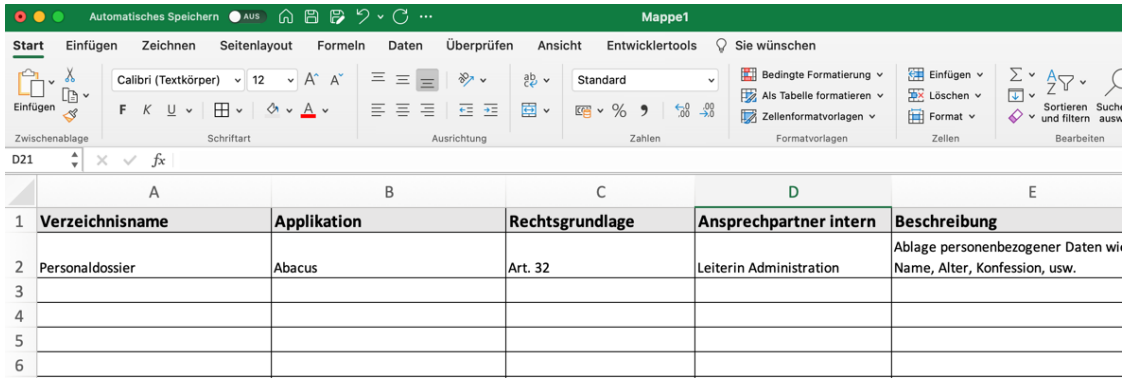
Datensicherheit

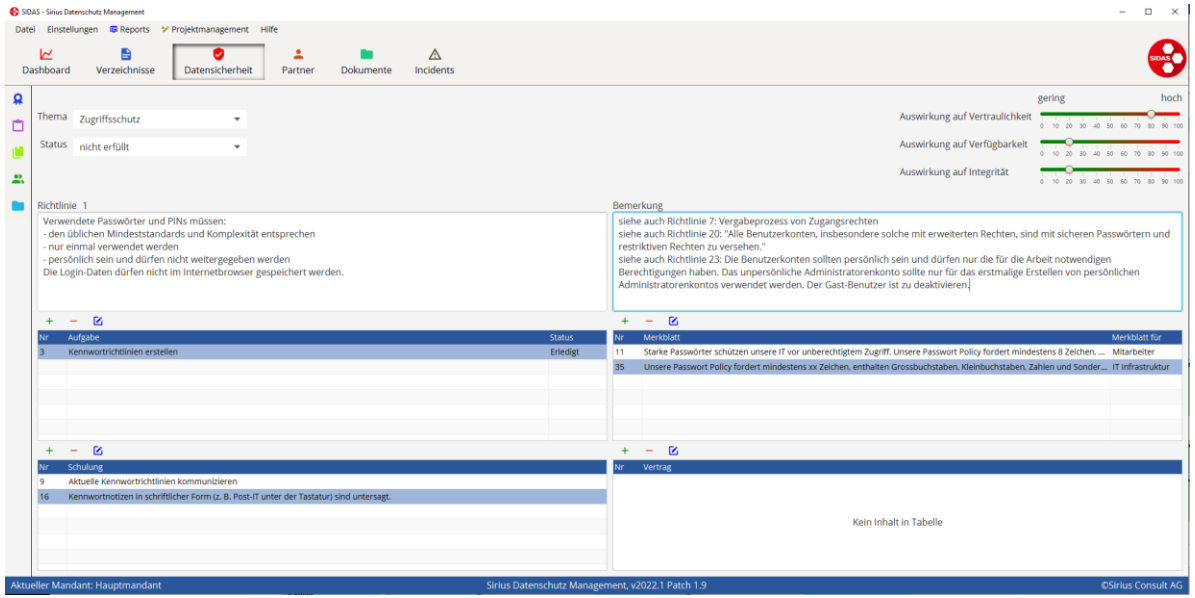
sevida
ganzheitlich gelöst.

