GEMEINDE EPPAN
an der Weinstraße
PROVINZ BOZEN - SÜDTIROL

COMUNE DI APPIANO
sulla Strada del Vino
PROVINCIA DI BOLZANO – ALTO ADIGE

VERORDNUNG

über die Privacy-Bestimmungen der Gemeinde Eppan

Verhaltensregeln für die Verarbeitung personen- und unternehmensbezogener Daten und für die Informationsinstrumente und -systeme für die Bediensteten der Gemeinde Eppan

REGOLAMENTO

privacy del Comune di Appiano

Regole di comportamento al trattamento dei dati personali e amministrativi, agli strumenti e sistemi informativi per i dipendenti degli Uffici Comunali di Appiano

ERSTFASSUNG — PRIMA VERSIONE

2016

VOM GEMEINDERAT GENEHMIGT MIT BESCHLUSS Nr. **69** vom **20.10.2016** — APPROVATO DAL CONSIGLIO COMUNALE CON DELIBERAZIONE N. del

IN KRAFT SEIT **05.11.2016** — IN VIGORE DAL

d.3.Akte Nr. 14433

Verordnung über die Privacy-Bestimmungen der Gemeinde Eppan

Regolamento privacy del Comune di Appiano

Inhalt

Indice

Artikel 1

ZWECK DIESES DOKUMENTS

Zweck dieses Dokuments ist die Festlegung einer Gesamtheit von Verhaltensnormen, die alle Bediensteten, Mitarbeiter und eventuell für die **Gemeinde Eppan** tätigen Drittunternehmen bei der Verarbeitung von Daten und Informationen zu berücksichtigen haben.

Die Richtlinien werden gemäß Datenschutzkodex (Legislativdekret 196/2003) definiert und umgesetzt, welche die Grundlage für die Ernennung und Beauftragung gemäß Art. 29 und 30 des Legislativdekrets 196/2003 und gemäß Verfügung des Garanten bilden.

Articolo 1

SCOPO E CAMPO DI APPLICAZIONE

Lo scopo del presente documento è quello di definire un insieme di norme comportamentali cui tutti i dipendenti, i collaboratori ed eventuali terze parti che operano per il **Comune di Appiano** devono uniformarsi nell'ambito delle attività che implicano un trattamento di dati ed informazioni.

Il Regolamento è realizzato in conformità alle richieste previste dal Codice in materia di protezione dei dati personali (D.Lgs. 196/2003 – Codice Privacy), parte integrante delle lettere di nomina e incarico ai sensi degli artt. 29 e 30 del D.Lgs. 196/2003, dei Provvedimenti del Garante Privacy.

Artikel 2

GRUNDBEGRIFFE DER PRIVACY IM SINNE DES LEGISLATIVDEKRETES 196/2003 – DATENSCHUTZKODEX

Die personenbezogenen Daten umfassen alle Informationen über eine natürliche Person, welche unter Bezugnahme irgendeiner anderen Information, auch mittels einer persönlichen Kennnummer, identifiziert werden können oder identifizierbar sind.

Es ist wichtig zu wissen, wann Daten als sensibel einzustufen sind: solche Daten unterliegen nämlich einem umfassenderen Schutz, weshalb für ihre Verarbeitung und Aufbewahrung strengere Vorschriften und Auflagen gelten.

Sensible Daten sind personenbezogene Daten, die Aufschluss geben können über die rassische und ethnische Herkunft, die religiöse, philosophische oder eine andere Weltanschauung, die politischen Anschauungen, die Mitgliedschaft bei einer Partei, Gewerkschaft, Vereinigung oder Organisation mit religiöser, philosophischer, politischer oder gewerkschaftlicher Ausrichtung.

Gerichtsdaten sind personenbezogene Daten, die Aufschluss geben können über Verfügungen und Maßnahmen in Zusammenhang mit dem Strafregister, dem Register über anhängige Verwaltungsstrafverfahren und die verhängten Verwaltungsstrafen oder über die Eigenschaft einer Person als Angeklagter oder als den Vorerhebungen unterworfene Person (Verdächtiger) im Sinne der Artikel 60 und 61 der Strafprozessordnung.

Mit besonderen Risiken verbundene Datenverarbeitung. Sind durch die Verarbeitung von anderen als den sensiblen oder Gerichtsdaten die Rechte und Grundfreiheiten oder die Würde der betroffenen Person wegen der besonderen Art der Daten, der Verfahrensweise oder der daraus entstehenden Folgen gefährdet, so ist diese Verarbeitung unter der Bedingung erlaubt, dass, soweit vorgeschrieben, besondere Maßnahmen und Vorkehrungen zum Schutze des Betroffenen getroffen werden.

Articolo 2

DEFINIZIONI FONDAMENTALI PRIVACY AI SENSI DEL D.LGS. 196/2003 – CODICE PRIVACY

I dati personali sono qualunque informazione relativa a persona fisica identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Si sottolinea l'importanza di comprendere quando un dato è considerato sensibile: a questi dati è infatti garantita una tutela più intensa, per cui sono imposti maggiori obblighi ed oneri nell'effettuare il trattamento e nella loro custodia.

I dati sensibili sono i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale.

I dati giudiziari sono i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del. d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale:

Trattamento che presenta rischi specifici. Il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti.

Mit der **Verarbeitung personenbezogener Daten** sind alle auch ohne elektronisches Gerät durchgeführten Aktionen im Zusammenhang mit der Erhebung, Speicherung, Organisation, Aufbewahrung, Abfrage, Verarbeitung im engeren Sinn, Änderung, Auswahl, Auslese, dem Vergleich, der Verwendung, Verknüpfung, Sperrung, Übermittlung, Verbreitung, Löschung und Vernichtung von Daten, auch wenn sie nicht in einer Datenbank gespeichert sind, gemeint. Es ist also unerheblich, ob die Vorgänge mit oder ohne Hilfe elektronischer oder sonstwie automatisierter Vorrichtungen durchgeführt werden, weshalb auch die Verarbeitung auf Papierträger den Vorschriften der Datenschutzbestimmungen unterliegt.

Unter **Übermittlung personenbezogener Daten** versteht man, einer oder mehreren bestimmten Personen, die nicht der Betroffene selbst sind, personenbezogenen Daten zur Kenntnis zu bringen, und zwar für ganz bestimmte Zwecke und mit einer ganz bestimmten und sicheren Art der Verarbeitung, auch mittels Zurverfügungstellung oder Bereitstellung zur Abfrage.

Verbreitung personenbezogener Daten heißt personenbezogene Daten unbestimmten Außenstehenden in jedweder Form, auch mittels Zuverfügungstellung oder Bereitstellung zur Abfrage, zugänglich zu machen.

Il trattamento dei dati personali corrisponde a qualunque operazione o complesso di operazioni, effettuata anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati. E' quindi indifferente che le operazioni vengano svolte con o senza l'ausilio di mezzi elettronici, per cui anche i trattamenti effettuati su supporto cartaceo sono assoggettati alla normativa privacy.

La comunicazione di dati personali corrisponde nel dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in base ad una precisa finalità ed una modalità certa e sicura di trattamento, anche mediante la loro messa a disposizione o consultazione.

