Weisung zur Informationssicherheit und zum Datenschutz der Gemeinde Langnau am Albis

vom 21. November 2023

Stand 21. November 2023

Inhaltsverzeichnis

Der Gemeinderat erlässt, gestützt auf § 48 des Gemeindegesetzes vom 20. April 2015 und Art. 24 der Gemeindeordnung der Gemeinde Langnau am Albis vom 9. Februar 2020 folgende Weisung:

1. Allgemeine Bestimmungen

1.1. Gegenstand und Zweck

Diese Weisung regelt die Nutzung der Informations- und Kommunikationstechnologie (IKT-Mittel), im Speziellen den Gebrauch von E-Mail und Internet und die Verwendung mobiler Geräte. Gegenstand der Weisung ist zudem der verantwortungsvolle Umgang mit Informationen (insbesondere besonders schützenswerte Personendaten) zur Gewährleistung des Datenschutzes.

Sie bezweckt den Schutz der Informationen vor einem Verlust der Vertraulichkeit, Verfügbarkeit und Integrität.

1.2. Geltungsbereich

Die Weisung gilt für alle Mitarbeiterinnen und Mitarbeiter sowie Behördenmitglieder der Gemeinde.

1.3. Grundlagen

Die Grundlagen der Gemeinde sind:

- Gesetz über die Information und den Datenschutz (IDG, LS 170.4)
- Verordnung über die Information und den Datenschutz (IDV, LS 170.41)
- Verordnung über die Informationsverwaltung und -sicherheit (IVSV, LS 170.8)
- Allgemeine Richtlinie für Informationssicherheit und Datenschutz Langnau am Albis
- Vertrag Rechenzentrum OBT Swiss Cloud Flex mit der OBT AG

2. Verantwortung Informationssicherheitsverantwortliche / -sicherheitsverantwortlicher

Die / der Informationssicherheitsverantwortliche/r (ISV) ist für die Umsetzung dieser Weisung verantwortlich und ist Ansprechstelle bei Fragen und bei sicherheitsrelevanten Vorkommnissen. Sie / er ist befugt, den Mitarbeiterinnen und Mitarbeiter Weisungen bezüglich Informationssicherheit zu erteilen. Die / der ISV kann die operativen Tätigkeiten für die Umsetzung der Minimalanforderungen delegieren.

Die / der ISV stellt sicher, dass Mitarbeiterinnen und Mitarbeiter folgende Minimalanforderungen einhalten können:

- Alle Mitarbeiterinnen und Mitarbeiter werden über ihre Verantwortlichkeiten bei klassifizierten Informationen (siehe auch Kapitel 3.2) orientiert.
- Die Weisung Informationssicherheit ist in der systematischen Rechtssammlung der Gemeinde jederzeit in der neusten Version abrufbar.
- Die Weisung Informationssicherheit wird gelebt und eingehalten.
- Das Bewusstsein für die Informationssicherheit wird geschaffen.
- Die Fähigkeiten und Qualifikationen in Bezug auf Informationssicherheit und Datenschutz von Mitarbeiterinnen und Mitarbeitern werden gefördert z.B. Schulungen.

2.2.Mitarbeiterinnen und Mitarbeiter, Behörden- und Kommissionsmitglieder

Die Mitarbeiterinnen und Mitarbeiter sowie Behörden- und Kommissionsmitglieder sind verpflichtet, die gesetzlichen Vorgaben, diese Weisung und andere interne Regelungen zu beachten. Sie haben die Kenntnisnahme dieser Weisung durch Unterzeichnung der Erklärung über die Nutzung von Internet und E-Mail sowie zu Informationssicherheit sowie zur Nutzung von mobilen IKT-Systemen der Gemeinde Langnau am Albis zu bestätigten.

Die Mitarbeiterinnen und Mitarbeiter sowie Behörden- und Kommissionsmitglieder sind verpflichtet, die ihnen zur Verfügung gestellten IT-Mittel recht- und zweckmässig einzusetzen und mit den Informationen sorgfältig umzugehen, insbesondere mit Personendaten und besonderen Personendaten.

Die Kenntnisnahme von Informationssicherheitsvorfällen sowie Schäden und Verlust von Hard- und Software sind durch die Mitarbeiterinnen oder Mitarbeiter sofort an die bzw. den ISV sowie die Vorgesetzte / den Vorgesetzten zu melden.

