villach

Magistratsdirektion

Datensicherheit

Schlussbericht des Stadtrechnungshofes

villach

Vorbemerkungen

Sprachliche Gleichbehandlung
Die in diesem Bericht verwendeten personenbezogenen Ausdrücke betreffen, soweit dies inhaltlich in Betracht kommt und nicht ausdrücklich anderes bestimmt ist, alle Geschlechter gleichermaßen.

Comply or Explain
Der Stadtrechnungshof erwartet sich zu seinen Feststellungen und Maßnahmenempfehlungen, dass diesen im Regelfall entweder zustimmend und zeitnahe nachgekommen wird (COMPLY), oder aber bei Nichterfüllung, nicht vollständiger und/oder nicht zeitgerechter Erfüllung, eine umfassende Darstellung und Begründung der zugrundeliegenden, diesbezüglichen Managemententscheidung vorgelegt wird (EXPLAIN).

Disclaimer des Stadtrechnungshofes
Sachverhalte, die dem Stadtrechnungshof im Rahmen der gegenständlichen Prüfung nicht zur Kenntnis gelangt sind, wurden von der Prüfeinrichtung nicht gewürdigt. Die Prüfeinrichtung und ihre Prüfer können für allfällige gesetzwidrige und strafrechtliche Sachverhalte – vor, während und nach der Einschau – nicht zur Verantwortung gezogen werden. Dasselbe gilt auch für strukturelle und allgemein organisatorische Fragestellungen, die nicht dezidiert Inhalt der Prüfung waren und dem Prüforgan auch im Zuge der Einschau nicht als problematisch und als akute Optimierungs- und Regelungsnotwendigkeit aufgefallen sind.

Darstellung von Zahlen und Beträgen
Sämtliche Beträge im Bericht sind in der Währung Euro (EUR) angegeben und zur leichteren Lesbarkeit grundsätzlich gerundet. Negative Beträge in Tabellen sind in spitzen Klammern ohne führendes Minuszeichen dargestellt (z. B. <15.265>).

Formatierungen und Darstellungen im Bericht
Im Bericht werden die Feststellungen und Empfehlungen des Stadtrechnungshofes nach Aufzählungszeichen (●) in **fetter Schrift** dargestellt. Die Stellungnahmen der überprüften Stelle/n sind *kursiv* kenntlich gemacht, allfällige Gegenäußerungen des Stadtrechnungshofs werden ***kursiv und fett*** festgehalten.

villach

Inhaltsverzeichnis

Abkürzungsverzeichnis

CSV	Comma-separated values – Textdatei mit strukturierten Daten
DA	Dienstanweisung
dPUM	Digitale Postumlaufmappe
DSG	Datenschutzgesetz
DSGVO	Datenschutzgrundverordnung
DS-RL	Datenschutzrichtlinie der Stadt Villach
DV	Datenverarbeitung
EAV	Elektronische Ausschussverwaltung
GR	Gemeinderat
HHO	Haushaltsordnung
IRM	Incident Response Management
ISMS	Informationssicherheitsmanagementsystem
IT, IKT	Informationstechnologie, Informations- und Kommunikationstechnologie
JSON	JavaScript Object Notation –Datenformat für strukturierte Daten
KVP	Kontinuierlicher Verbesserungsprozess
K-VStR	Villacher Stadtrecht
MS	Microsoft
NIS	Netzwerk- und Informationssicherheit
PC	Personal Computer
PDF	Portable Document Format
PUM	Postumlaufmappe
SSD	Solid-State-Drive
TLS	Transport Layer Security
USB	Universal Serial Bus
VPN	Virtual Private Network
XML	Extensible Markup Language
ZO	Zahlungsverkehrsordnung (früher Kassenordnung)

MD	Magistratsdirektion
StRH	Stadtrechnungshof
MD/IT	Abteilung Informations- und Kommunikationstechnologien
2/HL	Abteilung Hochbau und Liegenschaften

1 Prüfungsauftrag und –umfang

Der Stadtrechnungshof hat vom Kontrollausschuss der Stadt den Auftrag erhalten, die Datensicherheit der Stadt Villach auf Wirtschaftlichkeit, Zweckmäßigkeit und Effizienz zu prüfen.

Datensicherheit ist ein Begriff, der oft im Zusammenhang mit Datenschutz genannt wird. Datenschutz konzentriert sich auf die Wahrung der Privatsphäre und den Schutz personenbezogener Informationen. Die Datensicherheit zielt im Gegensatz dazu darauf ab, technische und organisatorische Maßnahmen zu ergreifen, um alle Arten von Daten vor Verlust, Manipulation und diversen anderen Bedrohungen zu schützen.

Die Aspekte des Datenschutzes sind demnach im Rahmen dieser Prüfung nur am Rande und/oder implizit umfasst.

Die gegenständliche Prüfung soll die Frage beantworten, ob die, zweifelsohne bisher in einschlägigen Bereichen getroffenen Maßnahmen und organisatorische Regelungen ausreichen, um Datensicherheit aktuell hausweit und auch für die Zukunft sicherzustellen.

Aus dem Risikomanagement sollte ein System / Controlling abgeleitet werden, das auf operativer Ebene Datensicherheit logisch & physisch sicherstellt und ständig im Sinne eines Kontinuierlichen Verbesserungsprozesses (KVP) an einer Optimierung arbeitet. Hinsichtlich der herrschenden und (abschätzbaren) zukünftigen BEDROHUNG soll das System präventiv Maßnahmen planen, regeln, umsetzen und auf Einhaltung kontrollieren. Diesen Regelkreis im Controlling der Datensicherheit schließt dann wiederum eine Um-/Neuplanung für die Zukunft im strategischen Bereich ab.

Die Datensicherheit wurde nach der Art der der zu sichernden Daten (logisch/physisch), der Verwendung der Daten (statisch/dynamisch) und nach dem Ort der Datenaufbewahrung (zentral/verteilt) überprüft.

2 Prüfungsergebnis

Die Prüfung ergab, dass der Magistrat eine detailliert ausgearbeitete Datenschutzrichtlinie aufweist. Diese ist auf aktuellem Stand und entspricht den gesetzlichen und organisatorischen Standards.

Die Mitarbeiter des Magistrats sind über die Richtlinie informiert, eine konkrete Schulung über den Inhalt ist allerdings nicht erfolgt. Eine regelmäßige Schulung über die Anwendung „KnowledgeCheckR“ wird vom Stadtrechnungshof empfohlen, um eine lückenlose und effektive Umsetzung der Richtlinie zu gewährleisten.

Die eingerichteten technischen Sicherheitsmaßnahmen werden als robust und effektiv beurteilt. Es wurde festgestellt, dass die Netzwerksicherheit durch Firewalls, Verschlüsselung und regelmäßige Sicherheitsüberprüfungen gewährleistet wird.

Die Anwendung von Sicherheits-Patches[1] und Updates erfolgt zeitnah und ein Incident-Response-Management wurde implementiert, um auf potenzielle Sicherheitsvorfälle schnell reagieren zu können.

Der Magistrat verfügt über sichere Zugangskontrollsysteme bei den Eingängen zum Rathaus, den Nebengebäuden und teilweise bei den dislozierten Abteilungen, um unautorisierten Zugang zu den Büro- und Technikräumen zu verhindern. Zusätzlich regelt die Datenschutzrichtlinie den Umgang mit Besuchern, magistratsfremden Personen und externen Dienstleistern, um das Risiko von Datensicherheitsverletzungen zu minimieren.

