

Datenschutz und ICT

von der Zitrone zum Limoncello



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

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

Datenschutzgrundverordnung (DSGVO, 2018)

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

- Datenverarbeitung
- Datenspeicherung und
- Datenweiterleitung

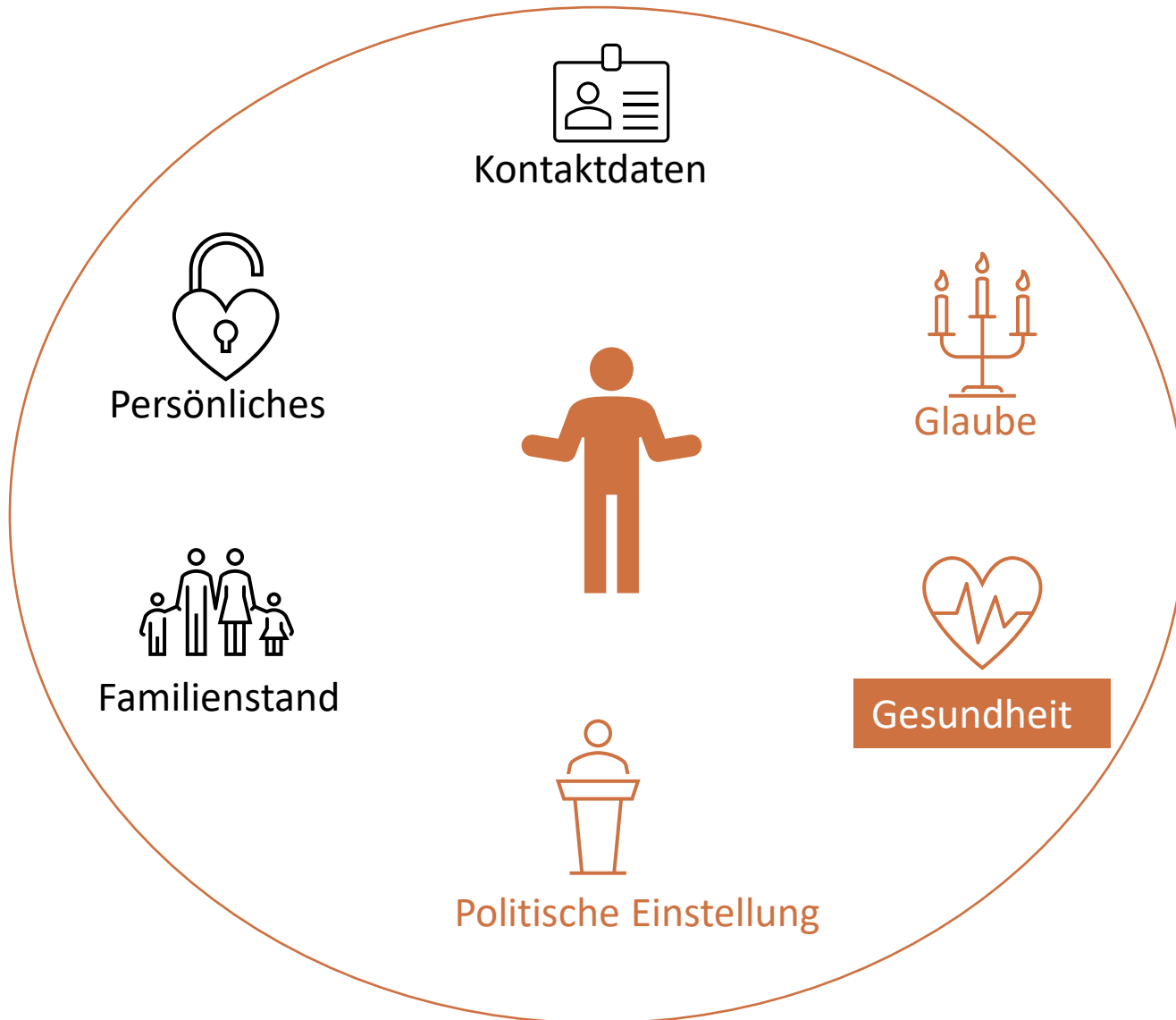


Angemessenheitsbeschluss

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

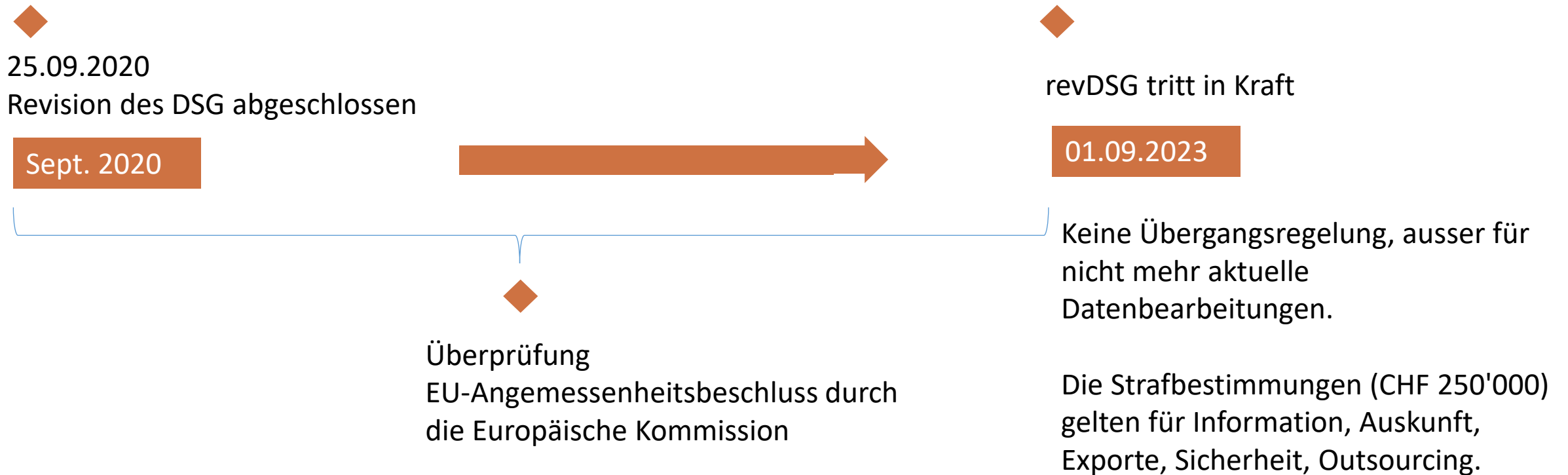


Datenschutz im Gesundheitswesen



Besonders schützenswerte
Daten (sensible Daten
personenbezogen)

Datenschutz Status Quo



Aufgaben und Pflichten bezüglich Datenschutz

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 externe IT

Interne Aufwände für Umsetzung

	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)	Ca. 16 Std.	Ca. 2 Std.
Umsetzung der technischen Richtlinien und Arbeitsvorschriften	Ca. 16 – 24 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








ARTISET CURAVIVA INESYS YOUWITA 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?		<ul style="list-style-type: none"> ▪ Grundsätze in Datenschutzkonzept festhalten ▪ Datenschutz ab Planung einer Datenbearbeitung berücksichtigen 		