Mögliche Informationssicherheitsvorfälle sind (nicht abschliessend):

- Verlust, unbeabsichtigte Löschung oder Vernichtung von Daten, unberechtigte Kopien von Daten oder von Datenträgern
- Veränderung oder Manipulation von Informationen
- Unberechtigter Zugriff oder Bekanntgabe an Unbefugte
- Funktionalität eines oder mehrerer Informationssysteme gestört
- Öffnen eines Anhanges eines möglichen Phishing-Mails

3. Datenschutz und Informationssicherheit**Umgang mit Informationen**

Informationen sind ausschliesslich gemäss den rechtlichen Vorgaben zu bearbeiten. Im Umgang mit Informationen ist die Vertraulichkeit jederzeit zu gewährleisten. Entsprechende Vorgaben sind jederzeit einzuhalten und entsprechende Massnahmen sicherzustellen. Dazu zählen:

- Informationen nur berechtigten Stellen und Personen zugänglich zu machen
- Verschlüsseln von sensitiven Informationen (besonders schützenswerte Personendaten) bei der Übertragung (beispielsweise Verschlüsselung eines USB-Sticks, einer E-Mail oder einer sonstigen elektronischen Übermittlung) soweit der Austausch nicht über eine sichere Datenplattform möglich ist
- Definition von Verfahren, die Informationen und Datenträger während eines physischen Transports schützen
- Sicherstellen der Vertraulichkeit beim Ausdrucken, Kopieren und/oder Weiterleiten von Dokumenten mit besonders schützenswerten Personendaten

3.2.Klassifizierung von Informationen

Elektronische Informationen sind in der betreffenden Fachapplikation oder im Geschäftsverwaltungssystem CMI Axioma zu speichern. In Ausnahmefällen kann das Laufwerk der entsprechenden Abteilung zur Speicherung genutzt werden. Empfangene E-Mails mit vertraulichen oder geheimen Informationen sind umgehend zu speichern und im Postfach unwiderruflich zu löschen. Microsoft Teams und One Drive dürfen nicht für die Speicherung von Daten genutzt werden; lediglich für den Datentransfer von nicht besonders schätzenswerten Daten sind die beiden Medien nutzbar.

Sobald physische und elektronische Information – soweit es sich um besonders schützenswerte Personendaten handelt - ausserhalb der oben genannten Orte gespeichert oder weitergegeben werden, sind die Daten zu klassifizieren. Die Klassifizierung erfolgt nach «Öffentlich», «Intern», «Vertraulich» oder «Geheim».

Für vertrauliche und geheime Informationen muss ein Klassifizierungsvermerk «Vertraulich» oder «Geheim» angegeben werden. Ist kein Klassifizierungsvermerk vorhanden oder aus dem Kontext erkennbar, gilt die Information als «Intern» klassifiziert.

Wer klassifizierte Informationen bearbeitet, ist für die Einhaltung der Informationsschutzvorschriften verantwortlich.

Wer feststellt, dass Informationen gefährdet, abhandengekommen oder missbraucht worden sind, informiert unverzüglich die beziehungsweise den ISV sowie die zuständige oder vorgesetzte Stelle.

Neu zu erstellende oder anzupassende «Intern», «Vertraulich» oder «Geheim» klassifizierte Dokumente müssen mindestens die folgende Kennzeichnung ausweisen:

a) Eindeutige Bezeichnung (aussagekräftiger Titel)
b) Ersteller, Autor oder Dokumenteninhaber
c) Funktion des Erstellers bei «Geheim»
d) Datum der letzten Überarbeitung

3.3. Klassifizierung

- Informationen, die der Öffentlichkeit zugänglich sein dürfen, werden als «Öffentlich» klassifiziert.
- Informationen, die keiner anderen Klassifizierung zugewiesen werden, gelten als «Intern» klassifiziert.
- Informationen werden als «Vertraulich» klassifiziert, wenn sie nur für einen definierten Benutzerkreis zugänglich sein sollen und/oder wenn durch deren Bekanntmachung (auch innerhalb der Verwaltung) ein wesentlicher Schaden verursacht werden könnte.
- Informationen werden als «Geheim» klassifiziert, wenn Unberechtigte durch deren Kenntnisnahme den Interessen der Gemeinde einen schweren Schaden zufügen könnten.

3.4. Schutzmassnahmen für klassifizierte Informationen

- Für «Öffentlich» klassifizierte Informationen gelten folgende Bearbeitungsregeln:
  a) Die Integrität der Informationen muss sichergestellt werden.