Der Magistrat verfügt über effektive Datensicherheitsmaßnahmen, die den Schutz der zu verarbeitenden Daten gewährleistet. Kontinuierliche Verbesserungen und stetige Aktualisierung der Datensicherheitsstrategien müssen weiterhin durchgeführt werden, um die Sicherheit der verwendeten Daten gewährleisten zu können.

In der Gemeinderatssitzung vom 5. Juli 2024 wurde zudem die Einführung der „Informationssicherheitsleitlinie“ zum Aufbau eines Informationssicherheitsmanagements mit Wirksamkeit ab 1. August 2024 beschlossen. Damit ist die Stadt auch für die Bestimmungen der NIS-2-Richtlinie (Richtlinie (EU) 2022/2555) und der sich daraus ergebenden gesetzlichen Vorgaben, vorbereitet.

[1] Als *Patches* werden Aktualisierungen für bestehende Anwendungen oder Betriebssysteme zur zeitnahen Behebung von Fehlern oder Sicherheitslücken bezeichnet.

3 Grundlagen der Prüfung

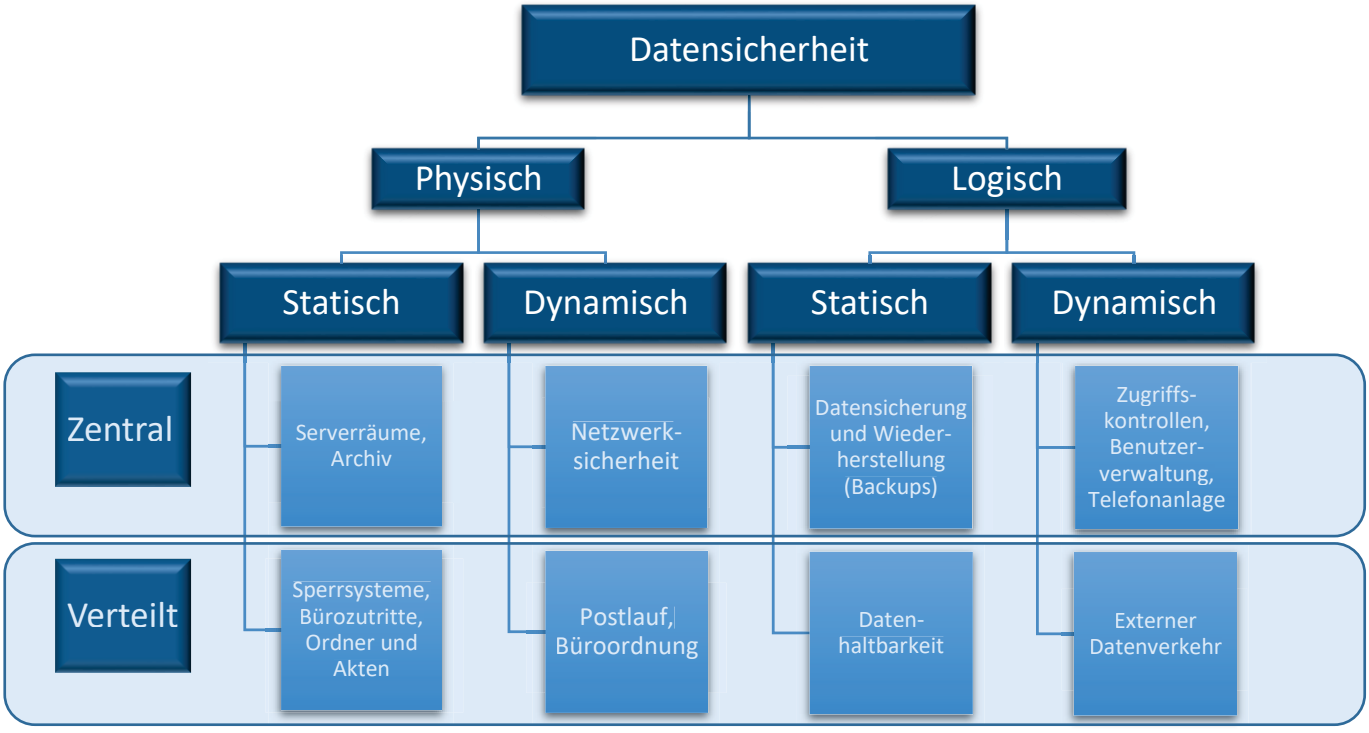
Als Grundlage für diese Prüfung gelten folgende Vorgaben:

- Datenschutzgesetz (DSG)
- Datenschutzgrundverordnung (DSGVO)
- Villacher Stadtrecht (K-VStR)
- Geschäftseinteilung
- Datenschutzrichtlinie der Stadt Villach (DS-RL)
- Dienstanweisungen des Magistrats

Der vorliegende Prüfbericht basiert zudem auf Informationen der geprüften Geschäftsgruppen und Abteilungen im Zuge der Prüfungshandlungen des StRH vor Ort.

4 Struktureller Aufbau der Prüfung / Betrachtungsfelder

Die vom Stadtrechnungshof gewählte systemische Perspektive zur Prüfung der Datensicherheit im Haus bildet verschiedene Handlungsfelder zur physischen und logischen Sicherung des erfassten, bearbeiteten und archivierten Datenbestandes ab. Grundsätzliche Unterscheidung bildet die physische Sicherung des analogen Datenbestandes und die logische Zugriffs- und Verwahrungssicherheit digitaler Daten.



Generelle Datensicherheit verbindet physische Sicherheitsaspekte, die sich auf analoge und faktische Schutzmaßnahmen beziehen, mit logischen Sicherheitsaspekten, die digitale und softwarebasierte Schutzmethoden umfassen.

Zusätzlich wird zwischen der statischen und dynamischen Dimension unterschieden. Statische Sicherheit bezieht sich auf Daten oder Objekte, die fest an einem Ort verbleiben, während dynamische Sicherheit für bewegliche, mobile Datenbestände oder Speicherobjekte steht. Schließlich wird die vorgefundene Sicherheitsarchitektur als zentralisiert oder verteilt klassifiziert, wobei zentralisierte Systeme an einem einzelnen Ort zu finden sind und verteilte Systeme über mehrere Standorte oder Komponenten gestreut sind.

Jeder Schnittpunkt in dieser Struktur repräsentiert eine Kombination dieser Eigenschaften, wodurch unterschiedliche Herausforderungen und Ansätze in der Datensicherheit betrachtet werden sollen.

4.1 Logische und physische Datensicherheit

Logische Datensicherheit bezieht sich auf die Schutzmaßnahmen, die dazu dienen, Daten vor nicht autorisiertem Zugriff und Manipulationen zu schützen, indem sie die Integrität, Vertraulichkeit und Verfügbarkeit der Daten sicherstellen. Die logische Datensicherheit konzentriert sich hauptsächlich auf die Implementierung von Software-basierten Schutzmechanismen, um unautorisierten Zugriff auf Daten oder Systeme zu verhindern. Dazu zählen etwa Firewalls, Antivirenprogramme, Datenverschlüsselung und Zugriffskontrollsysteme.

