**Datenschutzrichtlinie**

**14.11.2024, ÖDSMB**

Inhalt

[1. Grundlagen 4](#_Toc182463743)

[1.1. Zweck 4](#_Toc182463744)

[1.2. Geltungsbereich 4](#_Toc182463745)

[1.3. Begrifflichkeiten 4](#_Toc182463746)

[2. Grundprinzip 5](#_Toc182463747)

[3. Gesetzliche Grundlagen 5](#_Toc182463748)

[4. Umfang der Datenbearbeitung 5](#_Toc182463749)

[5. Datenschutzziele 6](#_Toc182463750)

[5.1. Schutz der Persönlichkeit 6](#_Toc182463751)

[5.2. Gewährleistung der Datensicherheit 6](#_Toc182463752)

[6. Vertraulichkeit 6](#_Toc182463753)

[7. Informations- und Kommunikationssysteme IKS 7](#_Toc182463754)

[8. Bearbeitung von Personendaten 7](#_Toc182463755)

[8.1. Dateneigentümerin 7](#_Toc182463756)

[9. Technische und organisatorische Massnahmen 7](#_Toc182463757)

[9.1. Datenbekanntgabe und Datenweitergabe 7](#_Toc182463758)

[9.2. Datenbearbeitung im Ausland 8](#_Toc182463759)

[9.3. Clear desk policy 8](#_Toc182463760)

[9.4. Verschlüsselung 8](#_Toc182463761)

[9.5. Klassifikation der Daten 9](#_Toc182463762)

[9.6. Anmeldeverfahren und Authentifizierung 9](#_Toc182463763)

[9.8. Vernichtung von Akten und Datenträgern 10](#_Toc182463764)

[9.9. Physische Sicherheit 10](#_Toc182463765)

[9.10. Computerarbeitsplätze 10](#_Toc182463766)

[9.11. Datenspeicherung 11](#_Toc182463767)

[9.12. Datensicherheitsvorfall 11](#_Toc182463768)

[9.13. Weiterbildung und Sensibilisierung 11](#_Toc182463769)

[9.14. Nutzung des Internets 11](#_Toc182463770)

[9.15. E-Mail 12](#_Toc182463771)

[9.16. Telearbeit 13](#_Toc182463772)

[10. Kontrolle der Aktivitäten und Verletzung der vorliegenden Richtlinien/Weisungen 13](#_Toc182463773)

[11. Rechte der betroffenen Personen 14](#_Toc182463774)

[12. Schlussbestimmungen 14](#_Toc182463775)

# Grundlagen

## Zweck

Das vorliegende Dokument definiert Richtlinien/Weisungen für den Datenschutz und die Informationssicherheit, welche das Gemeindepersonal im Rahmen seiner Aufgabenerfüllung in der Gemeinde einzuhalten hat.

Diese vom Gemeinderat erlassenen Datenschutz- und Informationssicherheitsrichtlinien/-Weisungen bezwecken, dem Angestellten Leitlinien für einen gesetzeskonformen Umgang mit Personendaten an die Hand zu geben.

Die Richtlinie bezweckt insbesondere:

* die Gewährleistung des Datenschutzes und die Wahrung des Amtsgeheimnisses.
* die Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit der ICT-Infrastruktur;
* die Gewährleistung der bestimmungsgemässen Nutzung der ICT-Infrastruktur.

## Geltungsbereich

Diese Leitlinien richten sich an das Gemeindepersonal, als Empfehlungen an die Kommissionen und an externe Auftragnehmer, für letztere im Rahmen der vertraglichen Aufgabenübertragung.

