Rimnada sistematica da dretg communal dalla vischnaunca da Sagogn

Nummera **0210.01.02**

Tetel **SBOZ Uorden d'informatica**

Ediziun Ediziun 14.02.2020

Valeivel XX.XX.XXXX

Remarcas preliminaras

Ord motivs da simplificaziun serefereschan indicaziuns da persunas, funcziuns e mistregns en questa publicaziun uffiziala mintgamai sin omisduas schlatteinas, expriu ch'ei vegn menziunau explicit zatgei auter.

Davosa correctura informala 06.05.2020 tras Thomas Candrian

Cuntegn

I. Allgemeine Bestimmungen

Um den Umgang mit Informatikmitteln sowie den Informationen und Dokumenten in der Gemeinde Sagogn zu regeln erlässt der Gemeindevorstand gestützt auf Art. 37 Abs. 2 des Gemeindegesetzes des Kantons Graubünden sowie des kantonalen Datenschutzgesetzes folgende Verordnung.

Geltungsbereich

Art. 1

[1] Diese Verordnung gilt für alle Mitarbeiter wie auch für die vom Volk gewählten Behörden und Kommissionen der Gemeinde Sagogn, nachfolgend vereinfacht «Anwender» genannt.

Grundsatz

Art. 2

[1] Die Informations- und Kommunikationsmittel (IKT) sind ein wertvolles und hilfreiches Werkzeug für die Informationsbeschaffung sowie Kommunikation und sollen zum Nutzen der Gemeinde für berufliche Zwecke eingesetzt werden.

[2] Der Gebrauch der IKT birgt jedoch technische, anwendungsmässige und datenschutzrechtliche Risiken, weshalb die ausgeführten Bestimmungen von jedem Anwender strikte eingehalten werden müssen.

[3] Widerhandlungen gegen diese Verordnung führen zu Sanktionen bzw. zu arbeits- und/oder strafrechtlichen Konsequenzen; vorbehalten bleiben Schadenersatzansprüche der Gemeinde gegenüber dem Anwender.

Persönliche Verantwortung

Art. 3

[1] Alle Anwender sind für die Verwendung der ihnen zur Verfügung gestellten Informatikmittel im Rahmen der geltenden Rechtsordnung (insbesondere der Datenschutzverordnung) und dieser Verordnung persönlich verantwortlich.

[2] Technische Mängel und sicherheitsrelevante Vorkommnisse sind dem IT-Verantwortlichen sofort zu melden.

II. Informatikmittel

Benutzerprofile, Benutzernamen und Passwörter

Art. 4

[1] Der IT-Verantwortliche erstellt die Benutzerprofile und weist den Anwendern die entsprechenden Benutzerrechte zu, welche sie zur Erfüllung ihrer Aufgaben benötigen.

[2] Jedem Anwender wird ein persönliches Login und das entsprechende Passwort für den Zugriff auf die Informatikmittel zur Verfügung gestellt. Mit diesen Benutzerinformationen kann auf die erforderlichen Daten und Systeme zugegriffen werden.

[3] Benutzernamen und Passwörter sind persönlich und nicht übertragbar. Benutzerkennungen und Passwörter sind geheim zu halten und dürfen unter keinen Umständen schriftlich aufbewahrt werden.

Software

Art. 5

[1] Der Anwender ist verpflichtet, ausschliesslich nur solche Software auf den Informatikmitteln einzusetzen, für die eine gültige Nutzungslizenz vorliegt.

[2] Anwender dürfen Software aus dem Internet nur mit ausdrücklicher Genehmigung des IT-Verantwortlichen downloaden und auf gemeindeeigenen Informatikmitteln installieren. Dies gilt nicht für den Bezug von Software für Mobilgeräte (Smartphone, Tablets) aus vertrauenswürdigen Quellen wie Google Play Store oder Apple App Store.

Private Nutzung

Art. 6

[1] Durch Kontroll- und Überwachungsmassnahmen könnten personenbezogene Daten der Anwender erfasst werden. Um die Erfassung von persönlichen Daten der Anwender auf ein Minimum zu reduzieren sollen die Informatikmittel deshalb nicht für privaten Gebrauch benutzt werden. Die Ablage von persönlichen Daten ist untersagt.

[2] Befolgt der Anwender diese Regelung nicht, kann er die Gemeinde nicht haftbar für allfällige Folgen seines Handelns machen.

III. Besondere Systeme

Email

Art. 7

[1] E-Mail ist ein modernes und schnelles Mittel der Kommunikation, ist jedoch kein geschütztes Medium und kann von Dritten eingesehen werden. Besonders schützenswerte Personendaten dürfen deshalb nicht ohne Einwilligung des Betroffenen per E-Mail übermittelt werden. Davon ausgenommen sind Übermittlungen an Amtsstellen und Behörden.

