REGION MALOJA
REGIUN MALÖGIA
REGIONE MALOJA

ICT-Benutzerreglement
(Informations- und Kommunikationsinfrastruktur)
Weisung zur Nutzung der ICT-Mittel und zu deren Überwachung

Art. 1 - Einleitung

Grundsatz

1) Die Informations- und Kommunikationsmittel (wie z.B. Tablets, Computer, Smartphones, Internet, E-Mail, Telefon, Chat o.ä.) sind ein wertvolles und hilfreiches Werkzeug für die Informationsbeschaffung sowie Kommunikation und sollen zum Nutzen der Region für berufliche Zwecke eingesetzt werden.

Risiken
Sanktionen
Schadensersatz

2) Der Gebrauch der Informations- und Kommunikationsmittel birgt technisch, anwendungsmässig und datenschutzrechtlich Risiken, weshalb die im vorliegenden Reglement ausgeführten Bestimmungen von jedem Anwender (d.h. Nutzer/-in der regionseigenen Informations- und Kommunikationsinfrastruktur) strikt eingehalten werden müssen. Widerhandlungen bzw. reglementwidrige Benützung dieser Mittel führen zu Sanktionen, bzw. zu arbeits- und/oder strafrechtlichen Konsequenzen; vorbehalten bleiben bei fahrlässigem Umgang und Verschulden des Nutzers Schadenersatzansprüche der Region gegenüber dem Nutzer.

Art. 2 - Nutzung der Informations- und Kommunikationsmittel

Allgemeinverbind-lichkeit

1) Jeder Anwender anerkennt mit Nutzung der resp. seiner Ausstattung mit Informations- und Kommunikationsmitteln dieses allgemein zugängliche Reglement. Es ist als allgemein verbindliche Weisung integrierter Bestandteil des Arbeits- und/oder Werkvertrages resp. als akzeptierte Bestimmung bei jeder Nutzung der Informations- und Kommunikationsmittel anzusehen.

Passwort

2) Die Anwender sind verantwortlich für die sorgfältige und vor Beschädigung, Diebstahl und/oder Verlust geschützte Aufbewahrung und Anwendung der vorhandenen Zugangskontrolleinrichtungen und -massnahmen (z.B. Passwort, Passwortwahl, -aufbau und -verwahrung usw.). Dabei sind die technischen Passwortrichtlinien zu beachten.

a) Jedes Passwort wird technisch mit einem Ablaufdatum versehen, welches im Normalfall 90 Tage beträgt. Kurz vor Ablauf dieser Zeit wird der Anwender auf das ablaufende Passwort hingewiesen und gebeten dieses zu erneuern. Ist das Kennwort abgelaufen, wird der Anwender bei nächster Anmeldung gezwungen das Passwort zu ändern. Zu beachten ist, dass bei abgelaufenem Passwort das Abrufen von E-Mails via Smartphone etc. und/oder das Login von extern sowie das interne Login über Notebooks oder ThinClients (Anwendung für den Zugriff auf den Terminalserver) nicht mehr möglich ist.

b) Bei der Definition eines neuen Passworts, wird technisch sichergestellt ob es den angeforderten Sicherheitsstandards entspricht. Zusätzlich zu den Standardanforderungen wie der passenden Komplexität und der Mindestlänge von sieben Zeichen, wird eine Passwort-Chronik von zehn Passwörtern hinterlegt, was ein wiederverwenden desselben Passworts verhindert.

Beschränkung von Zugang und/oder Nutzung

3) Der Zugang zu den und/oder die Nutzung der Informations- und Kommunikationsmitteln stellt keinen Rechtsanspruch dar und kann jederzeit ohne Angabe von Gründen entzogen werden. Die Region kann Quellen wie z.B. Webseiten mit ungeeigneten Inhalten (bspw. pornografisch, rassendiskriminierend, unethisch, unmoralisch) oder mit erkennbaren Risiken für die Region (Malwaregefahr o.ä.) durch technische Massnahmen vom Zugang und / oder der Nutzung ausschliessen. Über die Sperrmassnahmen kann jederzeit durch die Geschäftsstelle ohne Kommunikation und / oder Angabe von Gründen entschieden werden.

4) Beim Verlassen des Arbeitsplatzes muss ein Passwortschutz gesetzt werden.