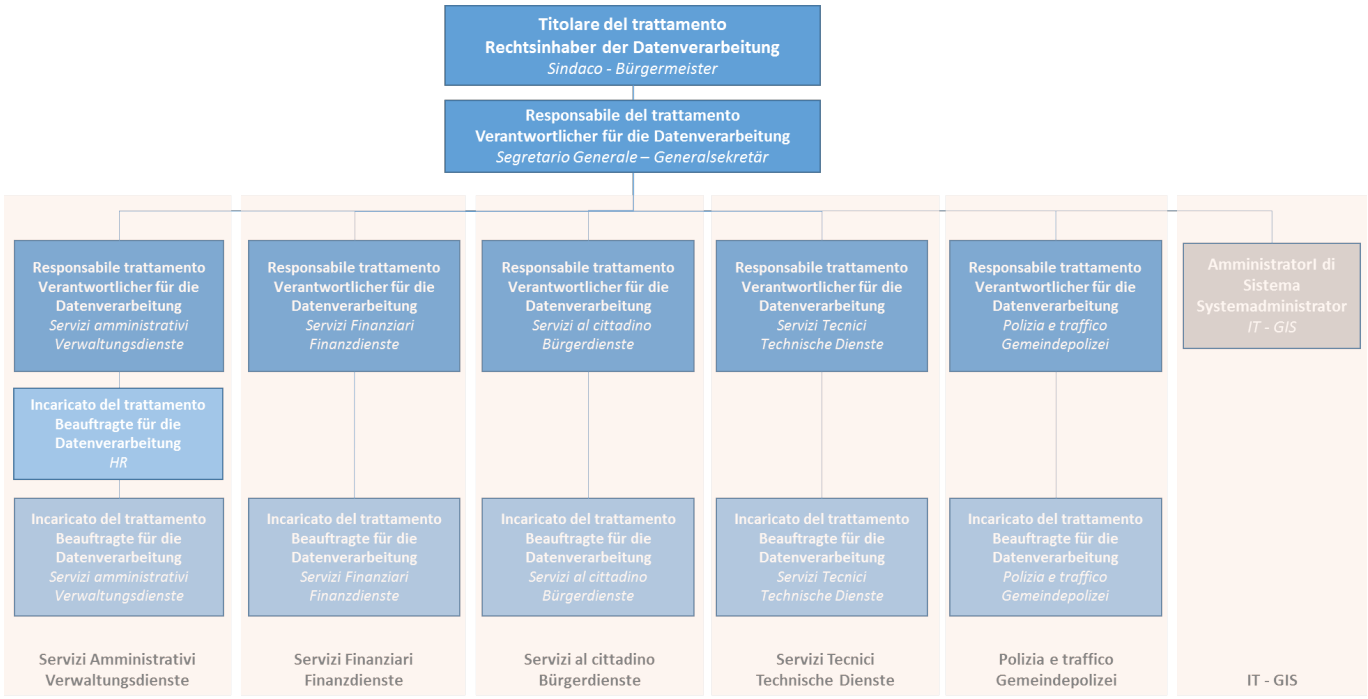
La diffusione di dati personali avviene quando viene data conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Artikel 3

DAS ORGANISATIONSMODELL PRIVACY

Articolo 3

MODELLO ORGANIZZATIVO PRIVACY



Rechtsinhaber der Datenverarbeitung (Rechtsinhaber) ist die Organisation insgesamt (Gemeinde Eppan) in Person ihres gesetzlichen Vertreters (Bürgermeister), der eine autonome Entscheidungsbefugnis in Bezug auf den Zweck und die Art und Weise der Verarbeitung personenbezogener Daten, einschließlich der Datensicherung, innehat.

Titolare del trattamento: (Titolare) è l'organizzazione nel suo complesso (Comune di Appiano) nella persona del suo legale rappresentante (Sindaco) che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza nel trattamento dei dati personali.

Verantwortlicher für die Datenverarbeitung ist die natürliche Person, juristische Person, die vom Rechtsinhaber mit der Kontrolle der Verfahren für die Verarbeitung der personenbezogener Daten betraut wird, wie sie von der Organisation festgelegt wurden.

Responsabile del trattamento: è la persona fisica, persona giuridica, preposta dal Titolare al controllo delle procedure e modalità di trattamento dei dati personali in base alle scelte organizzative.

Der Systemadministrator wird vom Rechtsinhaber zum Verantwortlichen für die Sicherheit des EDV-Systems ernannt.

Amministratore di sistema: è la persona preposta dal Titolare cui spetta la gestione della sicurezza del sistema informatico.

Beauftragter für die Datenverarbeitung ist die natürliche Person, die zur Durchführung von Verarbeitungsvorgängen nach den von der Organisation festgelegten Regeln ermächtigt ist. Laut Artikel 30 des Datenschutzkodex dürfen die Verarbeitungsvorgänge nur von Beauftragten vorgenommen werden, die direkt dem Rechtsinhaber oder dem Verantwortlichen unterstehen, an deren Anweisungen sie sich zu halten haben. Die Namhaftmachung der Beauftragten muss schriftlich erfolgen und den jeweils erlaubten Verarbeitungsbereich definieren.

Incaricato del trattamento: è la persona fisica autorizzata del trattamento a compiere operazioni di trattamento dati in base alle regole definite dall'organizzazione. L'articolo 30 del Codice Privacy dispone che le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite. La designazione degli incaricati deve essere effettuata per iscritto, individuando puntualmente l'ambito del trattamento consentito.

Artikel 4

MATRIX ZUR VERARBEITUNG VON PERSONEN- UND FIRMENBEZOGENEN DATEN

In der Matrix im Anhang sind alle von der Gemeinde verarbeiteten personen- und unternehmensbezogenen Daten aufgelistet, unterteilt nach Kategorie und Art entsprechend dem Datenschutzkodex sowie der betrieblichen Vertraulichkeitsstufe.

Jeder Bedienstete darf ausschließlich die mit seiner Beauftragung zusammenhängenden Informationen gemäß seiner Funktion und seinem Kompetenzbereich verarbeiten. Die personen- und unternehmensbezogenen Daten dürfen nie außerhalb der Gemeinde kommuniziert werden, außer in den von der Gemeinde selbst bestimmten Fällen und in Abstimmung mit dem jeweiligen Verantwortlichen.

Articolo 4

MATRICE DEL TRATTAMENTO DEI DATI PERSONALI E DEI DATI AZIENDALI

Nella matrice allegata sono riportati tutti i dati personali e amministrativi trattati dal Comune, suddivisi per categoria e natura in base al Codice Privacy e grado di riservatezza aziendale.

Ogni dipendente potrà trattare esclusivamente le informazioni indicate nella lettera di designazione ad incaricato del trattamento dei dati, in virtù della propria funzione ed area di competenza. I dati personali e le informazioni aziendali non potranno mai essere comunicati al di fuori della nostra organizzazione, tranne nei casi richiesti dall'organizzazione stessa e concordati con il proprio Responsabile.

Artikel 5

VERTRAULICHKEITSSTUFE DER DATEN UND INFORMATIONEN

Stufe 1 - Öffentlich

Öffentliche Daten und Informationen können durch Mitarbeiter und Dritte ohne Einschränkungen mit den vom Unternehmen zur Verfügung gestellten Kommunikationsmitteln (*E-Mail, Internetseite, Datenaustauschbereiche auf dem Server, Aushang im Betrieb, Mitteilungen, Briefe usw.*) verarbeitet werden. Diese Informationen erfordern keine besondere Aufmerksamkeit in Bezug auf die Vertraulichkeit.

