

Weisungen ICT

vom 12.06.2019 (Stand am 12.06.2019)

Inhaltsverzeichnis

1. Allgemeine Grundsätze.....	3
Zweck	3
Zuständigkeiten	3
2. Informatikmittel.....	3
Allgemein	3
Zugangsschutz / Zugriffsschutz und Zugriffspflicht	3
Fremdanschlüsse und Fremdprogramme.....	4
Mobile Informatikmittel	4
Datensicherung	4
Einschränkungen Internetnutzung	4
E-Mail	4
3. Überwachung.....	5
Missbräuche.....	5
Persönlichkeitsrechte der Mitarbeitenden.....	5
Massnahmen	6
Weitere Bestimmungen.....	6
4. Schlussbestimmungen	6
Inkrafttreten	6
Anhang: Individuelle Bestimmungen der Gemeinde Münsingen	7
Zugangsschutz / Zugriffsschutz und Zugriffspflicht	7
Einschränkungen Internetnutzung	7
Drucker	7
Telefonie	7

Der Gemeinderat der Gemeinde Münsingen erlässt die folgenden Weisungen:

Zweck	<p>1. Allgemeine Grundsätze</p> <p>Art. 1</p> <p>¹ Diese Weisung definiert die Verwendung der Informatikmittel der Gemeinden des regionalen Informatikzentrums Münsingen (RIZ).</p> <p>² Mit dieser Weisung soll die Informationssicherheit (Datenschutz und Datensicherheit) gewährleistet, sowie die korrekte und wirtschaftliche Nutzung der Informatikmittel sichergestellt werden.</p> <p>³ Zur Sicherstellung des ordnungsgemässen Betriebs der Informatikmittel am Arbeitsplatz trifft die Gemeinde in erster Linie technische Massnahmen.</p>
Zuständigkeiten	<p>Art. 2</p> <p>¹ Der Gemeinderat Münsingen ist für die Festlegung der Weisungen ICT (Informations- und Kommunikationstechnologie) verantwortlich.</p> <p>² Weiterführende Vorgaben durch die Gemeinden können individuell im Anhang geregelt werden.</p> <p>³ Die Umsetzung der Weisungen sowie laufende Sensibilisierung und Information über den Inhalt obliegen dem Kader der Gemeinden und dem RIZ.</p>
Allgemein	<p>2. Informatikmittel</p> <p>Art. 3</p> <p>¹ Die Informatikmittel sind modern, zweckdienlich, auf die Aufgabenerfüllung beschränkt und zur Verwendung zu dienstlichen Zwecken bestimmt.</p> <p>² Die private Nutzung ist auf ein Minimum zu beschränken. Sie darf den Dienstbetrieb nicht beeinflussen und nicht für kommerzielle Zwecke verwendet werden. Missbräuchliche Nutzung wird sanktioniert.</p> <p>³ Für bewilligte besondere Arbeitsformen wie z.B. Homeoffice werden durch das RIZ keine zusätzlichen Installationen vor Ort vorgenommen.</p> <p>⁴ Über die Informatikmittel wird durch das RIZ ein Inventar geführt.</p>
Zugangsschutz / Zugriffsschutz und Zugriffspflicht	<p>Art. 4</p> <p>¹ Der Zugriffsschutz auf die Arbeitsstation kann mit einem allgemeinen Passwort geregelt werden.</p> <p>² Der Citrix-Zugriff muss immer mit einem persönlichen Passwort geschützt werden. Die Absätze 3 – 11 beziehen sich auf den Zugriffsschutz im Citrix.</p> <p>³ Die Benutzerinnen und Benutzer schützen die von ihnen verwendeten Informatikmittel vor unberechtigtem Zugriff und Gebrauch. Die Verantwortung (Missbräuche, Verletzung des Datenschutzes oder Datensicherheit) liegt bei der am Netzwerk angemeldeten Person.</p> <p>⁴ Alle Mitarbeitenden der Verwaltung kommunizieren über einen persönlichen Account, sofern sie diesen zur Ausführung ihrer Tätigkeiten benötigen.</p> <p>⁵ Passwörter sind persönlich und dürfen nicht weitergegeben werden. Die Verwendung von Abteilungspasswörtern ist nicht erlaubt.</p> <p>⁶ Passwörter müssen mindestens acht Stellen aufweisen und sollten aus Zahlen, Buchstaben (gross und klein) und Sonderzeichen zusammengesetzt werden. Nicht geeignet sind Namen, Vornamen, Geburtstage, Autokennziffern oder Einträge aus einem Wörterbuch.</p> <p>⁷ Passwörter dürfen nicht aufgeschrieben oder abgespeichert werden. Die Einstellung von automatisierten Logins ist nicht erlaubt.</p> <p>⁸ Ein regelmässiger Wechsel der Passwörter richtet sich nach den Vorgaben des RIZ.</p> <p>⁹ Beim Verlassen des Arbeitsplatzes sind die Computer gegen den Zugriff von nicht berechtigten Personen zu schützen (Aktivieren Passwortschutz / Ausschalten Gerät).</p> <p>¹⁰ Bevor der PC heruntergefahren wird, muss eine korrekte Abmeldung beim Citrix-Receiver erfolgen.</p>

¹¹ Externe Zugriffe auf geschäftliche Daten via Citrix-Netscaler benötigen eine Bewilligung der zuständigen Stellen der Gemeinden und werden beim RIZ registriert.

¹² Der Verlust von mobilen Geräten mit Datenabgleich ist unverzüglich dem RIZ zu melden.

Fremdanschlüsse
und Fremdpro-
gramme

Art. 5

¹ Das Einrichten und Anschliessen von fremden oder privaten Informatikmitteln an geschäftliche Informatikmittel ist vorgängig mit dem RIZ abzuklären.

² Installationen / Konfigurationen für private Zwecke (private Newsletters, Spiele, Chat usw.) sind nicht gestattet. Das RIZ übernimmt nur die Verantwortung, Wartung, Support und Wiederherstellung für die geschäftlichen Standardinstallationen.