Diese Maßnahmen sollen nicht nur die Daten selbst, sondern auch die Netzwerkressourcen und -dienste schützen. Darüber hinaus spielen Aspekte wie die Authentifizierung und Autorisierung von Benutzern, Netzwerksicherheitsprotokolle und Sicherheitsrichtlinien eine entscheidende Rolle, um die logische Integrität und Sicherheit der Daten innerhalb eines Systems oder Netzwerks zu gewährleisten.

Physische Datensicherheit dagegen konzentriert sich darauf, die physischen Systeme und Infrastrukturen, die die Daten speichern und verarbeiten, vor schädlichen Eingriffen und Umwelteinflüssen zu schützen. Das umfasst Maßnahmen gegen Umweltkatastrophen wie Brände oder Überschwemmungen, aber auch vor menschlichen Bedrohungen wie Einbruch, Vandalismus oder Diebstahl.

Um die physische Datensicherheit zu gewährleisten, können verschiedene Mittel und Strategien eingesetzt werden, darunter beispielsweise physische Zutrittskontrollen, Sicherheitsschlösser, Überwachungskameras, Alarmsysteme und Umweltkontrollsysteme, die vor extremen Temperaturen, Feuchtigkeit oder anderen potenziell schädlichen Bedingungen schützen.

Durch die Kombination von logischer und physischer Sicherheit kann ein umfassendes Sicherheitsnetzwerk geschaffen werden, um Daten und Systeme auf vielfältige Weise zu schützen und die Risiken, die mit Datenverlust und -beeinträchtigung verbunden sind, minimieren.

4.2 Statische und dynamische Datensicherheit

Statische Datensicherheit betrifft den Schutz von Daten, die gespeichert und nicht aktiv verwendet oder verarbeitet werden, also Daten, die sich in einem Zustand der "Ruhe" befinden. Hierbei konzentriert sich der Schutz auf die Gewährleistung der Integrität, Verfügbarkeit und Vertraulichkeit dieser gespeicherten Daten. Es geht darum, dass die Daten vor unberechtigtem Zugriff, Verlust oder Beschädigung geschützt sind, während sie auf einem Datenträger, wie einer Festplatte, SSD, einem USB-Stick oder in der Cloud, gespeichert sind.

Ein wesentliches Element der statischen Datensicherheit ist die Verschlüsselung, bei der Daten in eine nicht lesbare Form umgewandelt werden, um sie vor unberechtigtem Zugriff zu schützen. Weitere Maßnahmen könnten Backups, Redundanzen und bestimmte physikalische Sicherheitsmechanismen umfassen, die sicherstellen, dass die Daten auch im Falle eines Ausfalls oder eines Sicherheitsvorfalls wiederhergestellt werden können.

Dynamische Datensicherheit, im Gegensatz dazu, bezieht sich auf den Schutz von Daten, während sie aktiv erzeugt, verarbeitet, übertragen oder abgerufen werden. Hierbei liegt der Fokus darauf, die Daten während des gesamten Lebenszyklus, vor allem, wenn sie sich in Bewegung befinden, zu sichern. Das umfasst beispielsweise den Schutz von Daten während der Übertragung über Netzwerke, also die Sicherstellung, dass Daten, die von einem Ort zum anderen gesendet werden, nicht abgefangen, eingesehen oder manipuliert werden können.

Hierbei spielen Verschlüsselung während der Übertragung, sichere Übertragungsprotokolle wie TLS, VPNs und weitere Technologien eine Rolle, die sicherstellen, dass die Daten während ihrer "Reise" durch das Netzwerk oder über das Internet geschützt sind. Dynamische Datensicherheit erfordert ein besonderes Augenmerk auf Netzwerksicherheit, um sicherzustellen, dass Daten während der Verarbeitung und Übertragung vor Angriffen geschützt sind. Beide Sicherheitsansätze, sowohl statisch als auch dynamisch, sind wesentliche Bestandteile einer umfassenden Datensicherheitsstrategie, um Daten in allen Phasen ihres Lebenszyklus zu schützen.

4.3 Zentrale und verteilte Datensicherheit

Zentrale Datensicherheit konzentriert sich auf den Schutz von Daten, die an einem zentralen Ort gespeichert oder verarbeitet werden. Bei dieser Art von Datenmanagement werden alle Daten an einem einzigen, zentralen Punkt oder Server gespeichert, der dann für die Verarbeitung, Verwaltung und Sicherung dieser Daten verantwortlich ist. Dies ermöglicht eine konzentrierte Steuerung und Überwachung der Daten und kann dazu beitragen, dass Sicherheitsrichtlinien und -verfahren konsequent umgesetzt und eingehalten werden.

Da alle Daten an einem Ort gespeichert sind, können Sicherheitsmaßnahmen, wie Backups und Verschlüsselung, zentralisiert durchgeführt werden, was sowohl in Bezug auf Effizienz als auch Sicherheit Vorteile bieten kann. Allerdings stellt diese zentrale Datenspeicherung auch einen attraktiven Angriffspunkt für Cyberkriminelle dar und kann zu einem Flaschenhals in Bezug auf Datenzugriff und -verarbeitung werden, insbesondere in großen Organisationen oder bei hohem Datenverkehr.

Verteilte Systeme sind hingegen jene, in denen Daten über mehrere Standorte, Server oder Plattformen verteilt gespeichert und verarbeitet werden. Diese Strategie teilt Daten und Verarbeitungslasten auf, um eine bessere Skalierbarkeit und Ausfallsicherheit zu gewährleisten. In einem verteilten Datenspeicherungsmodell muss jedes System oder jeder Knoten, der Daten speichert, sicher sein, und die Daten müssen während der Übertragung zwischen den Knoten geschützt werden. Hierbei spielen Netzwerksicherheit, sichere Datenübertragung und Authentifizierung eine wesentliche Rolle, um die Integrität und Vertraulichkeit der Daten zu wahren.

Ein verteiltes System kann die Resilienz gegenüber Ausfällen erhöhen, da der Ausfall eines einzelnen Knotens nicht zwangsläufig zu einem Totalausfall des Systems führt. Allerdings kann die Verwaltung der Sicherheit in verteilten Systemen komplexer sein, da es viele verschiedene Knotenpunkte zu überwachen und zu sichern gilt.

Beide Ansätze, zentrale und verteilte Systeme, haben Vorteile und Herausforderungen in Bezug auf Datensicherheit und müssen basierend auf den spezifischen Anforderungen gewählt werden.

5 Prüfungsfeststellungen

5.1 Physische Absicherung

5.1.1 Serverräume

Die Errichtung und Ausstattung eines modernen Serverraums ist eng mit dem Thema der Datensicherheit verknüpft.

Kontrollsysteme, die einen unbefugten Zutritt verhindern, schützen kritische Daten vor physischen Bedrohungen. Zusätzliche Unterstützung dabei kann durch Videoüberwachungssysteme und Bewegungsmelder zur Erkennung und Dokumentation verdächtiger Aktivitäten, ermöglicht werden.

Ein weiterer Aspekt hinsichtlich der Datensicherheit ist der Brandschutz im Serverraum. Bei der Standortwahl für einen Serverraum ist daher zu beachten, dass dieser idealerweise in einem eigenen Brandschutzbereich untergebracht sein sollte. Zusätzliche Maßnahmen wie leicht erreichbare Feuerlöscher, Rauchmelder und automatische Löschanlagen stellen sicher, dass im Falle eines Brandes schnell reagiert werden kann, um Datenverluste zu vermeiden.