Articolo 5

GRADI DI RISERVATEZZA DEI DATI E DELLE INFORMAZIONI

Livello 1 – Pubblico

I dati e le informazioni pubbliche sono liberamente trattabili da dipendenti e terze parti esterne, attraverso i mezzi di comunicazione messi a disposizione dell'azienda (*e-mail, Sito internet, aree di scambio su server e computer, bacheca, comunicati, lettere,* etc.). Queste informazioni non richiedono particolari attenzioni di riservatezza.

Stufe 2 - Vertraulich

Vertrauliche Daten und Informationen können von bestimmten Mitarbeitergruppen und Dritten verarbeitet werden, die dazu vom Inhaber oder Verantwortlichen für die Verarbeitung der Daten für einen bestimmten Zweck beauftragt wurden. Die Daten und Informationen können nur an (interne bzw. externe) Benutzer weitergeleitet werden, die zur Datenverarbeitung berechtigt sind, wobei das jeweils geeignete, von der Gemeinde zur Verfügung gestellte Kommunikationsmittel zu verwenden ist; sie dürfen jedoch nicht allgemein verbreitet und weitergegeben werden, außer sie werden so verändert, dass sie der *Stufe 1 - öffentlich* zugeordnet werden können.

Livello 2 - Riservato

I dati e le informazioni riservati possono essere trattati da gruppi di dipendenti individuati e esterni incaricati in virtù di una precisa finalità di trattamento individuata dal Titolare o Responsabile del trattamento. Tali dati e le informazioni devono essere comunicate solo ad utenti (interni ed esterni) legittimati al trattamento valutando lo strumento più appropriato di comunicazione messo a disposizione dall'organizzazione, ma non dovranno mai essere diffuse o divulgate, a meno di essere rielaborate in modo da declassarle al livello pubblico 1.

Stufe 3 – Streng vertraulich

Streng vertrauliche Daten und Informationen können nur von einem bestimmten und eingeschränkten Personenkreis verarbeitet werden, die mit Namen und Position durch den Inhaber bestimmt werden. Diese Informationen können ausschließlich an namentlich genannte Benutzer mitgeteilt und dürfen in keiner sonstigen Weise verbreitet oder weitergegeben werden.

Livello 3 – Strettamente riservato

I dati e le informazioni strettamente riservate possono essere trattati solo da una specifica e ristretta categoria di utenti, individuabili per nome e posizione, nominati dal Titolare. Tali informazioni potranno essere comunicate esclusivamente agli utenti nominati e in nessun modo potranno essere diffuse o divulgate.

Artikel 6

VERHALTENSREGELN

1. ZUGANG ZU DEN BÜROS

Sämtliche Räumlichkeiten und Strukturen der Gemeinde sind mit höchster Sorgfalt zu benutzen und zu überwachen, um ein effizientes Arbeiten und ein angemessenes Informationssicherheitsniveau zu gewährleisten.

Gemeindeämter. Der Zugang zu den Gemeindeämtern, den geschützten Bereichen, den Bereichen mit eingeschränktem Zutritt und den Dokumentenarchiven ist nur jenen Personen gestattet, die vom Verantwortlichen dazu ausdrücklich ermächtigt wurden; der Zugang erfolgt mittels Schlüssel und ausschließlich zu genau definierten und begründeten Arbeitszwecken. Audio-/Video-Aufnahmen (Bilder, Filme, Ton usw.) sind in keinem Bereich der Gemeinde gestattet, außer es liegt eine entsprechende Genehmigung durch den Verantwortlichen der Datenverarbeitung vor.

Data Center. Der Zugang zum Data Center ist ausschließlich in Anwesenheit von dazu ermächtigtem Gemeindepersonal gestattet.

2. ARBEITSPLATZ

Die Benutzung des Arbeitsplatzes und in der Folge der Zugang zu den Dokumenten, Unterlagen und Archiven ist nur im Rahmen der eigenen Funktion und der zugeteilten Aufträge gestattet.

Aufgeräumter Schreibtisch. Der eigene Schreib-

Articolo 6

REGOLE DI COMPORTAMENTO

1. ACCESSO AGLI UFFICI

I locali e tutte le risorse fisiche del Comune devono essere utilizzate e custodite con la massima diligenza al fine di garantire un'efficiente conduzione dell'attività lavorativa ed un adeguato livello di sicurezza delle informazioni.

Uffici Comunali. L'accesso agli uffici, alle aree protette, alle aree riservate ed agli archivi cartacei, è permesso solo a personale espressamente incaricato dal Responsabile, munito di chiave, in base a precise e motivate esigenze di accedere a tali ambienti, per finalità lavorative. In qualunque area del Comune è vietato l'utilizzo di strumenti in grado di effettuare foto/riprese video/audio, a meno che non sia stato preventivamente e formalmente autorizzato dal Responsabile del trattamento.

Sala Server. L'accesso alla sala server può avvenire esclusivamente in presenza di personale autorizzato del Comune.

2. POSTAZIONI DI LAVORO

L'utilizzo della postazione di lavoro e il conseguente accesso ai documenti, atti e archivi è consentito nei limiti della propria funzione e dei propri incarichi assegnati.

Scrivania pulita. La propria scrivania deve essere

tisch muss während der Pausen, nach Arbeitsende und/oder bei längeren Abwesenheiten aufgeräumt sein, sodass vertrauliche Dokumente und solche mit sensibeln oder Gerichtsdaten Dritten ohne Aufsicht nicht zugänglich sind.

3. PHYSISCHE MASSNAHMEN BEI DER VERWAHRUNG VON PAPIERDOKUMENTEN

Daten in Papierform, die der Ausführung der eigenen Aufgaben dienen, müssen in den Schränken im Büro aufbewahrt werden. Sämtliche Archive sind nur beschränkt zugänglich, der Zugang ist nur soweit gestattet, wie es für die Entnahme und Rückgabe der Unterlagen bzw. Datenträger zur Ausführung der eigenen Aufgaben notwendig ist. Bei Abwesenheit bzw. Abschluss der Tätigkeit sind die Dokumente wieder in die entsprechenden Archive zurückzustellen.

Die Archive der Dokumente und Unterlagen, die sensible personenbezogene Daten enthalten, müssen in verschlossenen Schränken aufbewahrt werden.

Papierdokumente, die personen- und/oder unternehmensbezogene Informationen enthalten, sind mit einem entsprechenden Aktenvernichter zu **vernichten**.

4. VERWALTUNG VON DATEN

Bei der Verarbeitung von jeglicher Art von Daten und Informationen hat der beauftragte Bedienstete oder Mitarbeiter alle notwendigen Maßnahmen zu treffen, um sie entsprechend zu schützen; Daten, Informationen und Dokumente, welche im Rahmen der eigenen Funktion erstellt werden, dürfen ausschließlich in diesem Bereich/Aufgabenfeld angewandt werden und dürfen nicht an unberechtigte Dritte kommuniziert werden.

Es ist strengstens verboten, ohne ausdrückliche Genehmigung des Verantwortlichen Daten, Informationen und Dokumente, welche der Gemeindeverwaltung vorbehalten sind, an nicht ermächtigte Dritte weiterzugeben.

Jede Art der Verarbeitung der Daten und Informationen (in Form von Mitteilung, Veränderung, Kopie, Löschung, Weiterleitung an Dritte, usw.) ist ohne ausdrückliche Zustimmung des jeweiligen Verantwortlichen untersagt.