1.2	Wann und wie wird der Datenschutz thematisiert und Situation beurteilt in: <ul style="list-style-type: none"> ▪ Stiftungsrat/Vorstand? ▪ Geschäftsleitung? 		<ul style="list-style-type: none"> ▪ 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.)?		<ul style="list-style-type: none"> ▪ Datenschutzkonzept erstellen ▪ Datenschutzweisung erstellen 		
1.4	Gab es bisher bereits besondere Vorfälle bzw. Probleme bzgl. Datenschutz?		Gemachte Erfahrungen berücksichtigen		
1.5	Untersteht die Institution		<ul style="list-style-type: none"> ▪ 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

#	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 <ul style="list-style-type: none"> • „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		<ul style="list-style-type: none"> • 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

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

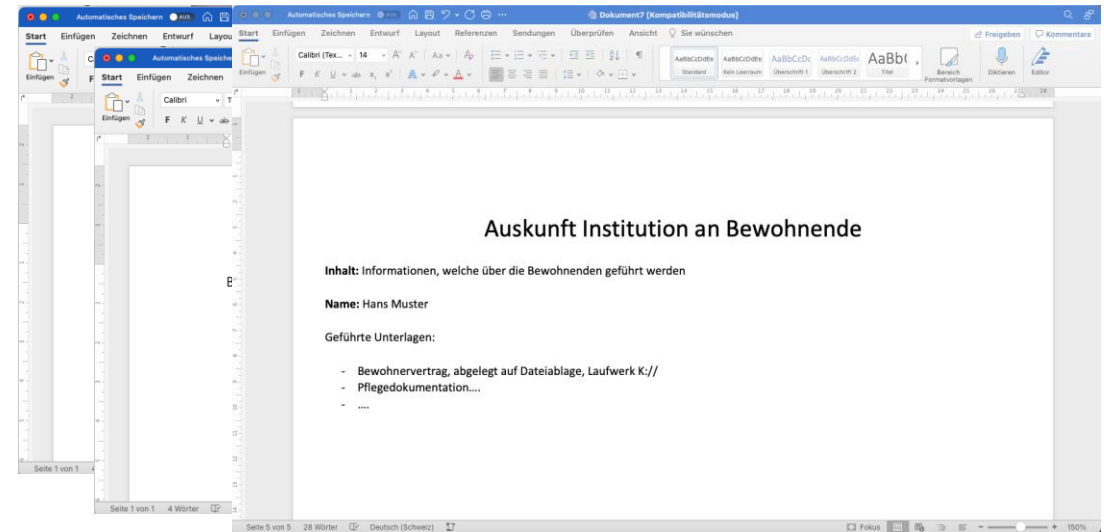
	A	B	C	D	E
1	Verzeichnisname	Applikation	Rechtsgrundlage	Ansprechpartner intern	Beschreibung
2	Personaldossier	Abacus	Art. 32	Leiterin Administration	Ablage personenbezogener Daten wie Name, Alter, Konfession, usw.
3					
4					
5					
6					

