VERTRAG ÜBER AUFTRAGSVERARBEITUNG IM SINNE VON ART. 28 ABS. 3 DSGVO

ZWISCHEN

- im Folgenden: Auftraggeber -

UND

AccountOne GmbH
Schiffbrücke 66
24939 Flensburg

- im Folgenden: Auftragnehmer -

1. Allgemeine Bestimmungen und Vertragsgegenstand

1. 1. Gegenstand des vorliegenden Vertrags ist die Verarbeitung personenbezogener Daten im Auftrag durch den Auftragnehmer (Art. 28 DSGVO). Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO ist der Auftraggeber. Die Auftragsdetails entnehmen Sie der **Anlage 1**.

1. 2. Die Verarbeitung der vertragsgegenständlichen personenbezogenen Daten außerhalb der Europäischen Union ist nur zulässig, wenn die gesetzlichen Voraussetzungen der Art. 44 ff. DSGVO gegeben sind und der Auftraggeber zugestimmt hat.

2. Vertragslaufzeit und Kündigung

2. 1. Der vorliegende Vertrag wird auf unbestimmte Zeit geschlossen und kann von jeder Vertragspartei mit einer Frist von drei Monaten ordentlich gekündigt werden. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. Weisungen des Auftraggebers

3. 1. Dem Auftraggeber steht ein umfassendes Weisungsrecht in Bezug auf Art, Umfang und Modalitäten der Datenverarbeitung ggü. dem Auftragnehmer zu. Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung des Auftraggebers gegen gesetzliche Vorschriften verstößt. Wird eine Weisung erteilt, deren Rechtmäßigkeit der Auftragnehmer substantiiert anzweifelt, ist der Auftragnehmer berechtigt, deren Ausführung vorübergehend auszusetzen, bis der Auftraggeber diese nochmals ausdrücklich bestätigt oder ändert. Besteht die Möglichkeit, dass der Auftragnehmer durch das Befolgen der Weisung einem Haftungsrisiko ausgesetzt wird, kann die Durchführung der Weisung bis zur Klärung der Haftung im Innenverhältnis ausgesetzt werden.

3. 2. Weisungen sind grundsätzlich schriftlich oder in einem elektronischen Format (z. B. per E-Mail) zu erteilen. Mündliche Weisung sind in begründeten Einzelfällen zulässig und werden vom Auftraggeber unverzüglich schriftlich oder in einem elektronischen Format bestätigt. In der Bestätigung ist ausdrücklich zu begründen, warum keine schriftliche Weisung erfolgen konnte. Der Auftragnehmer hat Person, Datum und Uhrzeit der mündlichen Weisung in angemessener Form zu protokollieren.

3. 3. Der Auftraggeber benennt auf Verlangen des Auftragnehmers eine oder mehrere weisungsberechtigte Personen. Personelle Änderungen sind dem Auftragnehmer unverzüglich mitzuteilen.

4. Kontrollbefugnisse des Auftraggebers

4. 1. Der Auftraggeber ist berechtigt, die Einhaltung der gesetzlichen und vertraglichen Vorschriften zum Datenschutz und zur Datensicherheit vor Beginn der Datenverarbeitung und während der

Vertragslaufzeit regelmäßig im erforderlichen Umfang zu kontrollieren. Der Auftraggeber hat dafür

zu sorgen, dass die Kontrollmaßnahmen verhältnismäßig sind und den Betrieb des Auftragnehmers nicht mehr als erforderlich beeinträchtigen.

4. 2. Die Ergebnisse der Kontrollen und Weisungen sind vom Auftraggeber in geeigneter Weise zu protokollieren.