## Begrifflichkeiten

* Daten: Sämtliche Informationen und Inhalte, die von der Gemeinde bearbeitet werden
* Personendaten: Alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Siehe <https://www.fr.ch/de/staat-und-recht/regierung-und-verwaltung/wichtige-informationen-zum-datenschutz>
* Besonders schützenswerte Personendaten: siehe <https://www.fr.ch/de/staat-und-recht/regierung-und-verwaltung/wichtige-informationen-zum-datenschutz>
* ICT-Infrastruktur: Die Gesamtheit aller Anlagen, Geräte, Einrichtungen und Dienste von der Gemeinde, die zur elektronischen Bearbeitung von Daten eingesetzt werden, sowie die Daten selbst.
* Bearbeiten: Jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Speichern, Archivieren oder Vernichten von Daten.

# Grundprinzip

Das Gemeindepersonal engagiert und verpflichtet sich zu einem sorgsamen Umgang mit Informationen und Personendaten, die Gegenstand einer Bearbeitung in der Gemeinde sind.

# Gesetzliche Grundlagen

Die Gemeinde ist für den Schutz der Personendaten, die sie bearbeitet, verantwortlich.

Die Personendaten sind gemäss den Vorgaben des kantonalen Datenschutzrechts, zu bearbeiten, insbesondere nach

* dem kantonalen Datenschutzgesetz vom 12. Oktober 2023 (Gesetz über den Datenschutz, DSchG, SGF 17.1),
* dem Reglement vom 29. Juni 1999 über die Sicherheit der Personendaten (DSR, SGF 17.15),
* dem Gesetz vom 7. Dezember 2010 über die Videoüberwachung (VidG, SGF 17.3) und seine Verordnung (Verordnung vom 23. August 2011 über die Videoüberwachung, VidV, SGF 17.31) sowie
* der Spezialgesetzgebung, insbesondere dem Gesetz vom 25. September 1980 über die Gemeinden (GG, SGF 140.1);
* dem Gesetz vom 23. Mai 1986 über die Einwohnerkontrolle (EKG; SGF 114.21.1).

Ergänzend sind auf allfällige externe Dienstleister das revidierte Bundesgesetz über den Datenschutz vom 25. September 2020 (Datenschutzgesetz, DSG, SR 235.1) sowie die Verordnung vom 31. August 2022 über den Datenschutz (Datenschutzverordnung, DSV, SR 235.11) anwendbar.

Die Gemeinde bzw. die für die Auslagerung der Datenbearbeitung verantwortlichen Personen achten auf die Verpflichtung der externen Dienstleister auf eine datenschutzkonforme Bearbeitung gemäss Artikel 18 ff. DSchG (insb. vertragliche Vereinbarung, sorgfältige Auswahl der Dienstleister, Vertraulichkeitsklauseln, Überwachung von deren Tätigkeit [z.B. Zugriffs-, Zugangskontrolle, vertragliche Einräumung von Kontroll- und Auditrecht] usw.).

# Umfang der Datenbearbeitung

Der/die Angestellte darf nur jene Personendaten bearbeiten, die erforderlich sind, um die gesetzlichen Aufgaben dauerhaft, sicher und zuverlässig zu erfüllen.

Die Gemeinde meldet ihre verschiedenen Bearbeitungsaktivitäten im Bearbeitungsregister der ÖDSMB an. Diese können im Register unter der Rubrik [Bearbeitungsregister | Staat Freiburg](https://www.fr.ch/de/sk/oedsmb/bearbeitungsregister) auf der Webseite der ÖDSMB eingesehen werden.

# Datenschutzziele

## Schutz der Persönlichkeit

Das Hauptziel des Datenschutzes ist der Schutz der Persönlichkeit vor widerrechtlicher und unverhältnismässiger Bearbeitung von Personendaten.