No.	Verzeichnisname	Beschreibung/Zweck	Applikationsname	verantwortlich	Intern	Status
1	Zelterfassung und Einsatzplanung	Zelterfassung, Einsatzplanung	PEP	HR	<input type="checkbox"/>	Offen
2	intern: Medikationsliste inkl. Reservemedikation pro Bewohner	Komplette aktuelle Medikationsliste pro Bewohner für interne Bestellungen	Excel, DataShare, physisch	SL	<input checked="" type="checkbox"/>	Offen
3	intern: Beladungsmittel Bestandsliste	Medikationssicherheit, Kontrolle Beladungsmittelabgabe pro Bewohner	physisch	Aziz / Heimpapotheke	<input checked="" type="checkbox"/>	Offen
4	eMail-Kommunikation	Kommunikation mit eMail	Outlook	InformaStk	<input type="checkbox"/>	Offen
5	Website	Website: Beschreibung der Dienstleistungen des Pflegeheims, Namen des Kaders, Video/Fotoreportagen, offene Stellen, Anfahrtsweg, Adresse		GL, BL-Administration	<input type="checkbox"/>	Offen
6	intern: Zusatzgeräte (Mobility Monitor, etc.)	Messungen des Schlafverhaltens (Dekubitusprophylaxe)		BL Pflege und Betreuung und Wohnbereichsleitungen	<input checked="" type="checkbox"/>	Offen
8	Bewohner-Pflegedokumentation	Bewohner Pflegedokumentation für bedarfsgerechte Pflege & Betreuung	Lobos	BL Pflege und Betreuung	<input type="checkbox"/>	Offen
10	Bewohner - Pflegebedarfs-Erfassungsinstrument RAI, BESA, Palstr	Bewohner Pflegestufen-Ermittlung	RAI-Soft	PDL	<input type="checkbox"/>	Offen
11	intern: Pflegebedarfs-Beurteilung (physische Dokumentation)	Pflegestufen-Ermittlung		BL Pflege und Betreuung und Wohnbereichsleitungen	<input checked="" type="checkbox"/>	Offen
12	Physisches Bewohnerdossier (Administration)	Ablage der relevanten Informationen zum Bewohner/zur Bewohnerin (Pflegedokumentation, Pensionsvertrag, Patientenverfügung, Bestandschaft, etc.)	physisch	GL, BL-Administration	<input checked="" type="checkbox"/>	Offen
13	interne Bilderverwaltung	Verwaltung von Bildern für die Dokumentation von Veranstaltungen, die Nutzung auf der Homepage und Broschüren.	Fileshare	GL	<input type="checkbox"/>	Erledigt
15	Mitarbeiter - Personalverwaltung (elektronisch)	Verwaltung von Arbeitsverträgen, Zeugnissen, Weiterbildungen, Krankheits- und Unfälle, Überzeiten, Löhne, Personalreglement, Stellenbeschreibungen	physisch / elektronisch	GL, HR	<input type="checkbox"/>	Offen
16	Mitarbeiter - Lohnabrechnungen	Lohnabrechnungen	Lobos Lohn	GL, HR	<input type="checkbox"/>	Offen
17	Buchhaltung	Führung der Buchhaltung	Lobos	GL, Buchhaltung	<input type="checkbox"/>	Offen
19	InfoScreens (öffentliche Infodesk inhouse)	Information und Orientierung für Besucher, Information Jubiläen, Gratulation, Veranstaltungen		GL	<input type="checkbox"/>	Offen
22	Bewohneradministration	Leistungsverrechnung und Buchhaltung	Abacus	GL, BL-Administration	<input type="checkbox"/>	Offen
24	Mitarbeiter - Personalverwaltung (physisch)	Verwaltung von Arbeitsverträgen, Zeugnissen, Weiterbildungen, Krankheits- und Unfälle, Überzeiten, Löhne, Personalreglement, Stellenbeschreibungen	physisch / elektronisch	GL, HR	<input checked="" type="checkbox"/>	Offen
25	Heppitätis Impfstoffe	Impfstoffe	Excel, DataShare, physisch		<input type="checkbox"/>	Offen
27	SIDAS - Datenschutzmanagement Software	Datenschutzmanagement Software, Verwaltung Auftragsbearbeitungsverträge	SIDAS Datenschutzmanagement Software		<input checked="" type="checkbox"/>	Erledigt

Informationspflichten

Informationen an Bewohner:innen,
Angehörige, Lieferanten usw.