Die Geräte in einem Serverraum müssen vor Kontakt mit Wasser geschützt sein. So sollte der ausgewählte Standort möglichst keine Fenster (Eintritt von Regenwasser) oder wasserführende Leitungen in der Decke oder den Wänden aufweisen.

Abseits der physischen Sicherheit ist die Stabilität der IT-Infrastruktur wichtig. Eine entsprechende Klimatisierung schützt die Server vor Überhitzung, wodurch die Integrität und Verfügbarkeit der Daten gewährleistet wird.

In einem schriftlichen Berechtigungskonzept muss festgelegt sein, wer organisatorisch und technisch den Serverraum betreten darf. Jeder Aufenthalt und der Zweck bzw. die durchgeführten Arbeiten im Serverraum sollten dabei dokumentiert werden.

Insgesamt bildet die Ausstattung des Serverraums die Grundlage für eine robuste Datensicherheitsstrategie, indem sie sowohl den physischen Schutz der Hardware, als auch die Aufrechterhaltung einer stabilen Betriebsumgebung gewährleistet.

Die Implementierung eines Serverraums erfordert eine sorgfältige Planung und Analyse der Anforderungen, Auswahl eines geeigneten Standorts, Installation, Konfiguration und die regelmäßige Wartung der Geräte.

- **Eine schriftliche Dokumentation der getroffenen und noch durchzuführenden Maßnahmen für die Ausstattung zur Wahrung der Datensicherheit liegt vor. Die geplanten Schritte und real umgesetzten Maßnahmen werden vom Stadtrechnungshof im Zuge einer Follow-up-Prüfung begutachtet.**

Stellungnahme MD/IT: Die Stadt Villach betreibt ein auf zwei Standorten verteiltes Rechenzentrum. Die Idealanforderungen an die Serverräume wurden schriftlich festgelegt und der bauausführenden Abteilung 2/HL übermittelt. Im Rahmen des Planungsprozesses wurden im Hinblick auf bauliche, technische als auch finanzielle Rahmenbedingungen alternative Lösungsansätze realisiert. Grundsätzlich sind die Anforderungen der Abteilung MD/IT an die Ausführung von Serverräumen der Stadt Villach erfüllt. Aufgrund der begrenzten räumlichen Möglichkeiten mussten lediglich Abstriche bei der Verhinderung flüssigkeitsführender Leitungen eingegangen werden, welche jedoch durch Sensortechnik für die frühzeitige Erkennung möglicher Schadensfälle minimiert werden. Dieses Risiko stellt im Kontext des gerade im Aufbau befindlichen Informationssicherheitsmanagementsystems (ISMS) ein akzeptables Risiko dar.

StRH: Die städtischen Anforderungen an die Serverräume wurden schriftlich festgelegt. Alternative Lösungsansätze aufgrund der vorliegenden Rahmenbedingungen werden realisiert. Das, durch diese notwendige Kompromisslösung hinsichtlich der flüssigkeitsführenden Leitungen, erhöhte Risiko wird vom StRH allerdings kritisch betrachtet. Die detailliertere Risikobewertung und die dazugehörige entsprechende Dokumentation hat im ISMS zu erfolgen. Die getroffenen Entscheidungen und das akzeptierte Risiko sind zu dokumentieren.

5.1.2 Archiv

Das Villacher Stadtrecht legt im § 80 (3) folgendes fest:

```
(3) Im Magistrat ist ein Archiv zur sicheren Aufbewahrung von Akten,
Urkunden und Verhandlungsschriften zu führen. Sofern Daten bei der
Stadt elektronisch vorhanden sind, darf dieses Archiv elektronisch
geführt werden.
```

Dieses Archiv hat die essentielle Funktion, wichtige Dokumente und Aufzeichnungen systematisch zu sichern, um sowohl den laufenden Betrieb als auch historische Referenzen und Rechenschaftspflichten zu unterstützen.

Eine elektronische Führung dieses Archivs ist explizit erlaubt, sofern die entsprechenden Daten bei der Stadt bereits in digitaler Form vorliegen. Digitale Lösungen zur Archivierung zu nutzen, welche Effizienz und Zugänglichkeit verbessern können, haben gegenüber physischen Systemen klare Vorteile.

Für die elektronische Aufbewahrung von Akten und Dokumenten kommt beim Magistrat die Software DocuWare zum Einsatz.

Bei der Stadt ist in der Dienstanweisung „Büroordnung“ (DA 6) geregelt, welche Dokumente elektronisch und welche physisch zu archivieren sind. Ebenso ist hier geregelt, wie die Aufbewahrung im Detail zu erfolgen hat.

Akten werden teils elektronisch und teils physisch aufbewahrt. Die Nichtbeachtung der geltenden Vorschrift kann zu Ineffizienzen führen und das Risiko von Datenverlust oder -verfälschung erhöhen.

Für eine effektive und sichere Archivierung sind klare Richtlinien unerlässlich, die festlegen, unter welchen Bedingungen Dokumente elektronisch und/oder physisch zu archivieren sind und wie die Langzeitsicherung und Integrität der Dokumente gewährleistet werden kann.

Nach Auskunft der Magistratsdirektion sind für die Kontrolle und Einhaltung der Dienstanweisung „Büroordnung“ (DA 6) die Leitungen der Organisationseinheiten zuständig.

- **Die Prüfung ergab für den StRH keine Anmerkungen und nötigen Ergänzungen zu den bestehenden Vorschriften.**

5.1.3 Schließsysteme, Bürozutritte, Ordner und Akten

Die physische Sicherheit ist ein unverzichtbarer Aspekt der Datensicherheitsstrategie, besonders in Bezug auf den Schutz sensibler Informationen und bestehender Vermögenswerte.

Ein wesentlicher Bestandteil physischer Sicherheitsmaßnahmen ist das Sperrsystem, das den Zugang zu Räumlichkeiten und sensiblen Bereichen kontrolliert. Dies kann durch traditionelle Schlüsselsysteme, elektronische Schließanlagen oder biometrische Zugangssysteme erfolgen, die sicherstellen, dass nur autorisierte Personen Zutritt haben.

Die Einhaltung strikter Zutrittsregeln auch nach Dienstschluss ist bedeutend für die Sicherheit und den Schutz des jeweiligen Gebäudes sowie der darin befindlichen Daten und Vermögenswerte. Außerhalb der Öffnungszeiten müssen Zugänge gesichert und der Zugang streng kontrolliert werden, wobei nur autorisiertem Personal Zutritt gewährt wird.

Der Umgang mit organisationsfremden Personen erfordert dabei besondere Aufmerksamkeit. Besucher sollten außerhalb der regulären Öffnungszeiten generell keinen Zutritt erhalten, es sei denn, es liegt eine vorherige Genehmigung oder ein spezifischer Grund vor. Zusätzlich sollten alle Vorfälle oder verdächtigen Beobachtungen sofort gemeldet werden.

Hinsichtlich Datensicherheit ist die Etablierung einer „Clean-Desk-Policy“ notwendig, die vorsieht, dass Mitarbeiter ihren Arbeitsplatz am Ende des Tages frei von sensiblen Dokumenten hinterlassen. Dies verringert das Risiko des Informationsdiebstahls oder der unbefugten Einsichtnahme.

Die sichere Aufbewahrung physischer Ordner und Akten muss einerseits möglich sein und andererseits im Arbeitsalltag gelebt werden. Dazu gehört die Verwendung von abschließbaren Aktenschränken und die regelmäßige Überprüfung, wer Zugang zu diesen Informationen hat.

