

Reglement zur Benutzung von Informatikmitteln und zur Überwachung des Vollzugs (Informatikreglement)

vom 30. März 2015

Der Gemeinderat Beinwil am See,

gestützt auf § 12 des Gesetzes über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) vom 24. Oktober 2006¹, die §§ 4 und 5 der Verordnung zum Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (VIDAG) vom 26. September 2007² sowie § 36 des Gesetzes über die Einwohnergemeinden (Gemeindegesetz) vom 19. Dezember 1978³,

beschliesst:

§ 1 Geltungsbereich

1 Dieses Reglement gilt für die Behörden der Gemeinde Beinwil am See, insbesondere die Mitglieder des Gemeinderats, die Mitglieder der gemeinderätlichen Kommissionen sowie die Mitarbeitenden der Gemeindeverwaltung Beinwil am See.

2 In diesem Reglement verwendete Personenbezeichnungen beziehen sich auf beide Geschlechter.

§ 2 Zweck

1 Das Reglement regelt die Benutzung von Informatikmitteln der Gemeindeverwaltung zwecks Gewährleistung der Informationssicherheit als integrierender Bestandteil von Geschäftsprozessen jeglicher Art bzw. der Verfügbarkeit und Vertraulichkeit von Informationen.

2 Das Reglement soll sicherstellen, dass beim Einsatz der Informatikmittel

- a) die technischen Möglichkeiten zur Erfüllung der dienstlichen Aufgaben zweckmässig genutzt werden;
- b) die Datenbestände geschützt und Schäden sowie Missbräuche verhindert werden;
- c) der Schaden infolge Störungen und Problemen minimiert wird;
- d) die Persönlichkeitsrechte der Anwender gewahrt werden.

¹ SAR 150.700

² SAR 150.711

³ SAR 171.100

§ 3 Persönliche Verantwortung

- 1 Alle Anwender sind für die Verwendung der ihnen zur Verfügung gestellten Informatikmittel im Rahmen der geltenden Rechtsordnung und dieses Reglements persönlich verantwortlich.
- 2 Feststellungen über technische Mängel und sicherheitsrelevante Vorkommnisse sind dem Informatikverantwortlichen sofort zu melden.

§ 4 Gebrauch von Informatikmitteln

- 1 Es dürfen grundsätzlich nur die von der Gemeinde bereitgestellten Informatikmittel benutzt werden. Der Einsatz privater Informatikmittel ist nur in besonderen Fällen mit Bewilligung des Informatikverantwortlichen und unter Einhaltung der entsprechenden Sicherheits- und Installationsbestimmungen zulässig.
- 2 Die Informatikmittel dürfen grundsätzlich nur zur Erfüllung dienstlicher Aufgaben benutzt werden.
- 3 Die Verwendung von Informatikmitteln zu nicht kommerziellen privaten Zwecken ist ausnahmsweise zulässig, wenn der Dienstbetrieb dadurch nicht erschwert wird. Es ist die Zustimmung der vorgesetzten Stelle erforderlich.
- 4 Benutzernamen und Passwörter sind persönlich und nicht übertragbar. Die Passwörter sind geheim zu halten und nach Anweisung des Informatikverantwortlichen regelmässig zu ändern.
- 5 Informatikmittel dürfen, mit Ausnahme der speziell für den mobilen Einsatz vorgesehenen Infrastruktur, nicht mit nach Hause genommen werden. Über Ausnahmen entscheidet die Verwaltungsleitung nach Rücksprache mit dem Informatikverantwortlichen.

§ 5 Gebrauch von E-Mail

- 1 Vertrauliche Informationen und Personendaten dürfen nicht ohne Einwilligung des Betroffenen per E-Mail übermittelt werden. Vorbehalten bleibt die Übermittlung über E-Mail-Anschlüsse, die mit entsprechenden Sicherheitseinrichtungen (Verschlüsselung) ausgestattet sind und vom Informatikverantwortlichen bewilligt wurden.
- 2 Private E-Mails, die über das Postfach der Gemeinde verschickt werden, sind im Betreff mit „Privat“ zu kennzeichnen.
- 3 Der Gebrauch privater E-Mail-Adressen ist mit Bewilligung des Informatikverantwortlichen zulässig.