Art. 3 - Nutzung von privater Infrastruktur innerhalb der Regionsinfrastruktur

Grundsatz

1) Die Installation von privater Hard- und/oder Software auf den regionseigenen Systemen ist grundsätzlich untersagt und wird ggf. technisch unterbunden.

Spezialfälle

2) In speziellen Fällen, sofern die geschäftliche Nutzung begründet ist und keine regionseigene Lösung zur Verfügung gestellt wird, ist die ausdrückliche und vorgängige, schriftliche Zustimmung der Geschäftsstelle zusammen mit dem Amtsstellenleiter erforderlich. Diese Zustimmung kann bei Vorliegen wichtiger Gründe jederzeit durch die Geschäftsstelle zusammen mit dem Amtsstellenleiter wieder entzogen werden.

Ausnahme

3) Von der in Absatz 2) genannten Zustimmungspflicht ausgenommen ist die Installation von privat bezahlten Apps auf Smartphones und/oder Tablets etc., sofern diese aus vom Plattformhersteller offiziell freigegebener Quelle stammen, d.h. bspw. Google Play oder Apples App Store.

Vergütung

4) Allgemein besteht keine Pflicht der Region, die unter Verwendung des privaten Accounts (wie z.B. Apple-ID) bezogenen und/oder gekaufter Apps zu vergüten, auch wenn die Nutzung beruflichen Zwecken dient. Die Region kann Beiträge sprechen, die über den Spesenprozess abgerechnet werden, wenn die Geschäftsstelle zusammen mit dem Amtsstellenleiter dem vorgängig zustimmt.

Art. 4 - Anwendungsbereich berufliche Nutzung

Grundsatz der beruflichen Nutzung

1) Internet, Telefonie, Telefax und E-Mail etc. sind in erster Linie für geschäftliche Zwecke, d.h. zur Erfüllung der zugewiesenen beruflichen Aufgaben im Sinne der Region einzusetzen.

Internet

2) Folgende Grundsätze gelten für die Nutzung des Internets:

Zugangsvorrichtungen

a) Die Anwender sind verantwortlich für die sorgfältige und vor Beschädigung, Diebstahl und/oder Verlust geschützte Aufbewahrung und Anwendung der vorhandenen Zugangskontrolleinrichtungen und –massnahmen (z.B. Passwort, Passwort-Verwahrung usw.).

Persönlichkeit der Zugangsmittel

b) Wo nicht speziell bezeichnet, sind Zugangsdaten (Benutzerkennungen, Passwörter etc.) persönlich und dürfen grundsätzlich nicht weitergegeben werden.

Dienste

c) Über die zur Verfügungsstellung von den unterschiedlichen im Internet angebotenen Diensten und/oder Protokollen (inkl. Cloudlösungen) entscheidet die Geschäftsstelle. Es besteht kein Anspruch auf die Nutzung spezieller Dienste und/oder Protokolle.

d) Die Nutzung von Social Media wie Twitter, Facebook o.ä. und Chat-Dienste wie z.B. Skype o.ä. ist - ausser bei explizit dafür zuständigen und bezeichneten Stellen zur beruflichen Nutzung - grundsätzlich als private Nutzung einzustufen. Die Region kann daher deren Nutzung begrenzen und/oder unterbinden. Über die Einschränkung entscheidet die Geschäftsstelle. *Social Media*

3) Folgende Grundsätze gelten für die Nutzung von E-Mail: *E-Mail*

a) E-Mail ist zur Beschleunigung, Vergünstigung und Vereinfachung von Vorgängen gegenüber der Briefpost und Fax vorrangig zu nutzen, sofern technische, rechtliche oder wirtschaftliche Gründe dem nicht entgegenstehen. *Primat der Kommunikationsform*

b) Der Anwender muss den elektronischen Briefkasten täglich auf den Eingang von E-Mails kontrollieren. *Kontrollpflicht*

c) Bei Absenzen ist der Abwesenheitsassistent einzuschalten und den Zeitraum der Abwesenheit anzugeben. Bei gegebener und definierter Stellvertretung ist diese ebenfalls anzugeben. *Absenzen*

d) Die automatische Umleitung von E-Mails ins Internet (z.B. bei Abwesenheiten) an nicht regionseigene E-Mail-Adressen (z.B. die eigene private Mailbox) ist aus Gründen der Datensicherheit und des Datenschutzes grundsätzlich nicht erlaubt und wird technisch unterbunden. *Grundsatz Automatische Weiterleitung*