Bewertung und Risikoeinschätzung

- Grundlage für die Erstellung eines Datenschutzreglementes

- Vorlagen-Richtlinien mit dazugehörigen Aufgaben etc. – beliebig erweiterbar



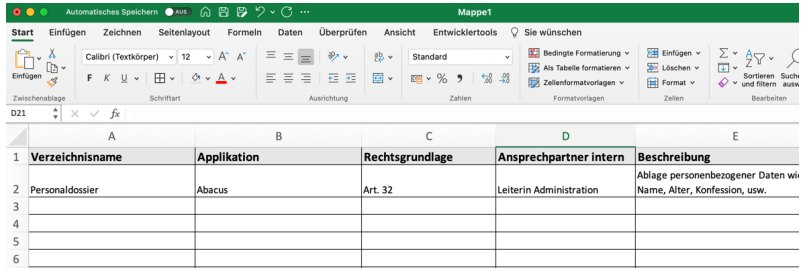


Datenschutz im laufenden Betrieb

sevida
ganzheitlich gelöst.

Aufgaben und Übersicht allgemein sicherstellen

- Sind alle Verzeichnisse nachgeführt?
- Wurden die Datenschutz-Massnahmen geplant und umgesetzt?
- Risikobewertungen bezüglich Vertraulichkeit, Verfügbarkeit und Integrität
- Übersicht über die Erfüllung der Datensicherheitsrichlinien
- Wurden alle Datensicherheitsaufgaben erledigt?



	A	B	C	D	E
1	**Verzeichnisname**	**Applikation**	**Rechtsgrundlage**	**Ansprechpartner intern**	**Beschreibung**
2	Personaldossier	Abacus	Art. 32	Leiterin Administration	Ablage personenbezogener Daten wi Name, Alter, Konfession, usw.
3					
4					
5					
6					

Weitere Aufgaben

- Auskunftspflicht sicherstellen
- Löschpflicht gewährleisten
- Massnahmen bei Ein-/Austritte MA oder BW
- Meldung bei Datenschutz-Vorfällen
- Notfallkonzept

Kantonale Unterschiede

sevida
ganzheitlich gelöst.

Unterschiede möglich bei

- Haftung bezüglich Verletzungen BW-seitig
- Institution muss sämtliche kantonalen Bestimmungen einhalten

Jedoch überall notwendig

- Führen eines Verzeichnisses
- Informationspflichten
- Anpassung Verträge und Vereinbarungen
- Sensibilisierung und Schulung Mitarbeitende
- Prüfung und Umsetzung technischer Massnahmen (Netzwerk, Firewall, Passwörter usw.)
- Mitarbeitende unterstehen revDSG

