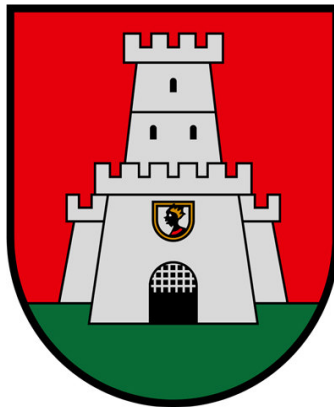


Marktgemeinde Innichen

Comune di San Candido

AUTONOME PROVINZ BOZEN-SÜDTIROL
PROVINCIA AUTONOMA DI BOLZANO-ALTO ADIGE



Verhaltenskodex für das Personal der Gemeinde Innichen

Codice di comportamento del personale del Comune di San Candido

Genehmigt mit Ausschussbeschluss Nr. 365/14 vom 02.12.2014

Approvato con deliberazione consiliare n. 365/14 del 02.12.2014

Ergänzt mit Ausschussbeschluss Nr. 652/22 vom 29.12.2022

Modificato con delibera della Giunta comunale n. 652/22 del 29.12.2022

Prämissen

Der Artikel 4 des Gesetzesdekrets Nr. 36 vom 30. April 2022 (zur Änderung von Artikel 54 des Gesetzesdekrets Nr. 165 vom 30. März 2001) verpflichtet die öffentlichen Verwaltungen, ihre Verhaltenskodexe zu ergänzen mit:

"einer Sektion, die sich mit der korrekten Nutzung der Informationstechnologie und der sozialen Medien durch öffentliche Bedienstete befasst, auch um das Image der öffentlichen Verwaltung zu schützen".

Der in Artikel 54 des gesetzesvertretenden Dekrets Nr. 165 vom 30. März 2001 genannte Verhaltenskodex "wird bis zum 31. Dezember 2022 aktualisiert, auch um die in Absatz 1 genannten Bestimmungen umzusetzen".

"Die öffentlichen Verwaltungen sehen die Durchführung eines obligatorischen Schulungszyklus vor, der sowohl nach der Einstellung als auch bei jeder Übertragung höherer Aufgaben oder Funktionen sowie bei Personalversetzungen durchgeführt wird und dessen Dauer und Intensität dem Grad der Verantwortung in Fragen der öffentlichen Ethik und des ethischen Verhaltens, im Rahmen der nach den geltenden Rechtsvorschriften zur Verfügung stehenden finanziellen Mittel angemessen ist".

Die erste Anwendung der Verpflichtung zur Aktualisierung des Ethik- und Verhaltenskodex wurde mit der Verabschiedung des "Leitfadens für die Nutzung von Cloud-Lösungen" und der "Anleitung für die Arbeit mit Privat- oder Betriebsgeräten" umgesetzt, die diesem Kodex beigefügt sind und einen integrierten Bestandteil desselben bilden.

Premessa

L'art. 4 del D.L. n° 36 del 30 aprile 2022 (modifica dell'art. 54 del dec. legisl. 165 del 30 marzo 2001) impone alle Pubbliche amministrazioni di integrare i propri codici di comportamento con:

"una sezione dedicata al corretto utilizzo delle tecnologie informatiche e dei mezzi di informazione e social media da parte dei dipendenti pubblici, anche al fine di tutelare l'immagine della pubblica amministrazione".

Il codice di comportamento di cui all'articolo 54 del decreto legislativo 30 marzo 2001, n. 165, "è aggiornato entro il 31 dicembre 2022 anche al fine di dare attuazione alle disposizioni di cui al comma 1".

"Le pubbliche amministrazioni prevedono lo svolgimento di un ciclo formativo obbligatorio, sia a seguito di assunzione, sia in ogni caso di passaggio a ruoli o a funzioni superiori, nonché di trasferimento del personale, le cui durata e intensità sono proporzionate al grado di responsabilità, nei limiti delle risorse finanziarie disponibili a legislazione vigente, sui temi dell'etica pubblica e sul comportamento etico".

Una prima attuazione dell'obbligo di aggiornamento del Codice Etico e di Comportamento è stata data con l'adozione delle "Linee guida per l'utilizzo di soluzioni cloud" e delle "Istruzioni per il lavoro con dispositivi privati o aziendali" che si allegano al presente Codice e ne costituiscono parte integrante.

INHALTSVERZEICHNIS

INDICE

Art.	Beschreibung	Descrizione
	Prämissen	Premessa
Art. 1	Anwendungsbereich	Ambito di applicazione
Art. 2	Dienstplichten	Obblighi di servizio
Art. 3	Verhalten im Parteienverkehr	Rapporti con il pubblico
Art. 4	Verhaltenspflichten im Dienst	Obblighi di comportamento in servizio
Art. 5	Verhalten des Gemeindesekretärs und der Leiter und Leiterinnen der Organisationseinheiten	Comportamento del segretario comunale/della segretaria comunale e dei/delle responsabili di unità organizzativa
Art. 6	Korruptionsvorbeugung	Prevenzione della corruzione
Art. 7	Interessenkonflikt und Enthaltungspflicht	Conflitto di interessi e relativo obbligo di astensione
Art. 8	Transparenz und Rückverfolgbarkeit	Trasparenza e tracciabilità
Art. 9	Gesundheit und Sicherheit am Arbeitsplatz	Salute e sicurezza sul posto di lavoro
Art. 10	Sicherheit im Bereich der Informatik	Sicurezza informatica
Art. 10.1	IT-Ausstattung (Hardware und Software)	Dotazioni informatiche (hardware e software)
Art. 10.2	Beziehungen mit den "Medien"	Rapporti con i "media"
Art. 10.3	Nutzung der "social Networks"	Utilizzo dei "social network"
Art. 10.4	Außerberufliche Nutzung von "sozialen Medien"	Utilizzo extralavorativo dei "social-media"
Art. 10.5	Haftung	Responsabilità
Art. 10.6	Dritte Parteien	Terze parti
Art. 11	Aus- und Weiterbildung	Attività formative e di aggiornamento
Art. 12	Haftung bei Verletzung von Pflichten des Kodexes	Responsabilità conseguente alla violazione dei doveri del codice

Anlagen

Allegati

1.A)	Anleitung für die Arbeit mit Privatgeräten	Istruzioni per il lavoro con dispositivi privati
1.B)	Anleitung für die Arbeit mit Betriebsgeräten	Istruzioni per il lavoro con dispositivi aziendali
1.C)	Verwendungsvorgaben für die Nutzung von Cloud-Lösungen	Linee guida per l'utilizzo di soluzioni cloud

Art. 1

Anwendungsbereich

1. Dieser Verhaltenskodex legt die dienstlichen Pflichten und Verhaltensregeln des Gemeindepersonals, in der Folge „Personal“ genannt, fest. Die Bestimmungen gelten auch, sofern vereinbar, für die folgenden Kategorien von Personen: Mitarbeiter und Mitarbeiterinnen sowie Berater und Beraterinnen mit jeder Art von Vertrag oder Auftrag, aufgrund welchen Rechtstitels auch immer, Personen, die Organe vertreten, Inhaberinnen und Inhaber von Aufträgen, Mitarbeiterinnen und Mitarbeiter, aufgrund welchen Rechtstitels auch immer, von Unternehmen, die der Gemeindeverwaltung Waren liefern, Dienstleistungen für sie erbringen oder Arbeiten für sie ausführen. Zu diesem Zweck werden in den Beauftragungen und in den Verträgen, die eine Zusammenarbeit, eine Beratung oder eine Dienstleistung zum Gegenstand haben, entsprechende Bestimmungen oder Klauseln zur Aufhebung oder Verwirkung des Rechtsverhältnisses für den Fall eingefügt, dass in diesem Kodex vorgesehene Pflichten verletzt werden.

Art. 2

Dienstplichten

1. Das Personal verhält sich im Dienst nach den Grundsätzen der guten Verwaltung und der Unparteilichkeit der Verwaltung; dabei übt es seine Aufgaben unter Beachtung der Gesetze und unter Berücksichtigung des öffentlichen Interesses aus. Das Personal gewährleistet die optimale Qualität des Dienstes; in diesem Sinne

- a) hält es die Arbeitszeit nach den Vorgaben der Verwaltung ein,
- b) erfüllt es seine Aufgaben mit Sorgfalt,
- c) befolgt es die von den Vorgesetzten im Rahmen der institutionellen Tätigkeit erteilten Anweisungen loyal und unverzüglich,
- d) wahrt es das Amtsgeheimnis.

2. Wer sich weigern will, einer Anweisung Folge zu leisten, weil sie für rechtswidrig gehalten wird, muss dies der vorgesetzten Führungskraft mit Angabe der Gründe schriftlich mitteilen. Erteilt die Führungskraft die Anweisung daraufhin schriftlich, so muss ihr Folge geleistet werden, es sei denn, es handelt sich um eine vom Strafgesetz verbotene Handlung.

3. Das Personal leitet Unberechtigten weder Informationen über laufende oder abgeschlossene Maßnahmen und Verfahren der Verwaltung weiter noch Informationen, von denen es in Ausübung seiner Funktionen Kenntnis erhalten hat. Ausgenommen sind die Fälle und Vorgehensweisen, die die Vorschriften über das Recht auf Aktenzugang anführen. Das

Art. 1

Ambito di applicazione

1. Il presente codice di comportamento definisce gli obblighi di servizio e di comportamento del personale comunale, di seguito denominato "personale". Le disposizioni in esso contenute si applicano, per quanto compatibili, anche alle seguenti categorie di persone: a tutti i collaboratori e le collaboratrici nonché ai/alle consulenti, con qualsiasi tipologia di contratto o incarico e a qualsiasi titolo, ai/alle titolari di organi e di incarichi nonché nei confronti di collaboratrici e collaboratori - a qualsiasi titolo - di imprese fornitrici di beni o servizi e che realizzano opere in favore dell'Amministrazione comunale. A tal fine, negli atti di incarico o nei contratti di acquisizione delle collaborazioni, delle consulenze o dei servizi, sono inserite apposite disposizioni o clausole di risoluzione o decadenza del rapporto in caso di violazione degli obblighi derivanti dal presente codice.

Art. 2

Obblighi di servizio

1. Il personale conforma la propria condotta in servizio ai principi del buon andamento e dell'imparzialità dell'Amministrazione, svolgendo i propri compiti nel rispetto della legge e dell'interesse pubblico. Per garantire la migliore qualità del servizio, il personale in particolare:

- a) osserva l'orario di lavoro secondo le modalità stabilite dall'Amministrazione;
- b) espleta con diligenza i propri compiti;
- c) esegue lealmente e prontamente le disposizioni impartite dai superiori nell'ambito dell'attività istituzionale;
- d) mantiene il segreto d'ufficio.

2. Chi intende rifiutare l'esecuzione di disposizioni ritenute illegittime, deve comunicarlo per iscritto al/alla propria dirigente, specificando i motivi del rifiuto. Se il/la dirigente rinnova le disposizioni per iscritto, queste devono essere eseguite, salvo che si tratti di attività vietate dalla legge penale.

3. Il personale non trasmette a chi non ne abbia diritto informazioni riguardanti operazioni o provvedimenti amministrativi in corso o conclusi, ovvero notizie di cui sia venuto a conoscenza nell'esercizio delle sue funzioni, fatta eccezione per le ipotesi e le modalità previste dalle norme sul diritto di accesso agli atti. Il personale osserva le norme

Personal beachtet die Datenschutzbestimmungen, insbesondere im Hinblick auf sensible Daten und Gerichtsdaten.

4. Das Personal vermeidet Situationen und Verhaltensweisen, die die korrekte Ausübung der Aufgaben verhindert oder das Ansehen der Gemeinde schädigen könnten.

5. Das Personal darf mit Ausnahme der mit Verordnung geregelten freien Tätigkeiten ohne entsprechende Ermächtigung der Verwaltung keine Nebentätigkeit ausüben.

Art. 3

Verhalten im Parteienverkehr

1. Im Parteienverkehr verhält sich das Personal stets korrekt, entgegenkommend und höflich; es gewährleistet die Gleichbehandlung der Bürgerinnen und Bürger so, dass zwischen diesen und der Verwaltung sowie unter den verschiedenen Sprachgruppen ein Verhältnis des Vertrauens und der loyalen Zusammenarbeit entsteht.

2. In der schriftlichen und in der mündlichen Kommunikation mit den Bürgerinnen und Bürgern verwendet das Personal eine klare, einfache und verständliche Sprache; es sorgt dafür, dass die Bürgerinnen und Bürger aller drei Sprachgruppen im Sinne der geltenden Bestimmungen auf natürliche, spontane Art und Weise in ihrer Muttersprache kommunizieren können.

3. Im Parteienverkehr bemüht sich das Personal, eventuelle sprachliche und kulturelle Hürden zu überwinden und dadurch ein vertrauensvolles Verhältnis gegenseitiger Wertschätzung aufzubauen.