§ 6 Abwesenheitsmeldungen

- 1 Bei Abwesenheiten von mehr als einem Werktag ist eine Abwesenheitsmeldung mit den Kontaktangaben der Stellvertretung und der Dauer der Abwesenheit einzurichten.
- 2 Eintreffende E-Mails sind nicht weiterzuleiten, sondern es ist die Adresse der Stellvertretung in der Abwesenheitsmeldung anzugeben.

§ 7 Unzulässiger Gebrauch der Informatikmittel

- 1 Missbräuchlich ist jede Verwendung der Informatikmittel, die
 - a) gegen dieses Reglement verstösst;
 - b) gegen andere Bestimmungen der Rechtsordnung verstösst;
 - c) Rechte Dritter verletzt.
- 2 Missbräuchlich sind insbesondere folgende Handlungen:
 - a) Einrichten, Anschliessen oder Installation nicht bewilligter Informatikmittel (Hardware) und Verwendung oder Installation nicht bewilligter Programme (Software);
 - b) Versendung von E-Mails in Täuschungs-, Belästigungs- oder Beleidigungsabsicht und private Massensendungen;
 - c) widerrechtliches Downloaden oder Kopieren von Daten oder Software.
- 3 Unzulässige Handlungen sind:
 - a) der Zugriff auf Websites mit sexistischem, rassistischem oder pornografischem Inhalt, Gewaltdarstellungen, Geldspiel- und Börsenseiten, Musik-/Video- und Softwaretauschbörsen, Social Media-Plattformen und dergleichen;
 - b) das Chatten;
 - c) das Downloaden von Software und Daten für private Zwecke;
 - d) das Spielen von (Online-)Games.
- 4 Die Nutzung von Social Media-Plattformen (Facebook, Twitter etc.) als Kommunikationsmittel im Auftrag der Gemeinde ist von dieser Bestimmung ausgenommen.

§ 8 Speicherung von Informationen

- 1 Alle geschäftsrelevanten Daten müssen auf den dafür bestimmten Serversystemen (Laufwerk) gespeichert werden. Es ist nicht erlaubt, geschäftsrelevante Daten dauerhaft auf lokalen Laufwerken oder externen Datenträgern zu speichern.
- 2 Müssen geschäftsrelevante Informationen auf mobilen Informatikmitteln ausserhalb des internen Netzwerks bearbeitet werden, sind die benötigten Daten manuell zu übertragen und zu verwalten (Datenabgleich, Versionierung usw.).
- 3 Persönliche Daten dürfen auf lokalen Laufwerken von mobilen Informatikmitteln gespeichert werden, sofern sie den reibungslosen Betrieb von Informatikmitteln nicht beeinträchtigen. Diese Daten werden nicht gesichert. Bei Störungen oder sicherheitsrelevanten Vorfällen können diese Daten ohne Vorankündigung unwiderruflich gelöscht werden. Die Wiederherstellung und Verfügbarkeit dieser Daten ist somit nicht gewährleistet.
- 4 Persönliche Daten dürfen auf dem persönlichen Serverlaufwerk gespeichert werden. Diese Daten werden regelmässig gesichert.
- 5 Es ist nicht erlaubt, gegen urheberrechtlich (Copyright), durch das Handelsgeheimnis, Patent oder ähnliche Bestimmungen geschützte Rechte von Personen oder Firmen, zu verstossen (geschützte Musik, Bilder, Texte, Software usw.).

§ 9 Kontroll- und Überwachungsmaßnahmen

1 Kontroll- und Überwachungsmaßnahmen dienen in erster Linie der Überprüfung und Gewährleistung der technischen Sicherheit, der Funktionsfähigkeit und der Verfügbarkeit der Informatikmittel.

2 Die Internetzugriffe und der E-Mail-Verkehr der Anwender können aufgezeichnet (protokolliert) werden. Diese Protokolldaten können zur Überprüfung des Vollzugs dieses Reglements verwendet werden.

3 Zur Verhinderung von Missbrauch kann der Zugang zu bestimmten Internet-Adressen durch technische Massnahmen beschränkt oder verhindert werden. Es können Netzwerksüberwachungs- oder Netzwerkanalysewerkzeuge wie z.B. Portscanner oder Sniffer eingesetzt werden. Nicht gestattet ist der Einsatz von Spionageprogrammen.