[2] Das Versenden von privaten E-Mails ist nur zulässig, wenn diese klar in der Betreffzeile mit «[PRIVAT]» (ohne Anführungszeichen) gekennzeichnet sind. Der Zugriff auf Mailpostfächer der Gemeinde sind durch den IT-Verantwortlichen jederzeit möglich, er darf jedoch die so gekennzeichneten Mails nicht einsehen.

Nutzung WLAN

Art. 8

[1] In den Gebäuden der Gemeinde ist ein zugriffgeschütztes WLAN eingerichtet. Für den Zugriff auf das WLAN gelten alle Nutzungs- bzw. Sicherheitsbestimmungen gemäss dieser Verordnung. Die Zugangsdaten werden vom IT-Verantwortlichen resp. dessen Stellvertreter verwaltet und herausgegeben und dürfen nicht weitergegeben werden.

[2] Das WLAN «sagogn_public» kann von den Anwendern und Gästen gratis verwendet werden. Der Zugriff ist auf das Internet limitiert. Die Verfügbarkeit ist nicht garantiert.

[3] Das WLAN «sagogn_verw» darf ausschliesslich von Anwendern gem. Einleitung verwendet werden. Dies ist ein separiertes Netz, welches Zugriff auf bestimmte Geräte (Drucker und Datenspeicher) ermöglicht.

[4] Das WLAN «sagogn_scola» darf ausschliesslich von der Lehrerschaft der Primarstufe Sagogn verwendet werden. Dies ist ein separiertes Netz, welches Zugriff auf bestimmte Geräte (Drucker und Datenspeicher) ermöglicht.

Speichersystem

[1] Grundsätzlich müssen sämtliche Daten der Gemeinde auf dem dafür vorgegebenen Speichersystem abgelegt werden. Es ist insbesondere verboten, nicht freigegebene Cloudspeicherdienste im Internet für geschäftliche Daten zu nutzen, z.B. Dropbox, OwnCloud, iCloud oder OneDrive.

[2] Daten, welche sich lokal auf einem Client Computer befinden, können nicht gesichert werden. Sämtliche Daten und Dokumente, die der Gemeinde gehören, müssen daher zwingend auf dem von der Gemeinde vorgegebenen Speicher abgelegt werden. Ausnahmen können in begründeten Fällen durch den IT-Verantwortlichen bewilligt werden.

[3] Der Zugriff auf Daten der Gemeinde von privaten Computern ist erlaubt, soll soweit möglich vermeiden werden. Zugriff über Geräte von Dritten ist aus Sicherheitsgründen nicht gestattet.

[4] Daten der Gemeinde dürfen aus Datenschutz-, Amtsgeheimnis- und Sicherheitsgründen nicht auf Geräte abgelegt werden, die nicht vollständig der Kontrolle des jeweiligen Anwenders unterstehen (z.B. PC des Arbeitgebers).

IV. Datensicherheit

Datenschutz und Datensicherheit

Art. 9

[1] Computerausdrucke oder Kopien mit sensiblen Informationen dürfen nicht für Unbefugte frei zugänglich aufbewahrt werden, z.B. beim Kopierer. Solche Dokumente müssen sicher verwahrt oder zuverlässig vernichtet werden.

[2] Die Gemeindeverwaltung trifft im Hinblick auf den Datenschutz organisatorische und technische Massnahmen, damit die Daten angemessen geschützt sind.

[3] Computer müssen beim Verlassen des Arbeitsplatzes gesperrt werden (bei Windows z.B. „Windows-Taste + L").

[1] Der IT-Verantwortliche ist dafür besorgt, dass Server, Clients sowie alle weiteren Informatikmittel über ausreichenden Schutz vor Viren etc. verfügen.

[4] Zur Verhinderung von Missbrauch kann der Zugang zu bestimmten Internet-Adressen oder anderen Datenquellen durch technische Massnahmen beschränkt oder verhindert werden.

Datensicherung

Art. 10

[1] Der IT-Verantwortliche ist zuständig für die Sicherung aller Daten vor Manipulation oder Verlust und erstellt regelmässig Backups der Daten. Die Datensicherungen haben mindestens zweimal pro Woche zu erfolgen und die Datensicherung muss an einem anderen Ort aufbewahrt werden.

Kontroll- und Überwachungsmassnahmen

Art. 11

[2] Um die Sicherheitsanforderungen der Gemeinde zu gewährleisten (z.B. Schutz vor operationellen und rechtlichen Risiken, Interessen und Ruf der Gemeindeverwaltung) kann der IT-Verantwortliche periodisch die Benutzung der Informations- und Kommunikationsmittel unter Wahrung datenschutzrechtlicher Bestimmungen überprüfen.

[3] Für die Anordnung von Kontroll- und Überwachungsmassnahmen sowie die Durchführung von entsprechenden Auswertungen ist der IT-Verantwortliche zuständig. Diese Person hat dafür zu sorgen, dass solche Auswertungen nur von dazu autorisierten Personen durchgeführt und vertraulich behandelt werden.