Mobile Informatik-
mittel

Art. 6

¹ Mobile Informatikmittel (Notebooks, Mobile, Memory Sticks, CDs und DVDs usw.) sind besonders gefährdet durch Verlust oder Diebstahl. Deshalb ist der Zugriff mit Passwort zu schützen.

² Das Mitführen von Gemeindedaten auf externen Speichermedien ist auf ein Minimum zu beschränken. Nach Abschluss der Tätigkeit sind die Daten auf mobilen, physischen Datenträgern sofort zu löschen.

³ Daten aus externen Quellen (Memory Sticks, CD's usw.) werden vor der Nutzung mit einem aktuellen Virenschanner, welcher vom RIZ auf dem Gerät installiert ist, überprüft

⁴ Memory Sticks oder andere externe Datenträger unbekannter Herkunft oder als Werbegeschenke sind nicht zu verwenden.

Datensicherung

Art. 7

¹ Geschäftliche Daten sind immer auf einem Serverlaufwerk oder in der entsprechenden Geschäftsverwaltungssoftware (z.B. CMI AXIOMA, Nest, KLIB) zu speichern. Lokal gespeicherte Daten (C-Laufwerk) werden nicht gesichert. Im Falle eines HD-Defekts werden keine Bemühungen unternommen, die Daten zu sichern.

² Geschäftliche Bilder werden auf einer separaten Fotodatenbank gespeichert. Das Speichern von privatem Fotomaterial auf Serverlaufwerken ist nicht gestattet.

Einschränkungen In-
ternetnutzung

Art. 8

Aus Sicherheits- und Leistungsgründen dürfen folgende Dienste in Citrix nicht genutzt werden:

- Kostenpflichtige Internetseiten und Messenger-Programme
- Internet-Fernsehen
- Internetradio
- Videoportale (YouTube etc.)

E-Mail

Art. 9

¹ Für den gesamten geschäftlichen E-Mail Verkehr ist die gemeindeeigene, persönliche E-Mailadresse zu verwenden. Alle Mitarbeitende sowie wenn gewünscht alle Gemeinderäte erhalten eine persönliche E-Mailadresse.

² Die geschäftlichen E-Mail-Adressen dürfen nicht in öffentliche E-Mail-Register eingetragen werden. In Ausnahmefällen ist die Bewilligung des RIZ und der vorgesetzten Stelle einzuholen.

³ Aus Sicherheitsgründen darf die geschäftliche E-Mailadresse nur in Ausnahmefällen und unter Anleitung des RIZ auf eine externe (auch private) Adresse umgeleitet werden.

⁴ Wo immer möglich erfolgt die Korrespondenz elektronisch (unter Berücksichtigung der Datenschutzbestimmungen).

- ⁵ E-Mail-Anhänge (Dokumente, die einem E-Mail angehängt sind) unbekannter Herkunft oder Art sind sofort und ungeöffnet zu löschen. Bei Unklarheiten ist vor der Öffnung der Anhänge umgehend das RIZ zu kontaktieren.
- ⁶ Das E-Mailpostfach ersetzt keine Datenablage. E-Mails und Anhänge sind, sofern vorhanden, in der entsprechenden Geschäftsverwaltungssoftware (z.B. CMI AXIOMA, NEST, KLIB) oder im Explorer abzulegen.
- ⁷ Alle E-Mails inkl. private E-Mails werden mit einer zentralen E-Mailarchivierung alle zwei Stunden archiviert.
- ⁸ E-Mails und Anhänge sind von den Benutzern periodisch aus den Postfächern zu löschen, da diese viel Speicherplatz beanspruchen und weiterhin im E-Mailarchiv zur Verfügung stehen.

3. Überwachung

Art. 10

Missbräuchlich ist jede Verwendung der Informatikmittel, welche gegen Weisungen verstösst, Bestimmungen der Rechtsordnung oder Rechte von Dritten verletzt. Unter missbräuchliche Nutzung der Informatikmittel fallen insbesondere:

- Nutzung zu kommerziellen Zwecken
- Das Abrufen, Herunterladen, Bearbeiten, Speichern, zur Verfügung stellen oder Versenden von Dokumenten und Daten, die gegen geltendes Gesetz verstossen. Dies gilt insbesondere für Seiten, die gegen die Menschenwürde verstossen, die pornografischen, rassistischen Inhalt haben oder zu Gewalt/Gewaltverherrlichung aufrufen (Grundlagen: Strafgesetzbuch Art. 173, 197 und 261)
- Wiederrechtliches Kopieren von Daten und Software
- Erstellen oder bewusstes/unsorgfältiges/fahrlässiges Verbreiten von computerschädigenden E-Mails und Anwendungen
- Belästigungen anderer Personen mit elektronischen Hilfsmitteln
- Manipulation von gemeindeeigenen Informatikmitteln
- Unbefugtes oder versuchtes Eindringen in andere Computersysteme (Hacking)
- Ausspionieren von Passwörtern
- Störung des Betriebes von Computern und Netzwerken
- Verwenden von vorgetäuschten IP-Adressen
- Generell das Tätigen von persönlichen Meinungsäusserungen, die dem Ansehen der Gemeinde und dem Personal schaden können (z.B. auf Kontaktseiten, in sogenannten News-Groups, Chat-Foren etc.)