Die Bearbeitung hat sich strikt nach den gesetzlichen Vorgaben oder allenfalls aufgrund der Einwilligung der betroffenen Person zu richten. Das heisst:

* die Angestellten kennen die für ihren Aufgabenbereich anwendbaren Datenschutzvorschriften; sollte dies nicht der Fall sein, ist bei der vorgesetzten Person nachzufragen;
* die Bearbeitung von Personendaten ist restriktiv und umfasst nur solche Personendaten, die zur Aufgabenerfüllung notwendig sind (Grundsätze der Datensparsamkeit und Verhältnismässigkeit),
* jede und jeder Angestellte hat nur so weit Zugang zu den Daten, wie es für ihre/seine Aufgabenerfüllung notwendig ist (Zugangs- und Zugriffskontrolle),
* die Bearbeitung ist jederzeit kontrollierbar und transparent,
* die Rechte der Personen, über welche Personendaten bearbeitet werden, müssen gewahrt werden (Recht auf Auskunft, Berichtigung, Löschung, Datenherausgabe, Sperrung der Daten für Auskünfte an private Personen); bei Unklarheit ist beim/bei der Vorgesetzten oder dem/der Gemeindesekretär/-in nachzufragen;
* eine Datenbekanntgabe zu kommerziellen Zwecken ist untersagt.

## Gewährleistung der Datensicherheit

Die Gemeinde unternimmt die notwendigen technischen und organisatorischen Massnahmen, um die Sicherheit der Daten und Systeme zu gewährleisten.

Die Angestellten werden regelmässig über die technischen und organisatorischen Massnahmen zur Einhaltung der Datensicherheit informiert und entsprechend geschult. (vgl. auch Ziff. 9.9 nachfolgend).

# Vertraulichkeit

Das Gemeindepersonal untersteht dem Amtsgeheimnis. Es ist verpflichtet, die Vertraulichkeit von Personendaten über den gesamten Lebenszyklus der Datenbearbeitung (Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Speichern, Archivieren oder Vernichten)sicherzustellen. Diese Pflicht besteht auch nach der Beendigung des Anstellungsverhältnisses fort.

Externe Auftragnehmer unterstehen den gleichen Vertraulichkeitsregeln in der Erfüllung ihres Vertrags mit der Gemeinde.

# Informations- und Kommunikationssysteme IKS

Das Informations- und Kommunikationssystem (ICT) der Gemeinde umfasst technische und organisatorische Einrichtungen, die es ermöglichen, Informationen zu erfassen, zu verarbeiten, zu speichern und zwischen verschiedenen Nutzern oder Systemen zu übertragen.

Die wichtigsten Bestandteile eines IKS sind daher:

* Informationstechnologie (IT): Hierunter fallen alle technischen Geräte und Anwendungen zur Informationsverarbeitung, wie Computer, Server, Software und Datenbanken.
* Kommunikationstechnologie: Umfasst alle Technologien und Netzwerke, die den Austausch von Informationen ermöglichen, wie das Internet, Telefonie und andere Telekommunikationsnetze.
* Organisation: Die Regeln, Prozesse und Strukturen, die dafür sorgen, dass die Informationen effektiv und effizient verarbeitet und ausgetauscht werden.

Der Informationssicherheitsverantwortliche (CISO) der Gemeinde führt ein Inventar aller Komponenten. Dieses ist permanent zu aktualisieren.

# Bearbeitung von Personendaten

Die Informationen und Personendaten müssen gemäss den gesetzlichen Anforderungen bearbeitet werden. Die Bearbeitung von Personendaten und besonders schützenswerten Daten richtet sich nach den Sicherheitszielen von Vertraulichkeit, Intergität, Verfügbarkeit und Nachvollziehbarkeit.

## Dateneigentümerin

Ist die Gemeinde die Dateneigentümerin, so ist sie verantwortlich für die Implementierung, Umsetzung und Schulung der Informationssicherheits- und Datenschutzmassnahmen, die notwendig sind, um die Sicherheitsziele zu gewährleisten.

# Technische und organisatorische Massnahmen

## Datenbekanntgabe und Datenweitergabe

Die Daten dürfen nur an berechtigte Personen und Organe übermittelt oder bekanntgegeben werden (vgl. dazu das Merkblatt der ÖDSMB zur Kommunikation von Personendaten und besonders schützenswerten Personendaten per E-Mail, https://www.fr.ch/sites/default/files/2024-09/merkblatt-zur-kommunikation-von-personendaten-und-besonders-schutzenswerten-personendate-per-email.pdf )

Personendaten dürfen nur an Dritte und ins Ausland bekanntgegeben werden, nachdem die verantwortliche Person die Zulässigkeit der Bekanntgabe geprüft hat und die Voraussetzungen von Art. 14 ff. DSchG erfüllt sind.