Art. 4

Verhaltenspflichten im Dienst

1. Das Personal

a) arbeitet loyal sowohl mit den Vorgesetzten als auch mit den Kolleginnen und Kollegen zusammen;

b) behandelt alles, was der Gemeinde gehört, mit größter Sorgfalt;

c) beteiligt sich weder direkt noch indirekt an Werkverträgen, Lieferungen, Konzessionen oder anderen Geschäften, an denen die Gemeinde teil hat,

d) wirkt nicht an Entscheidungen oder Tätigkeiten mit, die einen Interessenskonflikt gemäß Artikel 7 zur Folge haben können,

e) enthält sich jeder Handlung, Verhaltensweise

sulla tutela dei dati personali, in particolare per quanto riguarda i dati sensibili e giudiziari.

4. Il personale evita situazioni e attitudini che impediscono l'espletamento corretto delle mansioni e che potrebbero danneggiare la reputazione del comune.

5. Il personale deve ad eccezione delle attività libere disciplinate con regolamento astenersi dallo svolgere attività extraservizio senza la relativa autorizzazione dell'Amministrazione.

Art. 3

Rapporti con il pubblico

1. Nei rapporti con il pubblico il personale mostra disponibilità e cortesia, si comporta correttamente e assicura parità di trattamento a cittadine e cittadini, in modo tale da stabilire un rapporto di piena fiducia e di leale collaborazione tra questi e l'Amministrazione, nonché tra i gruppi linguistici.

2. Nella redazione dei testi scritti e nelle comunicazioni orali con le cittadine e i cittadini, il personale usa un linguaggio chiaro, semplice e comprensibile e garantisce alle cittadine e ai cittadini di tutti e tre i gruppi linguistici l'uso naturale e spontaneo della madrelingua nel rispetto della vigente normativa.

3. Nei rapporti con il pubblico, il personale si adopera per superare eventuali difficoltà linguistiche e culturali e instaurare un rapporto di reciproca fiducia e rispetto.

Art. 4

Obblighi di comportamento in servizio

1. Il personale

a) si ispira ad uno spirito di leale collaborazione nei rapporti con i superiori e con le colleghe e i colleghi;

b) ha la massima cura di tutto quanto appartiene al Comune;

c) si astiene dal prendere parte, direttamente o indirettamente, ad appalti, forniture, concessioni e attività in cui sia interessato il Comune;

d) si astiene dal prendere parte a decisioni o ad attività che possano generare un conflitto di interessi ai sensi dell'articolo 7.

e) si astiene da atti, comportamenti o molestie

und Belästigung, die andere in ihrer Menschenwürde verletzt. Das Personal vermeidet somit jede Verhaltensweise, die eine Diskriminierung aufgrund des Geschlechts, der ethnischen Herkunft, der Religion, der Weltanschauung, eventueller Beeinträchtigungen, des Alters oder der sexuellen Ausrichtung darstellt.

f) gestaltet die Tätigkeit so, dass Wirtschaftlichkeit, Effizienz und Wirksamkeit der Verwaltungstätigkeit gewährleistet werden. Dabei sollen stets mögliche Einsparungen ohne Beeinträchtigung der Qualität der Ergebnisse geprüft werden.

g) wickelt die Verfahren unter Beachtung der diesbezüglichen Vorschriften zügig ab und vermeidet ungerechtfertigte Verzögerungen.

2. Das Personal

a) entfernt sich, außer in den zulässigen Fällen, nur aus dienstlichen Gründen vom Dienst;

b) geht im Amt keinen außerdienstlichen Geschäften und Beschäftigungen nach und nutzt das Amt nicht für private Zwecke;

c) entfernt amtliche Unterlagen nur aus dienstlichen Gründen aus dem Büro.

Art. 5

Verhalten des Gemeinsekretärs/der Gemeinsekretärin und der Leiter und Leiterinnen der Organisationseinheiten

1. Das Personal (Gemeinsekretär/Gemeinsekretärin sowie Leiter und Leiterinnen der Organisationseinheiten) übt seinen Auftrag mit Sorgfalt aus; es verfolgt die ihm vorgegebenen Ziele und ergreift im Rahmen der ihm zur Verfügung stehenden Mittel die organisatorischen Maßnahmen, die zur Erfüllung seines Auftrags notwendig sind.

2. Vor Übernahme des Auftrags erklärt es, ob es Verwandte und Verschwägerte bis zum zweiten Grad hat, welche politische, berufliche oder wirtschaftliche Tätigkeiten ausüben, sodass sie häufig mit der Gemeinde/Organisationseinheit, welcher es vorstehen wird, in Kontakt kommen, oder die in irgendeiner Form in Entscheidungen oder Tätigkeiten der Organisationseinheit eingebunden sind. Dasselbe gilt für die Ehepartner beziehungsweise die Person, mit der es zusammenlebt.

3. Das Personal verhält sich loyal und transparent; es ist unparteiisch im Umgang mit den Kolleginnen und Kollegen, den Mitarbeiterinnen und Mitarbeitern und mit den Bürgern. Es sorgt dafür, dass die der Gemeinde/der Struktur zugewiesenen Ressourcen ausschließlich für institutionelle und in keinem Falle für persönliche Zwecke genutzt werden.

4. Das Personal schafft innerhalb der Gemeinde/seiner Struktur ein positives Arbeitsklima

lesivi della dignità della persona. Il personale si astiene pertanto da ogni comportamento od omissione che comporti una discriminazione per motivi di sesso, provenienza etnica, religione, ideologia, disabilità, età e orientamento sessuale.

f) esercita le proprie mansioni garantendo economicità, efficienza ed efficacia dell'attività amministrativa e seguendo una logica di contenimento dei costi senza pregiudicare la qualità dei risultati;

g) svolge i procedimenti in osservanza delle relative disposizioni in modo tempestivo, evitando ritardi ingiustificati.

2. Il personale

a) non si assenta dal servizio per motivi estranei ai propri obblighi di servizio, salvo nei casi consentiti;

b) non attende in ufficio ad attività o ad occupazioni estranee al servizio e non usa l'ufficio per motivi privati;

c) non asporta dall'ufficio documenti, salvo che per ragioni di servizio.

Art. 5

Comportamento del segretario comunale/della segretaria comunale e dei/delle responsabili di unità organizzativa

1. Il personale (segretario comunale/segretaria comunale e responsabili di unità organizzativa) svolge con diligenza le funzioni ad esso spettanti, persegue gli obiettivi assegnati e adotta nel rispetto degli strumenti a disposizione un comportamento organizzativo adeguato per l'assolvimento dell'incarico.

2. Il personale, prima di assumere l'incarico dichiara se ha parenti e affini entro il secondo grado, coniuge o convivente che esercitano attività politiche, professionali o economiche che li pongano in contatti frequenti con l'unità organizzativa che dovrà dirigere o che siano coinvolti nelle decisioni o nelle attività inerenti alla stessa.

3. Il personale adotta un comportamento leale e trasparente e si rapporta in modo imparziale con le colleghe e i colleghi, le collaboratrici e i collaboratori e con il pubblico. Si occupa che le risorse assegnate al proprio ufficio siano utilizzate per finalità esclusivamente istituzionali e, in nessun caso, per esigenze personali.

4. Il personale promuove all'interno del comune/nella propria struttura un clima di lavoro positivo e di

Entscheidungen der Organisationseinheit von Verwandten oder Verschwägerten bis zum zweiten Grad sowie von zusammenlebenden Personen ebenfalls verbunden mit der Pflicht, Änderungen an diesen Umständen zu melden. Auf begründeten Antrag der vorgesetzten Führungskraft oder der Personalverwaltung liefert das Personal zusätzliche Informationen über das eigene Vermögen und Einkommen.

4. Das Personal hält sich an die Vorschriften des Antikorruptionsplans; es arbeitet mit dem oder der Antikorruptionsbeauftragten zusammen und meldet, unbeschadet der Meldepflicht bei der Gerichtsbehörde, der vorgesetzten Führungskraft rechtswidrige Situationen innerhalb der Verwaltung, von denen es Kenntnis erhält.

Art. 7

Interessenkonflikt und Enthaltungspflicht

1. Das Personal wirkt weder an Entscheidungen noch an Tätigkeiten, einschließlich der Vorbereitung und des Abschlusses von Verträgen mit, die mit folgenden Interessen in Zusammenhang stehen können: mit eigenen Interessen, mit Interessen von Verwandten und Verschwägerten bis zum zweiten Grad, mit Interessen des Ehepartners/der Ehepartnerin, mit Interessen von Personen, mit denen der oder die Bedienstete zusammenlebt, oder mit Interessen von Personen, mit denen der oder die Bedienstete selbst oder der Ehepartner/die Ehepartnerin häufigen Umgang pflegt, sowie mit Interessen von Rechtspersonen und Organisationen, gegen welche der oder die Bedienstete selbst oder der Ehepartner/die Ehepartnerin ein Streitverfahren anhängig ist oder mit denen er oder sie schwer zerstritten ist.

2. Jeder andere Fall, bei welchem sich schwerwiegende Gründe ergeben, ist der vorgesetzten Führungskraft unverzüglich zu melden; diese entscheidet über die allfällige Enthaltungspflicht.

Art. 8

Transparenz und Rückverfolgbarkeit

1. Das Personal erfüllt seine Pflichten im Hinblick auf die Transparenz nach den geltenden Bestimmungen; in diesem Sinne trägt es im Rahmen der jeweiligen Zuständigkeit so weit wie möglich dazu bei, dass die Daten, die auf der Homepage zu veröffentlichen sind, dementsprechend verarbeitet, beschafft und übermittelt werden.

2. Die Verfahrensschritte und Entscheidungsprozesse in der Verwaltung müssen so dokumentiert sein, dass sie jederzeit rückverfolgt und reproduziert werden können.

organizzativa da parte di parenti o affini fino al secondo grado o di persone conviventi. Su motivata richiesta della dirigente preposta/del dirigente preposto o dell'amministrazione del personale, il personale fornisce ulteriori informazioni sulla propria situazione patrimoniale e reddituale.

4. Il personale rispetta le prescrizioni contenute nel piano per la prevenzione della corruzione, collabora con il/la responsabile per la prevenzione della corruzione e, fermo restando l'obbligo di denuncia all'autorità giudiziaria, segnala alla dirigente preposta/al dirigente preposto eventuali situazioni di illecito nell'Amministrazione, di cui sia venuto a conoscenza.

Art. 7

Conflitto di interessi e relativo obbligo di astensione

1. Il personale si astiene dal partecipare all'adozione di decisioni o ad attività incluso la preparazione e la stipula di contratti che possano coinvolgere interessi propri, ovvero interessi di parenti o affini sino al secondo grado, della/del coniuge, di conviventi, oppure di persone con le quali abbia rapporti di frequentazione abituale, ovvero di soggetti od organizzazioni con cui il/la dipendente o il/la coniuge abbia causa pendente o grave inimicizia.

2. Ogni altro caso in cui esistano gravi ragioni di convenienza va immediatamente segnalato al dirigente preposto/alla dirigente preposta, che deciderà sull'eventuale obbligo di astensione.

Art. 8

Trasparenza e tracciabilità

1. Il personale assicura l'adempimento degli obblighi di trasparenza secondo le disposizioni normative vigenti nell'ambito di propria competenza, prestando la massima collaborazione nell'elaborazione, nel reperimento e nella trasmissione dei dati sottoposti all'obbligo di pubblicazione sul sito istituzionale.

2. La tracciabilità degli iter procedurali e dei processi decisionali adottati dall'Amministrazione deve essere garantita, in tutti i casi, attraverso un adeguato supporto documentale, che consenta in

ogni momento la replicabilità.

Art. 9

Gesundheit und Sicherheit am Arbeitsplatz

1. Die Gemeinde betrachtet die Gesundheit und die Sicherheit am Arbeitsplatz als vorrangiges Gut; sie fördert daher die Zusammenarbeit des gesamten Personals zur ständigen Verbesserung der Sicherheitsbedingungen.

2. Das Personal und die im Sinne der Bestimmungen im Bereich Gesundheit und Sicherheit am Arbeitsplatz bestimmten „Führungskräfte“ und „Vorgesetzten“ sind aktiv am Prozess zur Vorbeugung von Risiken und zum Schutz vor Risiken am Arbeitsplatz beteiligt.

3. Der Arbeitgeber und der/die Vorgesetzte im Sinne der Bestimmungen über die Gesundheit und Sicherheit am Arbeitsplatz;

a) erfüllen sämtliche Pflichten, welche die gesetzlichen Bestimmungen vorsehen;

b) organisieren die Tätigkeiten der Mitarbeiterinnen und Mitarbeiter im Einklang mit den gesetzlichen Bestimmungen im Bereich der Gesundheit und Sicherheit am Arbeitsplatz und sorgen dafür, dass sie die Bestimmungen einhalten;

c) nehmen an den jeweils vorgesehenen Weiterbildungsveranstaltungen im Bereich Sicherheit am Arbeitsplatz teil.

