

gem. Art. 28 Datenschutz-Grundverordnung (DSGVO)

Zwischen der

CVS Ingenieurgesellschaft mbH  
Otto-Lilienthal-Str. 10  
28199 Bremen

und

im Folgenden **Auftragnehmer/CVS** genannt –

im Folgenden **Auftraggeber/Kunde** genannt –

nachfolgend auch gemeinsam **die Parteien** genannt.

## Präambel

Die Parteien streben eine Zusammenarbeit im Bereich IT-Dienstleistungen und/oder die Einführung von ALPHAPLAN ERP, ALPHAPLAN Rechnungswesen und/oder ALPHAPLAN Webshop an. Insoweit ist zwischen den Parteien ein Vertrag über Auftragsverarbeitung zu schließen, da durch den Auftragnehmer personenbezogene Daten verarbeitet werden. Dieser AV-Vertrag regelt die Rechte und Pflichten von Auftraggeber und Auftragnehmer sowie ggfs. einzusetzenden Subdienstleistern.

## Teil 1 – Allgemeine Bestimmungen

### § 1 Gegenstand und Dauer des Auftrags

Gegenstand und Dauer des Auftrages richten sich nach dem schriftlichen Hauptvertrag (Software-Wartungsvertrag). Besteht zwischen den Parteien kein Hauptvertrag, so wird der Vertrag auf unbestimmte Zeit geschlossen. Er verlängert sich jeweils automatisch um ein Jahr, wenn er nicht unter Einhaltung einer Frist von drei Monaten zum Jahresende schriftlich gekündigt wird.

### § 2 Umfang, Art und Zweck der Datenverwendung, Datenarten sowie Kategorien betroffener Personen:

#### 1. Umfang, Art und Zweck der Datenverwendung

Die Tätigkeit des Auftragnehmers dient folgenden Zwecken: Wartung der ERP-Software (ALPHAPLAN), sonstige Software, Hardware.

#### 2. Datenarten

Datenarten, die Gegenstand dieses Auftrages sind, ergeben sich aus der **Anlage 1**.

#### 3. Kreis der Betroffenen

Der Kreis der betroffenen Personen ergibt sich aus der **Anlage 2**.

## Teil 2 – Auftragsverarbeitung gem. Art. 28 (DSGVO)

### § 1 Pflichten des Auftragnehmers

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.
- (2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

- (3) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.
- (4) Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.
- (5) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzerfordernisse laufend angemessen angeleitet und überwacht werden.
- (6) Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgenabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.
- (7) Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber, Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.
- (8) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.
- (9) Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.
- (10) Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Auftraggebers und unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.
- (11) Ist der Auftragnehmer nicht in der Europäischen Union niedergelassen, bestellt er einen verantwortlichen Ansprechpartner in der Europäischen Union gem. Art. 27 Datenschutz-Grundverordnung. Die Kontaktdaten des Ansprechpartners sowie sämtliche Änderungen in der Person des Ansprechpartners sind dem Auftraggeber unverzüglich mitzuteilen.
- (12) Beim Auftragnehmer ist als Beauftragter für den Datenschutz **Herr Nick Flory** bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Verantwortlichen unverzüglich mitzuteilen.

## § 2 Technische und organisatorische Maßnahmen

- (1) Die im **Anhang 1** beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum. Die Beschreibung der Maßnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jederzeit zweifelsfrei erkennbar ist, was das geschuldete Minimum sein soll. Ein Verweis auf Informationen, die dieser Vereinbarung oder ihren Anlagen nicht unmittelbar entnommen werden können, ist nicht zulässig.
- (2) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.
- (3) Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.
- (4) Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

- (5) Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.
- (6) Dedizierte Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein. Ein- und Ausgänge werden dokumentiert.
- (7) Der Auftragnehmer führt den regelmäßigen Nachweis der Erfüllung seiner Pflichten, insbesondere der vollständigen Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen sowie ihrer Wirksamkeit. Der Nachweis ist dem Auftraggeber spätestens alle 12 Monate unaufgefordert und sonst jederzeit auf Anforderung zu überlassen. Der Nachweis kann durch genehmigte Verhaltensregeln oder ein genehmigtes Zertifizierungsverfahren erbracht werden.