Der PC-Arbeitsplatz ist bei Nicht-Anwesenheit gegen Fremdzugriff zu schützen und Speichermedien sind unter Verschluss zu verwahren.

Die Verantwortung für die physische Sicherheit liegt hauptsächlich bei den Leitungen der Organisationseinheiten, schlussendlich aber auch bei jedem einzelnen Mitarbeiter.

Durch regelmäßige Schulungen und Bewusstseinsbildung über die Bedeutung der physischen Sicherheit ist sicherzustellen, dass alle Mitarbeiter die erforderlichen Praktiken verstehen und umsetzen, um den Schutz von Vermögenswerten und sensiblen Daten zu gewährleisten.

Die physische Sicherheit wird durch gesicherte Serverräume, Zugangskontrollen, den eingesetzten Sperrsystemen (Türen und Aktenschränke) sowie die Sicherung von Endgeräten gegen unbefugte Inbetriebnahme gewährleistet.

Die Sicherung von Daten in physischer Form, wie bspw. Akten und Ordner, ist organisatorisch geregelt und liegt im Verantwortungsbereich jedes Einzelnen und wird durch die Leitung der Organisationseinheiten überwacht.

Die Vergabe und Kontrolle des elektronischen Schließsystems erfolgt über die Berechtigungsverwaltung. Damit ist eine regelmäßige Aktualisierung möglich.

- **Die Umsetzung dieser Vorgaben ist in den Dienstanweisungen „Ordnung und Sauberkeit am Arbeitsplatz, in Archiven, Besprechungs- und Aufenthaltsräumen (DA 14)“ und „Sicherheit im Magistrat der Stadt Villach (DA 30)“ geregelt.**

- **Die Einhaltung der einschlägigen Dienstanweisungen in diesem Bereich ist zu kontrollieren. Die Bediensteten sind regelmäßig zu schulen. Auf das Risiko des unbefugten Datenzugriffs und eine missbräuchliche Verwendung bzw. die Möglichkeit von Datenlecks ist hinzuweisen und entsprechende Präventivmaßnahmen zu organisieren.**

StRH: In der Schlussbesprechung wurde von MD zugesagt, zukünftig regelmäßig das System der Vorschriften auf Aktualität und Einhaltung zu kontrollieren.

5.2 Logische Absicherung

5.2.1 Netzwerksicherheit

Die Netzwerksicherheit ist ein wesentlicher Aspekt in der IT-Sicherheit. Strenge Richtlinien und der Einsatz von bewährten Praktiken und Technologien sorgen dafür, dass die Integrität, Vertraulichkeit und Verfügbarkeit von Netzwerk- und Datensystemen jederzeit geschützt sind.

Dies beinhaltet nicht nur die Abwehr von externen Bedrohungen, sondern auch die Sicherstellung, dass interne Prozesse und das Know-How der Bediensteten den höchsten Sicherheitsstandards entsprechen. Die kontinuierliche Schulung des Personals in Bezug auf Sicherheitsprotokolle und die Sensibilisierung für potenzielle Cybergefahren spielen hierbei eine wesentliche Rolle.

Die Sicherung des Netzwerks gegen unbefugten Zugriff, Angriffe, Ausfälle und andere Bedrohungen hat höchste Priorität. Netzwerksicherheitsmaßnahmen beinhalten den Einsatz von Firewalls, Antivirenprogrammen, Intrusion Detection Systems (IDS) und regelmäßigen Sicherheitsaudits. Zusätzlich ist die Implementierung von Verschlüsselungstechniken und sicheren Authentifizierungsverfahren sehr wichtig, um sensible Daten und Kommunikationswege zu schützen. Die regelmäßige Aktualisierung und Wartung der Sicherheitssysteme ist ein weiterer Aspekt, um auf neue Bedrohungen und Schwachstellen zeitnah reagieren zu können.

Die Implementierung einer effektiven Netzwerksicherheitsstrategie ist daher unerlässlich, um kritische Daten des Magistrats zu schützen, Compliance-Standards zu erfüllen und das Vertrauen von Bediensteten und Bürgern in die Sicherheit ihrer Daten zu stärken.

Diese Strategie sollte eine umfassende Risikobewertung beinhalten, um Schwachstellen zu identifizieren und entsprechende Gegenmaßnahmen einzuleiten. Darüber hinaus ist es wichtig, dass Notfallpläne entwickelt und regelmäßig getestet werden, um im Falle eines Sicherheitsvorfalls schnell und effektiv reagieren zu können. Die Integration von Netzwerksicherheit in die Gesamtstrategie des Magistrats ist somit ein wesentlicher Bestandteil, um langfristig erfolgreich und sicher zu agieren.

- **Das IT-Netzwerk des Magistrats der Stadt Villach ist gegen unbefugten Zugriff, Angriffe und Bedrohungen durch verschiedene, oben besprochene Sicherheitsmaßnahmen in ausreichendem Maß geschützt.**

Stellungnahme MD/IT: Die IT-Systeme der Stadt Villach werden laufend, in unregelmäßigen Abständen durch interne oder externe Penetrationstests auf mögliche Sicherheitslücken geprüft. Mögliche erkannte Sicherheitslücken werden im Hinblick auf ihre Kritikalität bewertet und geschlossen. Im Rahmen der Einführung des Informationssicherheitsmanagementsystems (ISMS) erfolgt die Überführung der unregelmäßigen Penetrationstests in einen Planprozess im Auditmanagement.

StRH: Ein klar definierter Reporting-Mechanismus für die Ergebnisse der Penetrationstests und die durchgeführten Maßnahmen zur Schließung etwaiger Sicherheitslücken muss etabliert werden. Dies erleichtert die Überwachung des Fortschritts und die sich daraus ergebenden, weiteren Maßnahmen.

5.2.2 Postlauf, Büroordnung

Ein geordnetes Büro und das sachgerechte Entsorgen (Skartieren) von Akten sind wesentliche Aspekte des Informationsmanagements und der Datensicherheit.

Eine Büroordnung auf dem Stand der Technik sorgt nicht nur für eine effiziente und produktive Arbeitsumgebung, sondern minimiert auch das Risiko von Datenlecks oder Verlust sensibler Informationen. Durch eine systematische Organisation von Dokumenten werden der schnelle Zugriff auf benötigte Informationen und die Einhaltung von Compliance-Standards erleichtert.

Das Skartieren von Akten ist besonders wichtig, wenn es um vertrauliche oder veraltete Dokumente geht. Es muss sicher und gemäß den Datenschutzbestimmungen erfolgen, entweder durch sachgerechtes Schreddern oder mittels Entsorgung durch dafür befugte externe Unternehmen. Klare Richtlinien für die Aufbewahrungsfristen von Dokumenten sind dafür unerlässlich und diese müssen regelmäßig überprüft werden.

Somit kann sichergestellt werden, dass nur relevante und aktuelle Dokumente aufbewahrt werden. Die Kombination aus effektiver Büroordnung und verantwortungsbewusstem Skartieren von Akten trägt wesentlich dazu bei, die Integrität und Sicherheit organisationskritischer Daten zu wahren.