4. Das Personal

a) beachtet die Bestimmungen über Gesundheit und Sicherheit am Arbeitsplatz; insbesondere beachtet es die Vorschriften und Anweisungen des vorgesetzten Personals. Es achtet auf die eigene Gesundheit und Sicherheit sowie auf jene der anderen Personen im Arbeitsumfeld, auf die sich seine Handlungen und Verhaltensweisen oder auch das Unterlassen von Handlungen in irgendeiner Form auswirken, jeweils entsprechend der eigenen Ausbildung, den Anweisungen und den Mitteln, die vom vorgesetzten Personal zur Verfügung gestellt werden;

b) meldet dem vorgesetzten Personal sicherheitsgefährdende Verhaltensweisen von Kolleginnen und Kollegen, nicht angemessen gesicherte Gefahrenquellen, Risikosituationen am Arbeitsplatz sowie Vorbeugungs- und Schutzmaßnahmen, die für die durchgeführte Tätigkeit unzulänglich sind;

c) schlägt Maßnahmen zur Verbesserung der Arbeitsbedingungen im Hinblick auf die eigene Gesundheit und Sicherheit sowie jene der Kolleginnen und Kollegen vor;

d) nimmt an Aus- und Weiterbildungs-

Art. 9

Salute e sicurezza sul posto del lavoro

1. L'Amministrazione comunale considera la salute e la sicurezza sul posto di lavoro un bene primario e auspica pertanto una collaborazione fattiva da parte del personale, al fine di garantire un costante miglioramento delle condizioni di sicurezza.

2. Il personale, così come “le/i dirigenti” e “le preposte/i preposti” ai sensi della normativa in materia di salute e sicurezza sul lavoro, sono parte attiva del processo di prevenzione e protezione dai rischi sul posto di lavoro.

3. Il datore di lavoro e i preposti ai sensi della normativa in materia di salute e sicurezza sul lavoro;

a) adempiono agli obblighi previsti dalla normativa;

b) organizzano l'attività di collaboratori e collaboratrici nel rispetto della normativa in materia di salute e sicurezza sul lavoro e vigilano sulla osservanza degli obblighi di legge da parte degli stessi;

c) partecipano ai corsi di formazione in materia di sicurezza sul posto di lavoro, previsti per loro.

4. Il personale

a) osserva le norme in materia di salute e sicurezza sul lavoro e, in particolare, osserva le disposizioni e le istruzioni impartite dal personale preposto; si prende cura della salute e della sicurezza propria e delle altre persone presenti sul luogo di lavoro, sulle quali ricadono gli effetti delle sue azioni o omissioni, conformemente alla sua formazione, alle istruzioni e ai mezzi forniti dal personale preposto;

b) segnala al personale preposto comportamenti non sicuri da parte dei colleghi, pericoli non adeguatamente protetti, situazioni di rischio presenti sul posto di lavoro nonché eventuali misure di prevenzione e protezione non adeguate all'attività svolta;

c) propone misure di miglioramento delle condizioni di lavoro in relazione alla salute e sicurezza proprie e dei colleghi;

d) partecipa ai corsi di formazione e di

veranstaltungen teil und unterzieht sich den Kontrollvisiten, die eventuell aufgrund der Risikobewertung erforderlich sind.

Art. 10

Sicherheit im Bereich Informatik

1. Alle informationstechnischen Instrumente, die von der Verwaltung zur Verfügung gestellt werden, sowohl Software als auch Hardware, sind ausschließlich für dienstliche Zwecke zu verwenden.

2. Die Sicherheitserfordernisse verändern sich kontinuierlich und stellen dauerhaft eine Gefahr dar. Folgende Sicherheitsvorkehrungen sollen dazu beitragen, Situationen zu vermeiden, die für einzelne Personen und für die Verwaltung gefährlich sein können:

- a) sich nicht mit betrügerischen Mitteln verleiten lassen, vertrauliche Informationen weiterzuleiten;
- b) auf die Daten der Gemeinde nie über Computer ohne Virenschutzsoftware zugreifen;
- c) sensible Informationen nie unbeaufsichtigt im Büro liegen lassen;
- d) Computer und Mobiltelefone sperren, sobald sie nicht benutzt werden;
- e) Dateien und bewegliche Datenträger mit sensiblen Daten durch ein Passwort schützen;
- f) verdächtigen E-Mails und Links nicht trauen;
- g) keine persönlichen Geräte ohne vorherige Genehmigung durch die Verwaltung anschließen;
- h) keine Programme auf den Arbeitscomputer herunterladen, außer mit Ermächtigung.

Art. 10.1

IT-Ausstattung (Hardware und Software)

1. Der richtige Umgang mit IT-Geräten ist ein wesentlicher Bestandteil der Arbeit.

2. Die ständige Weiterentwicklung der Technologie erfordert eine immer größere Aufmerksamkeit für die Sicherheit der verwendeten Instrumente und eine Arbeitsethik, die auf die uneingeschränkte Achtung des Schutzes personenbezogener Daten und die Einhaltung des Gesetzes 633/1941 über das Urheberrecht abzielt (ausschließliche Verwendung von Computerprogrammen - von der Verwaltung zur Verfügung gestellte Software).

3. Es wird ausdrücklich auf die "Hinweise für die Arbeit mit privaten oder betrieblichen Geräten" und auf die oben erwähnten "Leitlinien für die Nutzung von

addestramento e si sottopone ai controlli sanitari, se necessari, sulla base della valutazione dei rischi.

Art. 10

Sicurezza informatica

1. L'uso di tutti gli strumenti IT, sia che si tratti di software o di hardware, messi a disposizione dall'Amministrazione, è limitato alle necessità lavorative.

2. Le minacce alla sicurezza si evolvono col trascorrere del tempo e rappresentano un rischio costante. Adottando i seguenti comportamenti si evitano situazioni compromettenti per le singole persone e per l'Amministrazione:

- a) Non lasciarsi indurre con l'inganno a fornire informazioni di natura riservata.
- b) Evitare di accedere ai dati del comune utilizzando un computer sprovvisto di protezione.
- c) Non lasciare incustodite in ufficio informazioni di natura sensibile.
- d) Bloccare computer e telefoni cellulari quando non sono in uso.
- e) Proteggere con password i file e i dispositivi mobili di natura sensibile
- f) Non fidarsi di e-mail e link sospetti.
- g) Non connettere dispositivi personali senza l'approvazione dell'Amministrazione comunale.
- h) Evitare di installare programmi non autorizzati sui computer utilizzati al lavoro.

Art. 10.1

Dotazioni informatiche (hardware e software)

1. Il corretto utilizzo delle dotazioni informatiche è parte fondamentale dell'attività lavorativa.

2. La continua evoluzione delle tecnologie impone una sempre maggiore attenzione alla sicurezza degli strumenti utilizzati ed un'etica del lavoro volta al pieno rispetto della protezione dei dati personali ed al rispetto della L. 633/1941 in materia di diritto d'autore (utilizzo dei soli programmi per elaboratore – software messi a disposizione dall'Amministrazione).

3. Si rimanda integralmente alle "Istruzioni per il lavoro con dispositivi privati o aziendali" ed alle "Linee guida per l'utilizzo di soluzioni cloud" sopra citate.

Cloud-Lösungen" verwiesen.

Art. 10.2

Beziehungen mit den "Medien"

1. Die Beziehungen der Verwaltung zu den so genannten "Medien" müssen von der Notwendigkeit geprägt sein, professionell, klar und zeitnah auf Aktivitäten, Dienstleistungen für die Bürger, Berichte über kritische Fragen oder Probleme, aber auch auf qualifizierende und positive Ereignisse zu reagieren, die die politisch-administrative Verwaltung der Körperschaft kennzeichnen. Mit dem Inkrafttreten des Gesetzesdekrets 33/2013 (das sogenannte Transparenzdekret) sind die Verwaltungen verpflichtet, über ihre Organisation und ihre Tätigkeiten Rechenschaft abzulegen, indem sie auf ihrer institutionellen Website die Rubrik "Transparente Verwaltung" einrichten.

2. Die Kommunikation mit den Medien muss mit dem übereinstimmen, was im Abschnitt "Transparente Verwaltung" veröffentlicht wird, und sie muss von größtmöglicher Transparenz gegenüber den Bürgern geprägt sein.

3. Für die Kommunikation mit den Medien (Presse, Fernsehen, Radio und soziale Netzwerke) sind die "politischen" Vertretungsorgane zuständig, d.h. Ausschuss und Rat.

4. Sollten Bedienstete oder externe Mitarbeiter der Gemeinde von den "Medien" kontaktiert werden, um Informationen oder Nachrichten über die Tätigkeit der Verwaltung zu verbreiten, müssen sie unverzüglich ihren direkten Vorgesetzten oder die politischen Vertretungsorgane informieren.

5. Der Arbeitnehmer muss bei allen Formen der direkten Kommunikation die gesetzlichen Bestimmungen über das Berufsgeheimnis und den Schutz personenbezogener Daten einhalten.

Art. 10.3

Nutzung der "social Networks"

1. Die "vernetzte Welt" begünstigt zweifellos die zwischenmenschliche Kommunikation, birgt aber andererseits auch ein hohes Risiko für die Verwaltungen. Daher ist es notwendig, die Aktivitäten von öffentlichen Bediensteten auf "sozialen" Plattformen, egal auf welcher Ebene, umfassend zu regeln.

2. Die "soziale" Tätigkeit der öffentlichen Bediensteten, sei es auf persönlichen oder institutionellen Konten, darf niemals die Würde und Ehre der Verwaltung gefährden.

3. Die oberflächliche, respektlose oder kriminelle Nutzung "sozialer" Plattformen kann nicht nur das Image der Verwaltung ernsthaft schädigen, sondern

Art. 10.2

Rapporti con i "media"

1. I rapporti dell'Amministrazione con i cosiddetti "media" devono essere improntati alla necessità di rispondere con professionalità, chiarezza e tempestività in merito all'attività, ai servizi ai cittadini, alle segnalazioni di criticità o problemi, ma anche agli eventi qualificanti e positivi che caratterizzano la gestione politico-amministrativa dell'Ente. L'entrata in vigore del dec. legisl. 33/2013 (cd. decreto trasparenza) ha imposto alle Amministrazioni di dare conto della propria organizzazione e delle proprie attività tramite l'istituzione della sezione "Amministrazione Trasparente" sul proprio sito web istituzionale.

2. Le comunicazioni con i mezzi di informazione dovranno essere coerenti con quanto pubblicato nella sezione "Amministrazione Trasparente" e dovranno essere improntate alla massima trasparenza nei confronti dei cittadini.

3. La titolarità delle comunicazioni con i media (stampa, televisioni, radio e social network) è in capo agli organi di rappresentanza "politica", ovvero al Consiglio ed alla Giunta.

4. Nel caso in cui i dipendenti o collaboratori esterni dell'Ente fossero contattati dai "media" al fine di rilasciare informazioni o notizie sull'attività dell'Amministrazione, questi dovranno informare tempestivamente il loro diretto superiore oppure gli organi di rappresentanza politica.

5. Il dipendente, nelle forme di comunicazione diretta, è tenuto a rispettare le disposizioni di legge in merito al segreto professionale ed alla protezione dei dati personali.

Art. 10.3

Utilizzo dei "social network"

1. Il "mondo interconnesso" favorisce indubbiamente le comunicazioni interpersonali ma rappresenta, di contro, un rischio elevato per le Amministrazioni. Nasce, quindi, l'esigenza di regolare compiutamente l'attività dei pubblici dipendenti, a qualunque livello, sulle piattaforme "social".

2. L'attività "social" dei pubblici dipendenti, sia con account personali che istituzionali, non deve mai compromettere la dignità e l'onorabilità dell'Amministrazione.

3. L'utilizzo superficiale, irrispettoso o delittuoso delle piattaforme "social", oltre a cagionare gravi danni di immagine all'Amministrazione può

auch den Straftatbestand der Beleidigung, Verleumdung und üblen Nachrede erfüllen.

4. Die Bediensteten des öffentlichen Dienstes müssen sich darüber im Klaren sein, dass sie nicht einfach nur Privatpersonen sind, sondern stets als Angehörige einer öffentlichen Einrichtung identifiziert werden können.

5. Jede auf "sozialen" Plattformen verbreitete Äußerung muss den Anforderungen der EU-Verordnung 679/2016 entsprechen, insbesondere dem Verbot der Verbreitung besonderer Daten (Art. 9) und von Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10).

6. Der Mitarbeiter kann seine Meinung frei äußern, sofern seine Äußerungen dem Ansehen der Verwaltung nicht schaden und die Grenzen der "inhaltlichen und formalen Kontinuität" respektieren.