5. Allgemeine Pflichten des Auftragnehmers

5. 1. Die Verarbeitung der vertragsgegenständlichen Daten durch den Auftragnehmer erfolgt ausschließlich auf Grundlage der vertraglichen Vereinbarungen in Verbindung mit den ggf. erteilten Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung ist nur aufgrund zwingender europäischer oder mitgliedsstaatlicher Rechtsvorschriften zulässig (z. B. im Falle von Ermittlungen durch Strafverfolgungs- oder Staatsschutzbehörden). Ist eine Verarbeitung aufgrund zwingenden Rechts erforderlich, teilt der Auftragnehmer dies dem Auftraggeber vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

5. 2. Der Auftragnehmer hat zu gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Vor der Unterwerfung unter die Verschwiegenheitspflicht dürfen die betreffenden Personen keinen Zugang zu den vom Auftraggeber überlassenen personenbezogenen Daten erhalten.

6. Technische und organisatorische Maßnahmen

6. 1. Der Auftragnehmer wird die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen, die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, sicherstellen sowie ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung unterhalten. 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 im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen. Die Vertragsparteien vereinbaren die in Anlage 2 „Technische und organisatorische Maßnahmen“ zu dieser Vereinbarung niedergelegten konkreten Datensicherheitsmaßnahmen. 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 und dem Auftraggeber mitzuteilen.

7. Unterstützungspflichten des Auftragnehmers

7. 1. Der Auftragnehmer wird den Auftraggeber gem. Art. 28 Abs. 3 lit. e DSGVO bei dessen Pflichten zur Wahrung der Betroffenenrechte aus Kapitel III, Art. 12 – 22 DSGVO, unterstützen. Dies gilt insbesondere für die Erteilung von Auskünften und die Löschung, Berichtigung oder Einschränkung personenbezogener Daten. Der Auftragnehmer wird den Auftraggeber ferner gem. Art. 28 Abs. 3 lit. f DSGVO bei dessen Pflichten nach Art. 32 – 36 DSGVO (insb. Meldepflichten) unterstützen. Die Reichweite dieser Unterstützungspflichten bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung und der Informationen, die dem Auftragnehmer zur Verfügung stehen.

8. Einsatz von Unterauftragsverarbeitern (Subunternehmer)

8. 1. Der Auftragnehmer ist zum Einsatz von Unterauftragsverarbeitern (Subunternehmern) berechtigt. Alle zum Zeitpunkt des Vertragsschlusses bereits bestehenden Subunternehmerverhältnisse des Auftragnehmers sind diesem Vertrag abschließend in Anlage 3 beigefügt. Für die in Anlage 3 aufgezählten Subunternehmer gilt die Zustimmung mit Abschluss dieses Vertrags als erteilt.

8. 2. Beabsichtigt der Auftragnehmer den Einsatz weiterer Subunternehmer, wird er dies dem Auftraggeber rechtzeitig - spätestens jedoch zwei Wochen - vor deren Einsatz in schriftlicher oder elektronischer Form anzeigen. Der Auftraggeber hat nach dieser Mitteilung zwei Wochen Zeit, der Hinzuziehung des / der Subunternehmer zu widersprechen. Erfolgt innerhalb dieser Frist kein Widerspruch, gilt die Hinzuziehung des / der Subunternehmer(s) als genehmigt. Im Falle eines Widerspruchs dürfen die betroffenen Subunternehmer nicht eingesetzt werden. Widersprüche sind nur zulässig, wenn der Auftraggeber begründete Anhaltspunkte dafür hat, dass durch den Einsatz des Unterauftragnehmers die Datensicherheit oder der Datenschutz eingeschränkt würde, die Einhaltung gesetzlicher oder vertraglicher Bestimmungen gefährdet wäre und / oder sonstige berechtigte Interessen des Auftraggebers entgegenstehen; die entsprechenden Verdachtsmomente sind dem Widerspruch beizufügen.

