Vertragsergänzung Auftragsverarbeitung

Vereinbarung über eine Auftragsverarbeitung gemäß Art. 28 DSGVO

Der Verantwortliche: (im Folgenden Auftraggeber)	Der Auftragsverarbeiter: **COUNT IT GmbH/ COUNT IT TAX GmbH** Softwarepark 49, 4232 Hagenberg ATU65856923/ ATU71435146 (im Folgenden Auftragnehmer)

1. Gegenstand der Vereinbarung

(1) Gegenstand

☐ Der Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben durch den Auftragnehmer: _____[1]

☐ Der Gegenstand des Auftrags ergibt sich aus einem Dienstleistungsvertrag vom _____, auf den hier verwiesen wird. Diese Vereinbarung ist als Ergänzung zu diesem Vertrag zu verstehen.

(2) Art und Zweck der Verarbeitung von Daten

☐ Nähere Beschreibung des Auftrages in Hinblick auf Art und Zweck der vorgesehenen Verarbeitung durch den Auftragnehmer: _____

☐ Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung vom _____.

(3) Art der Daten

Folgende Datenkategorien werden verarbeitet:
_____[2]

(4) Kategorien betroffener Personen

Folgende Kategorien betroffener Personen unterliegen der Verarbeitung:
_____[3]

[1] detaillierte Beschreibung der Aufgaben des Auftragnehmers

[2] Datenkategorien aufzählen, zB Personenstammdaten, Kontaktdaten, Vertragsdaten, Verrechnungsdaten, Bonitätsdaten, Bestelldaten, Abrechnungsrelevante Mitarbeiterdaten, Kundenhistorie, usw

[3] Betroffenenkategorien ergänzen, zB Kunden, Interessenten, Lieferanten, Ansprechpartner, Beschäftigte, Handelsvertreter, Abonnenten, usw.

2. Dauer der Vereinbarung

☐ Einmalige Durchführung
Der Auftrag wird zur einmaligen Durchführung erteilt; die Vereinbarung endet nach Ausführung der Arbeiten.

☐ Befristete Laufzeit
Die Vereinbarung ist befristet abgeschlossen und endet mit _____[4] .

☐ Unbefristete Laufzeit
Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von _____[5] zum _____[6] gekündigt werden. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. Pflichten des Auftragnehmers

(1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.

(3) Wahrung der Vertraulichkeit und Verschwiegenheit: Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

(4) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32ff DSGVO ergriffen hat. Konkret handelt es sich hierbei

[4] Fristende eintragen.

[5] Kündigungsfrist eintragen, zB ein Monat.

[6] Kündigungstermin eintragen, zB Kalenderviertaljahr.

um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Einzelheiten hierzu finden sich im Anhang (Technisch-organisatorische Maßnahmen).

(5) Mitwirkungspflicht bei Betroffenenrechten: Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Betroffenenrechte nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen.
Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

(6) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer durchzuführen (sicherzustellen).

(7) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten. Dazu gehören Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation.

(8) Der Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu erstellen hat.

(9) Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

(10) Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, sämtliche in seinem Besitz gelangten Unterlagen, erstellte Verarbeitungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem

Auftraggeber zu übergeben / in dessen Auftrag zu vernichten[7]. Wenn der Auftragnehmer die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen Format herauszugeben.
Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

(11) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

4. Qualitätssicherung des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt.

Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Herr Josef Kranzer, IT-Technical Services, Tel. 07236/20077-6636, Mail: j.kranzer@countit.at für den Bereich der Informationstechnologie genannt und für den Bereich der Organisation ist der Datenschutzbeauftragte Herr Daniel Braden, Tel. 07236/20077-6718, Mail: d.braden@countit.at bestellt.

5. Technisch-organisatorische Maßnahmen

Die technischen und organisatorischen Maßnahmen (TOMs) unterliegen dem technischen Fortschritt und der Weiterentwicklung. Es ist dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen, soweit das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren. Einzelheiten sind dem Anhang zu entnehmen.