## Datenbearbeitung im Ausland

Personendaten dürfen nur in der Schweiz oder in einem Staat, der ein angemessenes Schutzniveau gewährleistet, bearbeitet werden. Eine vollständige Liste dieser Staaten existiert (vgl. Anhang 1 zur Datenschutzverordnung des Bundes, DSV, RS 235.11; <https://www.fedlex.admin.ch/eli/cc/2022/568/de>).

Personendaten dürfen nur an Dritte und ins Ausland bekanntgegeben werden, nachdem die verantwortliche Person die Zulässigkeit der Bekanntgabe geprüft hat und die Voraussetzungen von Art. 14 ff. DSchG erfüllt sind.

## Clear desk policy

In öffentlich zugänglichen Räumlichkeiten ist es unumgänglich, Personendaten aktiv zu schützen.

Für den Arbeitsplatz gelten insbesondere folgende Regeln:

* Die Mitarbeitenden sind verpflichtet, den Computer auch beim kurzzeitigen Verlassen des Arbeitsplatzes zu sperren. Es ist eine automatische Sperrung des Bildschirmes nach einer bestimmten Zeit der Inaktivität einzurichten
* Vertrauliche Unterlagen sind auch bei kurzer Abwesenheit und bei Arbeitsende wegzuschliessen.
* Druckaufträge mit vertraulichem Charakter an einen zentralen Drucker sind mit einem Printout-Code zu versehen oder umgehend abzuholen.
* Bei Arbeitsende ist der PC herunterzufahren und abzuschalten.

## Verschlüsselung

Besonders schützenswerte Personendaten sind mit geeigneten Mitteln (Inhaltsverschlüsselung) zu verschlüsseln. Dies gilt für die Datenspeicherung wie auch für die Datenübertragung.

Die Gemeinde als für den Schutz der Personendaten verantwortliches Organ stellt die notwendige Infrastruktur zur Verfügung.

## Klassifikation der Daten

Jedes physische oder elektronische Dokument ist je nach seinem Inhalt gemäss Reglement vom 29. Juni 1999 über die Sicherheit der Personendaten (Art. 9 DSR, SGF 17.15) anhand der folgenden Kategorien zu klassifizieren:

* «öffentlich zugänglich» (Stufe 1),
* «für internen Gebrauch» (Stufe 2) oder
* «vertraulich oder geheim» (Stufe 3; Art. 9 DSR).

## **Anmeldeverfahren und Authentifizierung**

Anmeldung am System: Die Angestellten authentifizieren sich mit ihren persönlichen, vertraulich zu behandelnden, Anmeldedaten am System.

Das System prüft mit diesen Informationen, ob die Benutzer über eine Zugriffsberechtigung verfügen und autorisiert bei erfolgreicher Prüfung den Benutzer gemäss seiner Rolle und seinen Berechtigungen.

Mit der Authentifizierung stellt die Gemeinde sicher, dass nur die berechtigte Personen, Dienste und Apps mit den entsprechenden Berechtigungen auf Gemeinderessourcen zugreifen dürfen.

Die einfache Authentifizierung erfolgt i.d.R. mit persönlichem Benutzername und einem geheimen Kennwort.

Zur Erhöhung der Sicherheit kann eine dritte Information (Fingerprint, Badge, SMS) abgefragt werden.

Der Verlust von der oben erwähnten Anmeldedaten ist unverzüglich dem/der Sicherheitsverantwortlichen und/oder dem/der Vorgesetzten zu melden.