Art. 11

- ¹ Die Gemeinde wahrt die Privatsphäre ihrer Mitarbeitenden am Arbeitsplatz.
- ² Sämtliche Verkehrs- und Logdaten dürfen jedoch vollautomatisch aufgezeichnet und anonymisiert zu statistischen Zwecken ausgewertet werden. Diese Daten (unter anderem gewählte Telefonnummern, Protokolle des Internetzugangs und E-Mail-Verkehrs oder das Volumen der transportierten Daten) halten fest, wann welche Verbindungen hergestellt wurden.
- ³ Die aufgezeichneten Daten können sowohl bei technischen Problemen im Firmen-Netzwerk als auch bei begründetem Verdacht auf Missbrauch detailliert ausgewertet werden.
- ⁴ Ein Missbrauch liegt vor, wenn die vorliegende Weisung nachweislich verletzt worden ist.
- ⁵ Wird ein Missbrauch festgestellt, entscheidet der Gemeinderat über eine personenbezogene Auswertung. Vor Durchführung der Auswertung ist das Personal über den festgestellten Missbrauch und die folgende Datenauswertung zu orientieren.
- ⁶ Die Auswertung selbst wird von einer durch den Gemeinderat bestimmten Fachperson durchgeführt. Die Auswertung untersteht der strikten Schweigepflicht; in Verdacht stehende Personen werden in das Verfahren einbezogen.

Missbräuche

Persönlichkeitsrechte der Mitarbeitenden

Massnahmen

Art. 12

Stellt die vorgesetzte Stelle oder das RIZ Verfehlungen fest, können folgende Massnahmen und Sanktionen gegen die fehlbaren Mitarbeitenden durch die jeweilige Gemeinde eingeleitet werden

- Sperren oder Einschränken des Zugangs zu Informatikmitteln
- Löschen von missbräuchlich heruntergeladene Dateien
- Zurücksetzen des Gerätes in den Originalzustand
- Sperren von Webseiten
- Belastung der missbräuchlich verwendeten Arbeitszeit
- Personalrechtliche Sanktionen
- Strafverfolgung und/oder Geltendmachung zivilrechtlicher Ansprüche bleiben vorbehalten (z.B. Schadenersatz für grobfahrlässige oder mutwilligen Beschädigung)

Weitere
Bestimmungen

Art. 13

Gemeindespezifische Bestimmungen sind im Anhang geregelt.

Inkrafttreten

4. Schlussbestimmungen

Art. 14

¹ Die Inkraftsetzung der Weisungen ICT erfolgt auf den 12.06.2019.

² Mit Inkrafttreten wird die ICT-Weisung vom 30.01.2007 aufgehoben.



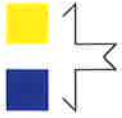
Beat Moser
Präsident



Thomas Krebs
Sekretär

Anhang: Individuelle Bestimmungen der Gemeinde Münsingen

Zugangsschutz / Zugriffsschutz und Zugriffspflicht	Art. 1 Mobile Datenabgleiche sowie webbasierte Outlookzugriffe benötigen eine Bewilligung durch die Abteilungsleitung und werden beim RIZ registriert.
Einschränkungen Internetnutzung	Art. 2 ¹ Aus Leistungsgründen dürfen folgende Dienste im lokalen Internetexplorer nicht zu privaten Zwecken genutzt werden: <ul style="list-style-type: none">• Kostspflichtige Internetseiten und Messenger-Programme• Internet-Fernsehen• Internetradio• Videoportale (YouTube etc.) ² Nicht gestattet während der Arbeitszeit ist die private Inanspruchnahme von folgenden Webseiten / Diensten: <ul style="list-style-type: none">• Soziale Medien (Facebook, Twitter, Snapchat, Instagram, Whatsapp, usw.)• E-Banking• Ticket- oder Reisebuchungen (z.B. Ticketcorner, Starticket)• Webshops• Dropbox
Drucker	Art. 3 Grundsätzlich wird nur über Multifunktionsgeräte gedruckt. Alle Multifunktionsgeräte sind standardmässig s/w doppelseitig eingestellt.
Telefonie	Art. 4 ¹ Die Kommunikationsmittel sind modern, zweckdienlich, auf die Aufgabenerfüllung beschränkt und zur Verwendung zu dienstlichen Zwecken bestimmt. ² Die private Nutzung ist auf ein Minimum zu beschränken. Sie darf den Dienstbetrieb nicht beeinflussen und nicht für kommerzielle Zwecke verwendet werden. Missbräuchliche Nutzung wird sanktioniert. ³ Die Telefongeräte befinden sich aus Sicherheitsgründen bei den Mitarbeitenden (wichtig wegen Alarmierung). ⁴ Bei Abwesenheiten wird entweder auf die eigene Voicemail oder andere Mitarbeitende umgeleitet. Bei einem Anruf in Abwesenheit erfolgt nach Rückkehr des Mitarbeitenden ein Rückruf. Bei Homeoffice wird das Telefon auf das Mobile umgeleitet. ⁵ Während der Arbeitszeit werden die internen und externen Kunden, welche über die direkte Nummer eingehen, auch ausserhalb der Schalteröffnungszeiten bedient. ⁶ Die Benützung von 0900-Nummern ist grundsätzlich erlaubt, mit folgenden Ausnahmen: <ul style="list-style-type: none">• Erotikbranche• Esoterik und Wahrsagerei ⁷ Bei Gefahr oder Bedrohung wird ein Personalarm über das Telefongerät ausgelöst. Detaillierte Infos über die Möglichkeiten der Telefonie sowie der Alarmierung können unter M:\Public\05 PRA\Telefonie nachgelesen werden.



Weisungen ICT der Gemeinde Münsingen

Anhang: individuelle Bestimmungen der Gemeinde Frauenkappelen

1. IT-Sicherheitsverantwortliche Person

IT-Sicherheitsverantwortliche Person ist die Gemeindeschreiberin.

2. Rollen und Rechte

Diese sind in der Beilage zu diesem Dokument geregelt.

3. Synchronisation mit persönlichen mobilen Geräten

Die Synchronisation von Kalenderdaten, Kontakten und Aufgaben ist intern und extern erlaubt. Das Gesuch für die Synchronisation von E-Mails wird durch den direkten Vorgesetzten beurteilt.

