Fachbereich IT

business@citynet.at
T +43 800 700 155

Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 EU-Datenschutz-Grundverordnung

gemäß Artikel 28 EU-Datenschutz-Grundverordnung für den Telekommunikations- und Managed IT-Bereich.

Als Verantwortlicher:	**Als Auftragsverarbeiter:**
Name (Unternehmen):	Name (Unternehmen):
	HALLAG Kommunal GmbH, Fachbereich IT
Ansprechperson:	Ansprechperson: Manuel Kofler, MSc
	Leiter Fachbereich IT
Adresse:	Adresse:
	Augasse 6, A-6060 Hall in Tirol
Kundennummer:	/

I. Präambel

Diese datenschutzrechtliche Vereinbarung gilt für alle in der Folge vom Auftragsverarbeiter abzuwickelnden Aufträge sowie Verträge für die Bereitstellung von Cloud-; Security-, Managed IT- bzw. Webhosting Dienstleistungen sowie der damit im Zusammenhang stehenden Leistungen wie z.B.: Datensicherung, virtuelle Server, E-Mail Dienst, Domainverwaltung etc. und dient insbesondere zur Absicherung der Einhaltung datenschutzrechtlicher Bestimmungen. Gegenstand dieser Vereinbarung ist nicht die originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch den Auftragsverarbeiter. Sollte für Einzelfälle eine Abänderung/Ergänzung der datenschutzrechtlichen Vereinbarung erforderlich sein, hat dies schriftlich zu erfolgen.

1. Allgemeine Informationen

Kategorien betroffener Personen:

(durch den Verantwortlichen vollständig und richtig auszufüllen bzw. anzukreuzen)

☐ Kunden
☐ Interessenten
☐ Abonnenten
☐ Beschäftigte
☐ Lieferanten
☐ Handelsvertreter
☐ Ansprechpartner
☐ Sonstige: _____

Art der personenbezogenen Daten:

(durch den Verantwortlichen vollständig und richtig auszufüllen bzw. anzukreuzen)

☐ Personenstammdaten
☐ Kommunikationsdaten (z.B.: Telefon, E-Mail)
☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
☐ Kundenhistorie
☐ Verbrauchsabrechnungs- und Zahlungsdaten
☐ Planungs- und Steuerungsdaten
☐ Auskunftsangaben (von Dritten, z.B.: Auskunfteien, oder aus öffentlichen Verzeichnissen)
☐ Sonstige: _____

2. Gegenstand und Art der Verarbeitung, Zweck der Verarbeitung:

Gegenstand und Art der Verarbeitung sowie Zweck der Verarbeitung ergeben sich aus dem zwischen den Vertragsparteien bestehenden Vertrag. Der Auftragsverarbeiter ist verpflichtet, die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich zur vertraglich vereinbarten Leistung zu verwenden. Dem Auftragsverarbeiter ist es gestattet, verfahrens- und sicherheitstechnisch erforderliche Zwischen-, Temporär- oder Duplikats-Dateien zur leistungsgemäßen Erhebung, Verarbeitung und / oder Nutzung der personenbezogenen Daten zu erstellen, soweit dies nicht zu einer inhaltlichen Umgestaltung führt. Nicht gestattet ist es, unautorisiert Kopien der personenbezogenen Daten zu erstellen. Daten aus Adressbüchern und Verzeichnissen dürfen nur zur Kommunikation im Rahmen der Auftragserfüllung mit dem Verantwortlichen verwendet werden. Eine anderweitige Nutzung und Übermittlung für eigene oder fremde Zwecke, einschl. Marketingzwecke, ist nicht gestattet. Soweit seitens Auftragsverarbeiter eine Erhebung, Verarbeitung und / oder

Nutzung der Daten erfolgt, geschieht dies ausschließlich in dem bestehenden Vertrag definierten Gebiet oder in einem Mitgliedsstaat der Europäischen Union sowie in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum.