- **Die Behandlung von Poststücken sowie die Skartierung von Akten ist beim Magistrat Villach durch die Dienstanweisung „Büroordnung (DA 6)“geregelt.**

5.2.3 Datensicherung und Wiederherstellung (Backups)

Die lückenlose Datensicherung und erfolgreiche Wiederherstellung verlorener Daten sind wesentliche Komponenten des IT-Managements. Diese Prozesse stellen sicher, dass wichtige Daten gegen Verlust durch Hardwareausfälle, menschliche Fehler, Cyberangriffe oder Naturkatastrophen geschützt sind.

Die Datensicherung umfasst das regelmäßige Kopieren und Archivieren von Daten, um sie im Falle eines Systemausfalls oder Datenverlusts wiederherstellen zu können. Eine effektive Strategie für die Datensicherung beinhaltet in der Regel redundante Speicherlösungen, wie beispielsweise lokale Backups, aber auch cloudbasierte Speicheroptionen.

Die Wiederherstellung ist der Prozess, verlorene Daten aus diesen Sicherungen effizient und zuverlässig wiederherzustellen, um den Regelbetrieb so schnell als möglich wieder aufnehmen zu können. Daten schnell und vollständig wiederherstellen zu können, um Unterbrechungen bei der täglichen Arbeit zu minimieren und die kontinuierliche Leistungsfähigkeit der Organisation zu gewährleisten, ist dabei ein wesentliches Kriterium.

- **Regelmäßige Backups, um die Wiederherstellungen im Falle eines möglichen Datenverlustes zu ermöglichen, werden im Magistrat durchgeführt.**

- **Die fehlerlose Wiederherstellung wird durch regelmäßige Tests des Systems garantiert.**

- **Das Generationenprinzip[2] (Großvater-Vater-Sohn-Prinzip) wird angewendet.**

Aufgrund des stetig zunehmenden Datenvolumens, wird seitens der Abteilung MD/IT eine Umstellung auf ein neues, modernes Datensicherungssystem vorbereitet und in naher Zukunft implementiert. Technische Details hierzu wurden dem Stadtrechnungshof mitgeteilt, bleiben für diesen Berichtsteil aber auf Grund des obligaten Geheimnisschutzes unerwähnt.

- **Die Kriterien für Backup und Wiederherstellung sind vollständig erfüllt.**

- **Außerdem konnte sich der StRH davon überzeugen, dass Maßnahmen zur Anpassung des Systems an den Stand der Technik umgesetzt werden, um die Leistungsfähigkeit und Sicherheit der Datenbackup-Systeme weiter zu optimieren.**

[2] Dieses Prinzip stellt sicher, dass immer mehrere Sicherungen in verschiedenen zeitlichen Abstufungen (Großvater - Vater - Sohn) vorhanden sind.

5.2.4 Datenhaltbarkeit – Langlebigkeit von Daten

Die Langlebigkeit von Daten, auch als "Datenhaltbarkeit" bezeichnet, spielt eine entscheidende Rolle in der digitalen Welt. Es handelt sich dabei um die Fähigkeit, digitale Informationen über längere Zeiträume hinweg zugänglich und nutzbar zu halten.

Ein Schlüsselelement dabei ist die Verwendung von offenen Dateiformaten, die eine breite Kompatibilität und Zugänglichkeit sicherstellen. Offene Formate sind dem Risiko der technologischen Obsoleszenz[3] nicht ausgesetzt, da sie nicht von der Unterstützung durch einzelne Software-Anbieter abhängig sind. Dies gewährleistet, dass Daten auch in Zukunft lesbar und bearbeitbar bleiben und eine entsprechende Langzeitarchivierung ermöglicht wird.

Der Magistrat, der die Haltbarkeit der verwalteten Daten gewährleisten muss, setzt zu einem großen Teil auf Dateien der Microsoft Office-Umgebung, wie Word oder Excel. Diese weit verbreiteten Formate bieten eine hohe Kompatibilität und Benutzerfreundlichkeit. Diese Dateiformate nutzen den „Office Open XML“-Standard und zählen daher zu den offenen Dateiformaten. Auch das vielfach verwendete Dateiformat „PDF“ zählt zu den offenen Dateiformaten.

Darüber hinaus sind Exportschnittstellen für maschinenlesbare Formate in anderen Softwareprodukten eingerichtet. Diese Schnittstellen ermöglichen es, Daten aus proprietären oder spezialisierten Anwendungen in allgemein zugängliche Formate wie CSV, JSON oder XML zu konvertieren. Dadurch wird sichergestellt, dass Informationen auch unabhängig von der ursprünglichen Erstellungssoftware genutzt und weiterverarbeitet werden können.

- **Indem sowohl auf gängige Formate der Microsoft Office-Umgebung, als auch auf flexible Exportschnittstellen gesetzt wird, ist der Bereich der Datenhaltbarkeit positiv zu bewerten. Diese Strategie unterstützt die langfristige Zugänglichkeit und Nutzbarkeit von Daten. Für die kontinuierliche Informationsnutzung in der sich schnell entwickelnden technologischen Landschaft ist das von großer Bedeutung.**

- **Die Datenhaltbarkeit bei der Stadt ist in ausreichendem Umfang gegeben. Die Integrität und Verfügbarkeit der Daten ist dauerhaft sichergestellt.**

[3] durch technologischen Fortschritt und Einsatz neuer Software nicht mehr nutzbare, veraltete Technologien und/oder Produkte

5.2.5 Zugriffskontrolle und Benutzerverwaltung

Wirksame Zugriffskontrollen und eine gelebte Benutzerverwaltung sind in der Sicherheitsstrategie ein wichtiger Faktor. Sie gewährleisten, dass nur autorisierte Personen Zugang zu sensiblen Informationen und Systemen erhalten, wodurch das Risiko von Datenlecks und anderen Sicherheitsverletzungen erheblich verringert wird.

Durch die sorgfältige Verwaltung von Benutzerrechten wird sichergestellt, dass Mitarbeiter nur auf die für ihre Arbeit notwendigen Ressourcen zugreifen können. In einer Zeit, in der die Bedrohung durch Cyberangriffe immer größer wird, ist eine robuste Zugriffskontrolle und Benutzerverwaltung unerlässlich, um die Integrität und Vertraulichkeit organisationskritischer Daten zu schützen.

Beim Magistrat der Stadt Villach ist dafür eine elektronische Berechtigungsverwaltung eingerichtet, bei der durch die Leitungen der Organisationseinheiten Berechtigungen für die Bediensteten beantragt und entzogen werden können. Die organisatorische Regelung ist durch die Dienstanweisung „Zugang zu Datenverarbeitungs- und informationstechnologischen Systemen und (mobilen) Endgeräten (DA 32)“ gegeben. Die DA ist mit 1. April 2020 in Kraft getreten.

- **Der Stadtrechnungshof empfiehlt, die Dienstanweisung Zugang zu Datenverarbeitungs- und informationstechnologischen Systemen und (mobilen) Endgeräten (DA 32) von der Magistratsdirektion, gemeinsam mit der Abteilung MD/IT, periodisch auf ihre Aktualität zu überprüfen. Das Ergebnis der Überprüfung muss entsprechend dokumentiert werden.**

5.2.5.1 Exkurs: Aktualität von Dienstanweisungen

Im Rahmen der Qualitätssicherung und der fortlaufenden Optimierung der internen Prozesse, ist es notwendig, dass die Dienstanweisungen, Richtlinien, Verordnungen und sonstige Anweisungen der Stadt regelmäßig, zumindest in einer jährlichen routinemäßigen Zusammenschau, auf ihre Aktualität und Relevanz hin überprüft und inhaltlich gegeneinander abgestimmt werden. Diese Praxis würde sicherstellen, dass diese Anweisungen den aktuellen gesetzlichen Bestimmungen, organisatorischen Bedürfnissen und „Best-Practices“ entsprechen und als Handlungsrahmen durch Mitarbeiter und Führungskräfte mitgetragen werden.