* 1. **Passwörter**

Der Benutzername und das persönliche Passwort dienen zur Identifizierung der Nutzer durch die ICT-Infrastruktur. (Siehe 9.6). Das persönliche Passwort darf niemandem bekanntgegeben werden, auch nicht anderen Mitarbeitenden.

Passwortvorgaben:

* das Passwort soll mindestens 11 Zeichen umfassen und eine ausreichende Komplexität besitzen (Ziffern und Sonderzeichen sowie Gross- und Kleinschreibung);
* Trivialpasswörter wie «EEEEEEEE» und «12345678» sind nicht zulässig;
* das Passwort soll keine Namen oder persönlichen Daten wie Geburtstage, Telefon- und Autonummern enthalten;
* das persönliche Passwort muss in regelmässigen Abständen geändert werden
* Passwörter dürfen sich nicht wiederholen und nicht inkrementiert werden (zum Beispiel Passwort23, Passwort24)
* wenn die Möglichkeit besteht, dass das Passwort anderen Personen bekanntgeworden ist, muss es sofort geändert werden;
* das Passwort darf weder in Papierform noch elektronisch unverschlüsselt am Arbeitsplatz aufbewahrt werden;

Die Vorgaben sind technisch und organisatorisch durchzusetzen.

Für mehr Informationen siehe Merkblatt der ÖDSMB zur Kommunikation von Personendaten und besonders schützenswerten Personendaten.

## Vernichtung von Akten und Datenträgern

* Vertrauliche Unterlagen dürfen nicht über die normalen Papier- und Abfallkörbe entsorgt werden. Es sind ausschliesslich dafür bereitgestellte Entsorgungscontainer zu benutzen.
* Nicht mehr benötigte Datenträger mit Personendaten müssen fachgerecht entsorgt/gelöscht werden. Eine einfache Löschung ist nicht zulässig.

## Physische Sicherheit

Der Zugang zu Büros, in denen Personendaten bearbeitet werden, ist nur den Angestellten der Gemeinde im Rahmen ihrer Aufgabenerfüllung gestattet. Es sind entsprechende Sicherheitssysteme einzurichten. (Schliessplan, etc.)

Der Zugang von Drittpersonen (wie z.B. Techniker, Reinigungspersonal) ist vom Informationssicherheitsbeauftragten zu genehmigen. Je nach Art der Aufgaben und Tätigkeiten sind besondere Schutzmassnahmen zu definieren und umzusetzen (persönliche Begleitung, Verschluss von Aktenschränken, Abmelden an Systemen etc.)

## **Computerarbeitsplätze**

Die Konfiguration der Computerarbeitsplätze der Gemeinde darf durch die Nutzer nicht verändert werden. Es darf ausschliesslich Software verwendet werden, die durch die Gemeinde beschafft und installiert worden ist. Verboten sind insbesondere, aber nicht ausschliesslich:

* jede eigenmächtige Installation von Software durch die Nutzer;
* jede Verwendung von nicht lizenzierter Software
* die Deinstallation oder Veränderung der von der Gemeinde installierten Software;
* der Anschluss von privaten Geräten an die ICT-Infrastruktur, insbesondere von privaten Geräten zur Datenverarbeitung,-speicherung oder -übertragung. (Als Anschluss gilt auch das Einrichten einer drahtlosen Verbindung (WLAN, Bluetooth etc.) an das Gemeindenetz.

## Datenspeicherung

Die Daten müssen auf den Systemen, die von der Gemeinde zur Verfügung gestellt werden, gespeichert werden (wie z.Bsp. interner Server, private Cloud der Gemeinde). Die Angestellten sind verpflichtet, geschäftliche Daten auf den Systemen der Gemeinde abzuspeichern. Jedes Kopieren oder Speichern von Personendaten an anderen als den dafür vorgesehenen Speicherorten innerhalb der Gemeinde-Infrastruktur (Netzlaufwerke) und den durch ICT angebotenen Cloud-Lösungen ist verboten. Dieses Verbot gilt insbesondere für die Ablage ausserhalb der Gemeinde in sogenannten Cloud-Speicherdiensten, wie Dropbox, Google Docs, Google Drive, OneDrive etc.