Es ist strengstens verboten, ohne Zustimmung des jeweiligen Verantwortlichen Daten und Informationen des Unternehmens im Internet (*Social media, Foren, Blogs, Chat, Internetseiten*) zu veröffentlichen.

Es ist strengstens verboten, ohne Genehmigung durch den Systemadministrator Daten und Informationen in cloud-basierten Systemen (Dropbox, Google+, Evernote usw.) zu speichern. Nur die vom Sys-

mantenuta in ordine, verificando di non lasciare documenti riservati, sensibili e giudiziari senza un proprio controllo all'accesso di terzi, in momenti di pausa, terminata la giornata di lavoro e/o in periodi di assenza.

3. MISURE FISICHE DI CUSTODIA DEI DOCUMENTI E ATTI CARTACEI

I dati cartacei necessari per lo svolgimento delle mansioni lavorative devono essere custoditi negli armadi posti nel proprio ufficio. Tutti gli archivi sono ad accesso limitato, per cui è possibile accedervi nei limiti della necessità per prelevare e riporre i documenti ed i supporti informatici necessari per lo svolgimento delle mansioni lavorative. I documenti dovranno essere riposti correttamente durante i periodi di temporanea assenza ed al termine dell'attività lavorativa negli appositi archivi.

Gli archivi di documenti e atti contenenti dati personali sensibili dovranno essere custoditi in armadi chiusi a chiave.

L'eliminazione fisica di ogni documento cartaceo contenente dati e informazioni aziendali e/o personali deve essere effettuata solo utilizzando l'apposito elimina-documenti.

4. GESTIONE DEI DATI

Il trattamento di qualunque dato e informazione deve prevedere da parte del dipendente o collaboratore incaricato ogni ragionevole misura per assicurare che tali dati e informazioni rimangano tali. I dati, le informazioni ed i documenti elaborati nell'ambito della propria funzione potranno essere utilizzati esclusivamente in tale ambito e non dovranno essere comunicati a terzi non legittimati.

È fatto assoluto divieto divulgare a terzi non autorizzati, dati, informazioni e documenti riservati dell'Amministrazione Comunale senza espressa autorizzazione del Responsabile.

È vietata ogni attività di trattamento di dati e informazioni (comunicazione, modifica, copia, cancellazione, fornitura ad esterni, etc.) non espressamente autorizzata e concordata con il proprio Responsabile.

È assolutamente vietato pubblicare in internet (*Social media, forum, chat, blog, siti internet*) dati ed informazioni di carattere aziendale non autorizzate e concordate con il proprio Responsabile.

È assolutamente vietato il salvataggio di dati e informazioni in sistemi *cloud* (*per esempio Dropbox, Google+, Evernote,* etc.) non autorizzati dall'Amministratore di sistema. È invece prevista la modalità di salva-

temadministrator angegebenen und genehmigten Datenspeicherungssysteme sind zulässig.

Der Inhaber kann, unter Berücksichtigung der Datenschutzbestimmungen, mit Hilfe des Systemadministrators auf alle unternehmenseigenen IT-Geräte und die darin enthaltenen Daten, sowie auf die Telefonabrechnungen zu folgenden Zwecken zugreifen: Gewährleistung der Sicherheit des IT-Systems, Wartung und andere technische Gründe (z.B. Aktualisierung, Ersatz und Aufbau von Programmen, Wartung von Hardware usw.) sowie zur Kontrolle und Planung der betrieblichen Kosten (z.B. Überprüfung der Ausgaben für Internetzugang und Telefonverkehr). Solche Maßnahmen erfolgen aber keinesfalls zur Kontrolle der Arbeitstätigkeit.

5. BENUTZUNG DES BETRIEBLICHEN PCs

Der dem Benutzer anvertraute Computer ist ein Arbeitsgerät. Jegliche Verwendung, die nichts mit der Arbeit zu tun hat, ist verboten, da sie zu Fehlfunktionen, Wartungskosten und vor allem zu Sicherheitsproblemen führen kann. Der PC muss mit Sorgfalt behandelt werden, um jegliche Beschädigung zu vermeiden.

Der dem Benutzer anvertraute Computer erlaubt den Zugang zum Gemeinde-Netzwerk nur über eigene **Zugriffscodes,** wie im nachfolgenden Punkt dieser Verordnung beschrieben.

Die Verwendung des PCs und somit der Zugang zu Daten, Programmen und IT-Ressourcen ist nur im Rahmen der eigenen Funktion und der zugeteilten Aufträge gestattet und im Rahmen der zugewiesenen Nutzerprofile.

Der anvertraute PC darf während einer Unterbrechung der Datenverarbeitung bzw. bei Pausen nicht unbeaufsichtigt gelassen oder zugänglich gemacht werden. Sind PCs unbeaufsichtigt, müssen sie manuell gesperrt werden und sie müssen mit einem passwortgeschützten Bildschirmschoner versehen sein, der sich nach maximal 5 Minuten Untätigkeit automatisch einschaltet.

Sämtliche PC-Arbeitsplätze sind zudem mit entsprechender Antivirussoftware ausgestattet.

6. PASSWORTVERWALTUNG FÜR DEN ZUGANG ZUM NETZWERK

Der Zugang zum Netzwerk und zu anderen Netzwerksystemen wird den Mitarbeitern vom Systemadministrator zugeteilt und ist streng persönlich.

Die Zugangsdaten bestehen aus einem Benutzernamen, der vom Systemadministrator zugewiesen wird, und einem geheimen Passwort, das der Mitarbeiter sorgfältig verwahren muss und nicht weitergeben darf. Falls man den Verdacht hegt, dass das Passwort nicht mehr geheim ist, muss dieses sofort aus-

taggio indicata e autorizzata dall'Amministratore di sistema.

Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/ sostituzione/ implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà del Titolare, tramite l'Amministratore di sistema, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti.

5. UTILIZZO DEL PC AZIENDALE

Il PC affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

Il PC dato in affidamento all'utente permette l'accesso alla rete del Comune solo attraverso specifiche **credenziali di autenticazione** come meglio descritto al successivo punto del presente Regolamento.

L'utilizzo del PC e conseguentemente l'accesso ai dati, programmi e risorse informatiche, è consentito nei limiti della propria funzione e dei propri incarichi assegnati, nei limiti del profilo utente assegnato.

È obbligatorio non lasciare incustodito o accessibile il PC assegnato durante la pausa di una sessione di trattamento. Per questo motivo tutti i PC devono essere bloccati manualmente se lasciati incustoditi e devono inoltre essere dotati di uno screen saver, protetto da password, ad attivazione automatica al massimo dopo 5 minuti di inattività.

Tutte le postazioni di lavoro sono dotate di *software antivirus*.

6. GESTIONE DELLA PASSWORD DI ACCESSO AI SERVIZI DI RETE

L'accesso alla rete e ad altri servizi di rete vengono assegnati dall'Amministratore di sistema e sono strettamente personali.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (username), assegnato dall'Amministratore di sistema, associato ad una parola chiave (password) riservata che dovrà venir custodita dall'incaricato con la massima diligenza e non divulgata. Nel caso si sospetti che la password

getauscht werden.

Beim Umgang mit den Zugangsdaten und Passwörtern hält sich jeder Nutzer an die Anweisungen im Dokument *Passwörter*.