4. Nutzung von privaten Geräten (u.a. im HomeOffice)

Werden private Geräte für den Zugriff auf das Netz der Gemeinde genutzt, erfolgt dieser Zugriff über eine Zweifach-Authentifizierung via SMS. Für die Freigabe von Zahlungsläufen dürfen private Geräte nicht genutzt werden.

5. Telefonie

Die Kommunikationsmittel sind modern, zweckdienlich, auf die Aufgabenerfüllung beschränkt und zur Verwendung zu dienstlichen Zwecken bestimmt. Die private Nutzung ist auf ein Minimum zu beschränken.

Während der Arbeitszeit werden die internen und externen Kunden, welche über die direkte Nummer eingehen, auch ausserhalb der Schalteröffnungszeiten bedient.

In Bezug auf die Mobiltelefonie ist die separate Dienstanweisung zu berücksichtigen.

6. Inkrafttreten

Diese Dienstanweisung tritt per 1. Juni 2021 in Kraft. Sie ersetzt die Dienstanweisung «IT-Sicherheit» vom 16. August 2018.

Genehmigt durch den Gemeinderat in seiner Sitzung vom 17. Juni 2021.

Einwohnergemeinde Frauenkappelen
Namens des Gemeinderates

M. Wyttenbach, Präsident

R. Hämmerli, Gemeindeschreiberin

Ich bestätige, die Weisungen ICT der Gemeinde Münsingen und den vorliegenden Anhang gelesen zu haben und verpflichte mich, diese einzuhalten.

Vorname _____ Name _____

Datum _____ Unterschrift _____

**Dienstweisung IT-Sicherheit
Rollen und Rechte**

Rolle	Rechte									
	CITRIX-Zugang	Abacus	NEST ISE	CMIAXIOMA Office	IS-NESKO	GRUDIS	AIB	CMIAXIOMA Mobile Clients	OWA (Zugriff via Internet)	
Gemeindeschreiber	X	X	X	X	nur Abfrage	nur Abfrage	X	X		
Finanzvewalter	X	X	nur Abfrage	X	X	X	X	X		
Leiter Infrastruktur	X	X	X	X			X	X		
Leiter AHV-Zweigstelle	X	nur Abfrage	X	X			X	X		
Mitarbeiter Sekretariat	X	X	X	X			X	X		
Lernender	X	X	X	X			X	X		
Schulleiter	X	nur Abfrage	nur Abfrage	X						
Lehrpersonen	X			X					X	
Leiter Werkhof	X			X					X	
Mitarbeiter Werkhof	X			X					X	
Hauswart	X			X					X	
Mitarbeiter Reinigung										
Praktikant Werkhof										
Gemeindepräsident								X	X	
Mitglied Gemeinderat								X	X	
Mitglied BVK								X	X	
Mitglied KPSK								X	X	
externe Bauverwalter	X			X						



Finances Publiques
AG für öffentliche Finanzen und Organisation

Einwohnergemeinde Frauenkappelen

Erläuterungsbericht
des Rechnungsprüfungsorgans
zur Prüfung der Jahresrechnung 2020

Frauenkappelen, 28. April 2021

Einleitung

Als Rechnungsprüfungsorgan der Gemeinde Frauenkappelen führte die Finances Publiques AG die Prüfung der Jahresrechnung durch. Als leitender Revisor amtierte Heinz Berger, dipl. Betriebsökonom FH und Geschäftsführer der Finances Publiques AG mit Sitz in Bowil. An der Schlussrevision wirkte zusätzlich mit: Monika Rüttimann, dipl. Finanzverwalterin. Die Schlussrevision sowie die Schlussbesprechung fanden am 28. April 2021 statt.

Die Zwischenrevision wurde durch Jacqueline Rupf, dipl. Finanzverwalterin, am 4.12.2020 durchgeführt.

Im Rahmen der obligatorischen Prüfungshandlungen haben wir auf der Basis der Arbeitshilfe für Rechnungsprüfungsorgane (Ausgabe 2016) insbesondere geprüft:

- Allgemeine Prüfungsfragen
- Bilanz und Verkehrsprüfungen
- Anhänge
- Erfolgsrechnung
- Investitionsrechnung

Im Rahmen der Revision haben wir Schwerpunkte gesetzt mit:

- 1 Allgemeine Prüfungsfragen, obligatorische Prüfungsfragen
Weitere Prüfungshandlungen: Allgemeine Organisationsfragen
Weitere Prüfungshandlungen: Mehrwertsteuer
Weitere Prüfungshandlungen: Versicherungen
Weitere Prüfungshandlungen: Datensicherheit in der Informatik
- 2 Flüssige Mittel und kurzfristige Geldanlagen
- 3 Forderungen
- 4 Kurzfristige Finanzanlagen
- 28 Anhang
- R Risikoprüfung Weitere: Internes Kontrollsystem

Allgemeiner Eindruck

Die Verwaltungsführung der Gemeinde Frauenkappelen wurde im Rahmen der Rechnungsprüfung als in Ordnung befunden. Wir bedanken uns für die gute Zusammenarbeit während der Rechnungsprüfung. Wir erhielten umfassenden Einblick in alle Akten und konnten uns dadurch ein gutes Bild von den Vorgängen in der Gemeinde Frauenkappelen machen.

Naturgemäss werden bei einer Rechnungsprüfung auch Bemerkungen und Anregungen gemacht, wenn **(mit Ausnahme der Zugangsberechtigungen Zahlungsverkehr) keine wesentlichen Mängel** vorliegen. Diese Bemerkungen und Anregungen betreffen Geschäftsvorfälle oder Verwaltungsabläufe, die verbesserungsfähig sind und sollen als präventive Massnahme die einwandfreie Verwaltungsführung über lange Zeit ermöglichen.
Die Bemerkungen und Anregungen sollen in keiner Weise das sehr positive Bild der Verwaltungsführung mindern.

Berichterstattung




Den Bericht des Rechnungsprüfungsorgans zur Jahresrechnung können wir im Normwortlaut abgeben und beantragen Genehmigung der Jahresrechnung.

