



Auftragsbearbeitungsvertrag

Vertrag über die Auftragsbearbeitung der Personendaten

Gemäss Art. 9 Abs. 1 Bundesgesetz über den Datenschutz vom 25. September 2020
(DSG)

zwischen

Gemeinde Buchrain
Hauptstrasse 18
CH-6033 Buchrain

(Verantwortlicher- nachfolgend: Auftraggeber)

und

achermann ict-services ag
Grabenhofstrasse 4
CH-6010 Kriens

(Auftragsbearbeiter- nachfolgend: Auftragnehmer)

Version 1.0
23.09.2024

Inhaltsverzeichnis

1	Parteien	4
1.1	Hauptvertrag der Parteien	4
2	Gegenstand und Dauer des Vertrages	4
2.1	Gegenstand	4
2.2	Dauer	4
3	Konkretisierung des Vertragsinhaltes	4
3.1	Grundsatz	4
3.2	Bekanntgabe von Personendaten ins Ausland	4
4	Technisch-Organisatorische Massnahmen	5
4.1	Umsetzung und Anpassung	5
4.2	Datensicherheit	5
4.3	Technischer Fortschritt und adäquate Massnahmen	5
5	Berichtigung, Einschränkung und Löschung von Daten	5
5.1	Grundsatz	5
5.2	Sicherstellung weiterer Rechte	5
6	Qualitätssicherung und sonstige Pflichten des Auftragnehmers	6
6.1	Wahrung der Vertraulichkeit	6
6.2	Kooperation mit Aufsichtsbehörden	6
6.3	Informationen über Kontrollhandlungen der Aufsichtsbehörde	6
6.4	Unterstützung bei Widrigkeiten	6
6.5	Regelmässige Kontrollen der internen Prozesse	7
6.6	Nachweisbarkeit der Massnahmen	7
7	Unterauftragsverhältnisse	7
7.1	Grundsatz	7
7.2	Zulässige Unterauftragsverhältnisse	7
7.3	Weitergabe von Daten an Unterauftragnehmer	8
7.4	Unterauftragsverhältnisse ausserhalb der Schweiz	8
7.5	Unterauftragsverhältnisse des Unterauftragnehmers	8
8	Kontrollrechte des Auftraggebers	8
8.1	Grundsatz	8
8.2	Nachweise	8
8.3	Vergütungsanspruch bei Kontrollen	9
9	Mitteilung bei Verstössen des Auftragnehmers	9
9.1	Grundsatz	9
10	Weisungsbefugnis des Auftraggebers	9
10.1	Bestätigung	9
10.2	Aussetzung der Weisungen	9
11	Löschung und Rückgabe von Personendaten	10

11.1	Kopien und Duplikate der Daten	10
11.2	Vernichtung und Nachweis	10
12	Haftung und Vertragsstrafe	10
12.1	Beweislast	10
12.2	Haftung	10
12.3	Ausschliessung der Haftung	10

Anhänge

Anhang A	Technische und organisatorische Massnahmen
----------	--------------------------------------------

Entwurf

1 Parteien

Parteien	
Auftraggeber	Gemeinde Buchrain
Auftragnehmer	achermann ict-services ag

1.1 Hauptvertrag der Parteien

Name des Hauptvertrages
Rahmenvertrag vom 23.09.2024

Dieser Auftragsbearbeitungsvertrag (ABV) erweitert den Rahmenvertrag.

2 Gegenstand und Dauer des Vertrages

2.1 Gegenstand

Der Gegenstand des Vertrages ergibt sich aus dem Rahmenvertrag vom 23.09.2024, sowie den Service Verträgen, welche darin enthalten sind.

2.2 Dauer

Die Dauer dieses Vertrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung (gemäss Kapitel 1.1 und 2.1).

3 Konkretisierung des Vertragsinhaltes

3.1 Grundsatz

Der Auftragnehmer verarbeitet Daten nur für Zwecke und nur auf dokumentierte Weisung des Auftraggebers. Jede Verletzung der Datensicherheit meldet der Auftragnehmer umgehend mit allen Informationen (Art der Verletzung, Folgen, geplante und umgesetzte Massnahmen) an den Auftraggeber.