6. Ort der Durchführung der Datenverarbeitung

☐ Ausschließliche Durchführung innerhalb der EU/des EWR
Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw des EWR durchgeführt.

☐ Bei Durchführung, wenn auch nur teilweise, außerhalb der EU/des EWR

[7] Nichtzutreffendes bitte streichen.

Datenverarbeitungstätigkeiten werden zumindest zum Teil auch außerhalb der EU bzw des EWR durchgeführt, und zwar in _____[8]. Das angemessene Datenschutzniveau ergibt sich aus[9]

☐ einem Angemessenheitsbeschluss der Europäischen Kommission nach Art 45 DSGVO.
☐ einer Ausnahme für den bestimmten Fall nach Art 49 Abs 1 DSGVO.
verbindlichen internen Datenschutzvorschriften nach Art 47 iVm Art 46 Abs 2 lit b DSGVO.
☐ Standarddatenschutzklauseln nach Art 46 Abs 2 lit c und d DSGVO.
☐ genehmigten Verhaltensregeln nach Art 46 Abs 2 lit e iVm Art 40 DSGVO.
☐ einen genehmigten Zertifizierungsmechanismus nach Art 46 Abs 2 lit f iVm Art 42 DSGVO.
☐ von der Datenschutzbehörde bewilligte Vertragsklauseln nach Art 46 Abs 3 lit a DSGVO.
☐ einer Ausnahme für den Einzelfall nach Art 49 Abs 1 Unterabsatz 2 DSGVO.

7. Sub-Auftragsverarbeiter

Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. 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 Datenverarbeitungsanlagen 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.

☐ Verbot der Hinzuziehung eines Sub-Auftragsverarbeiters
Der Auftragnehmer ist nicht berechtigt, einen Sub-Auftragsverarbeiter zur unmittelbaren Erbringung der Hauptdienstleistung heranzuziehen.

☐ Zulässigkeit der Hinzuziehung eines bestimmten Sub-Auftragsverarbeiters
Der Auftragnehmer ist befugt folgendes Unternehmen als Sub-Auftragsverarbeiter zur unmittelbaren Erbringung der Hauptdienstleistung hinzuziehen: _____ [10]

☐ Zulässigkeit der Hinzuziehung von Sub-Auftragsverarbeitern
Der Auftragnehmer kann Sub-Auftragsverarbeiter _____[11] zur unmittelbaren Erbringung der Hauptdienstleistung hinzuziehen.

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

- der Auftragnehmer dies dem Auftraggeber eine angemessene Zeit vorab schriftlich anzeigt und

[8] Staaten aufzählen.

[9] Siehe im Allgemeinen Merkblatt Internationaler Datenverkehr nach der EU-DSGVO.

[10] Firmenname und Sitz ergänzen, Art der Tätigkeiten.

[11] Tätigkeiten.

- der Auftraggeber nicht gegenüber dem Auftragnehmer schriftlich Einspruch gegen die geplante Auslagerung erhebt und
- die erforderlichen Vereinbarungen zwischen dem Auftragnehmer und dem Sub-Auftragsverarbeiter gemäß des Art. 28 Abs. 4 DSGVO abgeschlossen werden. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

8. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Einvernehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO 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.

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

9. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

_____, am _____	Hagenberg, am _____
Für den Auftraggeber:	Für den Auftragnehmer:
.....	.....
[Name samt Funktion]	DI(FH) Peter Berner, MA Geschäftsführender Gesellschafter COUNT IT Group

Anhang – Technisch-organisatorische Maßnahmen (TOMs)

Vertraulichkeit

- Zutrittskontrolle:

Eingangsbereich:
Der Eingangsbereich der COUNT IT GmbH ist durch ein elektronisches Zutrittssystem gesichert. Dieses verriegelt außerhalb der Bürozeiten automatisch die Eingangstüren, in diesen Zeiten ist der Zutritt zu dem Gebäude nur mittels personalisierter Chipkarten (Mitarbeiter), bzw. Schlüsseln (Geschäftsführung/ Eigentümer) möglich.