- Automatische Verfügbarkeit von Datenschutzerklärungen und Dokumenten für die Bescheinigung von Einwilligungen
- Nachvollziehbarkeit, wer wann welche Einwilligung benötigt



betroffene Personen	vz-Nr	Verzeichnisse	Auswahl
Bewohnende	5	Webseite	<input checked="" type="checkbox"/>
Dritte (Angehörige, Beistand)	8	Bewohner-Pflegedokumentation	<input checked="" type="checkbox"/>
Externe Dienstleister	19	InfoScreens (öffentliche Infodesk inhouse)	<input checked="" type="checkbox"/>
Gesundheitsinstitutionen	22	Bewohneradministration	<input checked="" type="checkbox"/>
Interessenten			
Kunden			
Lieferanten			
Mitarbeitende			
Personen mit Fotoeinwilligung			
Stellenbewerber			
Webseitenbesucher			

Bewertung und Risikoeinschätzung

- Grundlage für die Erstellung eines Datenschutzreglementes
- Vorlagen-Richtlinien mit dazugehörigen Aufgaben etc. – beliebig erweiterbar

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

Sirius Datenschutz Management

Thema: Zugriffsschutz
Status: nicht erfüllt

Auswirkung auf Vertraulichkeit: gering bis hoch
Auswirkung auf Verfügbarkeit: 0 bis 100
Auswirkung auf Integrität: 0 bis 100

Richtlinie 1
Verwendete Passwörter und PINs müssen:
- den üblichen Mindeststandards und Komplexität entsprechen
- nur einmal verwendet werden
- persönlich sein und dürfen nicht weitergegeben werden
Die Login-Daten dürfen nicht im Internetbrowser gespeichert werden.

Bemerkung
siehe auch Richtlinie 7: Vergabeprozess von Zugangsrechten
siehe auch Richtlinie 20: "Alle Benutzerkonten, insbesondere solche mit erweiterten Rechten, sind mit sicheren Passwörtern und restriktiven Rechten zu versehen."
siehe auch Richtlinie 23: Die Benutzerkonten sollten persönlich sein und dürfen nur für die Arbeit notwendigen Berechtigungen haben. Das unpersönliche Administratorkonto sollte nur für das erstmalige Erstellen von persönlichen Administratorkonten verwendet werden. Der Gast-Benutzer ist zu deaktivieren.

Nr	Aufgabe	Status	Nr	Merktblatt	Merktblatt für
3	Kenntwortrichtlinien erstellen	Erledigt	11	Starke Passwörter schützen unsere IT vor unberechtigtem Zugriff. Unsere Passwort Policy fordert mindestens 8 Zeichen...	Mitarbeiter
			35	Unsere Passwort Policy fordert mindestens xx Zeichen, enthalten Grossbuchstaben, Kleinbuchstaben, Zahlen und Sonder...	IT Infrastruktur