3. Dauer der Verarbeitung:

☐ Die Dauer dieser Vereinbarung (Laufzeit) entspricht der Laufzeit des Dienstleistungsvertrages (insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht).
☐ Die Vereinbarung ist befristet abgeschlossen und endet mit [TT.MM.JJJJ].
☐ Der Auftrag wird zur einmaligen Ausführung erteilt.
☐ Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von 3 Monaten gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

4. Pflichten des Auftragsverarbeiters

(1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. 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 bzw. allenfalls eine schriftliche Zustimmung.

(2) 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.

(3) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (Einzelheiten sind der Anlage /1 zu entnehmen).

(4) Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person 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. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenverarbeitung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (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).

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

(7) Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch von ihm nachweislich 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, so etwa:

- über die Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme

- über die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
- über ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(8) Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben / in dessen Auftrag zu vernichten1. 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.

(9) 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.

5. Pflichten des Verantwortlichen

Der Verantwortliche ist verpflichtet, dem Auftragsverarbeiter für eine allfällige Nachfrage durch betroffene Personen die nach Art. 13 DSGVO notwendigen Pflichtinformationen zur Verfügung zu stellen sowie eine Weisung über Vermittlung dieser Informationen an die betroffene Person zu geben. Des Weiteren informiert dieser den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

6. Inanspruchnahme von weiteren Auftragsverarbeitern

Der Auftragsverarbeiter ist berechtigt für die Durchführung der Verarbeitung weitere Auftragsverarbeiter zu beauftragen. Für diese Auftragsverarbeiter gelten gem. Art. 28 Abs. 4 DSGVO dieselben Pflichten wie für den Auftragsverarbeiter selbst. Der Verantwortliche erhält auf Anfrage eine Liste der weiteren Auftragsverarbeiter. Finden während der Verarbeitung Änderungen an bestehenden Auftragsverarbeitern statt oder werden neue Auftragsverarbeiter beauftragt, so wird der Verantwortliche davon gem. Art. 28 Abs. 2 DSGVO informiert.

7. Haftung und Recht auf Schadensersatz

Der Auftragsverarbeiter haftet gegenüber betroffenen Personen für den durch seine Verarbeitung verursachten Schaden nur dann, wenn er seinen auferlegten Pflichten aus dieser Verarbeitung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat (Art. 82 Abs. 2 DSGVO). Der Auftragsverarbeiter wird von der Haftung befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. (Art. 82 Abs. 3 DSGVO).

8. Meldung bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragsverarbeiter informiert gemäß Artikel 33 DSGVO den Verantwortlichen unverzüglich nach Bekanntwerden einer Verletzung des Schutzes personenbezogener Daten. Als Verletzung des Schutzes personenbezogener Daten gilt gem. Art. 4 Abs. 12 eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei einer allfälligen Benachrichtigung von betroffenen Personen nach einer Verletzung des Schutzes von personenbezogenen Daten, wenn diese Verletzung im Bereich des Auftragsverarbeiters aufgetreten ist.

9. Datenschutzfolgeabschätzung

Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Durchführung einer allfälligen Datenschutzfolgenabschätzung bzw. der vorherigen Konsultation der Aufsichtsbehörde.

10. Nachweise

Der Auftragsverarbeiter stellt auf Anfrage dem Verantwortlichen Nachweise über die Einhaltung der Vereinbarung zur Verfügung und ermöglicht Überprüfungen und Inspektionen durch den Verantwortlichen oder einen vom Verantwortlichen beauftragten Prüfer und trägt dazu bei. Die Überprüfungen oder Inspektionen erfolgen innerhalb der regulären Geschäftszeiten sowie ohne Störung des Betriebsablaufs.

11. Löschung von Daten

In Übereinstimmung mit Artikel 17 DSGVO („Recht auf Löschung“) werden die personenbezogenen Daten nach Abschluss der Verarbeitung bzw. nach der in der Einleitung der Verarbeitung genannten Dauer von den Systemen des Auftragsverarbeiters gelöscht. Nach § 4 (2) Datenschutzgesetz (DSG) wird die Verarbeitung bis zur tatsächlichen Löschung eingeschränkt.