Der StRH empfiehlt, dass dieser „Compliance-Check“ schriftlich dokumentiert wird. Eine Dokumentation sollte neben dem Datum und Zeitraum, die jeweils verantwortlich beteiligten Personen und den daraus resultierenden Handlungsbedarf und die konsequent betriebene Umsetzung beinhalten. Transparenz und Nachvollziehbarkeit der durchgeführten Normensetzung wäre damit gewährleistet und stünde als Basis für zukünftige Überprüfungen und Optimierungen zur Verfügung.

Die Verantwortung für die Durchführung und Dokumentation dieser Überprüfungen liegt beim Leiter des Inneren Dienstes und den Mitarbeitern der Stabstelle in der Magistratsdirektion. Diese beschriebene Vorgehensweise stellt sicher, dass die gegenseitige Stimmigkeit und Aktualität der Dienstanweisungen gewährleistet bleibt. Die Etablierung dieses definierten Prozesses zur regelmäßigen Überprüfung und Aktualisierung der Compliance schafft auch Klarheit für die Überantwortung von (Führungs)Kompetenzen innerhalb des Magistrates.

Die regelmäßige Überprüfung und Aktualisierung der Dienstanweisungen ist nicht nur eine formale Anforderung, sondern hilft, die Effizienz und Sicherheit bei den Handlungsanweisungen des Magistrats kontinuierlich zu verbessern.

- **Die periodische Überprüfung und Dokumentation der Aktualität aller relevanten Bestimmungen, Verwaltungsregelungen und Dienstanweisungen ist nach Ansicht des Stadtrechnungshofes durch die Magistratsdirektion sicherzustellen.**

StRH: In der Schlussbesprechung wurde ein Intervall von 3 Jahren zur Überprüfung der Dienstanweisungen auf Aktualität und Notwendigkeit mit der Magistratsdirektion vereinbart.

Im Anlassfall soll ein Update zu veränderten Rahmenbedingungen, gesetzlichen Grundlagen und organisatorischen Änderungen (Änderungen in der Geschäftseinteilung) erfolgen. Auf die strikte Einhaltung der Dienstanweisungen ist ein besonderes Augenmerk zu legen.

5.2.6 Telefonanlage

In der Bewertung der Softwarelösung für die beim Magistrat verwendete Telefonanlage wurde festgestellt, dass in diesem Bereich die Datensicherheit gewährleistet ist. Die Daten, die durch die Anlage übertragen oder gespeichert werden, sind mittels Verschlüsselungsmethoden geschützt. Die Integrität und Vertraulichkeit wird somit sicherstellt.

Nur autorisierte Benutzer können auf Funktionen und Daten zugreifen. Die Software ist mit diversen Netzwerksicherheitsfunktionen ausgestattet, die den Schutz gegen externe Bedrohungen verstärken.

Die Software wird kontinuierlich durch Updates und Patches verbessert.

Die Aspekte des Datenschutzes sind zwar kein Fokus dieser Prüfung, werden aber vom Stadtrechnungshof natürlich thematisiert, wenn sie erkannt werden. In der Webclient-Version der Software gab es ein Feature, das im Hinblick auf den Datenschutz problematisch war und vom Stadtrechnungshof der Verwaltungsleitung aufgezeigt wurde. Die Abteilung MD/IT hat in weiterer Folge die Behebung des Problems veranlasst.

Zusammenfassend lässt sich sagen, dass die Softwarelösung der Telefonanlage die Standards in den Schlüsselaspekten der Datensicherheit erfüllt und sich dahingehend als zuverlässig erweist.

- **Hinsichtlich der Datensicherheit gibt es bei der für die Telefonanlage verwendeten Softwarelösung seitens des Stadtrechnungshofes keine Beanstandung.**

- **Ein Problem im Bereich des Datenschutzes wurde vom StRH aufgezeigt. Hier gibt es zwischenzeitlich eine Lösung des Software-Anbieters, die von der Abteilung MD/IT implementiert wird.**

5.2.7 Externer Datenverkehr / Datentransport auf Datenträgern

Der ungehinderte E-Mail-Versand mit Anhängen an externe Empfänger ist für die täglichen Arbeitsprozesse (fast) aller Abteilungen unabdingbar, bringt jedoch gleichzeitig das systemimmanente Risiko der unabsichtlichen oder absichtlichen Weitergabe sensibler Informationen mit sich.

Die Möglichkeit, Daten auf (externe) Datenträger (wie z.B. USB-Sticks, externe Harddisks) zu speichern, erlaubt flexible Datenhandhabung und Transport. Aber auch hier ergibt sich ein erhöhtes Risiko des unbefugten Zugriffs auf Daten (bspw. bei Verlust oder Diebstahl des Datenträgers).

Die Freigabe von Uploads auf externe Webseiten ist für verschiedene Anwendungen notwendig. Es kann dadurch aber auch zu entsprechenden Sicherheitslücken bei missbräuchlicher Verwendung kommen und/oder es ist zusätzliche Verbundbarkeit für Cyberkriminalität gegeben.

Der Zugang zu abteilungsinternen Daten aus dem Homeoffice bietet eine flexible Arbeitsgestaltung, setzt jedoch voraus, dass die Sicherheit der Heimnetzwerke und der Endgeräte gewährleistet ist.

In Anbetracht dieser Punkte erfordert diese offene Gestaltung des Datenverkehrs eine kontinuierliche Risikobewertung und die Implementierung robuster Sicherheitsprotokolle. Dazu gehört vor allem die regelmäßige Schulung der Mitarbeiter in Bezug auf obligate Sicherheitsroutinen. Ziel ist es, ein Gleichgewicht zwischen operativer Flexibilität und dem Schutz vor Datenverlust, Datendiebstahl und Cyberkriminalität zu finden.

- **Der externe Datenverkehr ist für die Handlungsfähigkeit des Magistrats unerlässlich. Durch die IT wurden entsprechende technische Sicherheitsmaßnahmen getroffen und die Mitarbeiter auf Datensicherheit in diesem Bereich sensibilisiert.**

- **Ein gewisses Restrisiko ist aber systemimmanent und kann nicht gänzlich ausgeschlossen werden. Durch die ständige Weiterentwicklung der Sicherheitssysteme und die intensive Schulung und Sensibilisierung der Anwender wird dem seitens der Verantwortlichen der Stadt entgegengewirkt.**

5.3 Datenschutzrichtlinie

In der Datenschutzrichtlinie der Stadt Villach sind neben den Bestimmungen zum Datenschutz auch Vorgehensweisen und Regelungen für die Einhaltung und Sicherstellung der Datensicherheit vorhanden.

Datenschutzrichtlinien sind wichtig, um die Vertraulichkeit und Integrität von personenbezogenen Daten zu gewährleisten. Diese Prüfung fokussierte sich jedoch auf den Aspekt der Datensicherheit.