8. 3. Subunternehmer werden vom Auftragnehmer unter Beachtung der gesetzlichen und vertraglichen Vorgaben ausgewählt. Sämtliche Verträge zwischen Auftragsverarbeiter und Unterauftragsverarbeiter (Subunternehmerverträge) müssen den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen; dies betrifft insbesondere die Implementierung geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO im Betrieb des Subunternehmers. Nebenleistungen, welche der Auftragnehmer zur Ausübung seiner geschäftlichen Tätigkeit in Anspruch nimmt, stellen keine Unterauftragsverhältnisse im Sinne des Art. 28 DSGVO dar. Nebentätigkeiten in diesem Sinne sind insbesondere Telekommunikationsleistungen ohne konkreten Bezug zur Hauptleistung, Post- und Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen, die die Vertraulichkeit und / oder Integrität der Hard- und Software sicherstellen sollen und keinen konkreten Bezug zur Hauptleistung aufweisen. Der Auftragnehmer wird jedoch auch bei diesen Drittleistungen die Einhaltung der gesetzlichen Datenschutzstandards (insbesondere durch entsprechende Vertraulichkeitsvereinbarungen) sicherstellen.

8. 4. Sämtliche Verträge zwischen dem Auftragnehmer und dem Unterauftragsverarbeiter (Subunternehmerverträge) müssen den Anforderungen dieses Vertrags und den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen.

8. 5. Die Beauftragung von Subunternehmern in Drittstaaten ist nur zulässig, wenn die gesetzlichen Voraussetzungen der Art. 44 ff. DSGVO gegeben sind und der Auftraggeber zugestimmt hat.

9. Mitteilungspflichten des Auftragnehmers

9. 1. Verstöße gegen diesen Vertrag, gegen Weisungen des Auftraggebers oder gegen sonstige datenschutzrechtliche Bestimmungen sind dem Auftraggeber unverzüglich mitzuteilen; das gleiche gilt bei Vorliegen eines entsprechenden begründeten Verdachts. Diese Pflicht gilt unabhängig davon, ob der Verstoß vom Auftragnehmer selbst, einer bei ihm angestellten Person, einem Unterauftragsverarbeiter oder einer sonstigen Person, die er zur Erfüllung seiner vertraglichen Pflichten eingesetzt hat, begangen wurde.

9. 2. Ersucht ein Betroffener, eine Behörde oder ein sonstiger Dritter den Auftragnehmer um Auskunft, Berichtigung, Einschränkung der Verarbeitung oder Löschung, wird der Auftragnehmer die Anfrage unverzüglich an den Auftraggeber weiterleiten; in keinem Fall wird der Auftragnehmer dem Ersuchen des Betroffenen ohne Weisung / Zustimmung des Auftraggebers nachkommen.

9. 3. Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, wenn Aufsichtshandlungen oder sonstige Maßnahmen einer Behörde bevorstehen, von der auch die Verarbeitung, Nutzung oder Erhebung der durch den Auftraggeber zur Verfügung gestellten personenbezogenen Daten betroffen sein könnten. Darüber hinaus hat der Auftragnehmer den Auftraggeber unverzüglich über alle Ereignisse oder Maßnahmen Dritter zu informieren, durch welche die vertragsgegenständlichen Daten gefährdet oder beeinträchtigt werden könnten.

10. Vertragsbeendigung, Löschung und Rückgabe der Daten

10. 1. Nach Abschluss der vertragsgegenständlichen Datenverarbeitung bzw. nach Beendigung dieses Vertrags hat der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers zu löschen oder zurückzugeben, sofern keine rechtliche oder vertragliche Verpflichtung zur Speicherung der betreffenden Daten mehr besteht (z. B. gesetzliche Aufbewahrungsfristen).

11. Datengeheimnis und Vertraulichkeit

11. 1. Der Auftragnehmer ist unbefristet und über das Ende dieses Vertrages hinaus verpflichtet, die im Rahmen der vorliegenden Vertragsbeziehung erlangten personenbezogenen Daten vertraulich zu behandeln. Der Auftragnehmer verpflichtet sich, seine Mitarbeiter mit den einschlägigen Datenschutzbestimmungen und Geheimnisschutzregeln vertraut zu machen und sie zur Verschwiegenheit zu verpflichten, bevor diese ihre Tätigkeit beim Auftragnehmer aufnehmen.

12. Schlussbestimmungen

12. 1. Änderungen dieses Vertrags und Nebenabreden bedürfen der schriftlichen oder elektronischen Form, die eindeutig erkennen lässt, dass und welche Änderung oder Ergänzung der vorliegenden Bedingungen durch sie erfolgen soll.