4 Es können folgende Daten protokolliert werden:

- a) Internetzugriffe: Benutzername, aufgerufene Internet-Adressen, Zugriffszeit, Zugriffsdauer, Grösse des herunter geladenen Files;
- b) E-Mail-Verkehr: Absenderadresse, Empfängeradresse, Betreffzeile, Datum, Zeit, Grösse des E-Mails und allfällige Attachments.

5 Die Protokolldaten gemäss Abs. 4 dieser Bestimmung sind während zwei Monaten aufzubewahren und anschliessend zu vernichten. Zu den Protokolldaten dürfen ausschliesslich die vom Gemeinderat speziell autorisierten Systemverantwortlichen Zugang haben. § 5 Abs. 2 VIDAG bleibt vorbehalten.

6 Der Inhalt privater E-Mails darf ohne Zustimmung der betroffenen Anwender nicht gelesen werden.

§ 10 Sicherheit, Funktionsfähigkeit und Verfügbarkeit der Informatikmittel

1 Für die Anordnung von Kontroll- und Überwachungsmaßnahmen zur Überprüfung und Gewährleistung der technischen Sicherheit, der Funktionsfähigkeit und der Verfügbarkeit der Informatikmittel sowie die Durchführung von entsprechenden Auswertungen ist der Informatikverantwortliche zuständig. Diese Person hat dafür zu sorgen, dass solche Auswertungen nur von den dazu speziell autorisierten Systemverantwortlichen durchgeführt und streng vertraulich behandelt werden.

2 Die Protokolldaten sind in anonymisierter Form auszuwerten. Rückschlüsse auf bestimmte Anwender dürfen nicht möglich sein.

3 Werden Störungen festgestellt, welche die technische Sicherheit, die Funktionsfähigkeit oder die Verfügbarkeit der Informatikmittel erheblich gefährden, dürfen die Protokolldaten ausnahmsweise personenbezogen ausgewertet werden, sofern dies zur Störungsbehebung unumgänglich ist. Die betroffenen Anwender sind über die Tatsache und den Umfang der personenbezogenen Auswertung unverzüglich zu informieren.

4 Bei personenbezogenen Auswertungen hat der Informatikverantwortliche die vorgängige Einwilligung der Verwaltungsleitung einzuholen und erstattet dieser sowie der beauftragten Person für Öffentlichkeit und Datenschutz nachträglich Bericht über die durchgeführte Untersuchung und die allenfalls getroffenen Massnahmen. Kann eine Einwilligung vorgängig nicht eingeholt werden, darf die Auswertung durchgeführt werden, sofern die Gewährleistung der technischen Sicherheit, der Funktionsfähigkeit oder der Verfügbarkeit der Informatikmittel keinen Aufschub erlaubt.

§ 11 Vollzug

1 Der Gemeinderat bestimmt eine für die Informatik verantwortliche Person (Informatikverantwortlicher). Diese ist mit dem Vollzug dieses Reglements beauftragt. Sie kann zur Unterstützung externe Dienstleister beiziehen.

2 Der Gemeinderat kann beim Informatikverantwortlichen mittels der in § 9 Abs. 4 erwähnten Protokolldaten anonyme Plausibilitätskontrollen (Stichproben) über eine jeweils beschränkte Nutzungsdauer durchführen lassen, um den Vollzug dieses Reglements zu überprüfen.

3 Besteht erheblicher Verdacht auf Missbrauch der Informatikmittel, kann der Gemeinderat gegenüber einem begrenzten Personenkreis eine den Betroffenen schriftlich angekündigte, zeitlich befristete Kontrolle durchführen lassen.

4 Die Durchführung der Kontrollen hat unter Aufsicht des Informatikverantwortlichen zu erfolgen. Die beauftragte Person für Öffentlichkeit und Datenschutz ist vorgängig zu informieren, und es ist ihr über die durchgeführte Untersuchung und allfällig getroffene Massnahmen nachträglich Bericht zu erstatten.

5 Die Auswertungsergebnisse werden der Verwaltungsleitung zuhänden des Gemeinderats und, sofern nötig, der vorgesetzten Person des Betroffenen mitgeteilt.

§ 12 Inkrafttreten

1 Dieses Reglement tritt am 1. April 2015 in Kraft.

2 Es ist den Anwendern auszuhändigen.

Beinwil am See, 30. März 2015

Gemeinderat Beinwil am See

Gemeindeammann:
LENZIN

Gemeindeschreiber:
JETZER