Diese Richtlinien sollten diesbezüglich detailliert beschreiben, wie Daten gesammelt, verarbeitet, gespeichert und übertragen werden, um ein möglichst hohes Maß an Datensicherheit gewährleisten zu können. Sie müssen Maßnahmen zur Verhinderung von Datenlecks und unerlaubtem Zugriff enthalten, wie zum Beispiel die Verschlüsselung von Daten, regelmäßige Sicherheitsaudits und die Verwendung sicherer Netzwerkprotokolle.

Eine kontinuierliche Schulung der Mitarbeiter in Bezug auf diese Richtlinien ist unerlässlich, um das Bewusstsein und Verständnis für die Bedeutung der Datensicherheit (und des Datenschutzes) im Magistrat der Stadt Villach zu stärken.

Die Datenschutzrichtlinie der Stadt Villach behandelt grundsätzliche Verhaltensweisen bei der Verarbeitung von Daten.

- **Der Inhalt der Datenschutzrichtlinie muss den Bediensteten der Stadt nachweislich und wiederkehrend vermittelt werden.**

- **Sensibilisierung und Mystery-Mails[4] als Stresstest zum Datenschutz und zur Datensicherheit finden statt. Auch im Intranet können/müssen sich die Mitarbeiter nachweislich über den Knowledge-Checker zu diesem Thema „fit“ halten.**

[4] Mystery Mails sind Test-Emails, in denen ein beauftragter Tester (Mystery Shopper) eine typische Anfrage für ein vorgegebenes authentisches Szenario sendet und die Antwort gemäß objektiver Kriterien evaluiert.

6 Prüfungsergebnis und Maßnahmenempfehlungen

Zusammengefasst wurden vom StRH folgende Feststellungen getroffen und die dahingehend erforderlichen Maßnahmen empfohlen:

Prüfungsfeststellung	Maßnahme/Empfehlung	Wer	Wann
Serverräume Die bei der Stadt Villach im Einsatz befindlichen Serverräume erfüllen die geforderten Voraussetzungen. Bestehende Zugeständnisse und Kompromisse sind im Rahmen der Risikoabschätzung akzeptabel.	**Serverräume verbessern** Die im schriftlichen Konzept der Ausstattung für die Serverräume vorgelegten Handlungsalternativen werden bzgl. ihrer Umsetzung im Zuge der nächsten Follow-up-Prüfung betrachtet.	MD/IT	10/24
Archivierung / Skartierung Eine konkret definierte Vorgabe, wer, wann, welche Dokumente und Akten wie (physisch oder elektronisch) zu archivieren hat ist in der DA 6 geregelt.	**Büroordnung (DA 6) einhalten** Die Anwendung und Einhaltung der DA 6 ist von MD und Abteilungsleitungen zu kontrollieren und regelmäßig für deren stringente Umsetzung zu sorgen.	MD	laufend
Schließsysteme, Bürozutritte, Ordner und Akten Sperrsysteme sind eingerichtet und Regelungen für die Verwendung und Einhaltung sind vorhanden und werden technisch und organisatorisch schrittweise auf zeitgemäßen Stand gebracht.	**Periodische Schulung, Sensibilisierung, Kontrolle** Die Inhalte der relevanten Dienstanweisungen und Regelungen sind den Bediensteten der Stadt periodisch zu vermitteln und auf Einhaltung zu kontrollieren.	MD	10/24

Prüfungsfeststellung	Maßnahme/Empfehlung	Wer	Wann
Netzwerksicherheit Die Netzwerksicherheit ist durch verschiedene Maßnahmen und Routinen der MD/IT gewährleistet.	**Netzwerksicherheit gegeben** Absicherung des Systems und der Architektur ist in ausreichendem Maße gegeben.	-	erledigt
Postlauf, Büroordnung Die Büroordnung und das Vernichten/Entsorgen veralteter Dokumente ist in einer Dienstanweisung geregelt.	**Einhaltung kontrollieren** Im Rahmen der Compliance des Hauses ist die Einhaltung zur Regelungen der Büroorganisation, des (digitalen) Aktenlaufes und der Archivierung auf Einhaltung zu kontrollieren und die erforderlichen Maßnahmen zu setzen.	MD	10/24
Datensicherung und Wiederherstellung Mobile Datenträger sind für den Transport von Daten noch im Einsatz. Eine technische Absicherung fehlt derzeit. Backup und Sicherung der Daten erfolgt durch die Abteilung MD/IT. Eine Umstellung auf eine neue Technologie wird vorbereitet und in naher Zukunft umgesetzt.	**Datentransport über mobile Datenträger zentral sicherstellen, Passwortschutz, Verschlüsselung** Mobile Datenträger sind von den Usern mit Passwortschutz/Verschlüsselung zu versehen und gegen unberechtigten Zugriff zu sichern. MD/IT wird diesbezüglich eine technische Lösung umsetzen.	MD/IT	10/24

Prüfungsfeststellung	Maßnahme/Empfehlung	Wer	Wann
Datenhaltbarkeit Die Langlebigkeit verwendeter Daten ist durch die Verwendung offener Formate und eingerichteter Schnittstellen gegeben.	**Datenhaltbarkeit gegeben** Die Haltbarkeit und Verwendbarkeit des Datenbestandes ist über einen ausreichenden Zeitraum sichergestellt.	-	erledigt
Zugriffskontrolle und Benutzerverwaltung Eine entsprechende Dienstanweisung zur Regelung der IT-Zugriffe ist vorhanden.	**Regelmäßige Überprüfung und Anpassung der Dienstanweisungen** Dienstanweisungen sind (regelmäßig) routinemäßig einer Überprüfung nach Inhalt und Konnex zu parallelen Regelungen zu unterziehen. Gesetzliche und organisatorische Anpassungen sind erforderlichenfalls durchzuführen.	MD MD/IT	10/24
Telefonanlage Eine Datenschutzverletzung wurde bei einem Feature der verwendeten Software festgestellt.	**Anlage anforderungsgemäß optimieren und am Bedarf des Hauses ausrichten** Die Behebung der festgestellten Datenschutzverletzung ist bereits in Umsetzung. Der Komfort als Tool der jeweiligen Fachabteilung ist der fachlichen Anforderung kundenorientiert anzupassen.	MD/IT	10/24

Prüfungsfeststellung	Maßnahme/Empfehlung	Wer	Wann
Externer Datenverkehr Die Möglichkeit, Daten mit externen Sender/Empfängern auszutauschen, ist für die tägliche Arbeit des Magistrats obligat und alternativlos. Das dadurch entstehende systemimmanente Risiko ist daher risikoorientiert zu managen.	**Regelung externer Datenverkehr einhalten** Die Vorgaben zum externen Datenverkehr sind auf ihre Einhaltung weiter zu überwachen. Die Mitarbeiter sind diesbezüglich weiter zu sensibilisieren. Organisatorische Absicherungen des Risikos sind nach dem Stand der Technik vorzusehen.	MD MD/IT	10/24
Datenschutzrichtlinie In der Datenschutzrichtlinie der Stadt sind auch Aspekte zur Datensicherheit geregelt.	**Periodische Schulung zur Compliance im Datenschutz und im Datensicherheitsbereich** Die Inhalte der relevanten Dienstanweisungen sind den Bediensteten der Stadt periodisch zu vermitteln und auf Einhaltung zu überwachen.	MD	10/24

Eine Follow-Up-Prüfung zur gegenständlichen Thematik ist vom Stadtrechnungshof für das zweite Quartal 2025 vorgesehen.