e) Bei nachgewiesenem, beruflichem Bedarf stellt die Region den Zugang auf die Infrastruktur von ausserhalb des Regionsperimeters zur Verfügung; es entscheidet die Geschäftsstelle zusammen mit dem Amtsstellenleiter. *Externer Zugriff*

f) Werden die Nachrichten, welche auf persönliche E-Mail-Adressen gesandt wurden, während der Abwesenheit durch Dritte gelesen und/oder weitergeleitet, so sind die Absender mittels Abwesenheitsmeldung darüber zu informieren. *Weiterleitungsbenachrichtigung*

g) Personenbezogene oder anderweitig vertrauliche Informationen dürfen grundsätzlich nicht unter Ausübung einer beruflichen Funktion in oder für die Region übertragen werden, weil die Sicherheit bei der Übertragung nicht gewährleistet werden kann. Dies gilt nicht nur für den Inhalt der E-Mail, sondern auch für beigefügte Dokumente/Anlagen (Attachments). Bei Bedarf stellt die Informatikabteilung Verschlüsselungssoftware und/oder Dienste wie IncaMail (eingeschriebene E-Mails) mit entsprechender Kostenfolge zur Verfügung; es entscheidet die Geschäftsstelle zusammen mit dem Amtsstellenleiter. *Schützenswerte Information*

h) Das Übermitteln von potenziell schädlichen Daten und/oder Containern für Maleware (z. B. ausführbare Programme etc.) ist grundsätzlich nicht zulässig. Ausgenommen davon ist das für berufliche Zwecke notwendige Versenden durch berechtigte Personen. Das Senden und Empfangen potenziell schädlicher Software wird technisch unterbunden. *Einschränkung / Malware*

i) Die allgemein anerkannte Netiquette und/oder die gesetzlichen Vorschriften sind einzuhalten. So dürfen z.B. Newsletters etc. nur bei Vorliegen der vorgängig durch den Empfänger gegebenen Einverständniserklärung verschickt werden. *Newsletter*

j) Die Auslösung oder Weiterleitung von „Kettenmails“ und/oder sog. Spass-E-Mails mit Witzen, Multimediainhalten etc. ist grundsätzlich nicht erlaubt. *Kettenmails*

k) Wo immer möglich sind Hyperlinks zu verschicken oder Cloudlösungen zu wählen, die von der Informatikabteilung zur Verfügung gestellt werden und offiziell zur Nutzung freigegeben sind. *Hyperlinks*

Archivierung

l) Alle eingehenden und ausgehenden Nachrichten werden gemäss den gesetzlichen Vorschriften über die geschäftliche Kommunikation inkl. Anhänge für 10 Jahre durch die Anwender nicht veränder- und/oder löschbar archiviert.

Löschung

m) Um Speicherplatz und damit Kosten zu sparen, werden E-Mails nach 270 Tagen automatisch aus der primären E-Mail-Umgebung gelöscht und sind nur noch im Archiv verfügbar, d.h. über z.B. Smartphones und Tablets nicht mehr erreichbar. Die durch den Anwender gelöschten Nachrichten werden täglich aus der primären Umgebung gelöscht und befinden sich nur noch im E-Mail-Archiv.

Private Kommunikation

n) Private Kommunikation soll grundsätzlich ausserhalb der Geschäfts- und Arbeitszeit erfolgen. In Ausnahmefällen und in vertretbarem Ausmass ist diese über die von der Regionsinfrastruktur zugänglichen Dienste wie GMX, Bluewin o.ä. abzuwickeln.

Persönlichkeit

o) Die persönlich zugeteilten Geschäfts-E-Mail-Adressen sind grundsätzlich persönlich und werden durch Dritte im Normalfall nicht eingesehen. Falls geschäftlich notwendig, können diese Postfächer nach Freigabe der Geschäftsstelle zusammen mit dem Amtsstellenleiter gesichtet, protokolliert und analysiert werden.

Mittarbeiteraustritt

p) Bei Austritt eines Mitarbeiters und/oder Beendigung des Auftrages resp. Werks eines Anwenders wird die E-Mail-Adresse noch während einer von der Region bezeichneten Zeit aufrechterhalten und durch Dritte gesichtet. Dabei besteht kein Anspruch, dass private Inhalte dem Anwender weiterhin zugestellt werden.