3.2 Bekanntgabe von Personendaten ins Ausland

Die Erbringung der vertraglich vereinbarten Datenbearbeitung findet ausschliesslich in der Schweiz statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf zudem nur erfolgen, wenn das in Art. 16 Abs. 1 vom Bundesrat festgestellte angemessene Schutzniveau des Landes erfüllt ist. Ausnahmen bilden die Ausführungen in Art. 17 DSGVO.

4 Technisch-Organisatorische Massnahmen

4.1 Umsetzung und Anpassung

Der Auftragnehmer hat die Umsetzung der erforderlichen technischen und organisatorischen Massnahmen vor Beginn der Bearbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung, zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben, sofern der Auftraggeber dies verlangt. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Massnahmen Grundlage des Vertrags. Soweit die Überprüfung des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

4.2 Datensicherheit

Der Auftragnehmer hat die Sicherheit gem. Art. 8 DSGVO insbesondere in Verbindung mit Art. 19 Abs. 4 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Massnahmen um Massnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen.

4.3 Technischer Fortschritt und adäquate Massnahmen

Die technischen und organisatorischen Massnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Massnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Massnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

5 Berichtigung, Einschränkung und Löschung von Daten

5.1 Grundsatz

Der Auftragnehmer darf die Daten, die im Auftrag bearbeitet werden, nicht eigenmächtig, sondern nur nach Weisung des Auftraggebers berichtigen, löschen oder deren Bearbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich, spätestens innerhalb 48 Stunden, an den Auftraggeber weiterleiten.

5.2 Sicherstellung weiterer Rechte

Soweit vom Leistungsumfang beinhaltet, sind Rechte der Betroffenen wie die Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

6 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer kann zusätzlich zu der Einhaltung der Regelungen dieses Vertrags den gesetzlichen Vorschlag eines Datenschutzberaters gemäss Art. 10 DSG gewährleisten. Dessen aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

6.1 Wahrung der Vertraulichkeit

Auftragnehmer setzt bei der Durchführung der Arbeiten nur Mitarbeitende ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu den Personendaten hat, dürfen diese Daten ausschliesslich entsprechend der Weisung des Auftraggebers bearbeiten, einschliesslich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur eigenen Bearbeitung verpflichtet sind.

6.2 Kooperation mit Aufsichtsbehörden

Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde, namentlich dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB), bei der Erfüllung seiner Aufgaben zusammen. Anfragen von Aufsichtsbehörden direkt an den Auftragnehmer sind unverzüglich, spätestens jedoch innerhalb 48 Stunden, dem Auftraggeber mitzuteilen.

6.3 Informationen über Kontrollhandlungen der Aufsichtsbehörde

Die unverzügliche (jedoch spätestens innerhalb 48 Stunden) Information des Auftragnehmers über Kontrollhandlungen und Massnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen, wird vom Auftragnehmer gewährleistet. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Strafverfahrens in Bezug auf die Bearbeitung von Personendaten bei der Auftragsbearbeitung beim Auftragnehmer ermittelt.

6.4 Unterstützung bei Widrigkeiten

Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsbearbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

6.5 Regelmässige Kontrollen der internen Prozesse

Der Auftragnehmer kontrolliert regelmässig in angemessenen verhältnismässigen Abständen die internen Prozesse sowie die technischen und organisatorischen Massnahmen, um zu gewährleisten, dass die Bearbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Schweizer Datenschutzrechts und diesem Vertrag erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.

6.6 Nachweisbarkeit der Massnahmen

Alle getroffenen Massnahmen zur Sicherheit der Daten in Zusammenhang mit der Auftragsbearbeitung müssen nachweisbar sein, seien es technische oder organisatorische Massnahmen.

7 Unterauftragsverhältnisse

7.1 Grundsatz

Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht dazu gehören Nebenleistungen, die der Auftragnehmer zum Beispiel als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Massnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenbearbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmassnahmen zu ergreifen.