Der Zugang zu den IT-Systemen darf nur nach vorheriger Identifizierung und Authentifizierung des Benutzers aufgrund seiner Zugangsdaten erfolgen. Änderungen der Zugriffsrechte sind nur in Absprache mit dem jeweiligen Verantwortlichen zulässig.

Insbesondere gelten folgende Richtlinien für die Verwaltung der Passwörter:

– nur Passwörter verwenden, die die Kriterien für die Komplexität der Passwörter erfüllen;

– Passwörter nicht im Büro auf Papier notieren oder online abspeichern;

– das eigene Passwort niemandem mitteilen;

– das Passwort am Arbeitsplatz nicht in Gegenwart einer anderen Person eingeben, so dass diese es erkennen könnte;

– die Option "*Passwort merken*", die es in einigen Programmen gibt, nicht verwenden.

– Wurde das Passwort vergessen oder soll es wiederhergestellt werden, muss man sich an den Systemadministrator wenden.

Hinsichtlich Authentifizierung und Benutzerprofile ist der Systemadministrator für folgende Aufgaben zuständig:

– periodische Überprüfung der Benutzerzugänge jeglicher Art zu den Daten, Systemen und zum Netzwerk;

– periodische Überprüfung der Benutzerprofile und Abgleich mit den zugeteilten Aufgabenbereichen.

7. BENUTZUNG DES NETZWERKES

Es ist strengstens verboten, sich im Netzwerk oder den Softwaresystemen mit einem anderen Benutzernamen als dem eigenen anzumelden. Die Zugangscodes für das Netzwerk und für die Anwendungen sind geheim und müssen vorschriftsgemäß mitgeteilt und verwendet werden.

Es wird darauf hingewiesen, dass der Systemadministrator **keine** Sicherungskopien der lokalen Festplatten und anderer Speichermedien (z.B. Laufwerk C:) macht. Somit trägt jeder Benutzer selber die Verantwortung für die Speicherung der dort enthaltenen Daten.

abbia perso la segretezza, la stessa deve essere immediatamente sostituita.

La gestione delle credenziali di accesso e password deve essere realizzata da ogni utente in base alle indicazioni contenute nel documento *Passwörter*.

L'accesso ai sistemi informatici può avvenire esclusivamente se preventivamente identificati ed autenticati, attraverso la verifica delle proprie credenziali. Qualunque variazione delle abilitazioni di accesso dovrà essere concordata ed autorizzata dal Responsabile.

In particolare occorre seguire la seguenti regole per la gestione della *password*:

– utilizzare solamente *password* che rispettino i criteri di complessità previsti;

– evitare di annotare la propria *password* all'interno dell'ufficio, o di conservarla on-line;

– non comunicare la propria *password* a nessuno;

– fare attenzione a non digitare la propria *password* nel momento in cui ci sono altre persone, nei pressi della postazione di lavoro, che potrebbero osservare tale operazione;

– evitare di utilizzare l'opzione "*ricorda password*" presente in alcuni programmi;

– in caso di dimenticanza e/o ripristino della *password,* dovrà essere inoltrata una richiesta all'Amministratore di sistema.

Nell'ambito della gestione delle credenziali di autenticazione e dei profili utente ricordiamo che è compito dell'Amministratore di sistema:

– verificare periodicamente gli accessi effettuati dagli utenti, in qualsiasi modalità, ai dati, ai sistemi ed alla rete;

– verificare periodicamente i profili utente al fine di controllare che siano coerenti con le responsabilità assegnate.

7. UTILIZZO DELLA RETE

È assolutamente proibito connettersi alla rete ed ai sistemi applicativi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'accesso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

Si ricorda che i dischi o altre unità di memorizzazione locali - quali, ad esempio, disco C: interno PC - **non** sono soggette a salvataggio da parte dell'Amministratore di sistema. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente.

Sämtliche Daten und Informationen, welche im Rahmen der Arbeitstätigkeit vom Nutzer verarbeitet werden, dürfen ausschließlich auf den dafür vorgesehenen, von der Gemeinde bereitgestellten Netzlaufwerken gespeichert werden.

Tutti i dati e le informazioni elaborati durante il lavoro svolto dall'utente devono essere salvati esclusivamente sulle unità di rete predisposte.

8. ANTIVIRUS-SOFTWARE

Für die Verwaltung (Installation, Updates usw.) der Antivirus-Software ist der Systemadministrator zuständig.

Es ist verboten:

– das Antivirus-Programm, aus welchen Gründen auch immer, zu deaktivieren;

– ein anderes Antivirus-Programm als das bereits vom Systemadministrator eingerichtete zu installieren.

8. SOFTWARE ANTIVIRUS

La gestione (installazione, aggiornamento, etc.) del *software antivirus* è di competenza dell'Amministratore di sistema.

In ogni caso, è tuttavia vietato:

– disabilitare, per qualsiasi motivo, il sistema *antivirus*;

– installare *software antivirus* diverso da quello già installato dall'Amministratore di sistema.

9. DOWNLOAD UND VERWALTUNG DER SOFTWARE

Jeder Mitarbeiter hat ausschließlich jene Softwareprogramme zu verwenden, über die die Gemeinde verfügt und deren technische Details vom Systemadministrator geliefert werden, sobald es bedeutende Updates gibt.

Richtlinien für alle Mitarbeiter:

– Software oder Anwendungen, für die die Gemeinde über keine Lizenz verfügt, dürfen nicht installiert werden.

– Alle von außen empfangenen Dateien müssen systematisch überprüft werden und auch beim Versenden von Dateien sind entsprechende Vorkehrungen zu treffen.

– Private Software darf nicht verwendet werden, außer bei ausdrücklicher, schriftlich angesuchter Genehmigung durch den Verantwortlichen (gilt auch für Demoversionen).

9. DOWNLOAD E GESTIONE DEL SOFTWARE

Ogni utente deve utilizzare esclusivamente i software di cui dispone il Comune, le cui specifiche tecniche sono fornite dall'Amministratore di sistema, ogni volta che vi sono dei significativi aggiornamenti.

Ogni utente deve:

– evitare di installare *software* e/o applicativi che non appartengano all'organizzazione;

– controllare metodicamente tutti i *files* provenienti dall'esterno e adottare le opportune cautele al momento della trasmissione all'esterno di *files*;

– evitare qualunque utilizzo *di software* privato per usi aziendali, salvo esplicita autorizzazione da parte del Responsabile attraverso richiesta scritta (anche per *software* in versione *demo*).

10. VERWALTUNG DER BETRIEBLICHEN E-MAIL

Die Zuteilung des E-Mail-Accounts der Gemeinde (*Firmen-E-Mail*) erfolgt ausschließlich unter der Bedingung, dass dieser nur für die Arbeitstätigkeit verwendet wird. Benutzer eines E-Mail-Accounts sind für die korrekte Verwendung der E-Mail verantwortlich, dabei sind entsprechende Regeln zu beachten.

Insbesondere gelten folgende Richtlinien:

– Beim Öffnen von Dateianhängen und Links in E-Mails ist größte Vorsicht geboten. Ausführbare Dateien und Dokumente von unbekannten Internet-

10. GESTIONE DELLA E-MAIL AZIENDALE

L'assegnazione di una casella di posta elettronica del Comune (*e-mail aziendale*) deve essere seguita da un utilizzo della stessa esclusivamente per finalità legate alla attività lavorativa. Gli utenti dell'e-mail aziendale sono responsabili del corretto utilizzo delle stesse e devono mantenere un corretto comportamento nell'utilizzo della e-mail.