Wir erstatten sechsstufig Bericht:

1. Den öffentlichen **Bericht des Rechnungsprüfungsorgans zur Jahresrechnung** des Rechnungsprüfungsorgans zuhanden der Gemeindeversammlung können wir im Normwortlaut abgeben, mit Antrag an die Versammlung zur Genehmigung der Jahresrechnung. Wir empfehlen Ihnen, den Antrag des Rechnungsprüfungsorgans an der Versammlung zu verlesen und den Bericht des Rechnungsprüfungsorgans zur Jahresrechnung in die Jahresrechnung einzubinden.
2. Den öffentlichen **Jahresbericht der Datenschutzaufsichtsstelle** können wir ohne Einschränkungen abgeben.
3. Dieser interne **Erläuterungsbericht** zuhanden des Gemeinderates dient der Darstellung von wesentlichen Revisionsbemerkungen. Wir empfehlen Ihnen, den Erläuterungsbericht an einer Sitzung zu behandeln und über die Revisionsbemerkungen zu befinden. **Zur eindeutigen Dokumentation der Beschlüsse empfehlen wir Ihnen, zu jedem Punkt des Erläuterungsberichts einen Beschluss des Gemeinderates zu fassen und zu protokollieren.**
4. Zusätzlich geben wir dem Finanzverwalter eine Zusammenstellung mit **Detailbemerkungen** ab, zur direkten Erledigung. Wir empfehlen, diese Bemerkungen aufzuarbeiten und an der nächsten Revision zu besprechen.
5. Ab Einführung des HRM2 ist ein internes **Protokoll über die Schlussbesprechung** zu führen. Zusätzlich ist die Mehrjahresplanung mit der Körperschaft abzusprechen.
6. Exekutive und Rechnungsprüfungsorgan haben gegenüber dem Amt für Gemeinden und Raumordnung des Kantons Bern die **Bescheinigung über die Jahresrechnung** abzugeben. Diese Bescheinigung wird von der Finanzverwaltung internetbasiert erstellt und von Gemeinde und Rechnungsprüfungsorgan unterschrieben. Sie ist dem Kanton bis spätestens 30. Juli einzureichen.







Im Erläuterungsbericht als Rechnungsprüfungsorgan unterscheiden wir zwischen gravierenden Mängeln, wesentlichen Mängeln und keinen / kleinen Mängeln in der Rechnungslegung.

Die Legende zum Erläuterungsbericht:

	<p>Gravierende Mängel.</p> <p>Das Revisionsergebnis zeigt (einzeln oder kumuliert) grossen Handlungsbedarf oder wesentliche Fehler oder grossen Zeitdruck.</p>
	<p>Wesentliche Mängel.</p> <p>Es können sich Fehler kumulieren, es besteht ein planbarer Handlungsbedarf innerhalb einer zu definierenden Zeit.</p>
	<p>Keine Mängel oder kleine Mängel.</p> <p>Der Gemeinderat nimmt vom Prüfungsergebnis Kenntnis, allenfalls kann er punktuell verbessern. Es bestehen kleinere Mängel, die gelegentlich zu beseitigen sind.</p>





Revisionsbemerkungen zuhanden des Gemeinderates

In einer Tabelle zusammengefasst haben wir folgende Revisionsbemerkungen zuhanden des Gemeinderates:

Jahr und Revisionsbemerkung	Status 28.04.2021	Bewertung Finances Publiques
Bemerkungen aus den Vorjahren		
2018.01. Internes Kontrollsystem implementieren.	Erledigt	
2019.01. Bestätigung Geschäftsbeziehungen mit Banken	Erledigt	
2019.02. Vertiefte Kontrolle AGR	Erledigt	
2019.03. Neubewertungsreserve	Erledigt	
2019.04. Auswertungen zur Jahresrechnung	Erledigt	
2019.05. Einlagen in Werterhalt	Erledigt	
Bemerkungen zur Jahresrechnung 2020		
2020.01 Zugangsberechtigungen Zahlungsverkehr		
2020.02 Steuerteilungen, Rückstellungen		
2020.03 Konzessionsabgabe BKW		
2020.04 Datenschutz und Datensicherheit		

1. Bemerkungen aus dem letztjährigen Revisionsbericht

Die Revisionsbemerkungen aus den Vorjahren wurden erledigt und wir gratulieren zu diesem Ergebnis.

Bemerkungen zur Jahresrechnung 2020		
2020.01 Zugangsberechtigungen Zahlungsverkehr		
2020.02 Steuerteilungen, Rückstellungen		
2020.03 Konzessionsabgabe BKW		
2020.04 Datenschutz und Datensicherheit		

2. Bemerkungen zur Jahresrechnung 2020

2020.01 Zugangsberechtigungen Zahlungsverkehr

Am Revisionstag 28.4.2021 fanden wir im Tresor der Gemeindeverwaltung zwei Couverts mit den Zugangsberechtigungen im Zahlungsverkehr vor. Alle drei Sicherheitselemente waren in den beiden Couverts zweier Mitarbeiterinnen enthalten.

Somit hätte jemand unter anderem Namen im E-Banking mit einer Zugangsberechtigung Zahlungen erfassen und mit der anderen Zugangsberechtigung Zahlungen freigeben können. Das ist nicht zulässig und unbedingt zu vermeiden.

Wir haben das den beiden Mitarbeiterinnen gezeigt und sie werden sofort (bzw. wegen Corona-Abwesenheit morgen) die Zugangsberechtigungen separieren und die Passwörter ändern. Wir erwarten je eine Vollzugsmeldung per Mail an info@fpag.ch mit Kopie an den Ressortchef des Gemeinderates.