7.2 Zulässige Unterauftragsverhältnisse

Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsbearbeiter; Dritte) nach Art. 9 Abs. 3 DSG nur nach vorheriger ausdrücklicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber in einer angemessenen Zeit vorab schriftlich anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Art. 9 DSG zugrunde gelegt wird und
- der Unterauftragnehmer seinen Sitz und die Bearbeitung in der Schweiz hat. Wenn die Bearbeitung oder der Sitz ausserhalb der Schweiz erfolgt, müssen zusätzliche Bestimmungen nach Kapitel 7.4 dieses Vertrages sichergestellt werden.

7.3 Weitergabe von Daten an Unterauftragnehmer

Die Weitergabe von Personendaten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen nach Kapitel 7.2 für eine Unterbeauftragung gestattet.

7.4 Unterauftragsverhältnisse ausserhalb der Schweiz

Erbringt der Unterauftragnehmer die vereinbarte Leistung ausserhalb der Schweiz und wird dies durch den Auftraggeber akzeptiert, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Massnahmen nach Art. 16 DSGVO sicher.

7.5 Unterauftragsverhältnisse des Unterauftragnehmers

Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers. Sämtliche vertragliche Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

8 Kontrollrechte des Auftraggebers

8.1 Grundsatz

Der Auftraggeber hat das Recht, sich durch Kontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieses Vertrags durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Die Stichproben müssen jederzeit verhältnismässig sein und dürfen nur nach beweisbaren Vermutungen des Nichteinhaltens dieses Vertrages vorgenommen werden.

Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach diesem Auftragsbearbeitungsvertrag überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Massnahmen nachzuweisen.

8.2 Nachweise

Der Nachweis der technischen und organisatorischen Massnahmen kann in Absprache mit dem Auftraggeber erfolgen durch

- a) die Einhaltung genehmigter Verhaltenskodizes gemäss Art. 11 Abs. 1 DSGVO;
- b) die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäss Art. 13 Abs. 1 DSGVO;
- c) aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzberater, IT-Sicherheitsabteilung, Datenschutzauditoren);
- d) schriftliche Dokumente, wie bspw. mittels Anhang dieses Vertrages.

8.3 Vergütungsanspruch bei Kontrollen

Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

9 Mitteilung bei Verstößen des Auftragnehmers

9.1 Grundsatz

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der gemäss Art. 6, Art. 7, Art. 8, Art. 22 und Art. 24 DSG genannten Pflichten zur Sicherheit der Personendaten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherigen Konsultationen. Hierzu gehören:

- die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Massnahmen, die die Umstände und Zwecke der Bearbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen.
- die Verpflichtung, Verletzungen von Personendaten unverzüglich an den Auftraggeber zu melden.
- die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen.
- die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung.
- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

10 Weisungsbefugnis des Auftraggebers

10.1 Bestätigung

Mündliche oder schriftliche Weisungen des Auftraggebers betreffend der Auftragsbearbeitung bestätigt der Auftragnehmer unverzüglich, spätestens jedoch innerhalb 48 Stunden.

10.2 Aussetzung der Weisungen

Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstosse gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

11 Löschung und Rückgabe von Personendaten

11.1 Kopien und Duplikate der Daten

Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien soweit sie zur Gewährleistung einer ordnungsgemässen Datenbearbeitung erforderlich sind sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

11.2 Vernichtung und Nachweis

Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher - nach Aufforderung durch den Auftraggeber - spätestens mit Beendigung des Rahmenvertrages (gem. Kapitel 1.1) - hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Bearbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen, oder nach vorheriger Zustimmung des Auftraggebers datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial.

12 Haftung und Vertragsstrafe

12.1 Beweislast

Der Auftragnehmer trägt die Beweislast dafür, dass ein Schaden nicht Folge eines von ihm zu vertretenden Umstandes ist, soweit die relevanten Daten von ihm unter diesem Vertrag verarbeitet wurden.