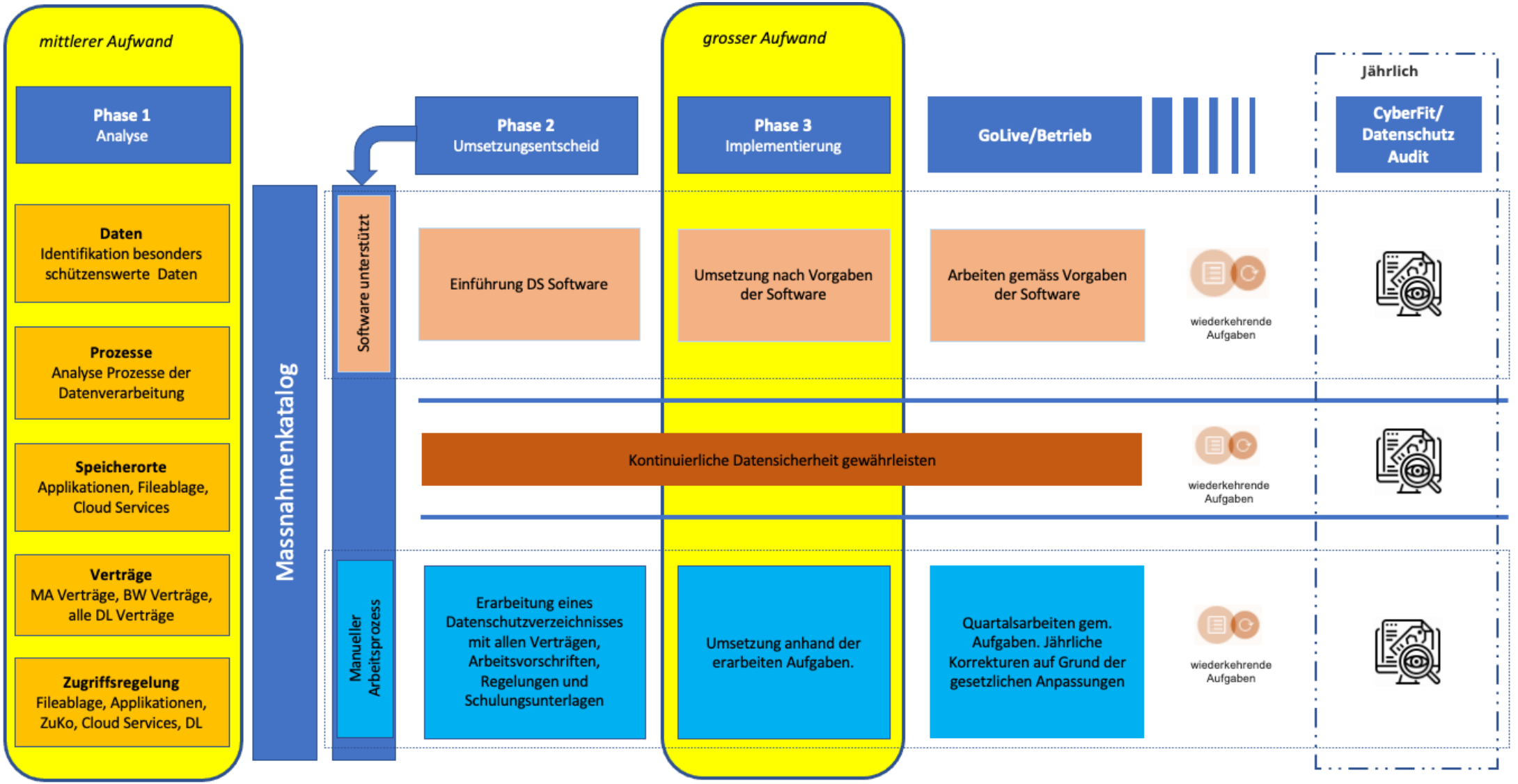
Umsetzung mit Tool vs. Manuell

sevida
ganzheitlich gelöst.

	Manuelle Umsetzung	Umsetzung mit DSG-Tool
Vorteile	Nach Kurs oder CAS vertieftes eigenes Know-How Möglichkeit, Verzeichnis, Nachweise, Verträge komplett selber zu gestalten/erstellen	Hohe Rechtssicherheit Gesetzliche Anpassungen über Updates Rückmeldung zu Auskunftsbegehren per Knopfdruck Effiziente Umsetzung, grosse Zeitersparnis Schulung Projektleitung inkl. Umsetzung Zentrale Ansprechpartner/Unterstützung Best Practice Ansatz
Nachteile	Grosses Wissen bezüglich Datenschutz notwendig Eigene Hilfsmittel/Tabellen für Verzeichnisse und Betrieb Keine Vertragsvorlagen Auskunftspflichten ohne Vorlagen Risiko bei Ausfall der Person, welche für Datenschutz verantwortlich ist Know-How muss zusammengesucht werden	Weiteres Softwaretool Laufende Softwarekosten (730 CHF/Jahr)