12. 2. Sollte sich die DSGVO oder sonstige in Bezug genommenen gesetzlichen Regelungen während der Vertragslaufzeit ändern, gelten die hiesigen Verweise auch für die jeweiligen Nachfolgeregelungen.

12. 3. Sollten einzelne Teile dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.

12. 4. Sämtliche Anlagen zu diesem Vertrag sind Vertragsbestandteil.

12. 5. Sind die Vertragsparteien Kaufleute, juristische Personen des öffentlichen Rechts oder öffentlichrechtliches Sondervermögen, ist der Sitz des Auftragnehmers Gerichtsstand für alle Streitigkeiten aus diesem Vertrag, sofern insoweit hierfür ein ausschließlicher Gerichtsstand nicht begründet wird.

Auftragnehmer | Auftraggeber

Gordian-Philipp Brockstedt

05.06.2025, AccountOne GmbH

Datum, Unterschrift | Datum, Unterschrift

Anlage 1 – Auftragsdetails

1. Der vorliegende Vertrag umfasst (ggf. im Zusammenhang mit dem Hauptvertrag) folgende Leistungen:

Den Abruf von Bestelldaten aus verschiedenen Verkaufskanälen des Auftraggebers, sowie die Annahme von Dateien die ebensolche Verkaufsdaten enthalten. Darüber hinaus die umsatzsteuerliche Würdigung und Bewertung jedes einzelnen Umsatzes und die Umformatierung in kompatible Datensätze für die Buchhaltung. Sofern beauftragt, werden aus den empfangenen Daten Rechnungen erstellt und den betroffenen Endkunden des Auftraggebers per Emails zugesendet.

2. Im Rahmen der vertraglichen Leistungserbringung werden regelmäßig folgende Datenarten verarbeitet:

2. 1. Anschrift

2. 2. Demographische Daten

2. 3. E-Mail-Adresse

2. 4. Kontaktdaten (Telefon, E-Mail)

2. 5. Kundendaten

2. 6. Namen

2. 7. Rechnungsdaten

2. 8. Standort

2.9. Zahlungseingänge und Zahlungsausgänge

3. Bei dem Kreis der von der Datenverarbeitung betroffenen Personen handelt es sich um:

3.1 Kunden des Auftraggebers

Anlage 2 – Liste der bestehenden technischen und organisatorischen Maßnahmen des Auftragsverarbeiters nach Art. 32 DSGVO

Der Auftragnehmer setzt folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden im Einklang mit Art. 32 DSGVO festgelegt und mit dem Auftraggeber abgestimmt.

Folgende Maßnahmen werden gewährleistet:

1. Datenschutzbeauftragter

Ist der Auftragnehmer nach Art. 37 DSGVO, § 38 BDSG gesetzlich dazu verpflichtet, einen Datenschutzbeauftragten zu benennen, teilt der Auftragnehmer dem Auftraggeber die Kontaktdaten des Datenschutzbeauftragten zum Zweck der direkten Kontaktaufnahme mit. Ein Wechsel des Datenschutzbeauftragten ist bei dem Auftraggeber unverzüglich anzuzeigen.

Als Datenschutzbeauftragter ist beim Auftragnehmer Herr

Dr. Nils Christian Haag
intersoft consulting services AG

Beim Strohhause 17
20097 Hamburg

Tel. +49 40 790 235 – 402
Fax. +49 40 790 235 – 170

E-Mail: **datenschutz@accountone.de**

bestellt.

2. Physische Sicherheit des Rechenzentrums

Wir hosten unsere Daten bei Hetzner im Rechenzentrum Falkenstein. Es gibt keine unverschlüsselte Kopie der Daten, außerhalb des Rechenzentrums, von Hetzner.