12.2 Haftung

Der Auftragnehmer haftet dem Auftraggeber für Schäden aus Persönlichkeitsverletzungen, die der Auftragnehmer, seine Mitarbeitenden oder seine Unterauftragsverhältnisse schuldhaft vorsätzlich oder grobfahrlässig verursachen.

12.3 Ausschluss der Haftung

Die Unterkapitel 12.1 und 12.2 gelten nicht, sofern der Schaden durch eine korrekte Umsetzung der beauftragten Leistungen und Bestimmungen durch den Auftragnehmer oder einer vom Auftraggeber erteilten Weisung entstanden ist.

Hiermit erklären wir uns mit dem vorgelegten Vertrag über den Art. 9 Abs. 1 des Bundesgesetzes vom 25. September 2020 über den Datenschutz (Datenschutzgesetz, DSG) einverstanden.

Unterzeichnung

Mit der rechtmässigen Unterzeichnung verpflichten sich beide Parteien, die Inhalte dieses Auftragsbearbeitungsvertrag und deren Anhänge anzuerkennen.

Gemeinde Buchrain	achermann ict-services ag
-------------------	---------------------------

Oliver Furrer

Gregor R. Naef Rolf Borkowetz

Ort und Datum

Ort und Datum

Entwurf

Anhang A Technische und organisatorische Massnahmen

Die technischen und organisatorischen Massnahmen (TOM) werden mit der Erklärung zur Anwendbarkeit nach ISO 27001:2022 nachgewiesen.

Entwurf

SoA (Statement of Applicability) Erklärung zur Anwendbarkeit nach ISO27001:2022

Controls		Im Anwendungsbe- reich	Nachweis der Implementierung
Kapitel	Control-Name	Ja/Nein	Erklärung
Organisatorische Massnahmen	Informationssicherheitspolitik und -richtlinien	Ja	<ul style="list-style-type: none"> Sicherheitspolitik, Sicherheitskonzept, Benutzer- und Rechtekonzept Hauptdokument, Benutzer- und Rechtekonzept AD, ICT-Benutzerrichtlinien, Geheimhaltungsvereinbarung, BCM-Konzept, Backup Konzept
	Informationssicherheitsrollen und -verantwortlichkeiten	Ja	<ul style="list-style-type: none"> Stellenbeschreibungen
	Aufgabentrennung	Ja	<ul style="list-style-type: none"> Stellenbeschreibungen
	Verantwortlichkeiten der Leitung	Ja	<ul style="list-style-type: none"> Stellenbeschreibungen
	Kontakt mit Behörden	Ja	<ul style="list-style-type: none"> Liste Behörden und spezieller Interessensgruppen
	Kontakt mit speziellen Interessensgruppen	Ja	<ul style="list-style-type: none"> Liste Behörden und spezieller Interessensgruppen
	Informationen über die Bedrohungslage	Ja	<ul style="list-style-type: none"> Vulnerability Response Prozess
	Informationssicherheit im Projektmanagement	Ja	<ul style="list-style-type: none"> Prozess Project
	Inventar der Informationen und anderen damit verbundenen Werte	Ja	<ul style="list-style-type: none"> Inventar-Übersicht
	Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten	Ja	<ul style="list-style-type: none"> Sicherheitskonzept
	Rückgabe von Werten	Ja	<ul style="list-style-type: none"> Austrittsprozess