7. Das Recht des Arbeitnehmers auf Kritik - das auf Verfassungsebene (Art. 21) als Konkretisierung des allgemeineren Rechts auf freie Meinungsäußerung garantiert und in Artikel 1 des Arbeitnehmerstatuts bekräftigt wird - muss in erster Linie den Parameter der "inhaltlichen Kontinuität" einhalten, der die notwendige Wahrhaftigkeit der vom Arbeitnehmer berichteten Fakten voraussetzt.

8. Die Behauptung falscher Tatsachen, die den Arbeitgeber in ein negatives Licht rücken oder, schlimmer noch, dem Image der Körperschaft offen schaden, stellt ein rechtswidriges Verhalten dar, das im Widerspruch zu den vom Arbeitnehmer übernommenen Pflichten der Loyalität und Treue steht.

9. Kritische Äußerungen des Arbeitnehmers müssen die weitere Grenze der "formalen Enthaltbarkeit" einhalten, d.h. es dürfen keine beleidigenden oder an und für sich ausfälligen Begriffe oder Ausdrücke verwendet werden, die über die Grenzen des Ausdrucks der eigenen Gedanken hinausgehen um in einer Beleidigung zu enden.

10. Das Recht auf freie Meinungsäußerung muss in einem angemessenen Verhältnis zu den Mitteln stehen, mit denen es ausgeübt wird.

11. Besonderes Augenmerk muss darauf gelegt werden, wie der Arbeitnehmer social Networks auch als "Ausdruck privater Gedanken" nutzt.

12. Es ist ausdrücklich verboten, social Networks während der Arbeitszeit zu nutzen, weder mit privaten noch mit Betriebsgeräten. Social Networks dürfen während der Arbeitszeit nur für institutionelle Zwecke und mit schriftlicher Genehmigung des Arbeitgebers genutzt werden.

configurare le ipotesi di reato di ingiuria, diffamazione e calunnia.

4. I pubblici dipendenti devono assumere la piena consapevolezza di non essere semplici, privati cittadini ma di poter essere sempre identificati come appartenenti ad una Pubblica Istituzione.

5. Qualunque espressione diffusa sulle piattaforme "social" dovrà rispettare le prescrizioni del Regolamento UE 679/2016, in particolare il divieto di diffondere dati particolari (art. 9) e dati relativi a condanne penali e reati (art. 10).

6. Il dipendente è libero di esternare il proprio pensiero, purché le sue dichiarazioni non arrechino un danno di immagine all'Amministrazione e rispettino i limiti di "continenza sostanziale e formale".

7. Il diritto di critica del lavoratore - garantito a livello costituzionale (art. 21) quale specificazione del più generale diritto di libera espressione del pensiero e ribadito dall'articolo 1 dello Statuto dei Lavoratori, deve rispettare innanzitutto il parametro della "continenza sostanziale", che impone la necessaria veridicità dei fatti riportati dal lavoratore.

8. L'attribuzione di fatti falsi che connotino in maniera negativa il datore di lavoro o, peggio, risultino apertamente lesivi dell'immagine dell'Ente, costituisce comportamento illecito che si pone in contrasto con gli obblighi di lealtà e fedeltà assunti dal lavoratore.

9. Le espressioni critiche utilizzate dal lavoratore devono rispettare l'ulteriore limite della "continenza formale", ovvero non devono essere utilizzati termini o espressioni di per sé offensive o ingiuriose, che travalichino i limiti dell'espressione del proprio pensiero, per sconfinare nell'offesa.

10. La libertà di espressione deve essere commisurata allo strumento utilizzato per manifestarla.

11. Va considerata di particolare importanza la modalità di utilizzo dei social network da parte del lavoratore anche quale "espressione del pensiero privato".

12. E' fatto espresso divieto di utilizzare i social network durante l'orario di lavoro, sia con dispositivi privati che con dispositivi dell'Amministrazione. I social network potranno essere utilizzati durante l'orario di lavoro solo per fini istituzionali e previa autorizzazione scritta del datore di lavoro.

Außerberufliche Nutzung von "sozialen Medien"

1. Der Zugang zu den sozialen Medien außerhalb der Arbeitszeit ist frei, aber in diesem Fall muss sich der Mitarbeiter bewusst sein, dass er von den übrigen Nutzern der sozialen Medien weiterhin als Mitarbeiter einer öffentlichen Verwaltung identifiziert werden kann und sich als solcher verpflichten muss, sich gemäß den in diesem Abschnitt dargelegten Grundsätzen zu verhalten.
2. Aus Respekt vor der in Artikel 21 der Verfassung verankerten Freiheit der Meinungsäußerung werden die Mitarbeiter aufgefordert, bei der Einrichtung, Nutzung und Verwaltung ihrer persönlichen „Account“ in sozialen Netzwerken bestimmte Verhaltensregeln einzuhalten, um die Organisation und die dort arbeitenden Menschen zu schützen.
 - a) Das Verhalten des Beamten muss anständig, würdevoll und von Redlichkeit gegenüber der Körperschaft geprägt sein, auch außerhalb des Arbeitsplatzes und der Arbeitszeiten;
 - b) Wenn man beabsichtigt in der Rubrik "Persönliche Informationen" des sozialen Netzwerks die Berufsbezeichnung, die berufliche Tätigkeit, die Rolle oder die spezifische Position, die man in der Körperschaft, der man angehört, innehat, offenzulegen, sollten diese Informationen in knapper Form angegeben werden, wobei die Preisgabe vertraulicher Informationen zu vermeiden ist;
 - c) Die eigenen Nutzerprofile sollten niemals für offizielle Erklärungen oder die Weitergabe offizieller Informationen verwendet werden;
 - d) Der Mitarbeiter hält sich an das Amtsgeheimnis und die Vorschriften zum Schutz und zur Verarbeitung personenbezogener Daten gemäß Absatz 5, Artikel 12 des DPR Nr. 62 von 2013. Es ist strengstens untersagt, vertrauliche und interne Informationen weiterzugeben, insbesondere: interne Korrespondenz, Informationen und Bilder von Dritten (z.B. in Bezug auf den Zugang der Personen zu den Räumlichkeiten der Verwaltung, usw.) oder Informationen über Arbeitstätigkeiten, von denen man aus dienstlichen Gründen Kenntnis hat;
 - e) Im Rahmen von Debatten und Diskussionen, ob in öffentlichen oder in privaten Gruppen, welche die Tätigkeiten der Verwaltung zum Inhalt haben, werden die Mitarbeiter aufgefordert, von Kommentaren und negativen Urteilen abzusehen, die dem Ansehen der Körperschaft schaden könnten. Geben Sie im Falle einer Stellungnahme immer an, dass die geäußerten Meinungen persönlicher Natur sind. Unbeschadet der ordnungsgemäßen Ausübung der Meinungsfreiheit und des Rechts auf Kritik ist insbesondere die Übermittlung und Verbreitung von bedrohlichen oder beleidigenden Botschaften, Kommentaren und öffentlichen Äußerungen, die die Verwaltung beleidigen, sich

Utilizzo extralavorativo dei "social-media"

1. L'accesso ai social media al di fuori dell'orario di lavoro è libero ma, in tal caso, il lavoratore deve essere consapevole di poter essere comunque identificato dal resto degli utenti del social come dipendente di una Pubblica Amministrazione e, come tale, deve impegnarsi a mantenere un comportamento conforme ai principi espressi nella presente sezione.
2. In ossequio e nel rispetto della libertà di ognuno di manifestare il proprio pensiero sancita dall'articolo 21 della Costituzione, si richiede ai dipendenti nella configurazione, nell'utilizzo e nella gestione dei propri account personali sui social network di rispettare alcune norme di comportamento a tutela dell'Ente e delle persone che vi lavorano.
 - a) Il pubblico dipendente ha l'obbligo di mantenere un comportamento decoroso e corretto anche fuori dal luogo e dall'orario di lavoro;
 - b) Qualora, nella sezione del social network relativa alle informazioni personali, si intenda rendere nota la qualifica, la propria attività lavorativa, il ruolo o l'incarico specifico ricoperto nell'ente di appartenenza, tali informazioni devono essere riportate in maniera sintetica, evitando di inserire informazioni riservate;
 - c) I profili personali non devono mai essere utilizzati per dichiarazioni ufficiali o per la divulgazione di atti, documenti o informazioni d'Ufficio;
 - d) Il dipendente deve osservare il segreto d'ufficio e la normativa in materia di protezione dei dati personali come previsto dall'art. 12, comma 5, del DPR n° 62 del 16 aprile 2013. È vietato divulgare informazioni riservate, nello specifico: corrispondenza interna, informazioni e immagini di terze parti (ad esempio relative al pubblico che accede ai locali dell'Amministrazione) o informazioni su attività lavorative di cui si è a conoscenza per ragioni d'Ufficio;
 - e) Nell'ambito di dibattiti e discussioni pubbliche o in gruppi privati che abbiano come oggetto l'attività dell'Amministrazione, i dipendenti sono invitati ad astenersi dal commentare e dare giudizi negativi che possano ledere l'immagine dell'Ente. Nei propri interventi, il pubblico dipendente deve sempre specificare che le opinioni espresse hanno carattere personale. Fermo restando il corretto esercizio delle libertà di pensiero e del diritto di critica, non è consentita la trasmissione e la diffusione di messaggi d'odio – hate speech, ingiuriosi, commenti e dichiarazioni pubbliche offensive nei confronti dell'Amministrazione, riferiti alle

auf die institutionelle Tätigkeit der Verwaltung und ganz allgemein auf dessen Arbeit beziehen und die in Form und Inhalt der Verwaltung schaden, ihr Ansehen oder ihr Prestige beeinträchtigen oder ihre Effizienz in Frage stellen können, nicht gestattet;

- f) Insbesondere ist der heikle Aspekt der Verwendung und Verbreitung von Bildern aus dem Arbeitsumfeld zu bedenken, die bei unangemessener Anwendung nicht nur dem Ansehen der Körperschaft schaden, sondern auch eine Verletzung der oben genannten Grundsätze der Vertraulichkeit der Bürger darstellen können, was zu Schadensersatzforderungen oder strafrechtlichen Sanktionen führen kann;
- g) Falls negative Kommentare über die Körperschaft auf sozialen Netzwerkplattformen gefunden und gesehen werden oder Bilder unrechtmäßig verbreitet werden, muss der Mitarbeiter darauf achten, dass er aufgrund seiner Zugehörigkeit zur Körperschaft nicht persönlich antwortet, sondern alles dem Gemeindesekretär meldet, welcher in Absprache mit dem Bürgermeister und Ausschuss die zu ergreifenden Maßnahmen bewertet;
- h) Wenn man für eine Initiative oder Tätigkeit der Verwaltung werben möchte, dürfen die auf der offiziellen Seite der Organisation veröffentlichten sozialen Inhalte (Beiträge, Geschichten) auf der persönlichen Seite geteilt werden. Hierbei sollte es vermieden werden, die offiziellen Inhalte zu kopieren und einzufügen, um nicht den Eindruck zu erwecken, im Namen der Organisation zu sprechen;
- i) Es ist verboten, ein Account/eine öffentliche Seite/einen Blog im Namen der Verwaltung oder in Verbindung mit der Körperschaft oder einem ihrer Projekte einzurichten, ohne die Verwaltung offiziell darüber informiert zu haben. Vor jeder Einrichtung muss eine förmliche schriftliche Genehmigung eingeholt werden.

Art. 10.5

Haftung

1. Die allgemeinen Regeln der Rechtsordnung gelten auch für die Nutzung der Medien und der sozialen Medien, einschließlich derjenigen, die eine zivil- und/oder strafrechtliche Haftung im Falle der Verbreitung von Falschnachrichten, beleidigenden oder verleumderischen Äußerungen oder von Äußerungen vorsehen, die die Rechte oder Interessen anderer sowie das Ansehen der Verwaltung schädigen.

Art. 10.6

Dritte Parteien

aktivitäten institutioneller des Entes und in allgemeinere al suo operato, che per le forme e i contenuti possano comunque nuocere all'Amministrazione, ledendone l'immagine o il prestigio o compromettendone l'efficienza;

- f) Nello specifico va considerato il delicato aspetto dell'utilizzo e della diffusione di immagini legate all'ambiente di lavoro che, se indebitamente applicato può, oltre che ledere l'immagine dell'ente, essere fonte di violazione dei sopracitati principi di riservatezza dei cittadini che possono generare richieste di risarcimento danni o essere sanzionate penalmente;
- g) Nel caso in cui si dovessero reperire e visionare sulle piattaforme di social network commenti negativi riferiti all'Ente, o immagini indebitamente diffuse, il dipendente avrà cura di non rispondere in prima persona, in virtù della propria appartenenza all'Ente, ma di segnalare il tutto al Segretario comunale, cui spetterà valutare insieme al Sindaco ed alla giunta comunale le azioni da intraprendere;
- h) Se si desidera promuovere un'iniziativa o un'attività dell'Amministrazione, è consentito condividere sulla propria pagina personale i contenuti social pubblicati sulla pagina ufficiale dell'Ente, evitando di copiare e incollare i contenuti ufficiali al fine di non generare l'idea di parlare a nome dell'Ente;
- i) È vietato aprire un account, una pagina pubblica, un blog o altro a nome dell'Amministrazione o legato ad essa o ad un suo progetto, senza averne formalmente informato l'amministrazione. Prima di ogni attivazione è necessario aver ricevuto formale autorizzazione scritta a procedere.