Während der Bürozeiten gibt es einen permanent besetzten Empfangsbereich, der Besucher begrüßt und der internen Kontaktperson bei COUNT IT Bescheid gibt, damit diese den Besucher in Empfang nimmt und durch das Haus begleitet

Bürobereich:
Der Bürobereich ist durch versperrbare Türen gesichert. Die Schlösser dieser Türen sind in verschiedene Sperrbereiche unterteilt, jeder Mitarbeiter bekommt einen Schlüssel, mit dem genau der Bereich, für den er tätig ist, sperrt. Die Mitarbeiter haben die Anweisung, dass der letzte Mitarbeiter, der ein Büro verlässt, dieses zu verschließen hat. Im 1. OG sind die Bürobereiche zusätzlich durch Türen mit Fallschloss gesichert, für deren Öffnung ebenfalls ein Büroschlüssel benötigt wird.

Serverräume/ Technikräume:
Die Server- und Technikräume sind permanent versperrt. Zutritt zu diesen Räumen haben nur die Mitarbeiter von COUNT IT, die im Rahmen ihrer täglichen Arbeiten Zutritt zu diesen Räumlichkeiten benötigen. Diese Räume sind entweder durch Schließsysteme mit Schlüsseln oder Zutrittssystemen mittels Chipkarten gesichert.

Server- und Technikschränke sind, genauso wie die Netzwerkverteilerschränke in den einzelnen Stockwerken, zusätzlich versperrt. Die Schlüssel hierfür sind wiederum nur den Mitarbeitern von COUNT IT zugänglich, die aufgrund ihrer täglichen Arbeit Zutritt zu diesen Systemen benötigen.

Sämtliche Serverräume sind mit Videoüberwachung ausgestattet, welche die Aktivitäten, die in diesen Räumlichkeiten passieren, aufzeichnen. Zugriff auf diese Aufzeichnungen haben wiederum nur Mitarbeiter, die für die Sicherung dieser Räume verantwortlich sind.

- Zugangskontrolle:

Passwörter:
Sämtliche IT-Systeme sind zumindest mittels Passwort gegen unerlaubten Zugriff gesichert. Diese Passwörter sind entweder den Mitarbeitern persönlich bekannt, oder in anerkannten Softwarelösungen verschlüsselt abgelegt (Passwort Safes) und können nur von Berechtigten Mitarbeitern zugegriffen werden. Passwörter, welche personifizierten Benutzerkonten zuzuordnen sind, sind in regelmäßigen Abständen zu ändern.

Es gibt eine IT Security Policy, die sämtlichen Mitarbeitern der COUNT IT bekannt und zugänglich ist und deren Inhalt regelmäßig geschult wird, in dem unter anderem die sichere Handhabung von Passwörtern beschrieben ist. Diese IT Security Policy wird jedem Mitarbeiter bei Eintritt vorgelegt, auf deren Beachtung wird laufend hingewiesen. In dieser IT Security Policy sind ebenso vermerkt, welchen Bedingungen ein Passwort genügen muss und wie oft es gewechselt werden muss. Die IT Security Policy wird in regelmäßigen Abständen reevaluiert und ggf. angepasst, um technisch zeitgemäß zu bleiben. Änderungen werden allen Mitarbeitern bekannt gemacht.
Mitarbeiter können bei Fragen zusätzlich auf die Mitarbeiter des Technical Service zukommen, welche konkrete Anfragen entgegennehmen und Handlungsvorschläge im Sinne eines sicheren Umgangs mit IT-Systemen und Informationen abgeben.