### § 3 Regelungen zur Berichtigung, Löschung und Sperrung von Daten

- (1) Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.
- (2) Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

### § 4 Unterauftragsverhältnisse

- (1) Die Beauftragung von Subunternehmern ist nur mit schriftlicher Zustimmung des Auftraggebers im Einzelfall zugelassen.
- (2) Die Zustimmung ist nur möglich, wenn dem Subunternehmer vertraglich mindestens Datenschutzpflichten auferlegt wurden, die den in diesem Vertrag vereinbarten vergleichbar sind. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmer und Subunternehmer.
- (3) Die Rechte des Auftraggebers müssen auch gegenüber dem Subunternehmer wirksam ausgeübt werden können. Insbesondere muss der Auftraggeber berechtigt sein, jederzeit in dem hier festgelegten Umfang Kontrollen auch bei Subunternehmern durchzuführen oder durch Dritte durchführen zu lassen.
- (4) Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.
- (5) Eine weitere Subbeauftragung durch den Subunternehmer ist nicht zulässig.
- (6) Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.
- (7) Die Weiterleitung von im Auftrag verarbeiteten Daten an den Subunternehmer ist erst zulässig, wenn sich der Auftragnehmer dokumentiert davon überzeugt hat, dass der Subunternehmer seine Verpflichtungen vollständig erfüllt hat. Der Auftragnehmer hat dem Auftraggeber die Dokumentation unaufgefordert vorzulegen.
- (8) Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag nicht ausschließlich aus dem Gebiet der EU oder des EWR erbringen, ist nur bei Beachtung der in Kapitel 4 (10) und (11) dieses Vertrages genannten Bedingungen möglich. Sie ist insbesondere nur zulässig, soweit und solange der Subunternehmer angemessene Datenschutzgarantien bietet. Der Auftragnehmer teilt dem Auftraggeber mit, welche konkreten Datenschutzgarantien der Subunternehmer bietet und wie ein Nachweis hierüber zu erlangen ist.
- (9) Der Auftragnehmer hat die Einhaltung der Pflichten des Subunternehmers regelmäßig, spätestens alle 12 Monate, angemessen zu überprüfen. Die Prüfung und ihr Ergebnis sind so aussagekräftig zu dokumentieren, dass sie für einen fachkundigen Dritten nachvollziehbar sind. Die Dokumentation ist dem Auftraggeber unaufgefordert vorzulegen.
- (10) Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber.

- (11) Zurzeit sind die in **Anlage 3** mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt und durch den Auftraggeber genehmigt. Die hier niedergelegten sonstigen Pflichten des Auftragnehmers gegenüber Subunternehmern bleiben unberührt.
- (12) Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

## § 5 Rechte und Pflichten des Auftraggebers

- (1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.
- (2) Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.
- (3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
- (4) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.

## § 6 Mitteilungspflichten

- (1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis an eine vom Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:
  - a. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
  - b. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
  - c. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
  - d. eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen
- (2) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftrags erledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.
- (3) Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.
- (4) Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 der Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

## § 7 Weisungen

- (1) Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.
- (2) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.
- (3) Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

## § 8 Beendigung des Auftrags

- (1) Bei Beendigung des Hauptvertrages oder jederzeit auf Verlangen des Auftraggebers hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers entweder zu vernichten oder an den Auftraggeber zu übergeben. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist. Eine physische Vernichtung erfolgt gemäß DIN 66399. Hierbei gilt mindestens **Schutzklasse II**.
- (2) Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.
- (3) Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber unverzüglich vorzulegen.
- (4) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

## § 9 Vergütung

Die Vergütung des Auftragnehmers ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

## § 10 Haftung

- (1) Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner.
- (2) 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 dieser Vereinbarung verarbeitet wurden. Solange dieser Beweis nicht erbracht wurde, stellt der Auftragnehmer den Auftraggeber auf erste Anforderung von allen Ansprüchen frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Auftraggeber erhoben werden. Unter diesen Voraussetzungen ersetzt der Auftragnehmer dem Auftraggeber ebenfalls sämtliche entstandenen Kosten der Rechtsverteidigung.
- (3) Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder die von ihm eingesetzten Subdienstleister im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen.
- (4) Nummern (2) und (3) gelten nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist.