Telefonie

4) Folgende Grundsätze gelten für die Nutzung der Telefonie:

Wirtschaftlichkeit

a) Die Anwender sind grundsätzlich verpflichtet, Telefonie-Services in der wirtschaftlich günstigsten Alternative zu nutzen.

Abgeltung privater Gespräche

b) Übermässige und/oder teure Privattelefonie (z.B. Überseegespräche) über Geschäftsnummern ist nicht zulässig.

Datenverkehr

c) Der Datenverkehr über Mobilgeräte soll sich grundsätzlich im Rahmen des monatlich inkludierten Datenvolumens bewegen. Dies gilt es insb. bei Nutzung von Tethering-Funktionalitäten (Modem) zu beachten.

Datenroaming

d) Auf Datenroaming bei Mobilgeräten (z.B. für die Synchronisation der E-Mail mit grossen Anhängen etc.) im Ausland ist grundsätzlich zu verzichten und nur in Ausnahmefällen zurückzugreifen.

SMS/MMS

e) Die Nutzung von kostenpflichtigen SMS und/oder MMS etc. ist im Regelfall privater Natur und daher auf ein vertretbares Mass zu beschränken.

Vergütung

f) Die Region ist nicht verpflichtet, über private Telefone geführte Gespräche am Arbeitsplatz zu vergüten, da genügend verfügbare Regionstelefoninfrastruktur zur Verfügung steht.

Datenauswertung

g) Die Region behält sich bei wichtigen Gründen und nach Freigabe der Geschäftsstelle zusammen mit dem Amtsstellenleiter vor, die Telefondaten der Anwender zu sichten, zu speichern und/oder zu analysieren.

Inhaber Mobilnummer

h) Falls die Region ein Mobiltelefon zur Verfügung stellt und Inhaberin der zugeteilten Mobiltelefonnummer ist, besteht bei Austritt des Mitarbeiters / Anwenders kein Anspruch auf Privatübernahme der Mobiltelefonnummer und / oder des Gerätes. Dies gilt ebenfalls, wenn Anwender seine private Mobiltelefonnummer der Region übergibt oder übergeben hat. Über Ausnahmen entscheidet die Geschäftsstelle.

SIM-Karten

i) Es ist nicht zulässig Region-SIM-Karten ohne vorgängige Genehmigung es Amtsstellenleiters in privaten Geräten zu betreiben.

Modelle / Vertragsverlängerung

j) Es besteht kein Anspruch der Anwender auf die Ausstattung mit regionseigener Infrastruktur zur mobilen Telefonie resp. die Region kann über die zur Verfügung gestellten Modelle, Vertragsverlängerungen etc. entscheiden.

Eigenständige Verlängerung

k) Die autonome Vertragsverlängerung bei Geräten zur mobilen Telefonie ist verboten und durch die Region unterbunden.

Austritt

l) Der Anwender ist verpflichtet vor Austritt und/oder Rückgabe der Geräte die Kontaktdaten zu bereinigen und rein private Kontaktdaten zu löschen; wenn möglich sind die Geräte auf Werkseinstellungen rückzusetzen.

Art. 5 - Sorgfaltspflicht

Nutzung / Wartung

1) Die Anwender sind verpflichtet die Regionsinfrastruktur sorgfältig zu behandeln und gemäss Herstellervorschrift/-empfehlung zu nutzen, zu bedienen, zu reinigen und zu warten.

Schadenersatz

2) Wird dem nicht nachgekommen und/oder Infrastruktur mutwillig und/oder fahrlässig beschädigt, kann die Region Schadenersatz geltend machen.

Art. 6 - Datenspeicherung

Grundsatz

1) Sämtliche in elektronischer Form vorliegende Geschäftsdaten sind ausschliesslich auf gesicherten Laufwerken bspw. Laufwerk O:\ der Region zu speichern und abzulegen. Es ist insbesondere verboten, nicht freigegebene Cloudspeicherdienste im Internet für geschäftliche Daten zu nutzen.

Dritte

2) Geschäftliche Daten dürfen nur berechtigten Dritten zur Verfügung gestellt werden.

Temporäre Speichermedien

3) Der Anwender ist verantwortlich, dass die Sicherheit von geschäftlichen Daten, die temporär und begründet auf anderen, nicht gesicherten Speichern - wie z. B. USB-Sticks etc. - abgelegt sind, jederzeit vollumfänglich gewährleistet ist.