In particolare devono essere seguite le seguenti disposizioni:

– è obbligatorio porre la massima attenzione nell'aprire i file *attachments* ed i *links* di posta elettronica prima del loro utilizzo (non eseguire download di file

und FTP-Seiten dürfen nicht heruntergeladen werden.

– Um den ordnungsgemäßen Betrieb des E-Mail-Dienstes zu gewährleisten und den Datenzugriff auf ein Mindestmaß zu reduzieren, werden die Benutzer angehalten, im Sinne des Grundsatzes von Notwendigkeit und Verhältnismäßigkeit, bei längerer, geplanter Abwesenheit (z.B. bei Urlaub oder Außendienst) eine Abwesenheitsnotiz einzurichten, welche die E-Mail-Adresse alternativer Kontaktpersonen oder andere Angaben für die Kontaktaufnahme mit der Gemeinde enthält. Diese Funktion ist vom Benutzer selbst zu aktivieren.

– Betriebliche E-Mails dürfen nicht für den Versand oder Empfang von privaten Nachrichten, die keinen Bezug zur Arbeit haben, für die Teilnahme an Diskussionen, Foren oder Mailing-Listen verwendet werden, es sei denn mit ausdrücklicher Genehmigung des Verantwortlichen.

– Ist die Verwendung der betrieblichen E-Mail für private Zwecke ausnahmsweise notwendig, so sind persönliche Nachrichten aus dem System zu löschen, sobald sie übertragen bzw. gelesen wurden.

– Es ist strengstens verboten, der Gemeinde vorbehaltene, vertrauliche und gemeindeeigene Informationen ohne ausdrückliche Genehmigung des Verantwortlichen weiterzuleiten.

– Es ist strengstens verboten, E-Mails und allgemein Daten, Programme oder sonstiges IT-Material mit beleidigenden, belästigenden, vulgären, blasphemischen, ausländerfeindlichen, rassistischen, pornographischen, pädophilen, terroristischen oder sonst unangemessenen, gefährlichen oder rechtswidrigen Inhalten zu verschicken oder aufzubewahren.

– Bei längerer Abwesenheit (wie Urlaub, Krankenstand, Wartestand, längerer Außendienst), auch wenn sie nicht vorherzusehen war, hat der Benutzer entsprechende Vorkehrungen zu treffen, um die Kontinuität der Tätigkeiten sicherzustellen.

Hinweis:

– Sämtliche Eingangsmails werden durch eine Antispam-Software kontrolliert. Es ist möglich, dass einzelne Nachrichten nicht vom Spamfilter abgefangen werden. Bei verdächtigen E-Mails ist daher größte Vorsicht geboten; bei Zweifeln über die Herkunft bzw. den Inhalt ist der Systemadministrator zu kontaktieren.

– Die erhaltenen, gesendeten oder gespeicherten E-Mails können vom Systemadministrator, Inhaber und Verantwortlichen für die Datenverarbeitung ausschließlich in folgenden Fällen gelesen werden:

  • bei Abwesenheit des Mitarbeiters, um die

eseguibili o documenti da siti Web o Ftp non conosciuti).

– al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, si invita, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede) ad attivare le "Regole Fuori Sede" per l'invio automatico di un messaggio di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura. In tal caso, la funzionalità deve essere attivata dall'utente.

– l'e-mail aziendale non deve essere utilizzata per l'invio o la ricezione di messaggi personali al di fuori dalle finalità lavorative o per la partecipazione a dibattiti, forum o mailing-list, salvo diversa ed esplicita autorizzazione del Responsabile.

– nell'eventualità in cui l'uso personale della posta elettronica aziendale si rendesse eccezionalmente necessario, gli utenti dovranno cancellare i messaggi di natura personale dal sistema non appena trasmessi e/o letti.

– è fatto assoluto divieto divulgare a terzi informazioni riservate, confidenziali o comunque di proprietà dell'Amministrazione Comunale senza espressa autorizzazione del Responsabile.

– è fatto assoluto divieto inviare o conservare messaggi di posta elettronica o più in generale dati, programmi o altro materiale di natura informatica pericolosi/vietati e/o aventi contenuti illegali, - a titolo esemplificativo e non esaustivo - dal contenuto offensivo, molesto, volgare, blasfemo, xenofobo, razziale, pornografico, pedopornografico, terroristico o comunque inappropriato o illegale.

– in caso di assenza prolungata (ferie, malattia, aspettativa, lunga attività fuori sede) o non programmata, l'utente deve prevedere delle opportune procedure in grado di garantire la continuità delle attività.

Si avvisa che:

– tutta la posta elettronica in entrata è controllata da un software antispam. È comunque possibile che alcune mail di spam superino i filtri impostati sul sistema centrale: quindi è necessario prestare la massima attenzione a e-mail sospette, avvisando l'Amministratore di sistema in caso di dubbi sulla provenienza/contenuto delle stesse.

– tutti i messaggi ricevuti, spediti o salvati, potranno essere letti dall'Amministratore di sistema, dal Titolare e dal Responsabile del trattamento esclusivamente per i seguenti motivi:

  • in caso di assenza per garantire una regolare

Kontinuität des Dienstes zu gewährleisten,

- aus IT-Sicherheitsgründen.

In jedem Fall wird der Nutzer darüber informiert.

11. NUTZUNG DES INTERNETZUGANGS

Der Internetzugang mittels Betriebscomputer, Tablet oder Smartphone erfolgt ausschließlich zum Zweck des Zugangs zu Informationen und Inhalten im Rahmen der Tätigkeit. Da es sich um ein Arbeitsmittel handelt, sind die Benutzer für die korrekte Verwendung verantwortlich.

Es ist zu beachten, dass die Nummer, die Dauer und der Inhalt des Internetzugangs stets aufgezeichnet werden. Die Aufzeichnungen können nur in anonymer und zusammengefasster Form ausgewertet werden, vorbehaltlich von rechtlich vorgesehenen Fällen und bei Missachtung der vorliegenden Verordnung. Eventuelle Kontrollen, durchgeführt vom Systemadministrator, erfolgen mittels Systemen zur inhaltlichen Analyse oder mittels „*log files*“ der Navigation.

Um einem eventuellen Missbrauch der Internetnutzung vorzubeugen, verfügt das System über Zugangsfilter und auf die eigene Funktion abgestimmte Beschränkungen. Deren Funktion ist in den entsprechenden Verfahren geregelt.

Folgende Regeln sind bei Nutzung des Internetzugangs zu beachten:

– Material und Programme, die Gesetze über Urheberrechte von Personen oder Firmen verletzen und die durch Copyright, Patente oder Rechte an geistigem Eigentum geschützt sind, dürfen nicht heruntergeladen werden; dieses Verbot gilt auch für die Installation oder Verteilung von Software, für die die Gemeinde keine Lizenz besitzt.

– Jegliche Art von persönlichen Finanztransaktionen, einschließlich Home-Banking, Online-Einkäufen und Ähnlichem ist verboten; außer bei ausdrücklicher Genehmigung des Verantwortlichen und jedenfalls unter Einhaltung der geltenden Vorschriften für Einkäufe, Zahlungen usw.