Kein Inhalt in Tabelle

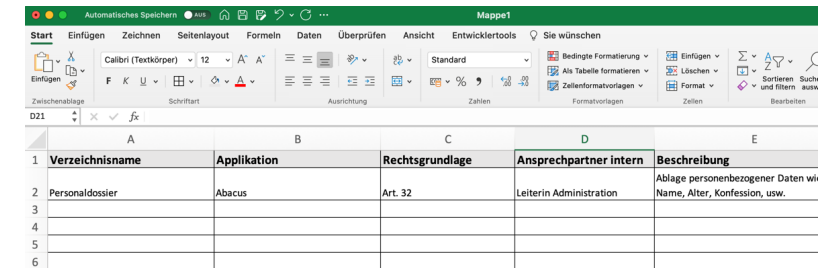
Datenschutz im laufenden Betrieb

Aufgaben und Übersicht allgemein sicherstellen

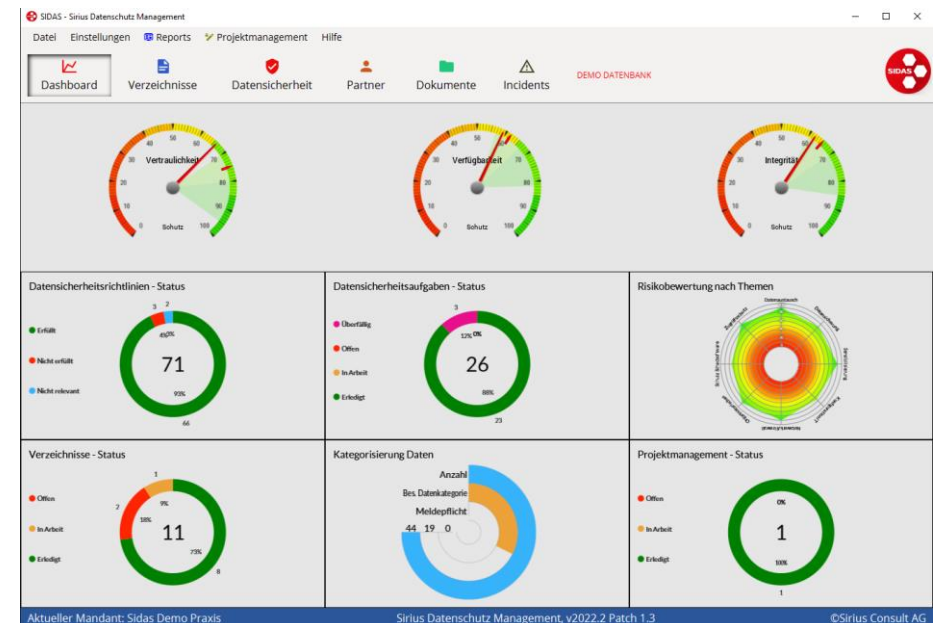
- Sind alle Verzeichnisse nachgeführt?
- Wurden die Datenschutz-Massnahmen geplant und umgesetzt?
- Risikobewertungen bezüglich Vertraulichkeit, Verfügbarkeit und Integrität
- Übersicht über die Erfüllung der Datensicherheitsrichtlinien
- Wurden alle Datensicherheitsaufgaben erledigt?