- Für «Intern» klassifizierte Informationen gelten zusätzlich zu den als «Öffentlich» klassifizierten Informationen folgende Bearbeitungsregeln:
  a) Informationen müssen zugriffsbeschränkt aufbewahrt bzw. gespeichert werden.

- Für «Vertraulich» klassifizierte Informationen gelten zusätzlich zu den Bearbeitungsregeln für als «Intern» klassifizierten Informationen:
  a) Informationsträger müssen an einem abschliessbaren Ort aufbewahrt werden.
  b) Der Zugriff muss beschränkt sein auf einen vom Dateneigner namentlich oder funktionsbezogenen definierten Personenkreis.
  c) Die Weitergabe nach aussen ist nur bei anerkannten Gründen und unter entsprechenden Sicherheitsmassnahmen zulässig, z.B. mit einem Vertrag mit einer Vertraulichkeitsklausel.

d) Der Versand in physischer Form darf nur in fest verschlossenem Umschlag, adressiert mit «Persönlich» erfolgen, d.h. nur der Empfänger selbst oder eine explizit autorisierte Stellvertretung darf Einsicht nehmen.
e) Der elektronische Versand von vertraulichen Dokumenten muss, soweit kein Versand via Geschäftsverwaltungssystem oder Fachapplikation (z.B. Link) oder einer sicheren Datenaustauschplattform möglich ist, verschlüsselt erfolgen. Verschlüsselte Mails sind im Postfach nach Versand oder Empfang umgehend unwiderruflich zu löschen.

– Für «Geheim» klassifizierte Informationen gelten zusätzlich zu den Bearbeitungsregeln für als «Vertraulich» klassifizierten Informationen:
f) Jedes Exemplar ist auf jeder Seite als «Geheim» zu kennzeichnen (z.B. mit Wasserzeichen).
g) Physische Dokumente müssen an einem stark gesicherten Ort (z.B. Tresor) aufbewahrt werden und stehen somit unter physischer Zugangskontrolle.
h) Elektronische Dokumente dürfen nur auf zugelassenen Speicherorten abgelegt werden.
i) Der Ersteller führt eine schriftliche Kontrolle über die Ausgabe und den Verbleib der einzelnen nummerierten physischen Dokumente oder bei elektronischen Dokumenten die nummerierten Informationsträger.
j) Der Versand muss nachvollziehbar sein.
k) Dokumente und elektronischer Versand müssen zusätzlich signiert sein.

3.5.Zugangs- und Zugriffsschutz

Die Mitarbeiterinnen und Mitarbeiter dürfen nur ihre persönlichen Benutzerkennungen oder die ihnen zugeteilten funktionellen Kennungen verwenden. Sie sind für die mit ihren Kennungen erfolgten Zugriffe verantwortlich und dürfen diese nicht weitergeben. Vorbehalten sind allgemeine Benutzererkennungen an Schalterarbeitsplätzen.

Clear Screen: Wo Bildschirmsperren von den Mitarbeiterinnen und Mitarbeiter selbst eingerichtet werden können, sind sie zu benützen. Bildschirmsperren dürfen nicht ausgeschaltet werden.

Austretende Personen haben unterschriftlich zu bestätigen, dass alle schützenswerten Informationen (insbesondere besondere Personendaten), die ihnen zugänglich waren und die ausserhalb der Gemeinde bearbeitet oder gespeichert wurden, unwiderruflich und vollständig gelöscht (einfaches Löschen genügt nicht) oder zurückgegeben wurden.

Der Verlust von Schlüsseln und Badges sind umgehend der Abteilung Liegenschaften zu melden. Der Verlust von Chipkarten ist dem ISV zu melden. Besteht der Verdacht, dass Zugangs- oder Zugriffsberechtigungen unberechtigt durch Dritte genutzt werden, ist die oder der ISV umgehend zu informieren.

Clear Desk: Der Arbeitsplatz ist bei Abwesenheiten so zu hinterlassen, dass keine vertraulichen oder schutzbedürftigen Unterlagen und Datenträger offen zugänglich sind (Abschliessen von Türen und Verschliessen von Fenstern des Büros, Abschliessen weiterer Räume gemäss Anweisung der / des ISV, Sperren oder Herunterfahren des PC). Ausdrucke mit vertraulichen Informationen sind umgehend aus dem Drucker zu entfernen.