12. Salvatorische Klausel, Gerichtsstand

Sollten eine oder mehrere Bestimmungen ganz oder teilweise unwirksam oder undurchführbar sein oder werden, so berührt dies die Wirksamkeit und Durchführbarkeit der übrigen Bestimmungen dieser Vereinbarung nicht. Die unwirksame oder undurchführbare Bestimmung gilt durch jene Bestimmung ersetzt, die der unwirksamen oder undurchführbaren Bestimmung nach dem wirtschaftlichen und technischen Zweck möglichst nahekommt. Das Gleiche gilt für den Fall, dass die Vereinbarung eine Regelungslücke aufweist. In diesem Fall soll jene angemessen Regelung gelten, die die Partner gewollt hätten, sofern sie bei Abschluss dieses Vertrages den entsprechenden Punkt bedacht hätten. Als ausschließlicher Gerichtsstand für sämtliche Streitigkeiten aus und in Zusammenhang mit dieser Vereinbarung ist das für die HALLAG Kommunal GmbH zuständige ordentliche Gericht vereinbart.

_____

Ort, Datum

----------	**----------**
Verantwortlicher	**Auftragsverarbeiter** **HALLAG Kommunal GmbH**

Anhänge: Anhang 1 – Technisch-organisatorische Maßnahmen zum Schutz von personenbezogenen Daten beim Auftragsverarbeiter.

Anhang 1: Technisch-organisatorische Maßnahmen zum Schutz von personenbezogenen Daten beim Auftragsverarbeiter

1. Organisationskontrolle

Ziel der Organisationskontrolle ist es, die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Gemeint ist damit, dass sich der Datenschutz nicht an die Organisation, sondern die Organisation an den Datenschutz anpassen sollte.

- Betriebsrat vorhanden
- Risikoanalyse nach ISO 27001 liegt vor
- Führung eines ISMS nach ISO 27001
- Schriftliche Regelungen über den Betrieb und die Abläufe der Datenverarbeitung sowie zu den verschiedenen Datensicherheitsmaßnahmen / IT-Sicherheitskonzeption, IT-Sicherheitsrichtlinien / Arbeits- und Verfahrensanweisungen / Stellenbeschreibungen
- Ausschluss einer Mitbenutzung der DV-Anlagen durch Fremdfirmen
- Ausschluss einer Mitbenutzung der TK-Anlagen durch Fremdfirmen
- Urlaubs-/Krankheitsvertretung des DV-Verantwortlichen
- DV-Revision, interne Revision (jährliche Penetration Tests und Datencenter Audits)
- Ausreichende Funktionstrennung, 4-Augen-Prinzip in kritischen Bereichen
- Regelungen zur Beschaffung von Hard- und Software
- Schriftliches Programmfreigabeverfahren im Rahmen des Beschaffungsprozesses
- Regelungen über Sicherung des Datenbestandes
- Regelmäßige Hinweise, Ermahnungen um das Problembewusstsein zu fördern
- Gelegentliche, unvermutete Kontrolle der Einhaltung von Datenschutz- und Datensicherungsmaßnahmen
- IT-Versicherungen (Cyber- und Betriebshaftpflicht (IG))

2. Zutrittskontrolle

Maßnahmen der Zutrittskontrolle dienen dazu, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- Betriebsgelände in alleiniger Nutzung
- Bewegungsmelder
- Bewachung des Geländes/Gebäudes außerhalb der Betriebsstunden mittels Gebäude-Alarmanlage mit Verbindung zur Polizei und Feuerwehr
- Zeitraum -> 24x7
- Serverräume abgegrenzt (Sperrbereich)
- PC-Arbeitsplätze abgegrenzt
- TK-Anlage abgegrenzt (Sperrbereich)
- Netzverteiler abgegrenzt (Sperrbereich)
- Zutritt ausreichend abgesichert: Türen, Türschlösser (alle Türen mit Keycard oder Schlüsselschließsystem gesichert)
- Elektrische Türschlösser
- Rollos gegen Hochschieben gesichert (Teilweise zentral gesteuert)
- Fenster gegen Einsicht von außen geschützt
- Schlüsselregelung bei auf- und Abschließen der Räume bei Arbeitsbeginn bzw. –ende
- Quittierung der Schlüsselausgabe
- (Schlüsselverwaltungssystem und zentrale Steuerung
- Aufbewahrung Generalschlüssel geregelt
- Überwachungseinrichtungen Räume mittels Alarmanlage, Videoüberwachung mit Aufzeichnung