Klassifizierung von Informationen	Ja	<ul style="list-style-type: none"> Sicherheitskonzept, ICT-Benutzerrichtlinien, Inventar-Übersicht
Kennzeichnung von Informationen	Ja	<ul style="list-style-type: none"> Sicherheitskonzept, ICT-Benutzerrichtlinien
Informationsübermittlung	Ja	<ul style="list-style-type: none"> Sicherheitskonzept
Zugangssteuerung	Ja	<ul style="list-style-type: none"> Benutzer- und Rechtekonzept
Identitätsmanagement	Ja	<ul style="list-style-type: none"> Prozess Eintritt, Mutationen und Austritt, Benutzerkonzept
Authentisierungsinformationen	Ja	<ul style="list-style-type: none"> Prozess Eintritt
Zugangsrechte	Ja	<ul style="list-style-type: none"> Prozess Eintritt, Mutationen und Austritt, Benutzerkonzept
Informationssicherheit in Lieferantenbeziehungen	Ja	<ul style="list-style-type: none"> Sitzungsplan, Prozess Partnermanagement, Sicherheitskonzept.
Behandlung von Informationssicherheit in Lieferantenvereinbarungen	Ja	<ul style="list-style-type: none"> Geheimhaltungsvereinbarung, Prozess Partnermanagement Lieferantenverzeichnis
Umgang mit der Informationssicherheit in der Lieferkette der Informations- und Kommunikationstechnologie (IKT)	Ja	<ul style="list-style-type: none"> Informations- und Kommunikationstechnologien im Bereich Datacenter sind vertraglich geregelt, Partnermanagement
Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen	Ja	<ul style="list-style-type: none"> Die Lieferantendienstleistungen und Verträge werden regelmässig überprüft und entsprechende Massnahmen ausgelöst, Prozess Partnermanagement.
Informationssicherheit für die Nutzung von Cloud-Diensten	Ja	<ul style="list-style-type: none"> Microsoft Competence Center, Partnermanagement bei achermann existiert eine Ausnahmegenehmigung für Cloud Services.
Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen	Ja	<ul style="list-style-type: none"> Rollen in Stellenbeschreibungen, Prozess Informationssicherheitsvorfall
Beurteilung und Entscheidung über Informationssicherheitsereignisse	Ja	<ul style="list-style-type: none"> Prozess Informationssicherheitsvorfall

	Reaktion auf Informationssicherheitsvorfälle	Ja	<ul style="list-style-type: none"> Prozess Informationssicherheitsvorfall
	Erkenntnisse aus Informationssicherheitsvorfällen	Ja	<ul style="list-style-type: none"> Prozess Risikomanagement, Risk Assessment
	Sammeln von Beweismaterial	Ja	<ul style="list-style-type: none"> Prozess Informationssicherheitsvorfall
	Informationssicherheit bei Störungen	Ja	<ul style="list-style-type: none"> BCM-Konzept, Prozess Qualitäts- und Risikomanagement
	IKT-Bereitschaft für Business Continuity	Ja	<ul style="list-style-type: none"> BCM-Konzept, Backupkonzept
	Juristische, gesetzliche, regulatorische und vertragliche Anforderungen	Ja	<ul style="list-style-type: none"> Sicherheitskonzept
	Geistige Eigentumsrechte	Ja	<ul style="list-style-type: none"> Sicherheitskonzept
	Schutz von Aufzeichnungen	Ja	<ul style="list-style-type: none"> Backup-Konzept, Sicherheitskonzept
	Datenschutz und Schutz von personenbezogenen Daten (PbD)	Ja	<ul style="list-style-type: none"> Umsetzung gemäss neuem Datenschutzgesetz: u. a. Datenschutzbeauftragter, Prozess Informationssicherheitsvorfall (inkl. Datenschutzvorfall), Prozess Auskunftsrecht, Interne Audits
	Unabhängige Überprüfung der Informationssicherheit	Ja	<ul style="list-style-type: none"> Prozess Management-System, Prozess Planung & Steuerung, interne Audits
	Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit	Ja	<ul style="list-style-type: none"> Prozesse Management-System, Planung & Steuerung.
	Dokumentierte Betriebsabläufe	Ja	<ul style="list-style-type: none"> Prozesslandschaft, Dokumentationen, IC Guides, Prozesse
Personenbezogene Massnahmen	Sicherheitsüberprüfung	Ja	<ul style="list-style-type: none"> Eintrittsprozess.
	Beschäftigungs- und Vertragsbedingungen	Ja	<ul style="list-style-type: none"> Personal- und Spesenreglement, ICT-Benutzerrichtlinien, Geheimhaltungsvereinbarung zu unterzeichnen
	Informationssicherheitsbewusstsein, -ausbildung und -schulung	Ja	<ul style="list-style-type: none"> Eintrittsprozess, Einführungsschulungen, Awareness-Kampagnen.