2020.02 Steuerteilungen, Rückstellungen

Die Bilanz der Gemeinde Frauenkappelen enthält keine Rückstellungen für Steuerteilungen. Der Steuerertrag im 2020 war extrem viel höher als erwartet und eine Durchsicht der Steuerstatistik und Auswertungen der Steuerunterlagen zeigt, dass Steuerteilungen mit anderen Gemeinden zu erwarten sind.

Wir empfehlen dem Gemeinderat, vor dem Abschluss der Jahresrechnung 2021 die Bildung von Rückstellungen für Steuerteilungen zu prüfen.

2020.03 Konzessionsabgabe BKW

Die Konzessionsabgabe von bisher CHF 55'839.--/Jahr steht in Frauenkappelen zur Diskussion, anstelle eines Reglements über die Konzessionsabgabe. Die finanzielle Situation lässt dies zu, es ist aber kreditrechtlich zu prüfen, wer für diesen Einnahmenverzicht zuständig ist.

Der Verzicht auf Einnahmen wird gemäss Artikel 100 der kantonalen Gemeindeverordnung für die Bestimmung der Zuständigkeit den Ausgaben gleichgestellt.

Art. 100 Ausgaben

¹ Ausgaben sind geld- und buchmässige Vorfälle, die der Erfolgs- oder Investitionsrechnung belastet werden. Sie dienen der Erfüllung öffentlicher Aufgaben. *

² Zur Bestimmung der Zuständigkeit werden den Ausgaben gleichgestellt:

- a * Gewährung von Darlehen mit Ausnahme von Anlagen des Finanzvermögens,
- b Bürgschaftsverpflichtungen und andere Sicherheitsleistungen,
- c * Beteiligung an juristischen Personen des Privatrechts mit Ausnahme von Anlagen des Finanzvermögens,
- d Rechtsgeschäfte über Eigentum und beschränkte dingliche Rechte an Grundstücken,
- e * Finanzanlagen in Immobilien,
- f Anhebung oder Beilegung von Prozessen oder deren Übertragung an ein Schiedsgericht,
- g die Entwidmung von Verwaltungsvermögen und
- h der **Verzicht** auf Einnahmen.

Im Organisationsreglement der Einwohnergemeinde Frauenkappelen ist diese kantonale Norm nicht anderweitig geregelt, somit gilt die kantonale Norm. Laut Artikel 4 und 5 des Organisationsreglements beträgt die Ausgabenbefugnis des Gemeinderates CHF 80'000 und für wiederkehrende Ausgaben (oder wie hier vorliegend Einnahmen) 1/10. davon.

Wir empfehlen dem Gemeinderat, vor einer Entscheidung über die Konzessionsabgabe die Zuständigkeit zu klären.

2020.04 Datenschutz und Datensicherheit

Wie überall in bernischen Gemeinden wurde Home-Office praktiziert. Teilweise wurden private Geräte eingesetzt und der Datenschutz und die Datensicherheit können dadurch beeinträchtigt werden.

Auf den Gemeindeggeräten ist das Virenschutzprogramm Trend Micro installiert und dieses war heute in Stichproben aktualisiert. Die Gemeinde nutzt das Rechenzentrum RIZ in Münsingen; gestern fand eine Weiterbildungsveranstaltung statt und die Zweifaktor-Authentifizierung für Geräte im Home-Office soll durch das Rechenzentrum bis Juni 2021 eingeführt werden. Dadurch wird die Sicherheit wesentlich erhöht.

Wir empfehlen dem Gemeinderat, gemeinsam mit dem Rechenzentrumsanbieter die beste Lösung für Frauenkappelen zu Datenschutz und Datensicherheit im Home-Office zu erarbeiten.

Prüfungsausblick für die nächste Revision

Die Mehrjahresplanung über die Revisionstätigkeit wurde an der Schlussbesprechung vom 28. April 2021 gemäss separatem Protokoll besprochen und als zielführend befunden.

Für die **Schlussrevision** der Jahresrechnung 2021 schlagen wir vor:

Mittwoch, 27. April 2022, 08.00 – 17.00 Uhr,
Schlussbesprechung mit Gemeinderatsdelegation und Verwaltungskader 17.00 – 18.00 Uhr.

Wir gratulieren zur Rechnungslegung 2020 und danken für die sehr gute Zusammenarbeit.

Das Rechnungsprüfungsorgan:

Frauenkappelen, 28. April 2021 Finances Publiques AG

Heinz Berger
Dipl. Betriebsökonom FH
Leitender Revisor

Monika Rüttimann
Dipl. Finanzverwalterin
Revisorin

Bemerkungen zuhanden Verwaltung

Kennzahlen. Die Kommentierung der Kennzahlen in der Jahresrechnung inklusive Mehrjahresvergleich ist vorbildlich und wir gratulieren aus Sicht Revision dazu.

Anschlussgebühren. Bei der nächsten Revision behandeln wir die Anschlussgebühren Wasser und Abwasser. Bitte halten Sie die Baubewilligungskontrolle der Jahre 2019 und 2020 in Listenform Papier oder Excel vor, sowie einen Uebersichtsplan der Ueberbauung mit Angabe der Grundeigentümer, damit wir ausgehend von Liste und Plan die Vollständigkeit und Richtigkeit der Anschlussgebührenrechnungen prüfen können.

Subventionskontrolle. Eine systematische schriftliche Subventionskontrolle besteht nicht. Bitte

Schlüsseldepot. Laut Bilanz besteht ein Schlüsseldepot von CHF 5'300.--. Bitte per 31.12.2021 den Bestandesnachweis erbringen.

Vorbericht, Folgebewertung. Das Kapitel Folgebewertung fehlt im Vorbericht, siehe auch vertiefte Prüfung AGR vom 31.7.2019. Bitte in den Folgejahren ergänzen.