Ein per Video überwachter Hochsicherheitszaun umschließt den gesamten Datacenter-Park. Zufahrten sind nur über Zutrittskontroll-Terminals mit Transponder bzw. Zutrittskarten möglich. Sämtliche Bewegungen werden aufgezeichnet und dokumentiert. Hochmoderne Überwachungskameras überwachen rund um die Uhr alle Zufahrten, Eingänge, Sicherheitsschleusen und Serverräume. Colocation Rack-Kunden verfügen über einen eigenen Schlüssel bzw. einen Zugangscode für den gesicherten Serverschrank.

Bei Erstbezug oder einem temporären Techniker-Besuch beauftragter Serviceunternehmen kann vorab in der Administrationsoberfläche Robot der Besuchstermin und die Zutrittsberechtigungen festgelegt werden. Mittels eines generierten Passworts erfolgt beim ServicePersonal vor Ort die Authentifizierung und die Aushändigung des Transponderchips für den Schleusen-Zugang zum Rack. Der Aufenthalt wird dabei protokolliert und aufgenommenes Bildmaterial in der Administrationsoberfläche zur Kontrolle archiviert.

Die unterbrechungsfreie Stromversorgung (USV) wird durch eine 15-minütige Batteriekapazität und Notstrom-Dieselaggregate garantiert. Sämtliche USV-Anlagen sind dabei redundant ausgelegt. Die

direkte freie Kühlung sorgt für eine umweltschonende Kühlung der IT-Hardware. Die Klimatisierung erfolgt über den Doppelboden. Ein modernes Brandfrühesterkennung System ist direkt mit der Brandmeldezentrale der örtlichen Feuerwehr verbunden.

2.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO) Zutrittskontrolle

Zutrittskontrolle durch Hetzner

Wir hosten unsere Daten bei Hetzner im Rechenzentrum Falkenstein. Es gibt keine unverschlüsselte Kopie der Daten, außerhalb des Rechenzentrums, von Hetzner.

Genau Informationen finden Sie hier: https://docs.hetzner.com/de/general/others/technical-and-organizational-measures/

	Erläuterung von Hetzner
Elektronisches Zutrittskontrollsystem mit Protokollierung	Der Zutritt zu unseren Datacenterparks, den Rechenzentren, Räumen sowie zu unserem Verwaltungsgebäude ist ausschließlich über unser Zutrittskontrollsystem möglich. Alle Zutritte werden protokolliert.
Serverraum in gesondertem Sicherheitsbereich	
Dokumentierte Vergabe von Zutrittsmedien	Zutrittsmedien wie Schlüssel werden ausschließlich an autorisierte Mitarbeitende, Subunternehmen und Colocation-Kunden ausgegeben. Jede Ausgabe wird dokumentiert, um eine lückenlose Nachverfolgbarkeit zu gewährleisten. Die Rollen- und Rechteverteilung für Mitarbeitende und Subdienstleister wird zentral verwaltet und regelmäßig überprüft. Colocation-Kunden sind für die Verwaltung und Überprüfung ihrer Zutrittsmedien selbst verantwortlich.
Flächendeckende Videoüberwachung	Alle relevanten Bereiche, darunter der Hochsicherheitszaun, Zufahrten, Ein- und Ausgänge, Sicherheitsschleusen und Serverräume werden kontinuierlich videoüberwacht. Sämtliche Bewegungen werden aufgezeichnet und dokumentiert. Das Videomaterial wird gemäß unseres Löschkonzeptes DSGVO-konform gespeichert und gelöscht. Zusätzlich wird bei unseren Colocation-Kunden jeder Zutrittsversuch (unter anderem an der Ein- und Ausfahrt sowie der Schleuse) mit einem Bild erfasst. Die Bilder sowie die zugehörigen Zeitstempel werden in der Administrationsoberfläche protokolliert und sind für den Kunden einsehbar.
Richtlinie zum Besuchermanagement	Der Zutritt betriebsfremder Personen unterliegt einer Besucherrichtlinie, die unter anderem klare Regeln für die Anmeldung, Autorisierung, Begleitung, und Ausweisung dieser festlegt. Colocation-Kunden werden im Rahmen der Ersteinweisung mit den für sie relevanten Vorgaben vertraut gemacht.
Hochsicherheitszaun mit Übersteigschutz und Untergrabenschutz um den gesamten Datacenter-Park	Unsere Datacenter-Parks sind von einem Hochsicherheitszaun mit Übersteigschutz umgeben. Zusätzlich setzen wir auf einen Untergrabenschutz.