– Das Aufrufen von Internetseiten und Herunterladen von gefährlichen/verbotenen Materialien mit beleidigenden, belästigenden, vulgären, blasphemischen, ausländerfeindlichen, rassistischen, pornographischen, pädophilen, terroristischen oder sonst unangemessenen oder rechtswidrigen Inhalten ist ausdrücklich verboten.

– Es ist verboten, von urheberrechtlich geschützten Unterlagen Kopien anzufertigen, einschließlich - aber nicht nur beschränkt auf - Digitalisierung und Verteilung von Bildern aus Zeitschriften, Büchern oder aus sonstigen Quellen, Musik und Videomate-

continuità dell’attività lavorativa;

- per motivi di sicurezza informatica.

In tutti questi casi l’utente verrà informato.

11. UTILIZZO DELLA NAVIGAZIONE INTERNET

L’accesso ad Internet (tramite PC, *tablet o smartphone* aziendali) è fornito allo scopo di consentire l’accesso ad eventuali informazioni e contenuti necessari allo svolgimento dell’attività lavorativa. Essendo uno strumento di lavoro, gli utenti cui si attribuisce l’accesso, sono responsabili del suo corretto utilizzo.

Si informa che il numero, la durata ed il contenuto degli accessi ad Internet sono costantemente registrati. La consultazione di tali registrazioni può avvenire solo in forma anonima e aggregata salvo i casi previsti dalla legge e dal mancato rispetto del presente Regolamento. Gli eventuali controlli, compiuti dall’Amministratore di sistema, potranno avvenire mediante un sistema di analisi dei contenuti o mediante “*file di log*” della navigazione svolta.

Per prevenire eventuali abusi nell’uso di Internet il sistema è provvisto di filtri d’accesso e limiti di utilizzo in base alla funzione ricoperta. Il loro funzionamento è regolato nelle relative procedure operative.

Si devono comunque osservare le seguenti regole di navigazione della rete Internet:

– è tassativamente vietato scaricare materiale e programmi in violazione della legislazione sui diritti di autore, che siano essi appartenenti a persone o aziende, coperti da *copyright*, brevetto o proprietà intellettuale, ivi compresa l’installazione o la distribuzione di software che non sia specificatamente licenziato per essere utilizzato all’interno dell’azienda;

– è tassativamente vietato effettuare ogni genere di transazione finanziaria di interesse personale ivi comprese le operazioni di home banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dal Responsabile;

– è tassativamente vietato navigare siti e scaricare materiale pericolosi/vietati o aventi contenuti illegali, - a titolo esemplificativo e non esaustivo - dal contenuto offensivo, molesto, volgare, blasfemo, xenofobo, razziale, pornografico, pedopornografico, terroristico o comunque inappropriato o illegale;

– è vietato effettuare copia non autorizzata di materiale coperto da *copyright* compreso, ma non limitato a, digitalizzazione e distribuzione di foto da riviste, libri o altre fonti, musica o materiale video;

rial.

– Es ist verboten, Dateien mittels *Peer-to-Peer*-Programmen auszutauschen.

– Es ist verboten, Programme herunterzuladen, auch wenn dazu keine Lizenz erforderlich ist bzw. auch im Falle von Demoversionen (*Freeware- oder Shareware-Programme*), außer bei ausdrücklicher Genehmigung durch den jeweiligen Verantwortlichen. Dateien aus dem Internet herunterladen ist grundsätzlich riskant, da dadurch Viren und *Malware* ins EDV-System eingeschleust werden können.

– Es ist verboten, die IT-Infrastruktur der Gemeinde für die Beschaffung und Verbreitung von Material zu nutzen, das gegen geltende Gesetze verstößt.

– Jegliche Überwachung des Netzwerks zum Abfangen von Daten, die nicht ausdrücklich an den *Host* des Benutzers gesendet wurden (*Sniffing*), ist verboten.

– Es ist verboten, Verfahren zur Benutzerkennung oder Sicherheitsvorkehrungen eines jeglichen *Hosts*, Netzwerks oder Accounts zu umgehen.

12. VERWENDUNG VON BETRIEBLICHEN SMARTPHONES, TABLETS UND TELEFONEN

Festnetztelefon der Firma. Das Firmentelefon ist ausschließlich im Rahmen der eigenen Arbeit zu nutzen. Zur Vermeidung einer missbräuchlichen Verwendung wird der Telefonverkehr eines jeden Anschlusses überprüft.

Smartphones und Tablets (Mobile). Der Zugang zu Smartphones oder Tablets muss durch die Einrichtung eines persönlichen Passwortes (automatischer Bildschirmschoner) erfolgen.

Heruntergeladene Dateien mit firmenbezogenen Daten als Anhängen (z.B. E-Mail, Skype, Whatspp, usw.) dürfen nur so lange gespeichert werden, wie dies für die Nutzung notwendig ist.

Bei der Verwendung von Apps ist hinsichtlich übermäßigen Datenverbrauchs und Sicherheit des Gerätesbesondere Sorgfalt geboten.

13. DRUCKER UND FAX

Die private Nutzung von Multifunktionsgeräten (Drucker, Kopierer, Fax) und Faxgeräten der Gemeinde ohne ausdrückliche Genehmigung des Verantwortlichen ist untersagt, sowohl für das Senden als auch für das Empfangen von Dokumenten.

Dokumente dürfen nicht unbeaufsichtigt bei den genannten Geräten gelassen werden.

– è vietata la condivisione di file in modalità *peer-to-peer*;

– è vietato scaricare programmi, anche se privi di licenza o in prova (*freeware e shareware*), se non in caso di espressa autorizzazione da parte del proprio Responsabile. Eseguire il *download* di file da Internet è infatti un'operazione intrinsecamente pericolosa in quanto può essere il veicolo per l'introduzione di *virus e malware*;

– è vietato utilizzare l'infrastruttura tecnologica aziendale per procurarsi e diffondere materiale in violazione con le normative vigenti;

– è vietato eseguire qualsiasi forma di monitoraggio della rete che permetta di catturare dati non espressamente inviati all'*host* dell'utente (*sniffing*);

– è vietato aggirare le procedure di autenticazione o la sicurezza di qualunque *host*, rete, *account*.

12. UTILIZZO DI SMARTPHONE, TABLET E TELEFONI AZIENDALI

Telefono fisso. L'utilizzo del telefono aziendale deve essere limitato allo svolgimento delle proprie attività lavorative. Per prevenire eventuali abusi all'uso del telefono è previsto un monitoraggio sul traffico di ogni utenza.

Smartphone e Tablet (Mobile). L'accesso allo *Smartphone o Tablet* deve avvenire attraverso l'attivazione di una *password* personale (attivazione dello *screen saver* automatico).

E' vietata la conservazione di documenti scaricati come allegati (a titolo esemplificativo: *e-mail, skype, Whatsapp, etc.*), il cui contenuto sia di carattere aziendale, se non per il tempo strettamente necessario.

Si raccomanda la massima attenzione nell'utilizzo di *App* sul proprio dispositivo, in relazione all'eccessivo consumo di traffico dati ed alla sicurezza del proprio apparato.

13. UTILIZZO DELLE STAMPANTI e FAX

È vietato l'utilizzo per fini personali dei sistemi multifunzione (sistemi di stampa, copia ed invio fax) e dei sistemi fax e aziendali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Responsabile.

Si raccomanda di non lasciare documenti incustoditi presso i suddetti dispositivi.