Aebischenstrasse, Durchlauf und Kredit. Die buchhalterische Abwicklung über die Gemeinde, falls sich die Privaten nicht bereiterklären, den Zahlungsverkehr zu übernehmen, ist dann revisionstechnisch über ein Durchlaufkonto unbedenklich, wenn ein schriftlicher Vertrag besteht und die Privaten mit Akontozahlungen vorfinanzieren. In der Verpflichtungskreditkontrolle ist ein alter Kredit von 50'000 Franken mit ähnlicher Bezeichnung und bisher noch nicht verwendet vorhanden. Bitte überprüfen, ob ein Zusammenhang besteht.

Hangrutsch. Wie besprochen hat die Abteilung Naturgefahren des Kantons Bern grosse Erfahrung in solchen Schadenfällen, inklusive Organisation und Finanzierung.

Kontierung. Konto 10717.01 Darlehen Genossenschaft Dorfladen. Bitte überprüfen, ob nicht eher 10710.xx

Herzliche Gratulation zur Rechnungslegung und vielen Dank für die sehr angenehme Zusammenarbeit!

Frauenkappelen, 28.4.2021

Heinz Berger, Monika Rüttimann

Amt für Informatik
und Organisation
Wildhainweg 9
3001 Bern

19. Dezember 2019

Kontaktstelle:

Stephanie Bucher, Recht KAIO
Tel.: 031 636 83 21
E-Mail: stephanie.bucher@be.ch

Geht an:

- Einwohner- und gemischte Gemeinden
- Regierungsstatthalterämter
- Kirchgemeinden
- Bürgergemeinden
- Diverse Abonnenten

Information

Inkrafttreten der neuen Randdatenverordnung (RDV) als Ausführungserlass zum revidierten Personalgesetz (PG)

1. Ausgangslage

Wenn die Mitarbeiterinnen und Mitarbeiter des Kantons Bern sich an ihrem Arbeitsplatz einloggen, die Eingangstüren mittels Schliesssystem öffnen oder einen Anruf über die Anwendung Skype tätigen, dann werden die dadurch entstehenden Daten, die so genannten Randdaten, in der Regel aufgezeichnet. Doch was genau geschieht mit diesen Randdaten? Die Antwort darauf liefert die neue Randdatenverordnung. Sie regelt den Umgang mit Personendaten, die Informationen über die Nutzung der elektronischen Infrastruktur enthalten.



Für die Gemeinden gilt die Randdatenverordnung auch, wenn sie das kantonale Personalrecht anwenden. Die Randdatenverordnung gilt auch für Randdaten von Personen, die nicht Staatsangestellte sind (Art. 48d OrG¹).

2. Inhalt der neuen Randdatenverordnung

Die Randdatenverordnung führt die Bestimmungen des per 1. Januar 2020 revidierten Personalgesetzes² näher aus. Sie enthält Regelungen zu den Zuständigkeiten, die konkreten technischen Belange der Datenbearbeitung und die Aufbewahrungsfristen für die jeweiligen Randdaten. Weiter regelt die Verordnung die Voraussetzungen und die Zuständigkeiten der Aufbewahrung, Auswertung und Vernichtung der Daten. Damit wird eine ausdrückliche rechtliche Grundlage für eine bereits heute bei der täglichen Arbeit der Verwaltung stattfindende Datenbearbeitung geschaffen.

Die Randdatenverordnung schützt die betroffenen Personen vor einer unzulässigen Bearbeitung der Randdaten. Eine Aufzeichnung und Auswertung der Randdaten ist nur zulässig, wenn das Personalgesetz diese ausdrücklich vorsieht. Die Verordnung bietet denn auch keine gesetzliche Grundlage für Verhaltensüberwachungen wie Live-Überwachungen oder Software, mit welcher PC-Arbeitsplätze ausspioniert werden können (Spyware). Weiter lässt die Verordnung sogenannte «Rasterfahndungen» nicht zu, bei denen ein grosser Personenkreis auf bestimmte Daten und Merkmale hin überprüft wird. Sie bestimmt ausschliesslich die Modalitäten der bereits auf Gesetzesebene festgelegten Grundzüge für die Bearbeitung von Randdaten.

Die Verordnung tritt per 1. Januar 2020 in Kraft. Weitere Informationen zum Umgang mit den Vorgaben finden Sie im beiliegenden Merkblatt.

¹ Gesetz über die Organisation des Regierungsrates und der Verwaltung (Organisationsgesetz, OrG; BSG 152.01, Fassung in Kraft ab 1.1.2020)

² Personalgesetz (PG; BSG 153.01)

3. Auftrag an die Adressaten

Bitte leiten Sie diese Erlasse sowie die Informationen zur neuen Randdatenverordnung an Ihre ICT-Verantwortlichen weiter. Diese müssen sicherstellen, dass auch die externen Betreiber der elektronischen Infrastruktur sowie sonstige Lieferanten diese Vorschriften umsetzen.

Für Fragen zur neuen Verordnung sowie deren Umsetzung wenden Sie sich bitte an den Rechtsdienst des KAIO unter Tel. 031 636 83 21 oder per E-Mail an stephanie.bucher@be.ch.

Amt für Informatik und Organisation

Randdatenverordnung (RDV) Merkblatt für ICT-Verantwortliche

Inkrafttreten der neuen Randdatenverordnung

Am 1. Januar 2020 tritt im Kanton Bern die neue Randdatenverordnung (RDV) in Kraft. Sie ist ein Ausführungserlass des revidierten Personalgesetzes (PG; BSG 153.01) und behandelt den Umgang mit Personendaten, welche bei der Nutzung der elektronischen Infrastruktur entstehen.

Zweck dieses Merkblattes ist es, insbesondere den ICT-Verantwortlichen einige der Auswirkungen der Verordnung aufzuzeigen. Selbstverständlich ist es jedoch weiterhin notwendig, das PG und die RDV zu lesen und für weitergehende Informationen den Vortrag zum PG und zur RDV zu konsultieren.

Als ICT-Verantwortliche sind Sie die Kontaktstelle zu externen Betreibern und sonstigen Lieferanten. Stellen Sie sicher, dass diese über die vorliegenden Vorgaben informiert sind und diese entsprechend umsetzen.