- Schriftliche Festlegungen zur Zutrittsberechtigung mittels Generalschlüsselentnahme (Protokoll) / Ausweisregelungen (Prozess zur Identitätsprüfungen bei permanentem Zutritt) / Trennung von Bearbeitungs- und Publikumszonen / Besucherregelungen (Prozess definiert) / Besucherbuch / Kundenabfertigung (Schalterbetrieb)
- Zutrittskontrollsystem mittels Transponderkarte
- Kontrolle Reinigungs- und Wartungsarbeiten
- Elektronisches Zeiterfassungssystem
- Anwesenheitskontrolle mittels Protokollierung von Zutritten (zentrale Protokollierung)
- Zutrittskontrolle bei Tele-/Heimarbeitern geregelt (Zugriff nur über SSL-Portal mit User/Passwort und zweitem Faktor)

3. Zugangskontrolle

Durch eine effektive Zugangskontrolle soll verhindert werden, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Sprich, hat ein Unbefugter die Hürde des verbotenen Zutritts überwunden und hat es beispielsweise bis in das Bürogebäude geschafft, in dem Unternehmensclients stehen, oder hatte er gar keine Hürde zu überwinden, da er selbst Angestellter der Firma ist, soll ihm durch Zugangskontrollmaßnahmen der Zugang zu Datenverarbeitungssystemen verwehrt werden, für die er keine Berechtigung besitzt.

- Passwortverfahren mittels Forderung einer unterschiedlichen Zeichenzusammensetzung / 8 Zeichen (Regelung unterteilt in unterschiedliche Devices (Organisationsrichtlinie)) / Regelmäßiger Wechsel (90 Tage) / Erstanmeldeprozedur
- Bildschirmsperre bei Pausen mit Passwort-Aktivierung
- Zugangssperre bei mehr als 5 Anmeldeversuchen
- Passworthistorie
- Passwortrichtlinie / Merkblatt (Organisationsrichtlinie)
- Elektronischer Passwort Safe
- Personalisierte Administrator Accounts
- Einmal-Passwörter (Token?) (bei Heimarbeitsplätzen)
- BIOS-Passwörter
- Single-Sign-On (SSO)? (vor allem bei kaufmännischen Systemen (Oauth))
- Bei Administratorzugang muss Passwort länger als 8 Zeichen sein
- Nur personalisierte Zugangskennungen
- Einsatz von dedizierten Service Useraccounts für Datenaustausch
- Einsatz eines Passwort-Managers (regelmäßige Sicherung der Datenbank auf Datenträger und Versperrung in Safe)
- Elektronische Signatur (Signierung von E-Mails bei gewissen Destinationen über X509)
- Transponderkarten (stattdessen Mehrfaktor-Authentifizierung für externe Arbeitsplätzen)
- Protokollierung des Zugangs (An-/Abmeldung)
- Verschlüsselung mobiler Datenträger/Festplatten (in der Regel BitLocker)
- Zugang von außerhalb des Intranets abgesichert
- Zugang ins Internet über Proxy-Server (mit SSL-Interception)
- Firewall Zugriffsberechtigungskonzept
- Firewall Änderungsberechtigungen eingeschränkt
- Nachvollziehbarkeit von Firewall Regeländerungen
- Prüfung des Firewall-Regelwerks mit eigenem Analyzer für Simulation und Tests
- Fortinet Hardware-Firewall mit Support und Wartungsvertrag
- Regelmäßige manuelle Firmwareupdates der Firewall
- Benachrichtigung bei Sicherheitslücken mittels abonniertem Feed Fortiguard
- Feed wird geliefert und Updates manuell eingespielt
- Browser-Updates laufend, automatisiertes Verfahren (Baramundi (Mobile, PC, Notebooks); definierte Gruppen zur Test-Installation von Patches
- Verwaltung der Browser-Konfiguration durch Administration
- Administrationsrichtlinie