Art.10.5

Responsabilità

1. Sono pienamente applicabili all'utilizzo dei media e dei social media anche le norme generali sull'ordinamento giuridico, comprese quelle che prevedono responsabilità civile e/o penale in caso di diffusione di notizie false, pensieri ingiuriosi o diffamatori o tali da ledere diritti o interessi altrui, oltre che l'immagine dell'Amministrazione.

Art. 10.6

Terze parti

1. Die in Artikel 1 Absatz 2 des Gesetzesdekrets Nr. 165 aus dem Jahr 2001 genannten öffentlichen Verwaltungen dehnen die in diesem Kodex festgelegten Verhaltenspflichten auf alle Mitarbeiter oder Berater mit jeder Art von Vertrag oder Ernennung und in jeder Eigenschaft auf die Inhaber von Stellen und Ernennungen in den Ämtern der direkten Zusammenarbeit mit den politischen Behörden sowie auf die Mitarbeiter in jeder Eigenschaft von Unternehmen aus, die Güter oder Dienstleistungen liefern und Arbeiten zugunsten der Verwaltung ausführen, soweit sie damit vereinbar sind.

2. Zu diesem Zweck fügen die Verwaltungen in die Ernennungsurkunden oder in die Verträge über den Erwerb von Mitarbeit-, Beratungs- oder Dienstleistungen geeignete Bestimmungen oder Klauseln über die Beendigung oder das Erlöschen der Beziehung im Falle eines Verstoßes gegen die sich aus diesem Verhaltenskodex ergebenden Verpflichtungen ein.

Art. 11

Aus- und Weiterbildung

1. Das Personal nimmt an Grund- und Weiterbildungsveranstaltungen teil, bei denen der Inhalt des Verhaltenskodexes vermittelt wird, insbesondere in den Bereichen Ethik, Korruptionsvorbeugung und Transparenz.

Art. 12

Haftung bei Verletzung von Pflichten des Kodexes

1. Die Verletzung von Pflichten, die dieser Verhaltenskodex vorsieht, gilt als Verstoß gegen die Dienstpflichten und ist ein Disziplinarhaftungsgrund; aufrecht bleiben sämtliche Fälle, in denen Pflichtverletzungen auch eine strafrechtliche, zivilrechtliche, verwaltungsrechtliche oder buchhalterische Haftung öffentlicher Bediensteter begründen.

1. Le pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo n. 165 del 2001 estendono, per quanto compatibili, gli obblighi di condotta previsti dal presente codice a tutti i collaboratori o consulenti, con qualsiasi tipologia di contratto o incarico e a qualsiasi titolo, ai titolari di organi e di incarichi negli uffici di diretta collaborazione delle autorità politiche, nonché nei confronti dei collaboratori a qualsiasi titolo di imprese fornitrici di beni o servizi e che realizzano opere in favore dell'amministrazione.

2. A tale fine, negli atti di incarico o nei contratti di acquisizioni delle collaborazioni, delle consulenze o dei servizi, le amministrazioni inseriscono apposite disposizioni o clausole di risoluzione o decadenza del rapporto in caso di violazione degli obblighi derivanti dal presente codice di comportamento.

Art. 11

Attività formativa e di aggiornamento

1. Il personale partecipa ad attività formative di base e di aggiornamento che favoriscano la conoscenza dei contenuti del codice di comportamento, in particolare in materia di etica, prevenzione della corruzione e trasparenza.

Art. 12

Responsabilità conseguente alla violazione dei doveri del codice

1. La violazione degli obblighi previsti dal presente Codice costituisce comportamento contrario ai doveri d'ufficio ed è fonte di responsabilità disciplinare, ferme restando le ipotesi in cui la violazione possa dar luogo anche a responsabilità penale, civile, amministrativa o contabile del pubblico dipendente/della pubblica dipendente.

1.A) Arbeitsanweisung für Angestellte mit Privatgeräten	1.A) Istruzioni di lavoro per dipendenti con dispositivi propri
<p>Diese Arbeitsanweisung soll dazu beitragen, dass die Rechtsvorschriften zur Verarbeitung personenbezogener Daten und zum Schutz der informationstechnischen Systeme eingehalten werden und insbesondere die Vertraulichkeit, Integrität und Verfügbarkeit von betrieblichen/geschäftlichen Dokumenten und Informationen sowie damit zusammenhängenden personenbezogenen Daten gewährleistet werden kann, sowohl am Arbeitsplatz im Büro als auch im Homeoffice.</p>	<p>Le presenti istruzioni di lavoro hanno lo scopo di contribuire a garantire il rispetto delle disposizioni di legge sul trattamento dei dati personali e della sicurezza informatica e, in particolare, che possa essere garantita la riservatezza, l'integrità e la disponibilità di documenti e informazioni aziendali/d'ufficio e dei collegati dati personali, sia sul posto di lavoro in ufficio, sia in sede di telelavoro.</p>
<p><i>Anwendbare Normen: Verordnung (EU) 2016/679, Art. 32, sowie Vorgaben der Autorità Garante per la protezione dei dati personali</i> <i>Präventionsrichtlinien der ENISA</i> <i>Präventionsrichtlinien von EUROPOL</i></p>	<p><i>Norme applicabili: Regolamento (UE) 2016/679, Art. 32, nonché specifiche dell'Autorità Garante per la protezione dei dati personali</i> <i>Linee guida ENISA</i> <i>Linee guida EUROPOL</i></p>
<p>1. VORGABEN PRIVATGERÄTE</p>	<p>1. DIRETTIVE PER L'UTILIZZO DI DISPOSITIVI PROPRI</p>
<p>UPDATES 1.1. Die Betriebssysteme und Programme auf PCs und Laptops sind immer auf dem aktuellen Stand zu halten. Deshalb muss regelmäßig geprüft werden, ob Updates zur Verfügung stehen. Diese sind zu installieren. Mit Updates werden meist Sicherheitsschwachstellen behoben.</p>	<p>UPDATES 1.1. I sistemi operativi e i programmi su PC e PC portatili/laptops devono essere sempre tenuti aggiornati. Pertanto, deve essere controllato regolarmente se sono disponibili aggiornamenti. Questi devono essere installati. Gli aggiornamenti vengono solitamente utilizzati per correggere le vulnerabilità della sicurezza.</p>
<p>PASSWÖRTER 1.2. Starke Passwörter schützen Systeme und Daten vor dem Zugriff durch Unberechtigte. Die Passwörter müssen den gängigen Sicherheitsstandards entsprechen.</p>	<p>PASSWORD 1.2. Password complesse proteggono sistemi e dati da accessi non autorizzati. Le password devono corrispondere agli standard attuali.</p>
<p>2. NUTZUNG DER VPN-VERBINDUNG</p>	<p>2. UTILIZZO DELLA CONNESSIONE VPN</p>
<p>VPN VERBINDUNG 2.1. Der Zugriff auf Daten des Arbeitgebers/Verantwortlichen darf ausschließlich über eine sichere, vom Arbeitgeber bereitgestellte, VPN-Verbindung/Remote Desktop erfolgen; davon abgesehen ist der Zugang mittels der betrieblich zugelassenen Cloud-Lösungen/webbasierten Anwendungen erlaubt (vgl. hierzu die eigenen "Verwendungsvorgaben für die Angestellten in Bezug auf Cloud-Lösungen"). Die Zugangsdaten werden Ihnen vorab mitgeteilt. Es ist keine Verwendung von VPN- oder anderen z.B. Tor – ähnlichen Diensten zur Verschleierung des Standortes, ob beabsichtigt oder nicht, zulässig.</p>	<p>CONNESSIONE VPN 2.1. È possibile accedere ai dati del datore di lavoro/Titolare di trattamento solo tramite una connessione VPN sicura/Remote Desktop messa a disposizione dal datore di lavoro; oltre a ciò, è ammesso l'accesso tramite soluzioni Cloud/applicazioni basate sul web autorizzate dall'azienda (cfr. in merito le specifiche "Linee guida per dipendenti per l'utilizzo di soluzioni Cloud"). Le verranno fornite le credenziali di accesso in anticipo. Non è ammesso l'utilizzo, intenzionale o meno, di VPN- o altri servizi (p.es. Tor) funzionali ad occultare la localizzazione.</p>
<p>SICHERE IDENTIFIKATION 2.2. Die im vorhergehenden Punkt beschriebenen Zugriffe sind als streng persönlich einzustufen und die</p>	<p>IDENTIFICAZIONE SICURA 2.2. Gli accessi descritti al punto precedente sono da intendersi come strettamente personali e le relative password non devono mai essere comunicate a terzi.</p>

entsprechenden Passwörter dürfen niemals an Dritte weitergegeben werden.	
3. WEITERE VORGABEN	3. ALTRE PRESCRIZIONI
<p>GESCHÄFTLICHE DOKUMENTE, INFORMATIONEN UND PERSONENBEZOGENE DATEN SCHÜTZEN</p> <p>3.1. Dokumente, Informationen und personenbezogene Daten sind zu schützen, auch im Homeoffice:</p> <ul style="list-style-type: none"> - die Inhalte des/r vom Arbeitgeber/Verantwortlichen erteilten Auftrags und Anweisungen gemäß Art. 29 EU-Verordnung Nr. 679/2016 für die Verarbeitung von personenbezogenen Daten sind auch im Zuge der Verwendung von Privatgeräten einzuhalten; - Zugangspasswörter sind geheim zu halten; - Interne Informationen und personenbezogene Daten sind vor Unberechtigten, auch Familienmitgliedern, zu schützen; - Der Bildschirm ist vor Einsicht zu schützen; - Auf dem privaten Gerät sind keine Dokumente, Informationen und personenbezogenen Daten zu speichern; - Papierdossiers und Ausdrücke sind vor unberechtigtem Zugriff zu schützen; - Nicht mehr benötigte Papierunterlagen sind zu schreddern oder sicher aufzubewahren, bis sie im Büro vernichtet werden können. 	<p>PROTEGGERE I DATI PERSONALI E SEGRETI D'UFFICIO (DOCUMENTI, INFORMAZIONI)</p> <p>3.1. Documenti, informazioni e dati personali devono essere protetti, anche durante il telelavoro:</p> <ul style="list-style-type: none"> - I contenuti dell'incarico e delle istruzioni del datore di lavoro/Titolare di trattamento ex art. 29 regolamento UE n. 679/2016 per il trattamento dei dati personali sono da rispettare anche nell'utilizzo dei dispositivi propri; - Le password di accesso devono essere tenute segrete; - Le informazioni interne e i dati personali devono essere protetti da persone non autorizzate, compresi i familiari; - Lo schermo deve essere protetto dalla vista di terzi, - Sul dispositivo privato documenti, informazioni e dati personali non devono mai essere salvati; - I fascicoli cartacei e le stampe devono essere protetti dall'accesso non autorizzato; - I documenti cartacei non più necessari devono essere distrutti o conservati in un luogo sicuro fino a quando non possono essere distrutti in ufficio;
<p>E-MAIL SICHER EINSETZEN</p> <p>3.2. Private und geschäftliche E-Mails sind auf dem Gerät zu trennen. Die Nutzung privater E-Mail-Konten für die geschäftliche Kommunikation ist verboten. Geschäftliche E-Mails dürfen nicht auf private Konten weitergeleitet werden.</p>	<p>UTILIZZO SICURO DELLE MAIL</p> <p>3.2. Le e-mail private e aziendali devono essere separate sul dispositivo. È vietato utilizzare account di posta elettronica privati per la comunicazione aziendale. Le e-mail aziendali non devono essere inoltrate ad account personali.</p>
<p>KOMMUNIKATIONS-TOOLS GEZIELT AUSWÄHLEN</p> <p>3.3. Neben dem Telefon und den E-Mails werden auch Messengers und Videokonferenzdienste eingesetzt. Informationen zu den Diensten erhalten Sie auf Anfrage beim IT-Verantwortlichen.</p>	<p>SELEZIONE MIRATA DEGLI STRUMENTI DI COMUNICAZIONE</p> <p>3.3. Oltre al telefono e alla posta elettronica, vengono utilizzati anche servizi di messaggistica e videoconferenza. Le informazioni sui servizi sono disponibili su richiesta presso il responsabile del reparto informatico.</p>
<p>SICH VOR PHISHING UND ANDEREN BEDROHUNGEN SCHÜTZEN</p> <p>3.4. Verdächtige E-Mails dürfen nicht geöffnet werden. Anhänge in Mails von unbekanntem Absendern dürfen nicht angeklickt werden. Im Zweifel ist die Absenderin oder der Absender per Telefon zu kontaktieren, damit sie oder er den Inhalt der E-Mail bestätigen kann.</p>	<p>PROTEGGETEVI DAL PHISHING E DA ALTRE MINACCE</p> <p>3.4. Le e-mail sospette non devono essere aperte. Non fare clic sugli allegati nelle e-mail di mittenti sconosciuti. In caso di dubbio, il mittente deve essere contattato telefonicamente in modo che possa confermare il contenuto dell'e-mail.</p>
<p>DATENSCHUTZVERLETZUNGEN SOFORT MELDEN</p> <p>3.5. Wenn Arbeitsmittel wie Dokumente oder auch Ihr PC oder Laptop verloren gehen oder</p>	<p>SEGNALARE IMMEDIATAMENTE I DATA BREACH</p> <p>3.5. In caso di smarrimento di documenti oppure del PC/PC portatile laptop è necessario segnalarlo immediatamente al responsabile di reparto.</p>