14. WIEDERVERWENDUNG VON DATENTRÄGERN

Nach der Verwendung von Datenträgern (USB-Sticks, interne und externe Festplatten, DVDs, CD-ROMs) sind die Daten gemäß vorgegebenen Verfahren zu löschen, damit sämtliche Informationen vor einer neuerlichen Nutzung der Datenträger entfernt sind.

15. ÜBERWACHUNGSSYSTEME

Der Inhaber kann, unter Berücksichtigung der Datenschutzbestimmungen und mit Hilfe des Systemadministrators, auf alle gemeindeeigenen IT-Geräte und die darin enthaltenen Daten sowie auf die Telefonabrechnungen zu folgenden Zwecken zugreifen: Gewährleistung der Sicherheit des IT-Systems, Wartung und andere technische Gründe (z.B. Aktualisierung, Ersatz und Implementierung von Programmen, Hardwarewartung usw.) sowie Kontrolle und Planung der betrieblichen Kosten (z.B. Überprüfung der Ausgaben für den Internetzugang und den Telefonverkehr). Solche Maßnahmen erfolgen aber keinesfalls zur Kontrolle der Arbeitstätigkeit.

Der Systemadministrator führt in geregelten Zeitabständen und bei Unregelmäßigkeiten (Antivirus-Eingriffe, Meldung über die Verlangsamung von Computern, unverhältnismäßige Nutzung des Internetzugangs, übermäßige Speicherbelegung der E-Mail-Box bzw. der Festplatte usw.) genaue Kontrollen durch. Dies kann Hinweise und Anweisungen an die Bediensteten der betroffenen Abteilungen / Bereiche zur Folge haben; die Benutzer werden dazu angehalten, die erteilten Anweisungen gewissenhaft zu befolgen.

Individuelle Kontrollen finden nur statt, wenn weitere Unregelmäßigkeiten auftreten.

Keinesfalls werden Kontrollen grundlos, kontinuierlich oder über längere Zeiträume durchgeführt.

16. SONSTIGE VORSCHRIFTEN

In Zweifeln bei der Verarbeitung der personen- und unternehmensbezogenen Daten bzw. über die Art der Verwendung der Mittel zur Datenverarbeitung, wenden Sie sich bitte an Ihren Verantwortlichen für die Datenverarbeitung.

Artikel 7

SANKTIONEN

Es ist verpflichtend für alle Nutzer, die Bestimmungen der vorliegenden Verordnung einzuhalten. Nichtbeachtung oder Verletzung der oben genannten Regeln durch die Bediensteten werden mit Disziplinarmaßnahmen und Schadenersatzforderungen gemäß geltendem Gesamtstaatlichem Kollektivvertrag sowie zivil- und strafrechtlich geahndet.

14. RIUTILIZZO DEI SUPPORTI DI MEMORIZZAZIONE

Al termine dell'utilizzo dei supporti di memorizzazione contenenti dati (chiavette USB, Hard Disk interni ed esterni, DVD, CD-Rom), questi dovranno essere cancellati secondo procedura, per eliminare ogni informazione contenuta prima di autorizzarne qualunque tipo di nuovo utilizzo.

15. SISTEMI DI MONITORAGGIO

Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/ sostituzione/ implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà del Titolare, tramite l'Amministratore di sistema, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali.

Periodicamente e in presenza di anomalie (intervento antivirus, segnalazione di rallentamenti del computer, utilizzo aziendalmente eccessivo dell'accesso Internet, dimensione elevata della casella di posta elettronica o dello spazio disco utilizzato, etc.), l'amministratore di sistema effettuerà verifiche di funzionalità approfondite che potranno determinare segnalazione ed avvisi generalizzati diretti ai dipendenti della funzione in cui è stata rilevata l'anomalia stessa e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.

In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

16. PRESCRIZIONE RESIDUALE

Per dubbi ed incertezze, in merito a come debba avvenire il trattamento dei dati e delle informazioni personali e aziendali, nonché sulle modalità di utilizzo degli strumenti di trattamento, può rivolgersi al proprio Responsabile del trattamento per ricevere le opportune istruzioni.

Articolo 7

SANZIONI

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL, nonché con tutte le azioni civili e penali consentite.

Artikel 8

AKTUALISIERUNG UND ÜBERARBEITUNG

Die vorliegende Verordnung wird laufend überarbeitet.

Alle künftigen Änderungen dieser Verordnung werden im Intranet der Gemeinde veröffentlicht.

Articolo 8

AGGIORNAMENTO E REVISIONE

Il presente Regolamento è soggetto a revisione con frequenza periodica.

Tutte le future modifiche del presente regolamento verranno rese pubbliche sull'intranet del Comune.

Artikel 9

In Kraft treten

1. Die vorliegende Verordnung tritt im Sinne des dritten Absatzes des Art. 8 der Gemeindesatzung ab dem Tag in Kraft, an dem der Genehmigungsbeschluss des Gemeinderates im Sinne der geltenden Bestimmungen vollstreckbar wird.

Articolo 9

Entrata in vigore

1. Ai sensi del terzo comma dell'art. 8 dello Statuto comunale il presente Regolamento entra in vigore dalla data in cui la deliberazione di approvazione del Consiglio comunale diviene esecutiva ai sensi delle norme vigenti.

Artikel 10

Schlussbestimmungen

1. Die Gemeinde sorgt im Sinne der Gemeindesatzung für eine weitestgehende Verbreitung dieser Verordnung.

2. Jeder Bürger hat nach Begleichung der Kopierkosten das Recht auf die Aushändigung einer vollständigen Kopie oder eines Auszuges dieser Verordnung.

3. Die vorliegende Verordnung hebt ab dem Tag ihrer Gültigkeit alle anderen vorhergehenden Verordnungen, welche dasselbe Sachgebiet regeln, auf.

Articolo 10

Disposizioni finali

1. Il comune garantisce la più ampia divulgazione di questo regolamento in conformità allo Statuto comunale.

2. Qualsiasi cittadino può ottenere copia, integrale o per estratto, del regolamento, previo rimborso delle spese di riproduzione.

3. Il presente regolamento revoca con il giorno della sua entrata in vigore tutte le ordinanze precedenti, le quali regolano la stessa materia.

DER GENERALSEKRETÄR
IL SEGRETARIO GENERALE
gez./f.to:
Bernhard Flor

DER BÜRGERMEISTER
IL SINDACO
gez./f.to:
Wilfried Trettl

CHRONOLOGIE

CRONOLOGIA

Genehmigung Ratsbeschluss Nr. Datum	**69** **20.10.2016**	Approvazione Delibera consiliare N. data
IN KRAFT AB	**05.11.2016**	IN VIGORE DAL

C:\Users\monika_eppan\Desktop\d3Archiv\Privacy-Bestimmungen der Gemeinde Eppan - Erstfassung Oktober 2016(A400174722).ODT

ÄNDERUNGEN

MODIFICHE

Genehmigungsbeschluss Deliberazione di approvazione		von der Änderung betroffene Artikel articoli soggetto alla modifica	Änderung in Kraft ab modifica in vigore dal
Nr.	Datum		

DER GENERALSEKRETÄR
IL SEGRETARIO GENERALE
gez./f.to:
Bernhard Flor

DER BÜRGERMEISTER
IL SINDACO
gez./f.to:
Wilfried Trett

Anmerkungen

zu Art.

Note

all'art.