Für Fragen oder sonstige Auskünfte zur neuen Verordnung wenden Sie sich bitte an den Rechtsdienst des KAIO unter Tel. 031 636 83 21 oder per E-Mail an stephanie.bucher@be.ch.

ICT-Systeme, die die Umsetzung der RDV nicht erlauben, müssen bis am 1.1.2025 angepasst werden (Art. 17 RDV).



1 Grundsätzliches

Personendaten, d.h. Daten, die Angaben über eine bestimmte oder bestimmbare Person enthalten, die bei der Nutzung der elektronischen Infrastruktur durch Mitarbeiterinnen und Mitarbeiter des Kantons (also bspw. bei der Nutzung des KWP, Skype, Drucker etc.) anfallen, dürfen nur zu bestimmten Zwecken aufgezeichnet und ausgewertet und nur während einer gewissen Dauer aufbewahrt werden.

Die RDV gilt auch für Daten von Drittnutzern der elektronischen Infrastruktur der kantonalen Verwaltung und der im Auftrag des Kantons betriebenen elektronischen Infrastruktur. Sie gilt demnach beispielsweise auch für Daten von Besuchern von kantonalen Websites.

Spezialgesetzliche Vorschriften, welche die Bearbeitung der bei der Nutzung der elektronischen Infrastruktur anfallenden Personendaten zum Gegenstand haben, gehen den Bestimmungen der RDV vor. Klären Sie vorgängig mit dem Rechtsdienst Ihrer Behörde ab, ob solche Bestimmungen bestehen.

2 Aufzeichnung

Personendaten dürfen aufgezeichnet werden, wenn die Aufzeichnung einem bestimmten Zweck dient. Die Zwecke sind abschliessend in Artikel 12c PG genannt. Damit diese Zweckbindung sichergestellt werden kann, sind externe ICT-Leistungserbringer entsprechend auf diesen Punkt hin zu überprüfen und entsprechend zu instruieren.

Da die Unterscheidung zwischen Personendaten und übrigen Daten, gerade bei grossen Datensätzen, sehr schwierig bis gar unmöglich ist, wird empfohlen, die Regelungen der Verordnung auf alle Arten der Daten anzuwenden oder jedenfalls dort, wo nicht ausgeschlossen werden kann, dass in einem Datensatz Personendaten enthalten sind.

3 Zugriff

Unter anderem für die Regelung der Zugriffsberechtigung (Art. 2 RDV) unterscheidet die Verordnung zwischen bewirtschafteten und nicht bewirtschafteten Daten (Art. 1 Abs. 1 Bst. a und b RDV).

Die Behörde, welche zur Erfüllung einer gesetzlichen Aufgabe Personendaten bearbeitet oder bearbeiten lässt, bleibt stets für die Datenbearbeitung verantwortlich. Dies gilt auch, wenn sie Dritte mit der Datenbearbeitung beauftragt.

4 Aufbewahrung und Vernichtung

Randdaten sind sicher (Art. 3 RDV) und nur während einer gewissen Dauer, die sich nach dem Zweck der Aufzeichnung richtet (Art. 4 Abs. 1 und 2 RDV), aufzubewahren. Es muss sichergestellt werden, dass alle Stellen, welche Daten aufbewahren, also auch externe Betreiber der Infrastruktur, die vorgegebenen Fristen einhalten. Die Fristen sind Maximalfristen. Wenn eine Aufbewahrung während dieser Dauer unverhältnismässig ist, müssen die Daten vorher vernichtet werden.

Bei nicht bewirtschafteten Daten sollte die Vernichtung idealerweise bereits durch das Gerät selbst erfolgen, d.h. beispielsweise durch ein automatisches Überschreiben der Daten. Spätestens mit der Weitergabe oder Entsorgung des Geräts müssen die Randdaten unwiederbringlich vernichtet werden (Art. 5 RDV).

5 Auswertung

Die Voraussetzungen für die Auswertungen von Randdaten sind in den Artikeln 12d PG und 8 bis 13 RDV geregelt. Diese Bestimmungen müssen in jedem Fall eingehalten werden. Ausserdem sind die Vorschriften über das Auswertungsergebnis zu berücksichtigen (Art. 15 und 16 RDV).

Nach Erhalt einer Anfrage bezüglich Auswertung von Randdaten wird empfohlen, vor einer allfälligen Auswertung insbesondere folgende Prüfpunkte zu berücksichtigen:

1. Dürfen die jeweilige Behörde oder der Dritte die Daten auswerten oder auswerten lassen?
2. Wurden die Randdaten dem jeweiligen Zweck entsprechend aufgezeichnet?
3. Ist die Herausgabe der Daten verhältnismässig?
4. Welche Art der Auswertung wird verlangt (anonymisiert, pseudonymisiert, namentlich)?
5. Sind die Voraussetzungen für die jeweilige Art der Auswertung erfüllt, insbesondere hinsichtlich dem Zweck der Auswertung?
6. Im Falle eines Verdachts auf Missbrauch oder Missbrauch der elektronischen Infrastruktur: Ist der konkrete Missbrauchsverdacht hinreichend schriftlich begründet oder der Missbrauch erwiesen?
7. Im Falle eines Verdachts auf Missbrauch oder Missbrauch der elektronischen Infrastruktur: Wurde die betroffene Person vorgängig über die Auswertung informiert und entweder ihre Zustimmung eingeholt oder aber liegt die Bewilligung der Leitung der Behörde, für die die betroffene Person arbeitet, vor?

8. Bei nicht bewirtschafteten Daten: Erfolgt die Auswertung wegen Verdachts auf Missbrauch oder Missbrauch der elektronischen Infrastruktur innerhalb der Fristen nach Artikel 4 Absatz 1 RDV oder hat die betroffene Person der Auswertung über diese Fristen hinaus ausdrücklich zugestimmt?