abhandenkommen, ist dies umgehend dem Vorgesetzten zu melden.	
Zusätzliche Informationen zum Thema IT-Sicherheit im Privathaushalt finden Sie unter: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold	Altre informazioni riguardanti la sicurezza informatica a casa Vostra trovate sotto: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold
4. KONTROLLEN	4. VERIFICHE
<p>4.1. Die Tätigkeiten der Mitarbeiter für den Arbeitgeber/Verantwortlichen, welche mittels Privatgeräten abgewickelt werden, werden nicht systematisch und kontinuierlich überwacht, die Systemadministratoren des Arbeitgebers/Verantwortlichen (auch in Zusammenarbeit mit der EDV-Abteilung des Gemeindenverbandes) können die Tätigkeiten auf den Servern des Arbeitgebers/Verantwortlichen (z.B. die erzeugten Logfiles; die Privatgeräte selbst werden klarerweise nicht kontrolliert) aber überwachen oder untersuchen; dies geschieht nur, um die Einhaltung der relevanten Richtlinien zu bestätigen und mögliche Sicherheitsverletzungen, unbefugte Zugriffe, technische Probleme, usw. zu untersuchen und nicht für die Zwecke der Überwachung der Arbeitstätigkeit. Die Verwendung von Logfiles erfolgt immer mit einer festgelegten zeitlichen Begrenzung (kurze Frist) und Tracing-Tätigkeit erfolgt nur bei allfälligen Verdachtsmomenten, in manueller Form und üblicherweise in direkter Zusammenarbeit mit dem betroffenen Nutzer.</p> <p>Die Kontrollen können wie folgt zusammengefasst werden:</p> <ol style="list-style-type: none"> 1) Kontrolle/Einschränkung auf der Grundlage der IP der Region, aus welcher der Verbindungszugriff erfolgt (ev. auch für weitere Dienste) 2) Kontrolle/Einschränkung auf der Grundlage der IP für den E-Mail-Zugang 3) Befähigung bestimmter IP's in Zusammenhang mit kritischen Diensten (z.B. Meldedaten an die Polizeikräfte) 4) mobile device management (betrifft nur die mobilen Betriebsgeräte) 5) zusätzliche Kontrollformen, die im Laufe der Zeit, zur best practice des Sektors zählen werden (z.B. conditional access und multifactor authentication, usw.) 	<p>4.1 Le attività dei dipendenti, svolte per datore di lavoro/Titolare utilizzando dispositivi propri, non sono soggetti a una sorveglianza sistematica e continua, ma gli amministratori di sistema del datore di lavoro/Titolare (anche in collaborazione con la Ripartizione EDP del Consorzio dei Comuni) possono monitorare o indagare le attività sui server dell' datore di lavoro/Titolare (p.es. i logfiles generati; i dispositivi propri in sé ovviamente non vengono controllati); ciò si verificherà solo per confermare la conformità ai requisiti della politica pertinente e per indagare su possibili violazioni della sicurezza, accessi non autorizzati, problemi tecnici, ecc. e non ai fini del monitoraggio dell'attività lavorativa. L'utilizzo di logfiles è limitato a tempistiche prefissate (breve termine) e l'attività di tracing viene espletata solo nei casi di dubbio, in forma manuale e di regola in collaborazione diretta con l'utente interessato.</p> <p>Le attività di controllo possono essere così riassunte:</p> <ol style="list-style-type: none"> 1) controllo/restrizione su base IP della regione di accesso per collegamento VPN (ev. anche per altri servizi) 2) controllo/restrizione su base IP per l'accesso alle e-mail 3) abilitazione su IP specifici dei servizi critici (es. anagrafe alle forze dell'ordine) 4) mobile device management (riguarda solo i dispositivi mobili aziendali) 5) ulteriori forme di controllo che costituiranno, nel continuo, la best practice di settore (p.es. conditional access e multifactor authentication, ecc.)
5. RECHT AUF NICHTERREICHBARKEIT	5. DIRITTO ALLA DISCONNESSIONE
Im Fall von Telearbeit/Smartworking sieht die individuelle Vereinbarung zwischen Arbeitgeber und	In caso di telelavoro/smartworking l'accordo individuale tra il datore di lavoro e il dipendente

Angestellten u.a. die Ruhepausen mit Anrecht auf Unterbrechung der Verbindung vor.	prevede, tra l'altro, i tempi di riposo con diritto alla disconnessione;
BEI ZWEIFELN KONTAKTIEREN SIE UNS GERNE!	IN CASO DI DUBBI NON ESITATE A CONTATTARCI!
Version 01.02.2022	Versione 01.02.2022
Letzte Abänderung: 01.02.2022	Ultima modifica: 01.02.2022
DIE VORLIEGENDE ARBEITSANWEISUNG WIRD ALLEN MITARBEITERN VOM GENERALEKRETARIAT AUF DEREN ZUGEWIESENE E-MAIL-ADRESSE ÜBERMITTELT. DIE ÜBERMITTLUNG WIRD PROTOKOLLIERT.	LE PRESENTI ISTRUZIONI DI LAVORO VENGONO INVIATE DALLA SEGRETERIA GENERALE A TUTTI I DIPENDENTI SULL'INDIRIZZO E-MAIL A LORO ASSEGNATO. L'INVIO VIENE PROTOCOLLATO.

1.B) Arbeitsanweisung für Angestellte mit Betriebsgeräten	1.B) Istruzioni di lavoro per dipendenti con dispositivi aziendali
<p>Diese Arbeitsanweisung soll dazu beitragen, dass die Rechtsvorschriften zur Verarbeitung personenbezogener Daten und zum Schutz der informationstechnischen Systeme eingehalten werden und insbesondere die Vertraulichkeit, Integrität und Verfügbarkeit von betrieblichen/geschäftlichen Dokumenten und Informationen sowie damit zusammenhängenden personenbezogenen Daten gewährleistet werden kann, sowohl am Arbeitsplatz im Büro als auch im Homeoffice.</p>	<p>Le presenti istruzioni di lavoro hanno lo scopo di contribuire a garantire il rispetto delle disposizioni di legge sul trattamento dei dati personali e della sicurezza informatica e, in particolare, che possa essere garantita la riservatezza, l'integrità e la disponibilità di documenti e informazioni aziendali/d'ufficio e dei collegati dati personali, sia sul posto di lavoro in ufficio, sia in sede di telelavoro.</p>
<p><i>Anwendbare Normen: Verordnung (EU) 2016/679, Art. 32, sowie Vorgaben der Autorità Garante per la protezione dei dati personali</i> <i>Präventionsrichtlinien der ENISA</i> <i>Präventionsrichtlinien von EUROPOL</i></p>	<p><i>Norme applicabili: Regolamento (UE) 2016/679, Art. 32, nonché specifiche dell'Autorità Garante per la protezione dei dati personali</i> <i>Linee guida ENISA</i> <i>Linee guida EUROPOL</i></p>
<p>1. VORGABEN BETRIEBSGERÄTE</p>	<p>1. DIRETTIVE PER L'UTILIZZO DI DISPOSITIVI AZIENDALI</p>
<p>UPDATES 1.1. Der Arbeitgeber/Verantwortliche stattet die Betriebsgeräte mit den nötigen Sicherheitsvorkehrungen aus (PC's und Laptops z.B. mit Antivirus; Tablets und Smartphones mit MDM-Software). Die Betriebssysteme und Programme auf PCs, Smartphones und Tablets sind immer auf dem aktuellen Stand zu halten. Deshalb muss vom Angestellten regelmäßig geprüft werden, ob Updates zur Verfügung stehen. Diese sind zu installieren. Mit Updates werden meist Sicherheitsschwachstellen behoben.</p>	<p>UPDATES 1.1. Il datore di lavoro/Titolare equipaggia i dispositivi aziendali con le necessarie misure di sicurezza (PC e laptop, p.es., con antivirus; tablet e smartphone con software MDM). I sistemi operativi e i programmi su PC, smartphone e tablet devono essere sempre tenuti aggiornati. Pertanto, da parte del dipendente deve essere controllato regolarmente se sono disponibili aggiornamenti. Questi devono essere installati. Gli aggiornamenti vengono solitamente utilizzati per correggere le vulnerabilità della sicurezza.</p>
<p>PASSWÖRTER 1.2. Starke Passwörter schützen Systeme und Daten vor dem Zugriff durch Unberechtigte. Die Passwörter müssen den gängigen Sicherheitsstandards des Arbeitgebers/Verantwortlichen entsprechen.</p>	<p>PASSWORD 1.2. Password complesse proteggono sistemi e dati da accessi non autorizzati. Le password devono corrispondere alle prescrizioni del datore di lavoro/Titolare di trattamento.</p>
<p>VPN VERBINDUNG 1.3. Der Zugriff auf Daten des Arbeitgebers/Verantwortlichen darf – abgesehen klarerweise von all jenen Fällen, in denen das Betriebsgerät direkt (z.B. mittels Ethernet-Kabel) am Netz des Arbeitgebers angeschlossen wird – ausschließlich über eine sichere, vom Arbeitgeber bereitgestellte, VPN-Verbindung/Remote Desktop erfolgen; davon abgesehen ist der Zugang mittels der betrieblich zugelassenen Cloud-Lösungen/webbasierten Anwendungen erlaubt (vgl. hierzu die eigenen "Verwendungsvorgaben für die Angestellten in Bezug auf Cloud-Lösungen"). Die Zugangsdaten werden Ihnen vorab mitgeteilt. Es ist keine Verwendung von VPN- oder anderen z.B. Tor – ähnlichen Diensten zur Verschleierung des Standortes, ob beabsichtigt oder nicht, zulässig.</p>	<p>CONNESSIONE VPN 1.3. È possibile accedere ai dati del datore di lavoro/Titolare di trattamento – e fatti comunque salvi tutti i casi in cui il dispositivo aziendale venga collegato direttamente alla rete del datore di lavoro (p.es. tramite cavo Ethernet) – solo tramite una connessione VPN sicura/Remote Desktop messa a disposizione dal datore di lavoro; oltre a ciò, è ammesso l'accesso tramite soluzioni Cloud/applicazioni basate sul web autorizzate dall'azienda (cfr. in merito le specifiche "Linee guida per dipendenti per l'utilizzo di soluzioni Cloud"). Le verranno fornite le credenziali di accesso in anticipo. Non è ammesso l'utilizzo, intenzionale o meno, di VPN- o altri servizi (p.es. Tor) funzionali ad occultare la localizzazione.</p>

