*Freiburg, 7. Januar 2025*

*Die ÖDSMB ist der Ansicht, dass die Legislative das zuständige Organ für die Verabschiedung eines Reglements für Datenschutz und Informationssicherheit ist. Sie stellt daher das nachfolgende, ausführliche Musterreglement zur Verfügung, das Raum für Anpassungen und eventuelle Kürzungen lässt.*

**Musterreglement für Datenschutz und Datensicherheit**

Die Gemeindeversammlung/Der Generalrat,

gestützt auf:

* das Gesetz vom 12. Oktober 2023 über den Datenschutz (DschG; SGF 17.1),
* das Reglement vom 29. Juni 1999 über die Sicherheit von Personendaten (DSR; SGF 17.15),
* das Gesetz vom 25. September 1980 über die Gemeinden (DSR; SGF 17.15),
* die Richtlinien der Gemeinde über den Datenschutz (GG; SGF 140.1),

erlässt:

**1 Allgemeines**

Art. 1 Zweck

Das vorliegende Reglement spezifiziert die in der Leitlinie zum Datenschutz definierten Zielsetzungen und beschreibt die Massnahmen, um die Bearbeitung von Personendaten entsprechend dem kantonalen Datenschutzgesetz sowie die Datensicherheit zu garantieren. Es bezweckt, die Einhaltung der Sicherheitsziele Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit und damit einen datenschutzkonformen Betrieb zu gewährleisten.

Im Interesse der Transparenz gegenüber den Nutzerinnen und Nutzern sowie der Förderung einer verantwortungsvollen und sicheren Nutzung der Informations- und Kommunikationssysteme, definiert es die Vorschriften über den Gebrauch dieser Ressourcen sowie die Kontroll- und Überwachungsmöglichkeiten dieser Nutzung.

Art. 2 Anwendungsbereich

Das vorliegende Reglement ist anwendbar auf:

1. alle Angestellten der Gemeinde, unabhängig ihres Status; es ist integrierender Bestandteil ihres Arbeitsvertrags. Die Angestellten akzeptieren es durch Unterzeichnung des Arbeitsvertrags;
2. die externen Auftragsbearbeiter und -innen sowie ihre Hilfspersonen ; es ist Bestandteil des Auftrags bzw. des Werkvertrags, welche die Gemeinde unterzeichnet;
3. auf die kommunalen Mandatsträger, vorbehalten bleiben die Bestimmungen der Spezialgesetzgebung, insbesondere des Gemeindegesetzes.

Art. 3 Informations- und Kommunikationssysteme

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

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

Art. 4 Verantwortlichkeiten

Die Gemeinde ist für den Datenschutz und die Informationssicherheit verantwortlich und trifft die notwendigen Massnahmen.

Die Aufgabe wird vom Gemeindesekretär oder von der Gemeindesekretärin oder von der vom Gemeinderat bezeichneten Person in ihrer/seiner Funktion als Verantwortliche/r für die Informationssicherheit und den Datenschutz wahrgenommen.

Art. 5 Sicherheitsziele und Vertraulichkeit

Die Angestellten der Gemeinde sind verpflichtet, die Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit von Personendaten, die sie bearbeiten (Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Speichern, Archivieren oder Vernichten) zu bewahren.

Die Angestellten der Gemeinde unterstehen dem Amtsgeheimnis. Diese Pflicht dauert nach der Beendigung des Anstellungsverhältnisses fort.

Externe Auftragnehmer unterstehen den gleichen Vertraulichkeitsregeln in Anwendung des Auftrags oder Werkvertrags mit der Gemeinde.

Hinsichtlich der Vertraulichkeit unterstehen die Gewählten der Gemeinde den gleichen Regeln in Anwendung der Spezialgesetzgebung, insbesondere des Gemeindegesetzes.

**2. Datenschutz und Datensicherheit**

Art. 6 Bearbeitung von Personendaten

Personendaten müssen gemäss den gesetzlichen Anforderungen bearbeitet werden.

Bei der Bearbeitung von Personendaten und besonders schützenswerten Daten müssen die Sicherheitsziele von Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit garantiert werden können.

Art. 7 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.

Art. 8Datenbekanntgabe 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.

Art. 9 Datenbearbeitung im Ausland

Personendaten dürfen nur in der Schweiz oder in einem Staat, der ein angemessenes Schutzniveau gewährleistet, bearbeitet werden (vgl. die abschliessende Staatenliste in 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, ob die gesetzlichen Voraussetzungen von Art. 14 ff. DSchG, insbesondere jene von Art. 15 DSchG, erfüllt sind.

Art. 10 Clear desk policy

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

Für den Arbeitsplatz gelten 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.

Art. 11 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.