Weitere Aufgaben

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



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



Kantonale Unterschiede

Unterschiede möglich bei

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



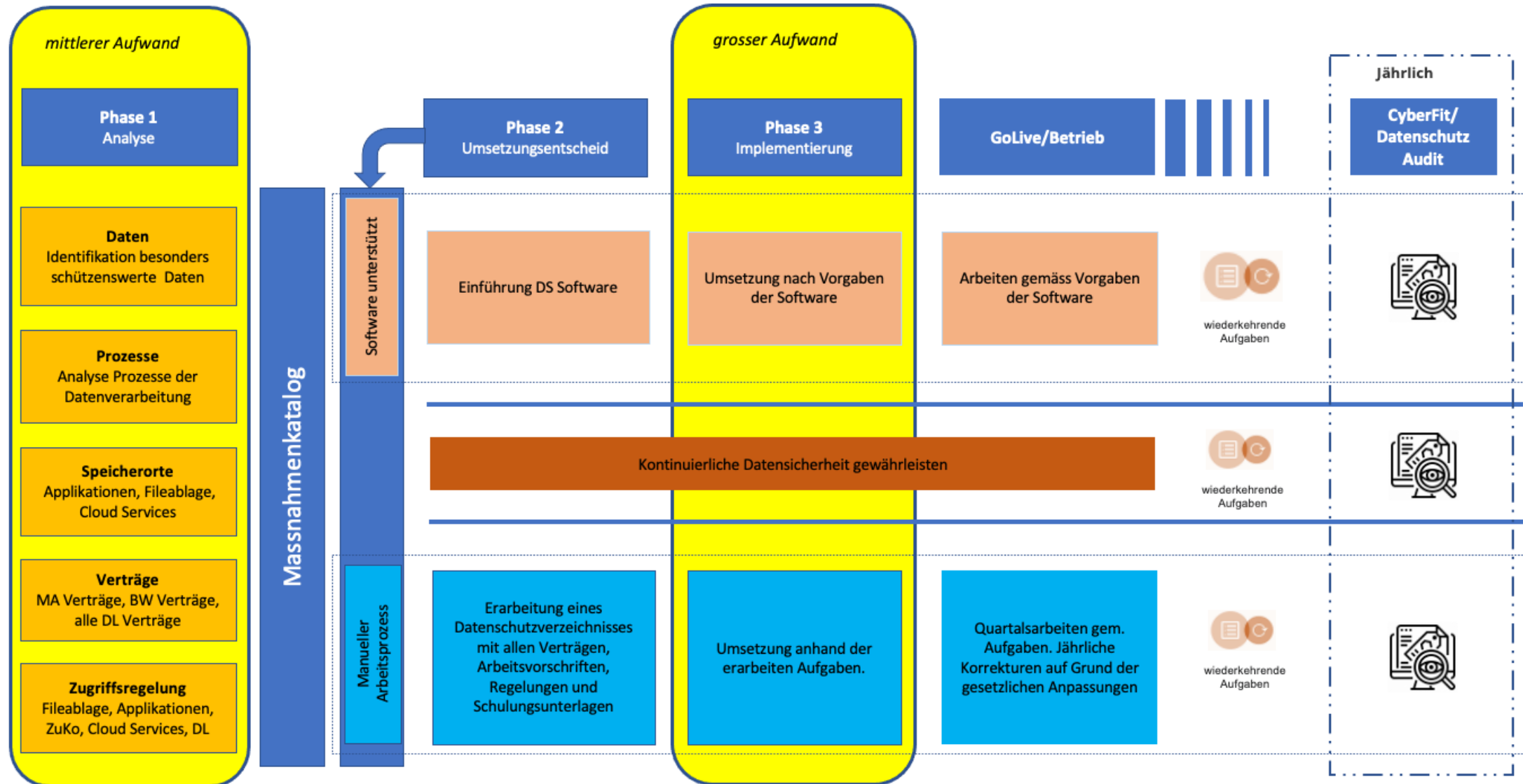
Jedoch überall notwendig

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

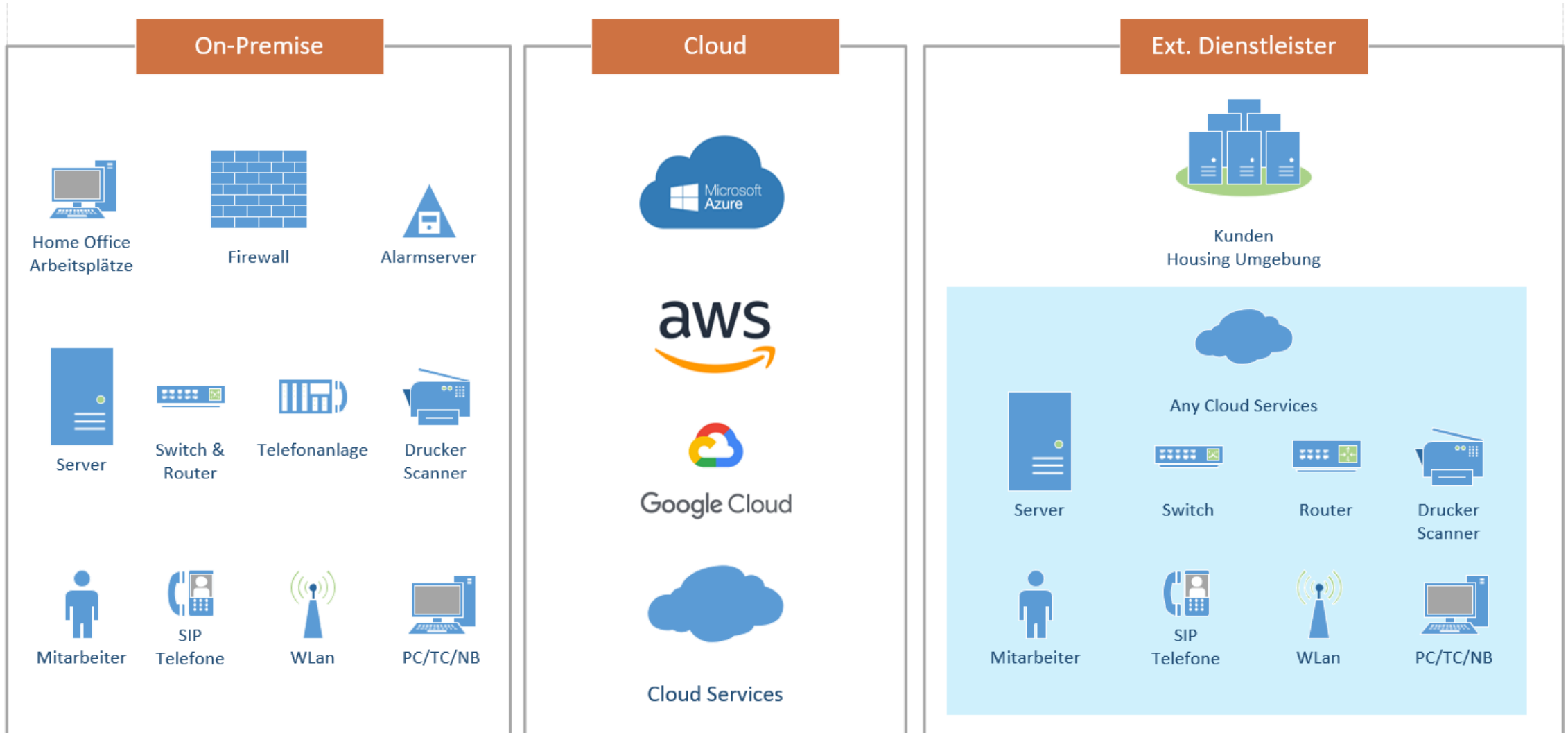
Umsetzung mit Tool vs. Manuell

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

Umsetzung konkretisiert

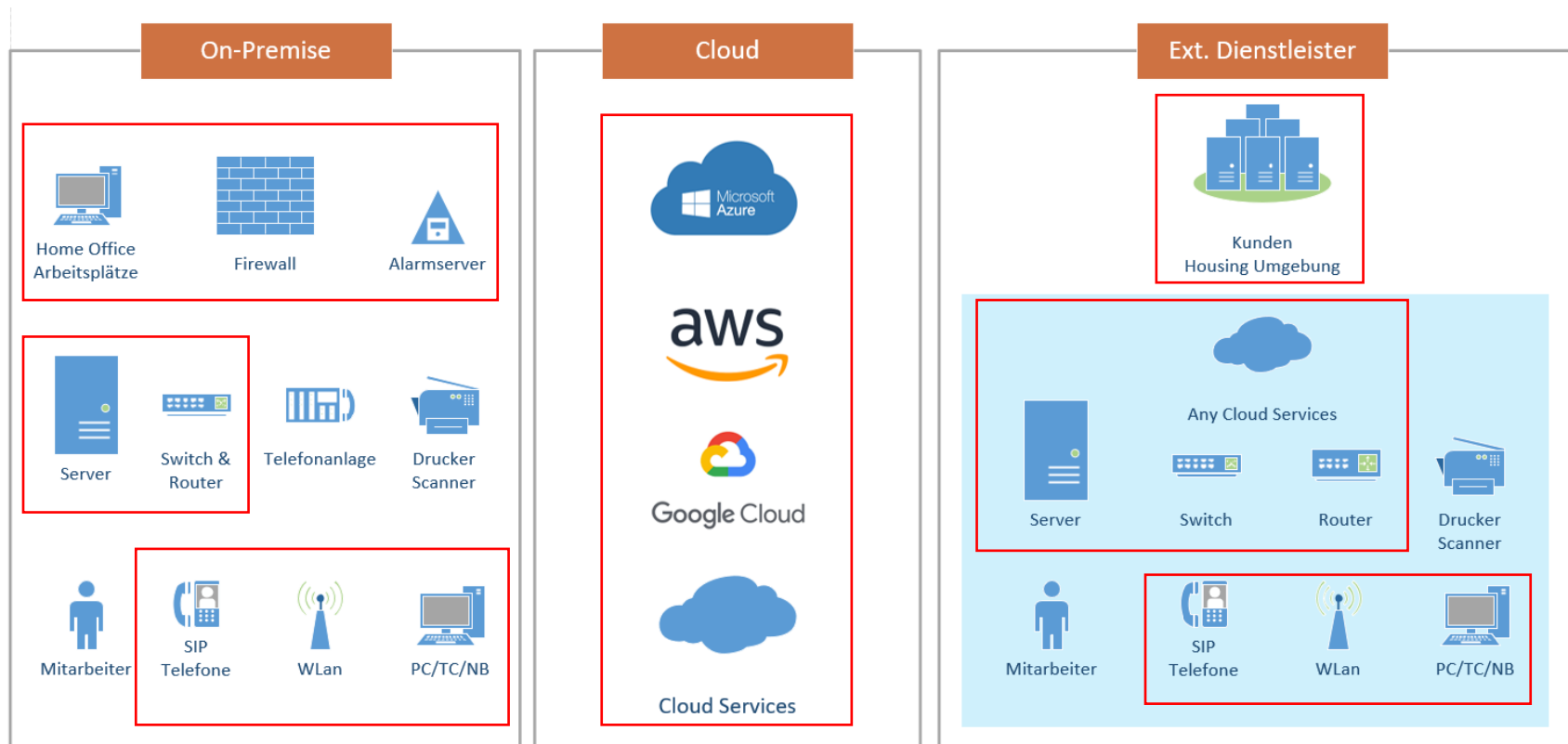