<p>SICHERE IDENTIFIKATION 1.4. Die im vorhergehenden Punkt beschriebenen Zugriffe sind als streng persönlich einzustufen und die entsprechenden Passwörter dürfen niemals an Dritte weitergegeben werden.</p>	<p>IDENTIFICAZIONE SICURA 1.4. Gli accessi descritti al punto precedente sono da intendersi come strettamente personali e le relative password non devono mai essere comunicate a terzi.</p>
<p>2. WEITERE VORGABEN</p>	<p>2. ALTRE PRESCRIZIONI</p>
<p>GESCHÄFTLICHE INFORMATIONEN UND PERSONENBEZOGENE DATEN SCHÜTZEN 2.1. Dokumente, Informationen und personenbezogene Daten sind zu schützen, auch im Homeoffice: - die Inhalte des/r vom Arbeitgeber/Verantwortlichen erteilten Auftrags und Anweisungen gemäß Art. 29 EU-Verordnung Nr. 679/2016 für die Verarbeitung von personenbezogenen Daten sind auch im Zuge der Verwendung von Betriebsgeräten einzuhalten; - Zugangspasswörter sind geheim zu halten; - Interne Informationen und personenbezogene Daten sind vor Unberechtigten, auch Familienmitgliedern, zu schützen; - Der Bildschirm ist vor Einsicht zu schützen; - Auf dem Betriebsgerät sind keine personenbezogenen Daten privater Natur zu speichern; - Papierdossiers und Ausdrücke sind vor unberechtigtem Zugriff zu schützen; - Nicht mehr benötigte Papierunterlagen sind zu schreddern oder sicher aufzubewahren, bis sie im Büro vernichtet werden können.</p>	<p>PROTEGGERE I DATI PERSONALI E SEGRETI D'UFFICIO (DOCUMENTI, INFORMAZIONI) 2.1. Documenti, informazioni e dati personali devono essere protetti, anche durante il telelavoro: - I contenuti dell'incarico e delle istruzioni del datore di lavoro/Titolare di trattamento ex art. 29 regolamento UE n. 679/2016 per il trattamento dei dati personali sono da rispettare anche nell'utilizzo dei dispositivi aziendali; - Le password di accesso devono essere tenute segrete; - Le informazioni interne e i dati personali devono essere protetti da persone non autorizzate, compresi i familiari; - Lo schermo deve essere protetto dalla vista di terzi, - Sul dispositivo aziendale non devono essere salvati dati di natura privata; - I fascicoli cartacei e le stampe devono essere protetti dall'accesso non autorizzato; - I documenti cartacei non più necessari devono essere distrutti o conservati in un luogo sicuro fino a quando non possono essere distrutti in ufficio.</p>
<p>E-MAIL SICHER EINSETZEN 2.2. Die Nutzung privater E-Mail-Konten für die geschäftliche Kommunikation ist verboten. Geschäftliche E-Mails dürfen nicht auf private Konten weitergeleitet werden.</p>	<p>UTILIZZO SICURO DELLE MAIL 2.2. È vietato utilizzare account di posta elettronica privati per la comunicazione aziendale. Le e-mail aziendali non devono essere inoltrate ad account personali.</p>
<p>KOMMUNIKATIONS-TOOLS GEZIELT AUSWÄHLEN 2.3. Neben dem Telefon und den E-Mails werden auch Messengers und Videokonferenzdienste eingesetzt. Informationen zu den Diensten erhalten Sie auf Anfrage beim IT-Verantwortlichen.</p>	<p>SELEZIONE MIRATA DEGLI STRUMENTI DI COMUNICAZIONE 2.3. Oltre al telefono e alla posta elettronica, vengono utilizzati anche servizi di messaggistica e videoconferenza. Le informazioni sui servizi sono disponibili su richiesta presso il responsabile del reparto informatico.</p>
<p>SICH VOR PHISHING UND ANDEREN BEDROHUNGEN SCHÜTZEN 2.4. Verdächtige E-Mails dürfen nicht geöffnet werden. Anhänge in Mails von unbekanntem Absendern dürfen nicht angeklickt werden. Im Zweifel ist die Absenderin oder der Absender per Telefon zu kontaktieren, damit sie oder er den Inhalt der E-Mail bestätigen kann.</p>	<p>PROTEGGETEVI DAL PHISHING E DA ALTRE MINACCE 2.4. Le e-mail sospette non devono essere aperte. Non fare clic sugli allegati nelle e-mail di mittenti sconosciuti. In caso di dubbio, il mittente deve essere contattato telefonicamente in modo che possa confermare il contenuto dell'e-mail.</p>
<p>DATENSCHUTZVERLETZUNGEN SOFORT MELDEN</p>	<p>SEGNALARE IMMEDIATAMENTE I DATA BREACH</p>

2.5. Wenn Arbeitsmittel wie Dokumente oder auch Ihr PC verloren gehen oder abhandenkommen, ist dies umgehend dem Vorgesetzten zu melden.	2.5. In caso di smarrimento di documenti o apparecchiature di lavoro è necessario segnalarlo immediatamente al responsabile di reparto.
Zusätzliche Informationen zum Thema IT-Sicherheit im Privathaushalt finden Sie unter: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold	Altre informazioni riguardanti la sicurezza informatica a casa Vostra trovate sotto: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold
3. KONTROLLEN	3. VERIFICHE
<p>3.1. Die Tätigkeiten der Mitarbeiter mittels Betriebsgeräten werden nicht systematisch und kontinuierlich überwacht, die Systemadministratoren des Arbeitgebers/Verantwortlichen (auch in Zusammenarbeit mit der EDV-Abteilung des Gemeindenverbandes) können die Nutzung (= die Tätigkeiten auf den Servern des Arbeitgebers/Verantwortlichen, so z.B. die erzeugten Logifiles; Überprüfung anhand des installierten mobile device managements; bei Bedarf auch direkte Überprüfung des Betriebsgerätes selbst; usw.) aber überwachen oder untersuchen; dies geschieht nur, um die Einhaltung der relevanten Richtlinien zu bestätigen und mögliche Sicherheitsverletzungen, unbefugte Zugriffe, technische Probleme, usw. zu untersuchen und nicht für die Zwecke der Überwachung der Arbeitstätigkeit. Die Verwendung von Logfiles erfolgt immer mit einer festgelegten zeitlichen Begrenzung (kurze Frist) und Tracing-Tätigkeit erfolgt nur bei allfälligen Verdachtsmomenten, in manueller Form und üblicherweise in direkter Zusammenarbeit mit dem betroffenen Nutzer.</p> <p>Die Kontrollen können wie folgt zusammengefasst werden:</p> <ol style="list-style-type: none"> 1) Kontrolle/Einschränkung auf der Grundlage der IP der Region, aus welcher der Verbindungszugriff erfolgt (ev. auch für weitere Dienste) 2) Kontrolle/Einschränkung auf der Grundlage der IP für den E-Mail-Zugang 3) Befähigung bestimmter IP's in Zusammenhang mit kritischen Diensten (z.B. Meldedaten an die Polizeikräfte) 4) mobile device management für die mobilen Betriebsgeräte 5) zusätzliche Kontrollformen, die im Laufe der Zeit, zur best practice des Sektors zählen werden (z.B. conditional access und multifactor authentication, usw.) 	<p>3.1 Le attività dei dipendenti svolte tramite dispositivi aziendali non sono soggetti a una sorveglianza sistematica e continua, ma gli amministratori di sistema del datore di lavoro/Titolare (anche in collaborazione con la Ripartizione EDP del Consorzio dei Comuni) possono monitorare o indagare sull'utilizzo (= le attività sui server dell' datore di lavoro/Titolare, così p.es. i logfiles generati; verifiche tramite il mobile device management installato; al bisogno anche verifica diretta del dispositivo aziendale); ciò si verificherà solo per confermare la conformità ai requisiti della politica pertinente e per indagare su possibili violazioni della sicurezza, accessi non autorizzati, problemi tecnici, ecc. e non ai fini del monitoraggio dell'attività lavorativa. L'utilizzo di logfiles è limitato a tempistiche prefissate (breve termine) e l'attività di tracing viene espletata solo nei casi di dubbio, in forma manuale e di regola in collaborazione diretta con l'utente interessato.</p> <p>Le attività di controllo possono essere così riassunte:</p> <ol style="list-style-type: none"> 1) controllo/restrizione su base IP della regione di accesso per collegamento VPN (ev. anche per altri servizi) 2) controllo/restrizione su base IP per l'accesso alle e-mail 3) abilitazione su IP specifici dei servizi critici (es. anagrafe alle forze dell'ordine) 4) mobile device management per i dispositivi mobili aziendali 5) ulteriori forme di controllo che costituiranno, nel continuo, la best practice di settore (p.es. conditional access e multifactor authentication, ecc.)
4. RECHT AUF NICHTERREICHBARKEIT	4. DIRITTO ALLA DISCONNESSIONE
Im Fall von Telearbeit/Smartworking sieht die individuelle Vereinbarung zwischen Arbeitgeber und	In caso di telelavoro/smartworking l'accordo individuale tra il datore di lavoro e il dipendente

Angestellten u.a. die Ruhepausen mit Anrecht auf Unterbrechung der Verbindung vor.	prevede, tra l'altro, i tempi di riposo con diritto alla disconnessione;
BEI ZWEIFELN KONTAKTIEREN SIE UNS GERNE!	IN CASO DI DUBBI NON ESITATE A CONTATTARCI!
Version 01.02.2022	Versione 01.02.2022
Letzte Abänderung: 01.02.2022	Ultima modifica: 01.02.2022
DIE VORLIEGENDE ARBEITSANWEISUNG WIRD ALLEN MITARBEITERN VOM GENERALESEKRETARIAT AUF DEREN ZUGEWIESENE E-MAIL-ADRESSE ÜBERMITTELT. DIE ÜBERMITTLUNG WIRD PROTOKOLLIERT.	LE PRESENTI ISTRUZIONI DI LAVORO VENGONO INVIATE DALLA SEGRETERIA GENERALE A TUTTI I DIPENDENTI SULL'INDIRIZZO E-MAIL A LORO ASSEGNATO. L'INVIO VIENE PROTOCOLLATO.

1.C) Verwendungsvorgaben für die Angestellten in Bezug auf betrieblich zugelassene Cloud-Lösungen (mittels Verschlüsselung gesicherte Verbindungen, z.B. SSL, IPsec, ecc.)	1.C) Linee guida per dipendenti per l'utilizzo di soluzioni cloud autorizzate dall'azienda (tramite connessioni crittografate, p.es. SSL, IPsec, ecc.)
<p>Diese Vorgaben sollen dazu beitragen, dass die Rechtsvorschriften zur Verarbeitung personenbezogener Daten und zum Schutz der informationstechnischen Systeme eingehalten werden und insbesondere die Vertraulichkeit, Integrität und Verfügbarkeit von betrieblichen/geschäftlichen Dokumenten und Informationen sowie damit zusammenhängenden personenbezogenen Daten gewährleistet werden kann, sowohl am Arbeitsplatz im Büro als auch im Homeoffice.</p>	<p>Le presenti istruzioni hanno lo scopo di contribuire a garantire il rispetto delle disposizioni di legge sul trattamento dei dati personali e della sicurezza informatica e, in particolare, che possa essere garantita la riservatezza, l'integrità e la disponibilità di documenti e informazioni aziendali/d'ufficio e dei collegati dati personali, sia sul posto di lavoro in ufficio, sia in sede di telelavoro.</p>
<p><i>Anwendbare Normen: Verordnung (EU) 2016/679, Art. 32, sowie Vorgaben der Autorità Garante per la protezione dei dati personali</i></p>	<p><i>Norme applicabili: Regolamento (UE) 2016/679, Art. 32, nonché specifiche dell'Autorità Garante per la protezione dei dati personali</i></p>
<p>ANWENDUNGSBEREICH 1.1. Alle Mitarbeiter müssen diese Richtlinien bei jeder Verwendung von betrieblich zugelassenen Cloud-Lösungen befolgen, um die einschlägigen Richtlinien und Gesetze einzuhalten. Mitarbeiter müssen immer daran denken, dass sie bei der Verwendung dieser Cloud-Lösungen einen Service nutzen, der ihnen für geschäftliche Zwecke zur Verfügung gestellt wird.</p> <p>Die Bereitstellung von Cloud-Lösungen zielt darauf ab, die Produktivität durch den Einsatz moderner Bürotechnologien zu verbessern, die eine größere Mobilität sowie eine effiziente Zusammenarbeit und Kommunikation zwischen Mitarbeitergruppen ermöglichen.</p> <p>Es ist wichtig, dass die Verwendung von Cloud-Lösungen so verwaltet wird, dass eine ordnungsgemäße Verwendung gewährleistet ist.</p>	<p>APPLICABILITÀ 1.1. Tutti i dipendenti devono seguire queste linee guida ogni volta che utilizzano le soluzioni cloud autorizzate dall'azienda, al fine di conformarsi alla politica e alla legislazione pertinenti. I dipendenti devono sempre ricordare che quando utilizzano queste soluzioni cloud, stanno utilizzando un servizio fornito loro per scopi lavorativi.</p> <p>La fornitura delle soluzioni cloud mira a migliorare la produttività attraverso l'uso di moderne tecnologie per l'ufficio che consentono una maggiore mobilità e una collaborazione e comunicazione efficiente tra gruppi di personale.</p> <p>È essenziale che l'uso di soluzioni cloud sia gestito per garantire che venga utilizzato in modo appropriato.</p>
<p>ZUGRIFFE AUF DIE CLOUD-LÖSUNGEN 1.2. Der Zugriff auf Daten des Arbeitgebers/Verantwortlichen darf <u>ausschließlich</u> a) direkt über dessen Netzwerk oder b) über eine sichere Verbindung erfolgen. Die Zugangsdaten werden Ihnen vorab mitgeteilt. Es ist keine Verwendung von VPN- oder anderen z.B. Tor – ähnlichen Diensten zur Verschleierung des Standortes, ob beabsichtigt oder nicht, zulässig.</p>	<p>ACCESSO ALLE SOLUZIONI CLOUD 1.2. È possibile accedere ai dati del datore di lavoro/Titolare di trattamento <u>solo</u> direttamente tramite a) la sua rete oppure b) tramite una connessione sicura. Le verranno forniti le credenziali di accesso in anticipo. Non è ammesso l'utilizzo intenzionale o meno, di VPN- o altri servizi – p.es. Tor – funzionali ad occultare la localizzazione.</p>
<p>REGELN 1.3. Alle Mitarbeiter sind verpflichtet, die Vertraulichkeit personenbezogener Daten oder anderer Informationen, die ihnen im Laufe ihrer Arbeitstätigkeit zur Verfügung stehen, zu wahren und die Informationen nur zur Erfüllung ihrer</p>	<p>REGOLE 1.3. Tutti dipendenti hanno il dovere di mantenere la riservatezza su dati personali o informazioni di altro tipo che diventa loro disponibile nel corso del loro impiego e di utilizzare le informazioni solo per lo svolgimento della loro prestazione lavorativa. Quando</p>