Berechtigungsvergabe:
Es können nur bestimmte Mitarbeiter Anpassungen an Zugriffsberechtigungen für bestimmte Systeme bzw. gespeicherte Daten (Fileshares/ Gruppenpostfächer/ …) beantragen.
Berechtigungsvergaben haben grundsätzlich schriftlich per E-Mail zu erfolgen – diese E-Mails werden zur Dokumentation abgelegt um nachvollziehen zu können, zu welchem Zeitpunkt bestimmte Mitarbeiter Zugriff auf bestimmte Systeme und Daten bekommen haben.
Der Entzug von Berechtigungen kann grundsätzlich auch auf Zuruf erfolgen, muss aber im Nachhinein schriftlich begründet werden.
Grundsätzlich werden (soweit von den IT Systemen unterstützt) personifizierte Zugriffskonten Gruppenkonten vorgezogen. Somit ist es bei Tätigkeitswechsel bzw. Austritt eines Mitarbeiters einfach möglich, dessen Zugriffsberechtigungen anzupassen bzw. zu sperren.

Trennungskontrolle:
Durch die Mandantenfähigkeit der Systeme in Kombination mit den Zugangsdaten (Username und Passwort) einem Rechtesystem für jeden Benutzer wird sichergestellt, dass die Datenbestände logisch voneinander getrennt gespeichert werden und keinerlei Zugriff durch nicht autorisierte Benutzer erfolgen kann.

Administrative Zugangsdaten zu Systemen sind nur denjenigen Personen zugänglich, welche diese auch verwalten. Zur sicheren Speicherung dieser Zugangsdaten (und um einfacher lange, komplexe und schwer merkbare Kennwörter für administrative Zugangsdaten verwenden zu können) sind diese Gruppen-, Projekt-, oder Kundenbezogen verschlüsselt abgelegt (Passwort Safes). Diese Passwortdateien sind nur den Personengruppen zugänglich, welche diese für diese tägliche Arbeit benötigen.

Für die periodische Kontrolle der Zugriffsberechtigungen sind die Mitarbeiter verantwortlich, welche auch die Vergabe von Zugriffsberechtigungen beauftragen können. Auf Anfrage wird ihnen von den jeweiligen Systembetreuern eine Übersicht über die aktuell vergebenen Berechtigungen auf Systeme und Daten zur Verfügung gestellt, Anpassungen an den Berechtigungen werden dann auf Wunsch durchgeführt.

Verschlüsselung:
Daten auf Festplatten in Notebooks und Computern werden verschlüsselt. Backupdaten auf Sicherungsbändern werden verschlüsselt abgelegt. Tages- und Wochensicherungen werden in einem Safe im Firmengengebäude der COUNT IT verwahrt, Monats- und Jahressicherungen werden extern in einem angemieteten Schließfach bei einer Bank in Linz verwahrt.

Drucken:
Drucker, welche mit einem leicht zugänglichen Bereich des Firmengebäudes stehen, sind mit einer eigenen Authentifizierung mittels Zugangschip ausgestattet. Ein Druckjob wird erst gestartet, wenn der jeweilige Mitarbeiter sich am Drucker authentifiziert. Dies soll verhindern, dass gedruckte Informationen unbefugten Personen zugänglich gemacht werden.

Integrität

- Weitergabekontrolle: Bei regelmäßiger elektronischer Übermittlung von Daten wird großes Augenmerk darauf gelegt, dass diese nur verschlüsselt erfolgt und auf gesicherten Systemen abgelegt werden. COUNT IT stellt hierfür verschiedene Systeme bereit, welche eine Verschlüsselung auf dem Stand der Technik bietet. Diese sind unter anderem:
    - SMTPS (verschlüsselte SMTP E-Mail Übertragung)
    - FTPS Server (SSL-gesicherte FTP Übertragung)
    - Verschlüsselte Client-VPN-Zugänge
    - Verschlüsselte Site2Site VPNs
    - …

Die Anwendbarkeit dieser gesicherten Übertragung ist stark abhängig von der technischen Ausstattung der einzelnen Kunden. Bei ungesicherten Zugriffen und Übertragungen machen die Techniker der COUNT IT den Kunden im Auftrag der jeweiligen Fachabteilung darauf aufmerksam, hat aber selbst keinen Eingriff in die Systeme des Kunden zu/ von dem Daten übertragen werden.