	Massregelungsprozess	Ja	<ul style="list-style-type: none"> Personalreglement, Prozess Informationssicherheitsvorfall, Disziplinarprozess
	Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung	Ja	<ul style="list-style-type: none"> Austrittsprozess, Personalreglement, Geheimhaltungsvereinbarung
	Vertraulichkeits- oder Geheimhaltungsvereinbarungen	Ja	<ul style="list-style-type: none"> Geheimhaltungsvereinbarung Datenverarbeitungsvereinbarung mit Partner
	Remote-Arbeit	Ja	<ul style="list-style-type: none"> Sicherheitskonzept
	Meldung von Informationssicherheitsereignissen	Ja	<ul style="list-style-type: none"> Einführungsprogrammes, Sensibilisierungskampagnen. Prozess Informationssicherheitsvorfall
Physische Massnahmen	Physische Sicherheitsperimeter	Ja	<ul style="list-style-type: none"> Sicherheitskonzept
	Physischer Zutritt	Ja	<ul style="list-style-type: none"> Sicherheitskonzept
	Sichern von Büros, Räumen und Einrichtungen	Ja	<ul style="list-style-type: none"> Sicherheitskonzept
	Physische Sicherheitsüberwachung	Ja	<ul style="list-style-type: none"> Sicherheitskonzept
	Schutz vor physischen und umweltbedingten Bedrohungen	Ja	<ul style="list-style-type: none"> Prozess Risikomanagement, Risk Assessment
	Arbeiten in Sicherheitsbereichen	Ja	<ul style="list-style-type: none"> Sicherheitskonzept
	Aufgeräumte Arbeitsumgebung und Bildschirm Sperren	Ja	<ul style="list-style-type: none"> Clean-Desk-Policy, Verhaltenskodex
	Platzierung und Schutz von Geräten und Betriebsmitteln	Ja	<ul style="list-style-type: none"> Sicherheitskonzept
	Sicherheit von Werten außerhalb der Räumlichkeiten	Ja	<ul style="list-style-type: none"> Risk-Assessments
	Speichermedien	Ja	<ul style="list-style-type: none"> Sicherheitskonzept, Entsorgungskonzept
	Versorgungseinrichtungen	Ja	<ul style="list-style-type: none"> Risk-Assessment
	Sicherheit der Verkabelung	Ja	<ul style="list-style-type: none"> In Büroräumlichkeiten und bei Kundeninstallationen wird die Verkabelung, sowie möglich unterirdisch oder

			in Kabelkanälen geführt. Im Datacenter ist die Verkabelung verschlossen und unterirdisch geregelt. Umsetzung der Sicherheitsmassnahmen gemäss Collocation-Anbieter. Auf zusätzliche Massnahmen wird verzichtet.
	Instandhalten von Geräten und Betriebsmitteln	Ja	<ul style="list-style-type: none"> eigener SLA und Patchmanagement.
	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	Ja	<ul style="list-style-type: none"> Entsorgungskonzept
Technologische Massnahmen	Endpunktgeräte des Benutzers	Ja	<ul style="list-style-type: none"> Sicherheitskonzept
	Privilegierte Zugangsrechte	Ja	<ul style="list-style-type: none"> Benutzer- und Rechtekonzept
	Informationszugangsbeschränkung	Ja	<ul style="list-style-type: none"> Benutzer- und Rechtekonzept
	Zugriff auf den Quellcode	Ja	<ul style="list-style-type: none"> Anpassungen am Software-Quellcode sind nicht gestattet.
	Sichere Authentisierung	Ja	<ul style="list-style-type: none"> Passwortmanager, Sicherheitskonzept
	Kapazitätssteuerung	Ja	<ul style="list-style-type: none"> Monitoring
	Schutz gegen Schadsoftware	Ja	<ul style="list-style-type: none"> Sicherheitskonzept
	Handhabung von technischen Schwachstellen	Ja	<ul style="list-style-type: none"> Patchnight, Vulnerability Response Prozess
	Konfigurationsmanagement	Ja	<ul style="list-style-type: none"> Sicherheitskonzept, Install and Configure Guides (IC Guides), Prozess Change Management
	Löschung von Informationen	Ja	<ul style="list-style-type: none"> Sicherheitskonzept, Entsorgungskonzept
	Verhinderung von Datenlecks	Ja	<ul style="list-style-type: none"> Sicherheitskonzept
	Sicherung von Informationen	Ja	<ul style="list-style-type: none"> Sicherheitskonzept, Backup Konzept
	Redundanz von informationsverarbeitenden Einrichtungen	Ja	<ul style="list-style-type: none"> achermann Datacenter sind Tier 3 resp. 4 klassifiziert.
	Protokollierung	Ja	<ul style="list-style-type: none"> Sicherheitskonzept