Private Daten

4) Private Daten dürfen nicht, auch nicht temporär, auf geschäftlichen Speichern abgelegt werden. Die Region kann dafür spezielle Bereiche auszeichnen bspw. Laufwerk P:\, haftet aber in keiner Weise für Beschädigung und/oder Verlust von privaten Daten. Bei Austritt eines Mitarbeiters und/oder Beendigung des Auftrages resp. Werks eines Anwenders werden die privaten Daten noch während einer von der Region bezeichneten Zeit aufrechterhalten und durch Dritte gesichtet. Dabei besteht kein Anspruch, dass private Inhalte dem Anwender zugestellt werden.

Kontingent

5) Das persönliche Laufwerk ist für jeden Anwender auf 250 MB beschränkt. Die Überschreitung dieses Kontingents wird technisch unterbunden.

Fotos/Videos

6) Grosse Dateien bspw. Fotos und/oder Videos dürfen nicht auf geschäftlichen Speichern abgelegt werden. Die Region kann dafür spezielle Bereiche auszeichnen bzw. es werden dafür geeignete ICT-Mittel zur Verfügung gestellt.

Art. 7 - Private Nutzung

Grundsatz

1) Die private Benützung der Informations- und Kommunikationsinfrastruktur ist als Ausnahme zu betrachten, zu beschränken und vernünftig zu betreiben.

Verhältnismässigkeit

2) Die Vorgesetzten haben das Recht die übermässige private Nutzung zu unterbinden und disziplinarisch zu ahnden.

Haftung

3) Die Region lehnt jegliche Ansprüche der Anwender für erlittenen Schaden durch die private Nutzung der Informations- und Kommunikationsinfrastruktur ab.

Art. 8 - Unangemessene Nutzung

1) Die Benützung der Informations- und Kommunikationsinfrastruktur muss unter Berücksichtigung der Interessen der Regionsverwaltung erfolgen, wobei insbesondere rechtliche und operationelle Risiken auszuschliessen sind. Es ist insbesondere verboten, auf Material mit widerrechtlichem, urheberrechtsverletzendem, rassistischem, beleidigendem, pornografischem oder herabwürdigendem Inhalt zuzugreifen, oder solches zu verbreiten

Art. 9 - Herunterladen von Informationen (Download)

Urheberrechts-schutz

1) Den Anwendern ist es untersagt, Software oder urheberrechtsgeschützte Inhalte aus dem Internet herunterzuladen oder zu installieren. Das Herunterladen und Installieren von Software aus dem Internet könnte Urheberrechte Dritter verletzen und somit widerrechtlich sein oder die Sicherheit des Netzwerkes der Regionsverwaltung beeinträchtigen.

2) Andere Daten oder Dateien (einschliesslich solcher mit Multimediainhalten) dürfen nur unter den folgenden Bedingungen auf das Netzwerk der Regionsverwaltung heruntergeladen werden:

Geschäftsrele-vanz / Lizenzen

a) Die Daten oder Dateien müssen geschäftsrelevant sein und unter Einhaltung aller Anforderungen der Regions(-verwaltung) sowie den gesetzlichen Bestimmungen beschafft oder verwendet werden.

Firewall

b) Die Daten oder Dateien dürfen nicht an den Sicherheitsvorkehrungen vorbeigeschleust (z.B. Firewall, Contentfilter, Malwarescanner etc.) werden. Dies gilt insb. beim Transfer/Upload über portable Speichermedien wie z.B. USB-Sticks.

Art. 10 - Benutzung von interaktiven Medien

Chatroom

1) Interaktive Medien des Internets (z.B. Chat-Rooms) machen es den Teilnehmern möglich, Mitteilungen zur gleichen Zeit an eine Vielzahl unbekannter Empfänger zu versenden. Da die elektronische Kommunikation von Anwendern den Namen der Region im Absender trägt, birgt die unkontrollierte Benutzung dieser Medien durch Anwender rechtliche Risiken für die Region sowie Risiken für ihren Ruf. Anwender dürfen deshalb interaktive Medien auf dem Internet für geschäftliche Zwecke nach Freigabe durch den Amtsstellenleiter nutzen.

Pay-Services

2) Kostenpflichtige Informationsdienste aus dem Internet dürfen nur mit der Einwilligung der Geschäftsstelle zusammen mit dem Amtsstellenleiter abonniert werden.