- Hauptamtliche Administratoren
- Aufgabenbezogene systemtechnische Trennung bei mehreren Administratoren (Zuständigkeiten und Rollen sind definiert)
- Spezielle Passwortkonventionen zur Administration (abweichend von Nutzer-Passwörter)
- Getrennte Benutzerkonten für Systemadministration, Sachbearbeitung, persönlichen Nutzungen
- Anwendung des 4-Augen-Prinzips (teilweise (Video-Auswertung, Log-Auswertung, Vorstandsanfragen; ein Mitglied des Betriebsrats jeweils dabei))
- Protokollierung der Administrationsarbeit mittels Protokoll-Server (u.a. SysLog-Server)
- Vorkehrungen gegen Protokollmanipulation
- Notfallpasswörter hinterlegt

4. Zugriffskontrolle

Die Zugriffskontrolle soll 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“.

- Schriftliches Berechtigungskonzept
- Programmtechnisches Berechtigungskonzept (SSO bei fast allen Anwendungen mit Berücksichtigung der jeweiligen AD-Berechtigungsgruppe)
- Rollendefinition
- Differenzierte Berechtigungen für Daten (Zugriffsberechtigungen für Shares)
- Differenzierte Berechtigungen für Anwendungen (SSO bei fast allen Anwendungen mit Berücksichtigung der jeweiligen AD-Berechtigungsgruppe)
- Ausgestaltung des Berechtigungskonzeptes und der Zugriffsrechte mittels Protokollierung und Verfahrensanweisung/Richtlinie (Bei neuen Berechtigungen Zustimmung des Vorgesetzten; Protokollierung über Ticketsystem)
- Protokollierung von Shell-Zugriff
- Protokollierung von Richtlinienverstoß
- Automatisierte Protokollauswertung
- Synchronisierung der Uhren zur Auswertung von Protokollen (via eigenen NTP-Servern mit GPS-Synchronisierung)
- Prozesse zur Erlangung und Veränderung von Berechtigungen bei Anlage eines Benutzers / bei Abteilungswechsel / bei Aufgabenänderung / bei Austritt
- Regelmäßige Überprüfung, ob vergebene Berechtigungen noch notwendig sind
- Rollenbasiertes Berechtigungskonzept kommt zum Einsatz
- Datenträger sind inventarisiert
- Nur registrierte USB-Sticks können verwendet werden
- SD-Karten nur nach Freigabe
- Interne gehostete Datenaustausch-Plattform
- Auslagerung von Sicherungsdatenträgern in zwei verschiedenen Data Centern
- Richtlinien zur Entsorgung/Vernichtung von Fehldrucken und unbrauchbaren bzw. nicht mehr gebrauchten Datenträgern als Teil der Organisationsrichtlinie
- Datenschutzgerechte Löschung verwendeter DT vor neuer Verwendung bzw. Weitergabe
- Sichere Zwischenlagerung von Datenträgern, welche zu vernichten sind
- Einsatz von „Reißwolf“/Shredder
- Einsatz von Geräten zum Verbrennen/Zerstören
- Kontrolle der ordnungsgemäßen Vernichtung
- Einsatz von zuverlässigem Entsorgungsunternehmen mit vertraglicher Regelung
- Entsorgungsbescheinigung, Löschprotokoll
- Sperrung der Laufwerke und Anschlüsse (USB, Diskette, CD/DVD ...) -> Einsatz spezieller Software (USB gesperrt, DVD keine Brennfunktion)
- Zugriffsschutz durch Bildschirmschoner mit automatischer Sperre und ausschließlich passwortgestützter Aufhebung
- Regelungen und Kontrolle von externer Wartung und Fernwartung