Überwachung von Aktivitäten	Ja	<ul style="list-style-type: none"> Sicherheitskonzept
Uhrensynchronisation	Ja	<ul style="list-style-type: none"> Die Zeitsynchronisation der Systeme ist wichtig und wird standardmässig über das Protokoll NTP (Net Time Protokoll) konfiguriert.
Gebrauch von Hilfsprogrammen mit privilegierten Rechten	Ja	<ul style="list-style-type: none"> Sicherheitskonzept.
Installation von Software auf Systemen im Betrieb	Ja	<ul style="list-style-type: none"> Sicherheitskonzept
Netzwerksicherheit	Ja	<ul style="list-style-type: none"> Managed Service Verträge, SLA , Sicherheitskonzept erwähnt.
Sicherheit von Netzwerkdiensten	Ja	<ul style="list-style-type: none"> Managed Service Vertrag und SLA
Trennung von Netzwerken	Ja	<ul style="list-style-type: none"> Sicherheitskonzept
Webfilterung	Ja	<ul style="list-style-type: none"> Sicherheitskonzept, Awareness-Kampagnen
Verwendung von Kryptographie	Ja	<ul style="list-style-type: none"> Sicherheitskonzept
Lebenszyklus einer sicheren Entwicklung	Ja	<ul style="list-style-type: none"> Es wird keine Softwareentwicklung vorgenommen. Netzwerk und Server Anpassungen werden in Rahmen der Projektphasen behandelt.
Anforderungen an die Anwendungssicherheit	Ja	<ul style="list-style-type: none"> Sicherheitskonzept
Sichere Systemarchitektur und Entwicklungsgrundsätze	Ja	<ul style="list-style-type: none"> Vorgehen gemäss Projekten und 4-Augen Prinzip.
Sichere Codierung	Nein	<ul style="list-style-type: none"> NICHT im Anwendungsbereich von achermann. Es wird keine Softwareentwicklung vorgenommen
Sicherheitsprüfung bei Entwicklung und Abnahme	Ja	<ul style="list-style-type: none"> Sicherheitskonzept
Ausgegliederte Entwicklung	Nein	<ul style="list-style-type: none"> NICHT im Anwendungsbereich von achermann. Bei achermann wird keine Systementwicklungstätigkeit ausgelagert. Zusammenarbeiten und Kontrolle im Rahmen von Lieferantenbeziehungen werden im Prozess Partner Management geregelt.

	Trennung von Entwicklungs-, Test- und Produktionsumgebungen	Ja	<ul style="list-style-type: none"> • Sicherheitskonzept
	Änderungssteuerung	Ja	<ul style="list-style-type: none"> • Prozess Project Services, 4-Augen-Prinzip, Change-Managements
	Testdaten	Ja	<ul style="list-style-type: none"> • Sicherheitskonzept
	Schutz der Informationssysteme während Tests im Rahmen von Audits	Ja	<ul style="list-style-type: none"> • Audits werden mit externen Partnern und im Rahmen von Projekten geplant.

Entwurf