Art. 11 - Sicherheitsrelevante Ereignisse (Awareness)

Meldung

1) Alle sicherheitsrelevanten Ereignisse (z.B. unerklärliches Systemverhalten, Verlust oder Veränderung von Daten und Programmen, Verfügbarkeit nicht explizit freigegebener Dienste, Verdacht auf Missbrauch der eigenen Benutzerkennung usw.) sind sofort der Geschäftsstelle und dem Amtsstellenleiter zu melden.

Eigene Nachfor-schungen

2) Es sind keine eigene Aufklärungsversuche zu unternehmen, weil dabei allenfalls wertvolle Hinweise und Spuren verwischt werden oder verloren gehen können.

Art. 12 - Kontrolle und Protokollierung

Protokollierung

1) Im Interesse und zum Schutze des Rufes der Regionsverwaltung ist es entscheidend, dass die Anwender die Bestimmungen dieses Reglements unbedingt befolgen. Das Verhalten des einzelnen Anwenders im Internet ist nicht anonym und kann jederzeit bis zu ihm selbst zurückverfolgt werden und wird automatisch protokolliert. Die Umgehung der Protokollierung durch z. B. Nutzung von Anonymisern und/oder fremden Proxys (Kommunikationsschnittstellen) ist verboten und führt bereits bei erstmaligem Verstoss verwarnungslos zu Disziplinarmassnahmen.

Anonymisierte Überprüfung

2) Um die Sicherheitsanforderungen der Region(-verwaltung) zu gewährleisten (z.B. Schutz vor operationellen und rechtlichen Risiken, Interessen und Ruf der Regionsverwaltung) kann die Geschäftsstelle zusammen mit dem Amtsstellenleiter periodisch die Benutzung der Informations- und Kommunikationsmittel unter Wahrung datenschutzrechtlicher Bestimmungen überprüfen. Diese Überprüfung auf Stufe des Einzelbenutzers erfolgt aber nur bei Vorliegen von Verdachtsmomenten und nach vorgängiger Genehmigung der Geschäftsstelle zusammen mit dem Amtsstellenleiter.

Kontrollzweck

3) Die Protokollierung berücksichtigt die Grundsätze des gültigen Datenschutzgesetzes des Kantons Graubünden und den Schutz der Privatsphäre im Rahmen der weiteren anwendbaren gesetzlichen Bestimmungen. Die Protokolldaten dienen ausschliesslich zu Zwecken der Datenschutzkontrolle, der IT-Revision, der Datensicherung und zur Sicherstellung eines ordnungsgemässen Betriebes. Sie werden nicht für Zwecke einer Verhaltens- oder Leistungskontrolle verwendet, sofern keine Indizien für ein nicht arbeitsvertrags- und/oder werkvertragskonformes Verhalten (wie z.B. übermässige private Nutzung) vorliegen.

Zugriff für Administratoren

4) Damit der Support für jeden Anwender den grösstmöglichen Nutzen erzielen kann, werden die Systemdaten für den Administrator (i-community) nicht anonymisiert und der Administrator hat Zugriff auf sämtliche E-Mail-Postfächer, Archive, geschäftliche Daten-Speicher o.ä. sowie auf Protokolldateien bspw. Contenfilter usw. Der Zugriff wird nur für den Support genutzt und nur beim Vorliegen eines entsprechenden Helpdesk-Tickets. In speziellen Fällen wird seitens Support mit der Geschäftsstelle sowie dem Amtsstellenleiter Rücksprache gehalten und eine allfällige schriftliche Befugnis eingeholt.

Art. 13 - Sanktionen

1) Eine widerrechtliche, reglementwidrige oder unangemessene Benützung der Informations- und Kommunikationsmittel oder jedes andere Verhalten, das einen Verstoss gegen die Pflichten aus dem Arbeitsverhältnis darstellt, können arbeits- und/oder disziplinarrechtliche Sanktionen zur Folge haben. Im Wesentlichen gelten die gültigen personalrechtlichen Bestimmungen der Region.

Art. 14 - Inkrafttreten / Übergangsbestimmungen

Dieses Reglement tritt mit der Genehmigung durch die Präsidentenkonferenz am 1. Januar 2018 in Kraft.

Genehmigt an der Präsidentenkonferenz vom 15. März 2018.

Region Maloja

Martin Aebli
Vorsitzender Präsidentenkonferenz

Jenny Kollmar
Geschäftsleiterin Region Maloja