3. Maßnahmen zur Gewährleistung der Vertraulichkeit

Zugangskontrolle Soll den Zugang Unbefugter zu Datenverarbeitungssystemen und deren unbefugte Nutzung verhindern. Systemabsicherung.
Zuordnung von Benutzerrechten
Erstellen von Benutzerprofilen
Berechtigungsmanagement
Dokumentierter Prozess zur Rechtevergabe bei Neueintritt von Mitarbeitern
Dokumentierter Prozess zum Rechteentzug bei Austritt von Mitarbeitern
Funktionelle und/oder zeitlich limitierte Vergabe von Benutzerberechtigungen
Verwendung von individuellen Passwörtern
Login mit Benutzername und Passwort
Login mit Zwei-Faktor Authentifizierung
Automatische passwortgesicherte Sperrung des Bildschirms nach Inaktivität (Bildschirmschoner)
Passwortrichtlinie mit Mindestvorgaben zur Passwortkomplexität: ● Mindestens 12 Zeichen ● Zwingend Enthalten: Groß- und Kleinschreibung, Sonderzeichen, Ziffer ● Verhinderung von Trivialpasswörtern (z.B. Passwort1, Passwort2, 123456, qwertz) ● Automatische temporäre Sperrung von Nutzeraccounts nach mehrfacher Fehleingabe von Passwörtern ● Angemessen sicheres Verfahren zum Zurücksetzen von Passwörtern
Hashing von gespeicherten Passwörtern mittels SHA512
Hashes werden „gesalzen“ (Salt) oder „gepfeffert“(Pepper)
Sperrung von externen Schnittstellen (z.B. USB) durch Data-Leak-Protection Software
Programmprüfungs- und Freigabeverfahren bei Neuinstallationen
Verwendung von Intrusion-Prevention-Systemen
Einsatz von Anti-Viren-Software: Server
Einsatz von Anti-Viren-Software: Clients
Einsatz einer Software-Firewall
Einsatz einer Hardware-Firewall
Mobile-Device-Management
Aufbewahrung personenbezogener Daten/Datenträgern in verschließbaren Sicherheitsschränken oder in gesondert gesicherten Räumen
Regelung zum Home Office / zu Telearbeit

Zugriffskontrolle Soll unerlaubte Tätigkeiten in Datenverarbeitungssystemen außerhalb eingeräumter Berechtigungen verhindern.
Nutzung eines Berechtigungskonzepts
Minimaler Einsatz von Administratoren-Konten
Trennung von Berechtigungsbewilligung (organisatorisch) und Berechtigungsvergabe (technisch)
Regelung zur Wiederherstellung von Daten aus Backups (wer, wann, auf wessen Anforderung)
Aufbewahrung von Datensicherungen (z.B. Cold-Storage) im zutrittsgeschützten Safe
Regelmäßige Überprüfung von Berechtigungen
Beschränkung der freien und unkontrollierten Abfragemöglichkeit von Datenbanken
Regelmäßige Auswertung von Protokollen (Logfiles)
Zeitliche Begrenzung von Zugriffsmöglichkeiten
Teilzugriffsmöglichkeiten auf Datenbestände und Funktionen (Read, Write, Execute)
Protokollierung von Dateizugriffen
Protokollierung von Dateilöschungen
Protokollierung von Dateiveränderungen
SPAM-Filter
Intrusiondetection (IDS)
Beschränkter Zugriff auf LogFiles (nur Log-Admin)
Verschlüsselte Speicherung der Daten durch AES (aes-256-cbc, aes-cbc-essiv:sha256)
Kontrollierte Vernichtung von Daten:
Shredder (Cross-Cut, mindestens Stufe 3, DIN 66399)
Datenträgerentsorgung - Sichere Löschung von Datenträgern (DIN 66399):
Physikalische Zerstörung (z.B. Shredder bei Partikelgrößen bis max. 1000 Quadrat-Millimeter)
Richtlinie zur Datenvernichtung
Clean Desk-Policy