Werden für bestimmte Arbeitsprozesse mobile Geräte ausserhalb der Gemeinderäumlichkeiten genutzt, sind die Daten danach schnellstmöglich auf die Gemeindedinfrastruktur zurückzuspeichern und lokal zu löschen.

## Datensicherheitsvorfall

Wird ein Datensicherheitsvorfall (Bsp. Virusbefall, Phishingmail, Passwortdiebstahl) festgestellt, hat der/die Angestellte sofort seinen/ihren Vorgesetzten sowie den/die Verantwortliche/-n der Informationssicherheit zu informieren.

Die Gemeinde stellt sicher, dass die Liste mit Kontakten und die einzuhaltenden Verfahren bei Sicherheitsvorfällen aktuell und für jede/jeden Angestellte/-n verfügbar sind. Siehe dazu das Formular der ÖDSMB und die Erläuterungen dazu unter <https://www.fr.ch/de/staat-und-recht/transparenz-und-datenschutz/meldung-von-datensicherheitsverletzungen>

## Weiterbildung und Sensibilisierung

Die Gemeinde bildet das Personal in Datenschutz und Informationssicherheit regelmässig weiter und weist auf Programme hin. Die Teilnahme an Weiterbildung und Sensibilisierung ist für das gesamte Gemeindepersonal obligatorisch. Der Gemeinderat bzw. die damit beauftragte Person bestimmt Häufigkeit und Dauer der Weiterbildung.

Die entsprechenden Weiterbildungskosten trägt die Gemeinde.

## Nutzung des Internets

Das Internet darf grundsätzlich nur für berufliche Zwecke genutzt werden.

Eine gelegentliche private Nutzung wird geduldet; Im Rahmen der geduldeten privaten

Nutzung darf das Internet als Informationsmedium genutzt werden. Nicht erlaubt ist aber die Nutzung von reinen Unterhaltungsangeboten, wie Spiele oder Videos. Die Gemeinde ist berechtigt, den Zugang zu Internetangeboten, deren Nutzung nicht erlaubt sind oder die erfahrungsgemäss zu einer übermässigen Nutzung führen, einzuschränken oder zu sperren.

Die Möglichkeit des Zugriffs auf eine Webseite bedeutet nicht, dass dieser erlaubt ist.

Die Internetaktivität durch die Nutzer und Nutzerinnen wird aufgezeichnet.

## E-Mail

Grundsatz: E-Mails garantieren keine Vertraulichkeit und Richtigkeit bezüglich Absender, Empfänger oder Inhalt. Es dürfen deshalb grundsätzlich keine sensiblen Daten (insbesondere schützenswerte Personendaten) ohne sichere Inhaltsverschlüsselung per E-Mail verschickt werden.

Jeder und jede Angestellte verfügt für seine/ihre beruflichen Bedürfnisse über eine standardisierte und persönliche elektronische Adresse (E-Mail-Adresse), die ihr/ihm vom Informationssicherheitsverantwortlichen zugeteilt wird. Die Adresse wird bei Eintritt zugeteilt und aktiviert sowie bei seinem/ihrem Austritt desaktiviert.

Die eingehenden E-Mails und dessen Inhalt durchlaufen eine Antiviren- und Antispam-Filterung. Die Verschlüsselung des Inhalts von ausgehenden E-Mails (mit dessen Anhängen), die besonders schützenswerte Personendaten enthalten, ist sichergestellt.

Trotz Sicherheitsmassnahmen ist nicht ausgeschlossen, dass Angestellte infizierte E-Mails erhalten. Es liegt im Verantwortungsbereich des Nutzers oder der Nutzerin offensichtlich zweifelhafte E-Mails (wie auch Links und Anhänge) nicht zu öffnen.

Das E-Mail-System ist einzig für berufliche Zwecke bestimmt.