- Nur unternehmenseigene Geräte dürfen mit dem internen Netzwerk verbunden werden
- Unternehmensfremde Geräte werden vom internen Netzwerk automatisch erkannt (MAC Adress-Filter)
- Offene WLAN-Segmente müssen mit einer Firewall vom internen Netz getrennt sein (eigene Hotspot-Lösung, Gäste WLAN)
- Zugriffe aus externen Netzen über eigenen VLANs
- Mobile Endgeräte sind verschlüsselt
- Die Nutzung externer E-Mail-Provider ist untersagt
- E-Mails mit vertraulichem Inhalt müssen verschlüsselt werden (Anhänge werden verschlüsselt, kritische Inhalte mittels E-Mail Verschlüsselung oder über Datenaustausch-Plattform)
- Die Nutzung von externen Instant Messaging Diensten ist verboten
- Prozess für Einsicht in fremde Mailboxen vorhanden (z.B. bei Krankheit des Eigentümers) (4-Augen Prinzip)
- Bei Internet-Anwendungen werden Anmeldedaten verschlüsselt übertragen (HTTPS als Default)
- Trennung von funktionalen Netzwerkgruppen in einzelne VLANs (Drucker, Zeit-Terminals, Kameras, Server-Plattform, …)
- Weitergabekontrolle

Die Weitergabekontrolle dient der Datensicherheit, wenn personenbezogene Daten weitergegeben werden. Durch eine effektive Weitergabekontrolle sollen die Integrität und die Vertraulichkeit während der Weitergabe gewährleistet sein. Vor allem dürfen während der Datenübermittlung oder des Transportes die Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden. Des Weiteren soll der Empfänger der Daten ausreichend geprüft und festgestellt werden. Dabei umfasst die Weitergabekontrolle jede Art von Übermittlung, auch eine Datenverarbeitung innerhalb der verantwortlichen Stelle.

- Transportsicherung mittels sicherer Versendungsformen wie Dateiverschlüsselung, E-Mail-Verschlüsselung, Elektronische Signatur, VPN, Festplattenverschlüsselung (mobile Arbeitsgeräte)
- Vorgesehene Datenübermittlungen in den Verfahrensübersichten vermerkt
- Dokumentation der Abruf- und Übermittlungsprogramme
- Protokollierung der Übermittlung
- Regelungen für Tele- / Heimarbeiter
- Vereinbarung zur Auftragsverarbeitung bei Fernwartung vorhanden
- Fernwartungs-Zugang via VPN, SSL-Portal
- Fernwartung Verschlüsselung des gesamten Übertragungsweges
- Verwendete kryptographische Algorithmen sind dokumentiert
- 05.12.08.01 - Fernwartung Zugang mittels 4-Augen-Prinzip (gesplittetes Passwort) und Einmal-Passwort (Token) (für externe Arbeitsplätze und in der IT-Administration)
- Monitoring der Fernwartungsaktivitäten
- Protokollierung der Fernwartung
- Regelungen zur Verwaltung und Konfiguration der Wartungszugriffe mittels Freigabeverfahren

5. Eingabekontrolle

Innerhalb der Eingabekontrolle soll die nachträgliche Überprüfbarkeit und Feststellung gewährleistet werden, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind.

Protokollierungs- und Protokollauswertungssysteme mittels Feldauditierung

Aufbewahrungsdauer der Protokolle definiert

6. Auftragskontrolle

Maßnahmen, die geeignet sind, „zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können"

- Sorgfältige Auswahl der Auftragnehmer

- Kriterien zur Auswahl der Auftragnehmer festgelegt (Informationssicherheit, KSV-Auszug, UID-Prüfung, Referenzen, Zertifizierungen, Gütesiegel)
- Detaillierte schriftliche Regelungen (Vertrag/Vereinbarung) der Auftragsverhältnisse und Formalisierung des gesamten Auftragsablaufes, auch zum Einsatz von Subunternehmen, eindeutige Regelungen der Zuständigkeiten und Verantwortlichkeiten (speziell auch bei der Datensicherung und dem DT-Transport)
- Auftragsdurchführung kontrolliert und dokumentiert
- Vereinbarungen nach Artikel 28 DSGVO
- (Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien betroffener Personen, Angabe der Pflichten und Rechte des Verantwortlichen)
- Mitarbeiter beim Auftragnehmer sind zur Vertraulichkeit verpflichtet
- Maßnahmen zur Sicherstellung der Verarbeitung sind getroffen (Art. 32 DSGVO)
- Informationen über Sub-Auftragnehmer und Verpflichtung zur Mitteilung von Änderungen bei Sub-Auftragnehmern
- Mithilfe bei der Erfüllung der Betroffenenrechte
- Nach Abschluss Rückgabe bzw. Löschung der Daten
- Auftragsverarbeiter müssen Nachweise über die getroffenen Maßnahmen erbringen