Tragweite der Datensicherheit



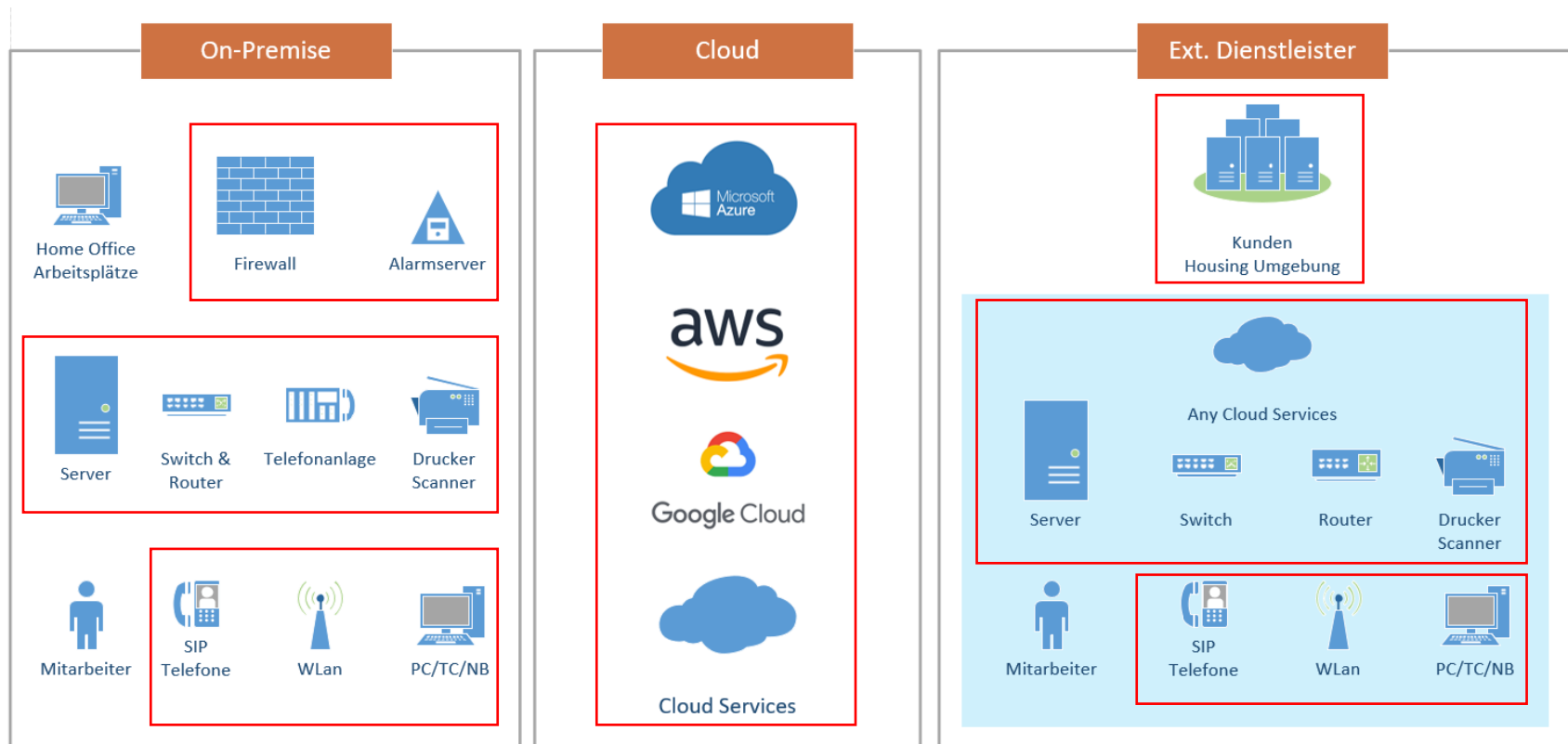
Beispiel

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



Beispiel

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



Von der Zitrone zum Limoncello, 360 Grad

ARTISET CURAVIVA INNOSTOS 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?		<ul style="list-style-type: none"> ▪ Grundsätze in Datenschutzkonzept festhalten ▪ Datenschutz ab Planung einer Datenbearbeitung berücksichtigen 		
1.2	Wann und wie wird der Datenschutz thematisiert und Situation beurteilt in: <ul style="list-style-type: none"> ▪ Stiftungsrat/Vorstand? ▪ Geschäftsleitung? 		<ul style="list-style-type: none"> ▪ 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.)?		<ul style="list-style-type: none"> ▪ Datenschutzkonzept erstellen ▪ Datenschutzweisung erstellen 		
1.4	Gab es bisher bereits besondere Vorfälle bzw. Probleme bzgl. Datenschutz?		Gemachte Erfahrungen berücksichtigen		
1.5	Untersteht die Institution		<ul style="list-style-type: none"> ▪ Unterstellung klären 		

Nächste Schritte

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