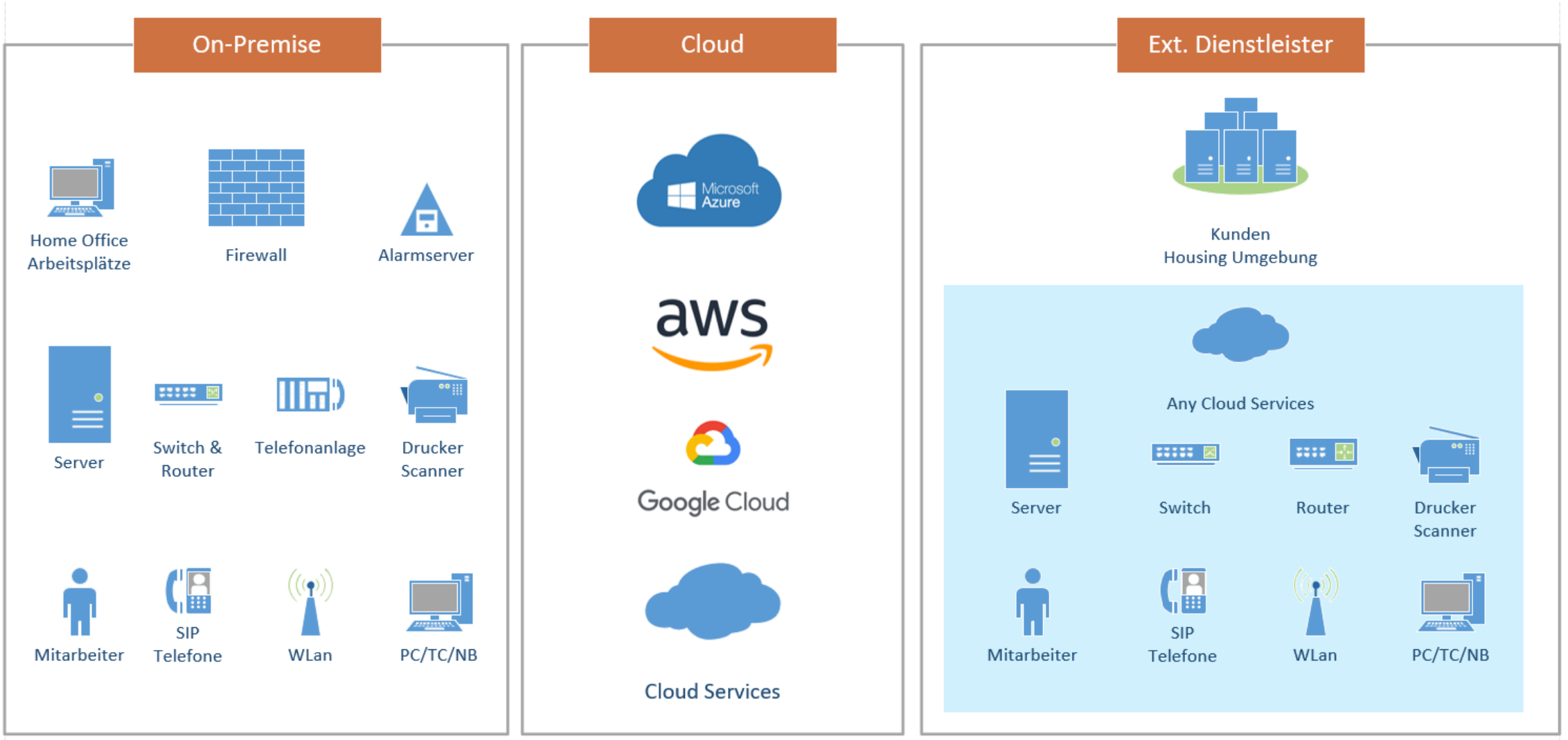
Umsetzung konkretisiert

sevida
ganzheitlich gelöst.