7. Verfügbarkeitskontrolle

Personenbezogene Daten sind vor Verlust und zufälliger Zerstörung zu schützen.

Brandschutzeinrichtungen (Feuerlöscher im Serverraum, Feuerlöscher an/in den PC-Arbeitsräumen, Rauch- oder Brandmelder, Feuerfeste Schränke (Feuerfester Safe), Brandschutztüren, Brandschutzklappen, Brandklasseneinteilung (Kennzeichnung besonders gefährdeter Räume), Löschanlage im Serverraum (Novec 1230 Gas), Rauchverbot in Server- und PC-Arbeiträumen

- Unterbrechungsfreie Stromversorgung (USV)
- Motorgenerator (Dieselaggregat)
- Überspannungsschutzeinrichtungen
- Klimatisierung Serverraum
- Datensicherungskonzept vorhanden
- Datenlöschkonzept bzw. -vorschrift vorhanden
- Sicherungen zur Sicherstellung eines ordnungsgemäßen Betriebes (Server, Netzwerkkomponenten, Konfiguration der Datensicherung, SAN-Switche, Benutzeradministration, Konfigurations- und Softwaremanagement, genutzte Programme, Datenbestand / -kategorien, Protokolle Zutrittsdaten, Protokolle Zugangsdaten, Technische Protokolle
- Räumlich getrennte Aufbewahrung von Datenträgern (getrennte data center und Backup-data center)
- Spiegeln der Festplatten (z.B. RAID) für zentrale Festplattensysteme (DS 1+2 spiegeln sich, DS 2+3 sind Backup, DS 3 hat auch noch Notfall-Ressourcen)
- Virenschutz mittels Sandboxing-Lösung
- Schutzsoftware erkennt unbekannte Schadsoftware (erkennt anomalien)
- Schutzsoftware erkennt auch Schadsoftware in verschlüsselten Dateien (Sandboxing)
- Automatisches Update der Schutzsoftware über zentralen Update-Server (Sentinel 1 (Sandboxing-Lösung))
- Spamfilter (FortiMail und FortiSandbox)
- Intrusion Detection System (IDS) / Intrusion Prevention System (IPS)
- Havariearchiv (Notfall-Ressourcen im Backup-Rechenzentrum)
- Notfallplan
- Monitoring von Hosts
- Monitoring von Hardware-Zuständen
- Monitoring von Services
- Monitoring der Service-Integrität

8. Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhobene wurden, müssen getrennt verarbeitet werden. Auch wenn es recht praktisch erscheint, die Daten aus verschiedenen Quellen einfach zusammenzuführen, ist dies nicht zulässig. Vielmehr muss durch geeignete Maßnahmen verhindert werden, dass die Daten einfach gemischt werden können.

- Interne Mandantenfähigkeit (Unternehmungen sind getrennt)
- Trennung der verarbeitenden Systeme in Produktion, Integration (Kommunikationsschnittstellen nach außen sind auf ein Minimum reduziert), Test (Kommunikationsschnittstellen nach außen sind auf ein Minimum reduziert)
- Trennung der verarbeitenden Systeme Arbeitsplätze und Server über Firewall und Unterschiedliche Subnetze (VLANs)
- Trennung der verarbeitenden Systeme Arbeitsplätze und Server über Unterschiedliche Nutzerkonten (named user mit entsprechenden Kennwörtern oder SSO)
- Trennung der Nutzerkonten von Produktion und Integration (named user mit entsprechenden Kennwörtern oder SSO)