Trennungskontrolle Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt voneinander zu verarbeiten.
Trennung von Kunden (Mandantenfähigkeit des verwendeten Systems)
Logische Datentrennung (z.B. auf Basis von Kunden- oder Mandantennummern)
Berechtigungskonzept, das der getrennten Verarbeitung der Auftraggeber-Daten von Daten anderer Kunden Rechnung trägt
Trennung von Entwicklungs-, Test- und Produktivsystem
Zuordnung von Datensätzen zu Zweckattributen

4. Maßnahmen zur Gewährleistung der Integrität

Weitergabekontrolle Soll die Sicherheit der Daten bei elektronischer Übertragung und Datentransport und die Nachvollziehbarkeit der Weitergabe gewährleisten.
Datenaustausch über https-Verbindung mittels Verschlüsselungsprotokoll TLS 1.3 - TLS_AES_256_GCM_SHA384
Verschlüsselung vertraulicher Datensätze
Verschlüsselung aller Festplatten (von Laptop-Festplatten bis Server-Festplatten)
Dokumentation der Stellen, an die eine Übermittlung vorgesehen ist, sowie der Übermittlungswege

Eingabekontrolle Soll gewährleisten, dass Nachvollzogen werden kann, ob, wer, wann personenbezogene Daten in Datenverarbeitungssysteme eingeben, geändert oder gelöscht hat.
Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
Differenzierte Benutzerberechtigungen: Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
Einzelne Benutzernamen, keine Benutzergruppen
Verpflichtung auf das Datengeheimnis
Über OS-Standard hinausgehendes Log-Konzept

Verfügbarkeitskontrolle
Tägliche Voll-Backups
Redundante Reihe unabhängiger Festplatten (RAID)
Redundante IT-Infrastuktur (Live-System, StandBy-System)
E-Mail-Archivierung
Durch Richtlinien Standardisierte Meldewege und Notfallpläne

5. Maßnahmen zur Gewährleistung der Belastbarkeit

Belastbarkeit (Widerstandsfähigkeit und Ausfallkontrolle) Soll Systeme befähigen, mit risikobedingten Veränderungen umgehen zu können und Toleranz und Ausgleichsfähigkeit gegenüber Störungen aufzuweisen.
Durchführung von Penetrationstests
Systemhärtung (Deaktivierung nicht erforderlicher Komponenten)
Unverzügliche und regelmäßige Aktivierung von verfügbaren Soft- und Firmwareupdates
Regelmäßige Sensibilisierung der Mitarbeiter (mind. jährlich)
Prozess zur unverzüglichen Meldung von Vorkommnissen an die IT ist allen Mitarbeitern bekannt

6. Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Kontrollverfahren Soll die Wirksamkeit der Datensicherheitsmaßnahmen gewährleisten.
Meldung neuer/veränderter Datenverarbeitungsverfahren an den Datenschutzbeauftragten
Prozesse zur Meldung neuer/veränderter Verfahren sind dokumentiert
Prüfung der Wirksamkeit getroffener Sicherheitsmaßnahmen mind. jährlich
Bei negativem Feststellungen im Rahmen der zuvor gen. Überprüfung werden die Sicherheitsmaßnahmen risikobezogen angepasst
Prozess zur Reaktion auf Sicherheitsverletzungen (Angriffe) und Systemstörungen existiert (Incident-Response-Management)
Dokumentation von Sicherheitsvorfällen

Anlage 3 – Liste der bestehenden Subunternehmer zum Zeitpunkt des Vertragsschlusses

(Keine Subunternehmer vorhanden)

Anlage 4 – Weisungsberechtigte Personen und Kommunikationsweg zur Weisung

Weisungsberechtigte Personen des Auftraggebers sind:

Weisungsempfänger beim Auftragnehmer sind:

Gordian Brockstedt - gb@accountone.de
Jan Engelhardt - je@accountone.de