[4] Werden Manipulationen oder Störungen festgestellt, welche die Sicherheit, die Funktionsfähigkeit oder die Verfügbarkeit der Informatikmittel gefährden, werden die Anwenderinnen und Anwender über diese Tatsache sowie der zu treffenden Massnahmen informiert.

[5] Wurden bei Kontroll- und Überwachungsmassnahmen personenbezogene Daten erfasst, so werden die Anwenderinnen und Anwender über diese Tatsache und den Umfang der personenbezogenen Auswertung informiert.

Gefährdung

Art. 12

[1] Besteht begründeter Verdacht auf Missbrauch der Informatikmittel für eine oder mehrere bestimmte Personen, kann der IT-Verantwortlichen gegenüber diesem begrenzten Personenkreis ohne Ankündigung eine zeitlich befristete Kontrolle durchführen bzw. durchführen lassen. Um rechtswidrige Überwachungsmassnahmen zu verhindern müssen diese mit der Polizei abgestimmt werden.

[2] Der Gemeindevorstand ist über die durchgeführte Untersuchung und allfällig getroffene Massnahmen zu informieren und beaufsichtigt diese.

[3] Die Auswertungsresultate werden dem Gemeindevorstand und, sofern nötig, der vorgesetzten Person der oder des Betroffenen mitgeteilt.

V. Schluss- und Übergangsbestimmungen

Kontrolle

Art. 13

[1] Der Gemeindevorstand kontrolliert und überwacht die Einhaltung der Bestimmungen dieser Verordnung.

[2] Die Geschäftsprüfungskommission hat das Recht, jederzeit in den Umgang der Anwender mit den Daten Einsicht zu nehmen.

Inkrafttreten

Art. 14

[1] Die vorliegende Verordnung tritt auf den XX.XX.2020 in Kraft.

Ediu tras			
Acceptau tras	Suprastonza communala	**ils**	XX.XX.XXXX
Acceptau tras		**ils**	
Publicaziun ufficiala dalla vischnaunca da Sagogn.			

Anhang 1: Richtlinien für Social Media

Social Media helfen, mit Menschen in Kontakt zu bleiben, vereinfachen die Kommunikation und helfen transparente, authentische Unternehmensbilder zu zeichnen. Doch bei allen Vorteilen bergen Social Media auch Risiken. Deshalb ist ein verantwortungsbewusster Umgang im geschäftlichen wie auch privaten Alltag wichtig.

Denken Sie immer daran, dass alles in den Social Media, was Sie eingeben, auch recherchiert werden kann, beruflich wie privat (Facebook, Twitter, YouTube, Google, Xing, Blogs usw.). Anbei einige Regeln:

- **Wer veröffentlicht übernimmt Verantwortung**. Sie sind für Ihre veröffentlichten Meinungsäusserungen selbst verantwortlich. Jede Veröffentlichung kann von Kunden, Partnern oder Journalisten aber auch von Vorgesetzten, Kollegen oder ehemaligen Anwendern gelesen werden. Eine Veröffentlichung bleibt immer im Internet bestehen. Diese zu löschen ist fast unmöglich und kann weitreichende Konsequenzen haben.

- **Schonen Sie Ihre Geschäftsbeziehungen**. Selbst wenn Bürger oder Partner Ihnen Stress und Ärger bereiten, sollten Sie niemals Ihren persönlichen Frust in der Öffentlichkeit ablassen. Respektloses über Bürger oder Partner zu verbreiten ist tabu.

- **Verraten Sie keine Geschäftsgeheimnisse**. Schreiben Sie nichts, was nicht für Aussenstehende bestimmt ist. Wenden Sie sich im Zweifelsfall an Ihre Vorgesetzten oder die entsprechende Stelle.

- **Seien Sie authentisch**. Geben Sie sich immer mit vollständigem Vor- und Nachnamen, Funktion und Gemeindenamen zu erkennen, sofern die veröffentlichten Inhalte Ihre Arbeit betreffen. Machen Sie zu Ihrem eigenen Schutz und dem Schutz der Gemeinde deutlich, wenn Sie sich als Privatperson äussern.

- **Umgangston**. Behandeln Sie andere Nutzer so, wie Sie selbst behandelt werden möchten. Argumentieren Sie in der Sache nie mit persönlichen Angriffen oder Argumenten, die sich auf Personen beziehen. Beleidigungen, Sexismus oder rassistische Äusserungen sind gesetzlich untersagt.

- **Offen mit Fehlern umgehen**. Jeder macht mal Fehler. Fehler oder Fehleinträge müssen aber aktiv und konstruktiv kommentiert werden. Sprechen Sie im Zusammenhang mit der Gemeinde im Zweifelsfall mit Ihrem Vorgesetzten oder der entsprechenden Stelle. Einen Fehler einzugestehen ist besser als der Versuch der Rechtfertigung, Vertuschung oder deren Löschung.

- **Social Media Einsatz während der Arbeitszeit**. Die private Nutzung von Social Media während der Arbeitszeit ist untersagt. Die geschäftliche Nutzung ist mit Ihren Vorgesetzten zu klären.