Tragweite der Datensicherheit

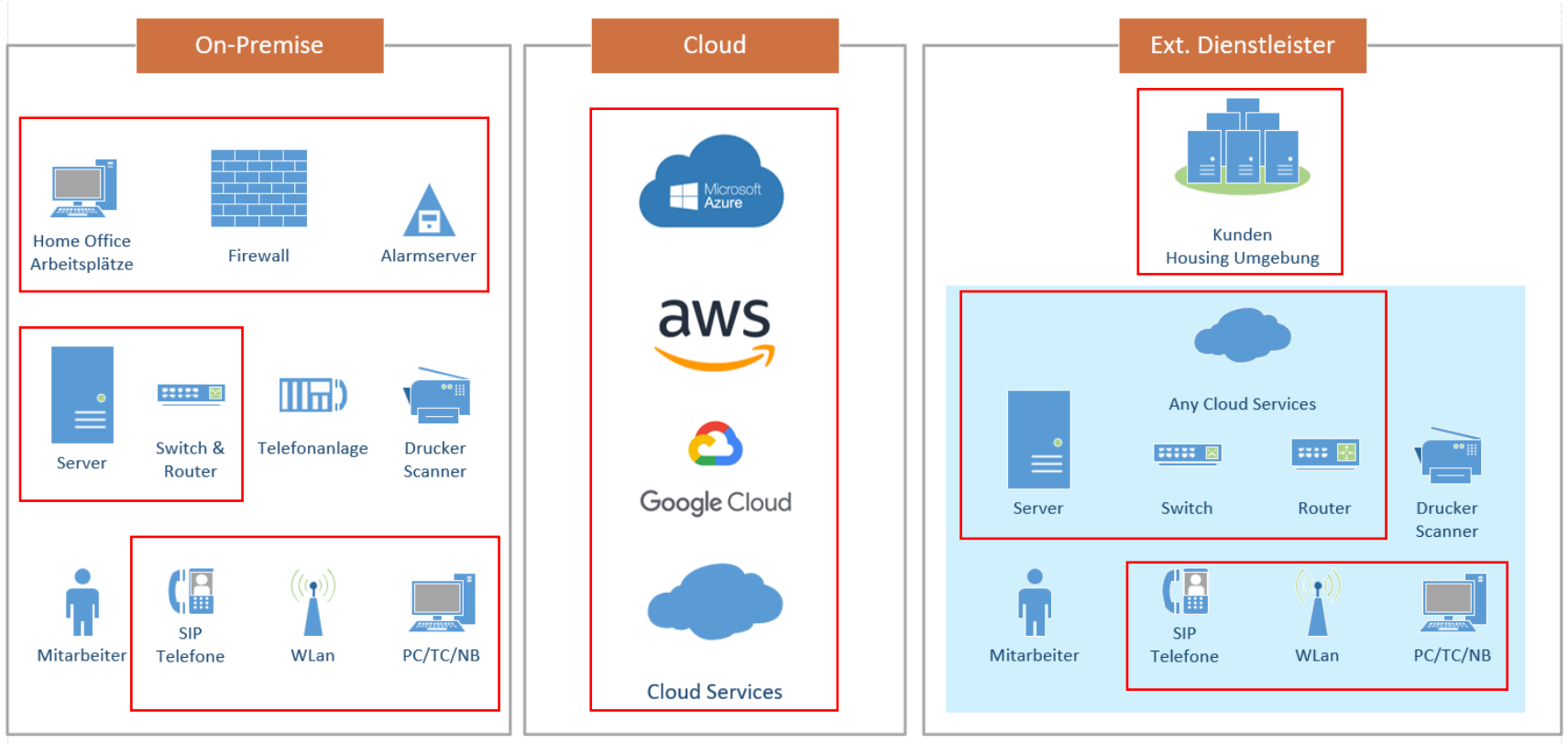
sevida
ganzheitlich gelöst.



Beispiel

sevida
ganzheitlich gelöst.

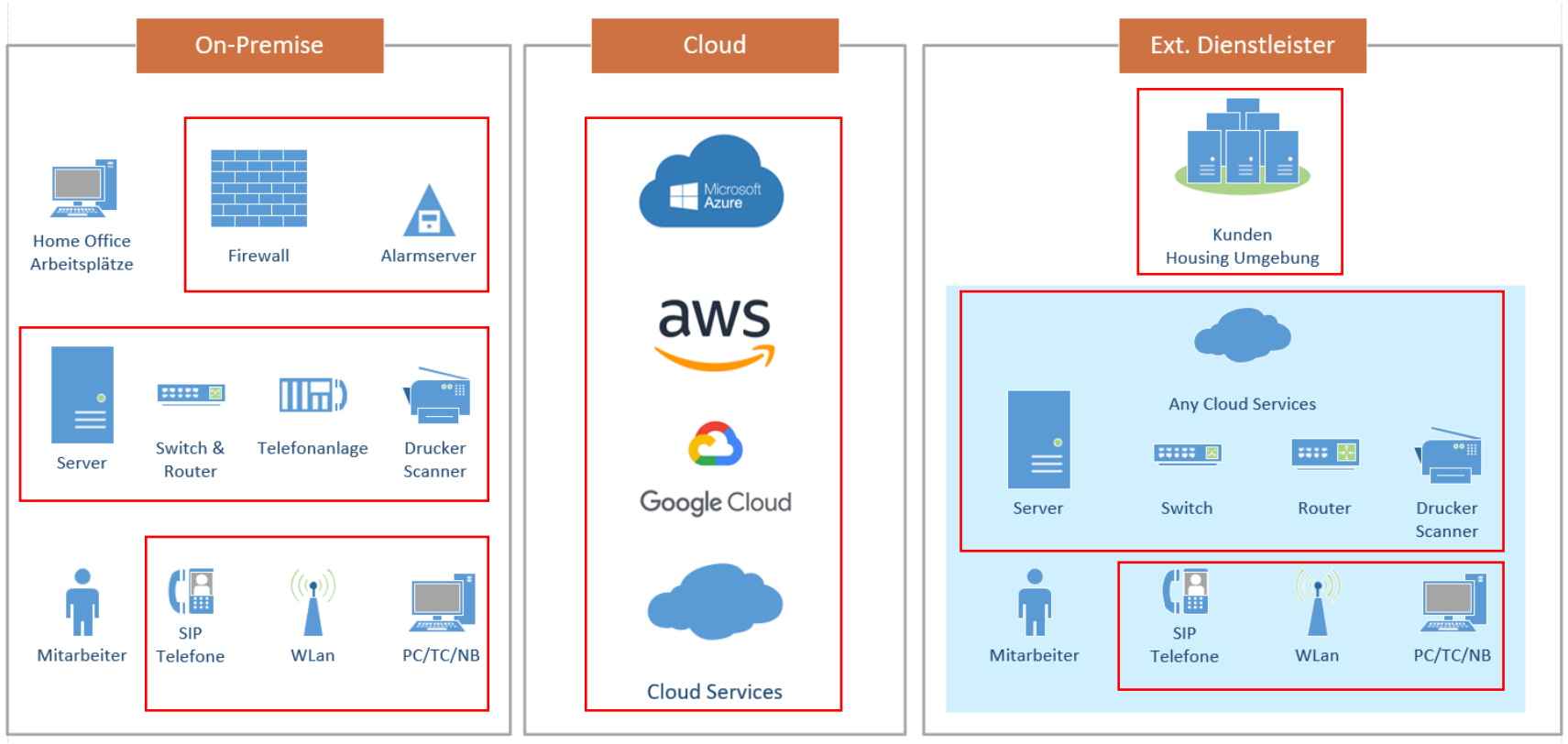
Datensicherheits-Richtlinie: Zur Überwachung des Netzwerkes sind Einbruchserkennungs- und Einbruchsverhinderungslösungen einzusetzen (IDS oder IPS).