Art. 12 Klassifikation der Daten

Jedes physische oder elektronische Dokument ist je nach seinem Inhalt anhand der folgenden Kategorien zu klassifizieren: «öffentlich zugänglich» (Stufe 1), «für internen Gebrauch» (Stufe 2) oder «vertraulich oder geheim» (Stufe 3), gemäss Reglement vom 29. Juni 1999 über die Sicherheit der Personendaten (Art. 9 DSR, SGF 17.15).

Art. 13 Authentifizierung und Autorisierung

Die Gemeinde stellt mit einem Authentifizierungsprozess sicher, dass nur berechtigte Personen, Dienste und Apps mit den richtigen Berechtigungen auf Gemeinderessourcen zugreifen dürfen.

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

Zur Erhöhung der Sicherheit kann eine dritte Information (Fingerprint, Badge, SMS) abgefragt werden, speziell für den Zugriff auf besonders schützenswerte Personendaten.

Die Angestellten dürfen einzig ihr persönliches Benutzungskonto bzw. ihr Login oder die funktionellen Accounts, die ihnen zugeteilt sind, nutzen. Sie sind für alle Zugriffe verantwortlich, die sie mit ihrem Account tätigen.

Sollte die Geheimhaltung der Anmeldedaten aus irgendeinem Grund kompromittiert worden sein, (Diebstahl, Verlust, irrtümliche Bekanntgabe), ist dies unverzüglich dem Informationssicherheitsbeauftragten zu melden.

Art. 14 Passwörter

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

Folgend Passwortvorgaben sind einzuhalten:

* 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 (min. 2 mal pro Jahr)
* Passwörter dürfen sich nicht wiederholen und nicht inkrementiert werden (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.

Art. 15 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.

Art. 16 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, Badge 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.)

Art. 17 Computerarbeitsplätze und -komponenten

Die Angestellten, die Gewählten und die Auftragnehmer sind verantwortlich für die Daten und alle Hardware- und Softwarekomponenten, die ihnen im Rahmen ihrer Funktion anvertraut werden. Sie müssen diese sorgfältig und achtsam behandeln und sind verpflichtet, jede Funktionsstörung, jeden Vorfall, jede Ungewöhnlichkeit oder Verlust zu melden.

Die Konfiguration der Computerarbeitsplätze (PC) sowie aller anderen zur Verfügung gestellten Endgeräte der Gemeinde dürfen durch die Nutzer nicht verändert werden. Es ist ausschliesslich Software zu verwenden, die durch die Gemeinde beschafft und installiert worden ist. Verboten sind insbesondere, aber nicht ausschliesslich:

* jede eigenmächtige Installation von Software / Apps durch die Nutzer;
* jede Verwendung von nicht lizenzierter Software
* die Deinstallation oder Veränderung der von der Gemeinde installierten Hard- und Softwarekomponenten;
* 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.

Art. 18 Datenspeicherung

Die Daten müssen auf den Systemen, die von der Gemeinde zur Verfügung gestellt werden, gespeichert werden (wie 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 Gemeindeinfrastruktur zurückzuspeichern und lokal zu löschen.

Art. 19 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

Art. 20 Nutzung des Internets durch die Angestellten

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 erfahrungs-gemäss 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.

Art. 21 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.

Vor dem Austritt hat der/die Mitarbeitende, die noch von ihm bearbeiteten bzw. pendenten Geschäfte sowie die E-Mails zu übergeben. E-Mails mit persönlichen Inhalten, z. B. 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.

Art. 22 Telearbeit

Für Telearbeit braucht es eine Bewilligung.

Ein Zugang zu den Informatikressourcen ausserhalb des Büros oder des Netzwerks der Gemeinde bedarf der vorgängigen 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 Person 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.

Art. 23 Kontrolle der Aktivitäten und Verletzung des vorliegenden Reglements

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 des Reglements 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.

Bei vorsätzlichen oder fahrlässigen Verletzungen des vorliegenden Reglements sind strafrechtliche oder disziplinarische Sanktion, die im übergeordneten oder kommunalen Recht vorgesehen sind, vorbehalten.

**3 Weiterbildung und Sensibilisierung**

Art. 24 Ziel

Um das Verständnis und die Einhaltung der Vorschriften über den Datenschutz und die Informationssicherheit zu garantieren, sieht die Gemeinde ein Programm für Weiterbildung und Sensibilisierung vor. Die Teilnahme an Weiterbildung und Sensibilisierung ist für Angestellte und Gewählte obligatorisch.

Gegebenenfalls vereinbart der Gemeinderat mit externen Auftragnehmern entsprechende Pflichten, soweit dies notwendig ist.

**4 Schlussbestimmungen**

Art. 25 Anpassung des Reglements

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

Dieses Reglement wird regelmässig der technischen und organisatorischen Entwicklung angepasst.

Art. 26 Inkrafttreten

Das vorliegende Reglement tritt nach seiner Annahme durch die Gemeindeversammlung/den Generalrat in Kraft, unter Vorbehalt der Genehmigung durch die Direktion der Institutionen und der Land- und Forstwirtschaft.

07.01.2025 – v2.6