## § 11 Sonstiges

- (1) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.
- (2) Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.
- (3) Für Nebenabreden ist die Schriftform erforderlich.
- (4) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
- (5) Sollten einzelne Teile dieser Vereinbarung unwirksam sein oder werden, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht. Die Parteien verpflichten sich, die unwirksame Bestimmung durch eine wirksame zu ersetzen, deren Zweck dem der weggefallenen Bestimmung möglichst nahekommt.

.....  
Ort, Datum

.....  
Ort, Datum

.....  
Auftragnehmer/CVS

.....  
Auftraggeber/Kunde

## Anlage 1

### Datenarten/-kategorien:

- Kundendaten
- Lieferantendaten
- Mitarbeiterdaten
- Kommunikationsdaten
- Vertragsstammdaten
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Kontodaten

### Besondere personenbezogene Daten:

- Gesundheitsdaten
- Gewerkschaftszugehörigkeit
- Religion und philosophische Überzeugungen
- Politische Meinungen
- Rassistische und ethnische Herkunft
- Sexualleben

## Anlage 2

Kategorien betroffener Personen:

- Kunden
- Interessenten
- Abonnenten
- Mitarbeiter
- Lieferanten
- Handelsvertreter
- Ansprechpartner



## Anlage 3

Liste der Subunternehmen:

LastPass

<https://www.lastpass.com/de/legal-center/privacy-policy>

Es handelt sich um ein Passwortverwaltungsprogramm, welches uns ermöglicht, mit weitreichenden Einstellungen, die relevanten Passworte, sicher und hochverschlüsselt, zu verwalten.

## Anhang 1

### Technische und organisatorische Maßnahmen (TOM) i. S. d. Art. 32 DSGVO

der Organisation CVS Ingenieurgesellschaft mbH | Stand 01.03.2023

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die o. g. Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

#### 1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

##### 1.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z. B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

| Technische Maßnahmen          | Organisatorische Maßnahmen               |
|-------------------------------|--|
| Alarmanlage                   | Schlüsselregelung/Liste                  |
| Chipkarten/Transpondersysteme | Empfang/Rezeption/Pförtner               |
| Sicherheitsschlösser          | Mitarbeiter-/Besucherausweise            |
| Schließsystem mit Codesperre  | Besucher in Begleitung durch Mitarbeiter |
| Türen mit Knauf-Außenseite    |  |
| Zeitsperre                    |  |
| Alarmverfolger extern         |  |

##### 1.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

| Technische Maßnahmen                      | Organisatorische Maßnahmen                       |
|---|--|
| Login mit Benutzername + Passwort         | Verwalten von Benutzerberechtigungen             |
| Login mit biometrischen Daten             | Erstellen von Benutzerprofilen                   |
| Anti-Viren-Software Server                | Richtlinie „Sicheres Passwort“                   |
| Anti-Virus-Software Clients               | Richtlinie „Löschen/Vernichten“                  |
| Anti-Virus-Software mobile Geräte         | Allg. Richtlinie Datenschutz und/oder Sicherheit |
| Firewall                                  |  |
| Intrusion Detection Systeme               |  |
| Einsatz VPN bei Remote-Zugriffen          |  |
| Verschlüsselung von mobilen Datenträgern  |  |
| Notebook BIOS Schutz (separates Passwort) |  |

|                                      |  |
|--------------------------------------|--|
| Automatische Desktopsperre           |  |
| Verschlüsselung von Notebooks/Tablet |  |
| PIM/Container                        |  |

### 1.3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z. B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

| Technische Maßnahmen  | Organisatorische Maßnahmen                      |
|---|---|
| Aktenschredder (mind. Stufe 3, cross cut)   | Einsatz Berechtigungskonzepte                   |
| Externer Aktenvernichter (DIN 32757)  | Minimale Anzahl an Administratoren              |
| Physische Löschung von Datenträgern   | Datenschutztresor                               |
| Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten | Verwaltung Benutzerrechte durch Administratoren |