Die Mitarbeiterinnen und Mitarbeiter sowie die Behördenmitglieder sorgen dafür, dass keine Unbefugten Zutritt zu den Arbeitsräumlichkeiten haben. Halten sich externe Personen, zum Beispiel Reinigungspersonal, Servicetechniker, Gäste usw., in den Büroräumlichkeiten auf, sind Massnahmen zu treffen, die einen unbefugten Zugang zu Informationen verhindern, z.B. mittels Verschluss der Dokumente in Aktenschränken.

3.6.Passwörter

Ein gutes Passwort besteht aus einem Passwort-Merksatz oder einer grossen und zufälligen Anzahl von Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen. Leicht zu erratende Passwörter und solche, die einen Bezug zur eigenen Person aufweisen (z.B. Name, Name von Angehörigen, Geburtsdatum usw.), sind nicht erlaubt.

Passwörter müssen mindestens 12 Zeichen lang sein und folgende Merkmale enthalten:

a) Grossbuchstabe
b) Kleinbuchstabe
c) Ziffer
d) Sonderzeichen

Alternativ kann ein Passwort mit mindestens 16 Stellen verwendet werden, wenn sichergestellt ist, dass das Passwort keine unzulässigen Merkmale (z.B. Begriffe aus Wörterbüchern, simple Muster, benutzer- oder servicebezogene Daten etc.) enthält.

Um die Sicherheit weiter zu erhöhen, können Intervalle zum Wechsel der Passwörter eingerichtet werden.

Dienstlich genutzte Passwörter dürfen nicht privat verwendet werden. Passwörter sind sofort zu ändern, wenn ein Verdacht besteht, dass sie Dritten zur Kenntnis gelangt sind. Ein früher bereits benutztes Passwort darf nicht mehr gewählt werden.

Passwörter und PINs sind vertraulich zu behandeln und vor Unbefugten zu schützen. Dies gilt beispielsweise, wenn Passwörter für den persönlichen Gebrauch gespeichert werden. Anderen Personen (Vorgesetzten, IT-Verantwortlichen, ISV usw.) sind Passwörter unter keinen Umständen bekannt zu gegeben.

3.7.Datensicherung, -löschung und Entsorgung von Informationsträgern

Dienstliche Daten müssen zentral in der Fachapplikation, der Geschäftsverwaltung oder dem Abteilungslaufwerk gespeichert werden. Die regelmässige Sicherung aller relevanten Daten und die sichere Lagerung der dazu benötigten Archivmedien erfolgt durch den / die ICT-Dienstleiter /in gemäss vertraglicher Regelung.

Nicht mehr benötigte Daten müssen von Datenträgern wie USB-Datenträger oder Speicherkarten unwiederbringlich gelöscht werden. Einfaches Löschen genügt nicht. Nicht mehr benötigte Datenträger (z.B. USB-Datenträger, CD-ROM usw.), die vertraulichen Informationen enthalten oder einmal enthielten, sind physikalisch zu vernichten, z.B. durch Schreddern).

3.8.Sicherheitssoftware

Die Mitarbeiterinnen und Mitarbeiter dürfen die Sicherheitssoftware wie Virenschutz oder Firewall nicht ausschalten, blockieren oder ihre Konfiguration verändern. Jeder Verdacht auf Virenbefall ist sofort der / dem ISV zu melden.

3.9.Hard- und Software

Die Mitarbeiterinnen und Mitarbeiter dürfen ohne Bewilligung der bzw. des ISV keine Software und keine Hardware-Erweiterungen installieren oder anschliessen, insbesondere keine Kommunikationseinrichtungen und externen Massenspeicher. Änderungen an den Systemeinstellungen (Installation, Deinstallation, Änderung der Konfiguration usw.) dürfen nur

durch die zuständige Stelle vorgenommen werden, zum Beispiel durch ISV oder Administrator/-in.

Die Mitarbeiterinnen und Mitarbeiter dürfen Informatiksysteme, die am Netzwerk angeschlossen sind, nicht gleichzeitig mit einem Netz oder System ausserhalb des internen Netzwerks verbinden.

Nur der bzw. die Bereichsleiter/-in ICT darf Geräte in die Reparatur oder zur Entsorgung der OBT übergeben. Sie bzw. er stellt sicher, dass keine schützenswerten Daten auf diesem Weg die Gemeinde verlassen.