Die Mitarbeitenden dürfen betriebliche E-Mails weder an ihre privaten noch an andere externe, von ihnen kontrollierte E-Mail-Adressen weiterleiten.

Bei Abwesenheit ab einem Tag sorgen die Mitarbeitenden dafür, dass jedes eingehende E-Mail automatisch mit einer Abwesenheitsmeldung und den Kontaktangaben der Stellvertretung beantwortet wird.

Die Gesamtheit der E-Mails sowie deren Inhalt, die sich im E-Mail-System der Gemeinde befinden, gilt als beruflich und gehört der Gemeinde.

Beim Austritt muss der/die Angestellte die laufenden Geschäfte sowie die dazugehörenden E-Mails der Gemeinde übergeben.

Vor dem Austritt hat der/die Mitarbeitende die noch von ihm bearbeiteten bzw. pendenten Geschäfte zu übergeben. E-Mails mit persönlichen Inhalten, z. Bsp. mit Arbeitskollegen, sind zu entfernen. Spätestens am letzten Arbeitstag wird der E-Mail-Account des austretenden Mitarbeitenden gesperrt. Absender, die E-Mails an die gesperrte E-Mail-Adresse senden, werden automatisch darüber informiert, dass die Empfängeradresse ungültig ist.

## Telearbeit

Ein Zugang zu den Informatikressourcen ausserhalb des Büros oder des Netzwerks der Gemeinde bedarf der Zustimmung des/der Vorgesetzten. Dies gilt auch für Home-Office bzw. Telearbeit.

Für den Fernzugriff sind grundsätzlich die Computer oder Mobiltelefone der Gemeinde zu nutzen.

Sofern der Einsatz von privaten Mobiltelefonen bewilligt wird, muss eine entsprechende Sicherheitslösung (Container) unter Einwilligung der betroffenen Personen auf den privaten mobilen Geräten installiert werden. Diese ist so zu konfigurieren, dass geschäftliche Daten (Email, Dokumente, Bilder etc.) nur in diesem Container bearbeitet werden.

Im Rahmen der Telearbeit dürfen Personendaten einzig auf den vom Informatikdienst der Gemeinde bewilligten und kontrollierten Speichermedien abgelegt werden.

Die in diesem Reglement beschriebenen Sicherheits- und Verhaltensmassnahmen sind ebenfalls auf die Heimtelearbeit anwendbar, inklusive Meldung von Sicherheitsverletzungen und entsprechende Verfahrensvorschriften.

# Kontrolle der Aktivitäten und Verletzung der vorliegenden Richtlinien/Weisungen

Die Bewirtschaftung und die Sicherheit der Informationssysteme sind Gegenstand einer regelmässigen Überwachung. Diese Überwachung ist grundsätzlich anonym und nicht gezielt.

Bei Verdacht auf eine Verletzung der Regeln können vertiefte Abklärungen mit Einverständnis der/des Vorgesetzten oder der/des Informationssicherheitsverantwortlichen der Gemeinde durchgeführt werden. Die so gewonnenen Informationen werden vollständig dem/der Vorgesetzten übermittelt, welche/-r die geeigneten Massnahmen in die Wege leitet und die Informationen datenschutzkonform behandelt.

# Rechte der betroffenen Personen

Die Rechte der durch die Bearbeitung betroffenen Personen sind zu wahren (vgl. Art. 27 ff. DSchG).

Die Anfragen zu ihren Daten sind an den/die zuständige/-n Gemeindesekretär/-in, allenfalls an die von ihm/ihr genannte Person weiterzuleiten (vgl. interne Organisation).

# Schlussbestimmungen

Die Sicherheit der Informationssysteme ist eine anhaltende und ständig voranschreitende Entwicklung.

Diese Leitlinien werden regelmässig der technischen und organisatorischen Entwicklung angepasst.

Die Richtlinien wurden am …. verabschiedet und treten am … in Kraft.