### 1.4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

| Technische Maßnahmen                                     | Organisatorische Maßnahmen                   |
|--|--|
| Trennung von Produktiv- und Testumgebung                 | Steuerung über Berechtigungskonzept          |
| Physikalische Trennung (Systeme/Datenbanken/Datenträger) | Festlegung von Datenbankrechten              |
|  | Datensätze sind mit Zweckattributen versehen |

### 1.5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

| Technische Maßnahmen   | Organisatorische Maßnahmen  |
|--|---|
| Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System (möglichst verschlüsselt) | Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren/pseudonymisieren |

## 2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

### 2.1. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z. B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

| Technische Maßnahmen  | Organisatorische Maßnahmen                                 |
|---|--|
| Einsatz von VPN   | Weitergabe in anonymisierter oder pseudonymisierter Form   |
| Protokollierung der Zugriffe und Abrufe in ALPHAPLAN            | Sorgfalt bei Auswahl von Transport Personal und Fahrzeugen |
| Bereitstellung über verschlüsselte Verbindungen wie sftp, https |  |

### 2.2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z. B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

| Technische Maßnahmen  | Organisatorische Maßnahmen  |
|---|---|
| Technische Protokollierung der Eingabe, Änderung und Löschung von Daten | Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) |
|   | Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts                    |
|   | Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden                           |
|   | Klare Zuständigkeiten für Löschungen  |

## 3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

### 3.1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlage, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raid-Systeme, Plattenspiegelungen etc.

| Technische Maßnahmen         | Organisatorische Maßnahmen                |
|------------------------------|---|
| Feuer- und Rauchmeldeanlagen | Backup & Recovery-Konzept (ausformuliert) |
| Feuerlöscher Serverraum      | Kontrolle des Sicherungsvorgangs          |

|   |   |
|---|---|
| Serverraumüberwachung Temperatur und Feuchtigkeit | Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse   |
| Serverraum klimatisiert                           | Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums |
| USV   | Existenz eines Notfallplans<br>(z. B. BSI IT-Grundschutz 100-4)                   |
| Schutzsteckdosenleisten Serverraum                | Getrennte Partitionen für Betriebssysteme und Daten                               |
| Datenschutztesor                                  |   |
| RAID System/Festplattenspiegelung                 |   |

#### 4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

##### 4.1. Datenschutz-Management

| Technische Maßnahmen  | Organisatorische Maßnahmen   |
|---|--|
| Software-Lösungen für Datenschutz-Management im Einsatz   | Interner/externer Datenschutzbeauftragter<br>Name/Firma/Kontaktdaten                           |
| Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf/Berechtigung<br>(z. B. Wiki, Intranet ...) | Mitarbeiter geschult und auf Vertraulichkeit/<br>Datengeheimnis verpflichtet                   |
| Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mindestens jährlich durchgeführt  | Regelmäßige Sensibilisierung der Mitarbeiter<br>mindestens jährlich                            |
|   | Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt                          |
|   | Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach                |
|   | Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden |

##### 4.2. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

| Technische Maßnahmen                                      | Organisatorische Maßnahmen  |
|---|---|
| Einsatz von Firewall und regelmäßige Aktualisierung       | Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen/Daten-Pannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde) |
| Einsatz von Spamfilter und regelmäßige Aktualisierung     | Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen  |
| Einsatz von Virens Scanner und regelmäßige Aktualisierung | Einbindung von DSB und ISB in Sicherheitsvorfälle und Datenpannen   |
| Intrusion Detection System (IDS)                          | Dokumentation von Sicherheitsvorfällen und Datenpannen  |
| Intrusion Prevention System (IPS)                         |   |
| Mehrstufiges Firewallkonzept                              |   |
| Sandbox   |   |

#### 4.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Privacy by design/Privacy by default

| Technische Maßnahmen  | Organisatorische Maßnahmen |
|---|----------------------------|
| Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind |                            |
| Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen                    |                            |

#### 4.4. Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

| Technische Maßnahmen | Organisatorische Maßnahmen |
|----------------------|----------------------------|
|                      |                            |
|                      |                            |
|                      |                            |
|                      |                            |
|                      |                            |
|                      |                            |
|                      |                            |

alternativ:

Hiermit versichern wir, keine Subunternehmer im Sinne einer Auftragsverarbeitung einzusetzen.