4. Nutzung von E-Mail und Internet**Allgemeine Bestimmungen**

E-Mail und Internet werden für die Erfüllung dienstlicher Aufgaben nach den Grundsätzen der Wirtschaftlichkeit, der Informationssicherheit und des Datenschutzes eingesetzt. Die Mitarbeiterinnen und Mitarbeiter haben sich unterschriftlich zur Einhaltung der Nutzungsvorschriften zu verpflichten.

4.2.E-Mail

Externe, von der Gemeinde nicht genehmigte Internetdienste dürfen nicht für dienstliche Zwecke verwendet werden. Dies betrifft beispielsweise Online-Dateiablagen, Online-Kalender oder Webmail.

E-Mails mit vertraulichem Inhalt wie besonderen Personendaten müssen verschlüsselt versandt werden. Ist eine Verschlüsselung nicht möglich, muss eine andere Versandart gewählt werden. Das automatische Weiterleiten von E-Mails und das Freigeben der persönlichen Mailbox an eine Drittperson sind nicht erlaubt. Bei mehrtägigen Abwesenheiten ist die Funktion des Abwesenheitsassistenten zu nutzen.

Das E-Mail-System darf in zurückhaltendem Mass auch für private Zwecke verwendet werden. Das Versenden von E-Mails mit rechtswidrigem, pornographischem, rassistischem, sexistischem oder gewaltverherrlichendem Inhalt, mit unnötig grossem Verteiler oder mit der Aufforderung zum Weiterversand im Schneeballsystem ist verboten. Private E-Mails müssen entweder gelöscht oder in einem persönlichen Ordner mit der Bezeichnung «Privat» abgelegt werden.

E-Mails mit unbekanntem Absender, verdächtigem Betreff oder unüblichem Inhalt sind vorsichtig zu behandeln, da sie von der Virenschutzsoftware nicht erkannte Viren enthalten könnten. Ihre Anhänge sowie Links auf Websites sind keinesfalls zu öffnen.

4.3.Internet / Internetdienste

Der Zugriff auf Websites mit rechtswidrigem, pornographischem, rassistischem, sexistischem oder gewaltverherrlichendem Inhalt ist verboten.

Das Herunterladen und Installieren von Software aus dem Internet ist nicht gestattet. Die oder der ISV kann das Herunterladen oder die Installation solcher Dateien erlauben.

Schützenswerte Informationen und grosse Mengen nicht anonymisierter Personendaten dürfen nur verschlüsselt über das Internet übermittelt werden, zum Beispiel über eine https-Verbindung.

Die Nutzung sozialer Netzwerke (Facebook, Linkedin usw.) soll möglichst ausserhalb der Arbeitszeit respektive nur für dienstliche Zwecke erfolgen. Während der Arbeitszeit ist sie auf ein Minimum zu beschränken.

5. Private Nutzung von IT-Mitteln

Die zurückhaltende Nutzung von IT-Mitteln für private Zwecke ist grundsätzlich gestattet, soweit dadurch die Systemressourcen wie Speicher und Übertragungskapazität nicht im Übermass belastet werden. Die private Nutzung soll möglichst ausserhalb der Arbeitszeit erfolgen. Während der Arbeitszeit ist sie auf ein Minimum zu beschränken. Dienstliche Daten dürfen nicht privat genutzt oder in privaten Datenablagen gespeichert werden. Private Daten müssen lokal in einem persönlichen Verzeichnis mit der Bezeichnung «Privat» oder auf dem persönlichen Netzwerklaufwerk abgespeichert werden.

Systemkomponenten und Peripheriegeräte dürfen nicht für private Zwecke vom Arbeitsplatz entfernt werden.

6. Mobiles Arbeiten und Einsatz mobiler Geräte

Beim mobilen Arbeiten ausserhalb der Räume der Gemeinde und beim Einsatz mobiler Geräte sind folgende Punkte zu beachten:

- Das mobile Arbeiten oder der Einsatz von mobilen Geräten ist von der vorgesetzten Stelle zu genehmigen.
- Beim Arbeiten ausserhalb der Räumlichkeiten der Gemeinde ist jederzeit sicherzustellen, dass Informationen nicht durch unbefugte Personen eingesehen werden können, z.B. in öffentlichen Verkehrsmitteln.
- Clear Desk und Screen gelten auch beim mobilen Arbeiten, z.B. zu Hause.
- Für dienstliche Zwecke dürfen nur durch die Gemeinde genehmigte Dienste und Produkte für Kommunikation und Datenaustausch verwendet werden.
- Dienstliche Unterlagen dürfen nicht zu Hause entsorgt werden, sondern sind im Büro der ordentlichen Vernichtung zuzuführen.
- Auf mobilen Geräten wie Notebooks oder Smartphones ist die Speicherung von dienstlichen Daten nach Möglichkeit zu vermeiden. Wo dies dennoch erfolgt, müssen Dokumente mit vertraulichem beziehungsweise schützenswertem Inhalt verschlüsselt gespeichert und gesichert werden.
- Auf mobilen Endgeräten sind das Betriebssystem und die Applikationen regelmässig zu aktualisieren.
- Apps sind vor der Installation auf ihren Inhalt und Quelle zu prüfen.
- Sicherheitsmassnahmen an mobilen Geräten dürfen nicht deaktiviert werden (Firewall, Virenschutz, Betriebssystem-Manipulationen etc.).
- Mobile Geräte dürfen in öffentlich zugänglichen Räumen nicht unbeaufsichtigt gelassen werden.
- Mobile Geräte dürfen Dritten nicht zur Nutzung überlassen werden.
- Der Verlust eines mobilen Gerätes ist unverzüglich der respektive dem ISV zu melden.
- Eine Verbindung zu drahtlosen Netzwerken (z.B. WLAN) ist nur zulässig, wenn eine Verschlüsselung eingesetzt wird.
- Die Ortungsdienste sind bei Nichtgebrauch zu deaktivieren.
- Idealerweise werden die Geräte per Mobile Device Management (MdM) oder Active Sync Policy verwaltet und es besteht die Möglichkeit, die Geräte aus der Ferne zu löschen, z.B. im Falle eines Diebstahls. Die Benutzer/innen sind über die Möglichkeit informiert, dass ihre Geräte im Notfall gelöscht werden könnten, und haben dieser zugestimmt.

7. Protokollierung

Aktivitäten der Benutzerinnen und Benutzer auf den IKT-Systemen der Gemeinde können aus Gründen der Nachvollziehbarkeitspflicht wie auch der Überwachung des richtigen Funktionierens, der Sicherheit, der Integrität und der Verfügbarkeit aufgezeichnet werden.

Diese Protokollierung wird nicht dazu genutzt, das Verhalten von Mitarbeiterinnen und Mitarbeitern zu überwachen.

Sollte rechtswidriges Verhalten festgestellt werden, so können Massnahmen zur Identifizierung der Verfehlenden eingeleitet werden. Eine personenbezogene Auswertung ist nur nach vorgängiger Information der Benutzerin respektive des Benutzers möglich.

8. Verwendung von Wechselmedien

- Der Einsatz von nicht genehmigten Wechselmedien ist verboten.
- Wechselmedien, die klassifizierte Informationen enthalten, müssen gesichert aufbewahrt werden, um den Datenverlust oder -diebstahl zu vermeiden.
- Verluste von Wechselmedien müssen der bzw. dem ISV gemeldet werden.
- Wechselmedien die klassifizierte Informationen enthalten müssen mit einem Passwortschutz versehen und durch Verschlüsselung geschützt werden.
- Wechselmedien die klassifizierte Informationen enthalten müssen zuerst mit einer anerkannten Methode gelöscht werden, bevor sie zum Einsatz kommen.
- Wechselmedien müssen bei der Entsorgung, mit einer anerkannten, sicheren Methode gelöscht oder physisch zerstört werden.
- Eine physische Übergabe von Wechselmedien darf nur an eine autorisierte Person erfolgen und muss protokolliert werden.
- Jede Information, die auf einem Wechselmedium abgelegt ist, muss mindestens auf einem weiteren Medium gesichert sein.

9. Schlussbestimmungen

9.1. Aufhebung früherer Vorschriften und Erlasse

Auf den Zeitpunkt des Inkrafttretens hin werden alle bisherigen, mit diesem Reglement in Widerspruch stehenden Vorschriften und Beschlüsse aufgehoben.

9.2.Strafbestimmungen

Ein widerrechtliches oder weisungswidriges Verhalten im Umgang mit Datenschutz und Informationssicherheit kann straf-, zivil- und/oder personalrechtliche Konsequenzen haben.

Namens des Gemeinderates

Reto Grau	Adrian Hauser
Gemeindepräsident	Gemeindeschreiber

Vom Gemeinderat mit Beschluss vom 21. November 2023 auf den 1. Januar 2024 in Kraft gesetzt.