In Ausnahmefällen werden Daten in gedruckter Form vom Kunden übernommen bzw. dem Kunden übergeben. In diesem Fall wird sehr stark darauf geachtet, dass diese ausgedruckten Daten persönlich von einem verantwortlichen Verarbeiter übernommen, bzw. einer Berechtigten Person beim Kunden übergeben werden. Diese ausgedruckten Daten werden zu Zeiten, in denen sie nicht verarbeitet werden, versperrt verwahrt.

Eingabekontrolle:
Datenmanipulationen (Einfügen, Bearbeiten und Löschen) werden in einem Änderungsprotokoll (Change Log bzw. Audit Log) festgehalten, welches selbst archiviert (Backup) wird. Das Protokoll basiert auf Änderungen, die an den Daten in den von Ihnen verfolgten Tabellen vorgenommen werden. Im Änderungsprotokoll sind Posten chronologisch gelistet und zeigt Änderungen an, die in den Feldern der angegebenen Tabellen vorgenommen wurden. Das Änderungsprotokoll erfasst alle Änderungen, die auf der Tabelle vorgenommen wurde.

Verfügbarkeit und Belastbarkeit

- Verfügbarkeitskontrolle

Sämtliche kritischen Systeme bei COUNT IT werden laufend durch entsprechende Monitoringsysteme auf ihre korrekte Arbeitsweise gemäß den technischen Möglichkeiten hin überwacht. Zusätzlich sind Benachrichtigungsmechanismen implementiert, welche via Applikation, E-Mail oder SMS die jeweils verantwortlichen Techniker und Applikationsbetreuer zu jeder Zeit alarmieren können.

- Schutz gegen Zerstörung/ Backupstrategien

Sämtliche kritischen Systeme sind durch entsprechende Zutrittskontrollen gegen unbefugten Zugriff und Zerstörung gesichert.

Es ist ein Backupkonzept implementiert, durch das die Backupdaten von den Echtsystemen gebäudeseitig getrennt abgelegt werden. Es werden tägliche Sicherungen auf Festplattenspeicher angelegt, wöchentliche Sicherungen werden auf Band verschlüsselt gespeichert. Wochenbänder werden dabei in einem Datensicherungssafe in einem eigenen Brandschutzbereich bei COUNT IT abgelegt, Monats- und Jahressicherungen in einem Schließfach einer Bank in Linz. Es hat nur eine eingeschränkte Personengruppe Zutritt zum Bankschließfach und es gibt einen nominierten Verantwortlichen, der für den direkten Transport der Sicherungsbänder zwischen dem Firmengebäude der COUNT IT und dem Bankschließfach und zuständig ist.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Datenschutzfreundliche Voreinstellungen
  Microsoft Security Development Lifecycle (SDL). Die Datenschutzanforderungen werden frühzeitig definiert und in den SDL integriert. Dabei handelt es sich um einen Softwareentwicklungsprozess, der Entwicklern ermöglicht, Produkte und Dienste mit größerer Sicherheit zu integrieren. Im Rahmen dieses Prozesses unterstützt der SDL die Datenschutz- und Privatsphärenanforderungen, einschließlich einer effektiven Datenschutzüberprüfung jeder Version eines Produkts oder Dienstes von Microsoft.
  In der verarbeitenden Software kommt ein restriktives Berechtigungssystem zu tragen. Jeglicher Zugriff auf Daten muss für verarbeitende Personen explizit vergeben müssen. Die aktuellen Zugriffsberechtigungen einzelner Personen sind auswertbar im System hinterlegt.