Beispiel

sevida
ganzheitlich gelöst.

Datensicherheits-Richtlinie: Der Zugriff auf Kernsysteme durch Administratoren muss mittels einer Zwei-Faktor-Authentifizierung (2FA) erfolgen.



Von der Zitrone zum Limoncello, 360 Grad

sevida
ganzheitlich gelöst.

ARTISET CURAVIVA INSOS YOUVITA senesuisse

#	Thema / Prüfpunkte	Resultat Beurteilung IST-Zustand	Vorschläge für Massnahmen	Termin	Verantwortlich
1	**Allgemeines / Ausgangslage**				
1.1	Wird Datenschutz in der Institution systematisch geplant und koordiniert?		▪ Grundsätze in Datenschutzkonzept festhalten ▪ Datenschutz ab Planung einer Datenbearbeitung berücksichtigen		
1.2	Wann und wie wird der Datenschutz thematisiert und Situation beurteilt in: ▪ Stiftungsrat/Vorstand? ▪ Geschäftsleitung?		▪ Erlass Datenschutzkonzept durch Stiftungsrat/Vorstand ▪ Datenschutz als Teil des Risikomanagements regelmässig auf Führungsebene behandeln		
1.3	Sind Grundsätze der Datenbearbeitung und Schutzmassnahmen bereits dokumentiert (Datenschutzkonzept, interne Reglemente und Weisungen etc.)?		▪ Datenschutzkonzept erstellen ▪ Datenschutzweisung erstellen		
1.4	Gab es bisher bereits besondere Vorfälle bzw. Probleme bzgl. Datenschutz?		Gemachte Erfahrungen berücksichtigen		
1.5	Untersteht die Institution		▪ Unterstellung klären		

Nächste Schritte

sevida
ganzheitlich gelöst.

1. Internes Projekt-Team bilden

2. Handlungsfelder identifizieren/priorisieren
   a) Entscheid Umsetzung mit/ohne Tool
   b) Rollen besetzen, Ausbildungsbedarf/Ausbildungen
   c) Entscheid Umsetzung mit/ohne externe Unterstützung

3. Massnahmen festlegen inkl. Budget

4. Umsetzung der technischen und organisatorischen Massnahmen

Empfehlung

Handeln Sie jetzt (keine Übergangsfrist des revDSG), Umsetzung muss am 1.9.2023 abgeschlossen sein