<p>Arbeitsaufgaben zu verwenden. Bei der Verwendung von Cloud-Lösungen müssen Mitarbeiter sicherstellen, dass sie alle Risiken der Offenlegung dieser Informationen über ihren rechtlichen Zweck hinaus berücksichtigen und verwalten.</p> <p>Die Mitarbeiter müssen sich des Umstandes bewusst sein, dass es public/öffentliche Clouds und private Clouds gibt: die öffentliche Cloud ist ein Angebot eines frei zugänglichen Providers, der seine Dienste offer über das Internet für jedermann zugänglich macht. Private Clouds werden hingegen von Unternehmen selbst betrieben und ausschließlich den eigenen Nutzern zugänglich gemacht. Der Arbeitgeber/Verantwortliche hat bei den selbst bereitgestellten privaten Clouds insgesamt bessere Möglichkeiten, die Bereiche Datenschutz und IT-Sicherheit zu wahren; bei Drittanbietern von public Clouds ist dies, selbst wenn es sich um renommierte Anbieter handelt, bedeutend schwieriger. Aus diesem Grund wird mit Nachdruck empfohlen, insbesondere die sog. besonderen Kategorien personenbezogener Daten gemäß Artt. 9 und 10 EU-Verordnung Nr. 679/2016 (z.B.: rassistische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, genetischen Daten, biometrischen Daten, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person, Daten über strafrechtliche Verurteilungen und Straftaten, usw.) ausschließlich im Rahmen privater Clouds des Arbeitgebers/Verantwortlichen zu verarbeiten, und in jedem Fall gilt, dass diese Daten immer nur mittels den jeweils für diese Daten spezifisch vorgesehenen Programmen innerhalb der Cloud-Lösung verarbeitet werden dürfen; denn bereits das einfache Teilen von Dokumenten betreffend die genannten besonders geschützten Personendaten während einer Cloud-Videokonferenz (z.B. Hochladen eines Dokuments in den Chatverlauf, usw.) stellt eine nicht zu unterschätzende informatische Risikoquelle dar.</p>	<p>si utilizzano le soluzioni cloud, i dipendenti devono assicurarsi di considerare e gestire qualsiasi rischio di divulgazione di queste informazioni oltre il loro scopo legale.</p> <p>I dipendenti devono essere consapevoli del fatto che esistono public clouds e private clouds: la cloud pubblica rappresenta l'offerta pubblicamente accessibile di un fornitore che offre i suoi servizi indipendentemente a tutti gli interessati tramite internet. Le cloud private sono invece gestite dalle aziende stesse e rese disponibili esclusivamente ai propri utenti. Il datore di lavoro/Titolare del trattamento riesce a garantire molto meglio la protezione dei dati e la sicurezza informatica nel caso di proprie cloud private; invece, nel caso di fornitori terzi di cloud pubbliche, anche se si tratta di fornitori rinomati, ciò è molto più difficile. Per questo motivo, si raccomanda incisivamente di trattare in particolare le c.d. categorie particolari di dati personali a.s. degli artt. 9 e 10 del Reg. UE n. 679/2016 (ad es.: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, dati relativi alle condanne penali e ai reati, ecc.) esclusivamente nell'ambito di cloud private del datore di lavoro/Titolare del trattamento, e, in ogni caso, questi dati vanno sempre trattati solo tramite gli applicativi specificamente previsti per il relativo trattamento all'interno della soluzione cloud; infatti, anche la semplice condivisione durante una videoconferenza in cloud (p.es. caricare un documento nella chat, ecc.) di un documento contenente la predetta categoria particolare di dati personali, può rappresentare un rischio informatico da non sottovalutare.</p>
<p>FERNZUGRIFF (unter Einhaltung der Vorgabe laut Punkt 1.2)</p> <p>1.4. Cloud-Lösungen sind von Natur aus von überall zugänglich. Mitarbeiter, die von zu Hause oder von einem anderen Ort aus, der nicht Teil des Netzwerks des Arbeitgebers/Verantwortlichen ist, auf Cloud-Lösungen zugreifen, müssen Folgendes beachten:</p> <ul style="list-style-type: none"> • Die Inhalte des/r vom Arbeitgeber/Verantwortlichen erteilten Auftrags und Anweisungen gemäß Art. 29 EU-Verordnung Nr. 679/2016 für die Verarbeitung von personenbezogenen Daten sind auch bei der Verwendung der Cloud-Lösungen zu beachten. 	<p>ACCESSO DA REMOTO (nel rispetto di quanto stabilito al punto 1.2)</p> <p>1.4. Le soluzioni cloud, per la loro stessa natura, sono accessibili da qualsiasi luogo. I dipendenti che accedono alle soluzioni cloud da casa o da un'altra posizione, che non fa parte della rete del datore di lavoro/Titolare, devono:</p> <ul style="list-style-type: none"> • I contenuti dell'incarico e delle istruzioni del datore di lavoro/Titolare del trattamento ex art. 29 regolamento UE n. 679/2016 per il trattamento dei dati personali sono da rispettare anche nell'utilizzo delle soluzioni cloud;

<ul style="list-style-type: none"> • Schützen Sie Ihre Konten besagter Cloud-Lösungen und Ihre Passwörter vor Offenlegung. Zugangspasswörter sind geheim zu halten. • Verwenden Sie sichere Passwörter und ändern Sie Passwörter, wenn Sie den Verdacht haben, dass jemand sie kennt. • Beachten Sie die Versuche Dritter, Kennwörter oder andere Anmeldeinformationen zu erhalten, z. B. per E-Mail oder Telefon. • Aktivieren Sie den Bildschirmschoner oder das Sperrsystem, wenn Sie sich nicht in der Nähe von Arbeitsstationen oder Geräten befinden. • Seien Sie vorsichtig bei der Verbindung mit öffentlichen oder unbekanntem Wi-Fi-Netzwerken. Seien Sie sich stets bewusst, dass Verbindungen zwischen dem Remote-Standort und Cloud-Lösungen ein potenzielles Risiko darstellen. • Beachten Sie, dass alle elektronischen Kommunikationsaktivitäten des Unternehmens Eigentum des Arbeitgebers/Verantwortlichen sind/werden. • Seien Sie sich bewusst, dass Sie für die Folgen verantwortlich sind, wenn der Fernzugriff missbraucht wird. • Benachrichtigen Sie sofort den Systemadministrator bei Verdacht auf Diebstahl oder Missbrauch Ihres Kontos. • Melden Sie sich in Bezug auf die Cloud-Lösungen immer direkt an: stellen Sie sicher, dass Sie nicht über eine (nicht vom Arbeitgeber/Verantwortlichen zur Verfügung gestellte) VPN, Tor oder andere Dienste, welche Ihre IP-Adresse verschleiern, zugreifen. Solche Maßnahmen erschweren die Feststellung, ob ein Account kompromittiert/angegriffen worden ist. • Melden Sie sich nach Gebrauch jeder einzelnen verwendeten Cloud-Lösung immer sofort und ordnungsgemäß ab. • Auf dem für den Zugang zur Cloud-Lösung verwendeten Gerät sind keine Dokumente, Informationen und personenbezogenen Daten zu speichern. 	<ul style="list-style-type: none"> • Proteggere i propri account delle soluzioni cloud e le relative password dalla divulgazione. Le password di accesso devono essere tenute segrete. • Utilizzare password complesse e modificare le password se si sospetta che qualcuno le conosca. • Essere consapevoli di tentativi da parti terze di ottenere password o altre credenziali di accesso, ad esempio tramite e-mail o truffe telefoniche. • Attivare lo screen saver o il sistema di blocco se si è lontani da workstation o dispositivi. • Diffidare della connessione a reti Wi-Fi pubbliche o sconosciute. Rimanere costantemente consapevoli del fatto che le connessioni tra la posizione remota e le soluzioni cloud determinano un potenziale rischio • Tenere presente che tutte le attività di comunicazione elettronica aziendale sono/diventano proprietà del datore di lavoro/Titolare. • Comprendere che hanno la responsabilità delle conseguenze nel caso in cui l'accesso remoto venga utilizzato in modo improprio. • Avvisare immediatamente l'amministratore di sistema in caso di sospetto furto o uso improprio del proprio account di accesso remoto. • Per quanto riguarda le soluzioni cloud, accedi sempre direttamente: assicurati di non accedere tramite una VPN, Tor o altri servizi (non forniti dal datore di lavoro/Titolare), funzionali ad occultare l'indirizzo IP. Tali misure rendono infatti difficile individuare se un account è stato compromesso. • Disconnettersi sempre regolarmente ed immediatamente da tutte le singole soluzioni cloud al termine dell'uso. • Sul dispositivo utilizzato per l'accesso alla soluzione cloud documenti, informazioni e dati personali non devono mai essere salvati.
---	--

<p>KONTROLLEN</p> <p>1.5. Der Arbeitgeber/Verantwortliche hat die Aufsicht über die Cloud-Lösungen, einschließlich der etwaigen Aufzeichnung von Kommunikationen. Der Zugriff auf die Cloud-Lösungen wird nicht systematisch und kontinuierlich überwacht, die Systemadministratoren des Arbeitgebers/Verantwortlichen (auch in Zusammenarbeit mit der EDV-Abteilung des Gemeindenverbandes) können die Nutzung aber überwachen oder untersuchen; dies geschieht nur, um die Einhaltung der relevanten Richtlinien zu bestätigen und mögliche Sicherheitsverletzungen, unbefugte</p>	<p>VERIFICHE</p> <p>1.5. Il datore di lavoro/Titolare ha la supervisione in relazione alle soluzioni cloud, inclusa l'eventuale registrazione di comunicazioni aziendali. Non si procede ad una sorveglianza sistematica e continua dell'accesso alle soluzioni cloud, ma gli amministratori di sistema del datore di lavoro/Titolare (anche in collaborazione con la Ripartizione EDP del Consorzio dei Comuni) possono monitorare o indagare sull'utilizzo; ciò si verificherà solo per confermare la conformità ai requisiti della politica pertinente e per indagare su possibili violazioni della sicurezza, accessi</p>
---	--

<p>Zugriffe, technische Probleme, usw. zu untersuchen und nicht für die Zwecke der Überwachung der Arbeitstätigkeit. Die Verwendung von Logfiles erfolgt immer mit einer festgelegten zeitlichen Begrenzung (kurze Frist) und Tracing-Tätigkeit erfolgt nur bei allfälligen Verdachtsmomenten, in manueller Form und üblicherweise in direkter Zusammenarbeit mit dem betroffenen Nutzer.</p> <p>Die Kontrollen können wie folgt zusammengefasst werden:</p> <ol style="list-style-type: none"> 1) Kontrolle/Einschränkung auf der Grundlage der IP der Region, aus welcher der Verbindungszugriff erfolgt (ev. auch für weitere Dienste) 2) Kontrolle/Einschränkung auf der Grundlage der IP für den E-Mail-Zugang 3) Befähigung bestimmter IP's in Zusammenhang mit kritischen Diensten (z.B. Meldedaten an die Polizeikräfte) 4) mobile device management für die mobilen Betriebsgeräte 5) zusätzliche Kontrollformen, die im Laufe der Zeit, zur best practice des Sektors zählen werden (z.B. conditional access und multifactor authentication, usw.) 	<p>non autorizzati, problemi tecnici, ecc. e non ai fini del monitoraggio dell'attività lavorativa. L'utilizzo di logfiles è limitato a tempistiche prefissate (breve termine) e l'attività di tracing viene espletata solo nei casi di dubbio, in forma manuale e di regola in collaborazione diretta con l'utente interessato.</p> <p>Le attività di controllo possono essere così riassunte:</p> <ol style="list-style-type: none"> 1) controllo/restrizione su base IP della regione di accesso per collegamento VPN (ev. anche per altri servizi) 2) controllo/restrizione su base IP per l'accesso alle e-mail 3) abilitazione su IP specifici dei servizi critici (es. anagrafe alle forze dell'ordine) 4) mobile device management per i dispositivi mobili aziendali 5) ulteriori forme di controllo che costituiranno, nel continuo, la best practice di settore (p.es. conditional access e multifactor authentication, ecc.)
<p>BEI ZWEIFELN KONTAKTIEREN SIE UNS GERNE!</p>	<p>IN CASO DI DUBBI NON ESITATE A CONTATTARCI!</p>
<p>Version 01.02.2022</p>	<p>Versione 01.02.2022</p>
<p>Letzte Abänderung: 01.02.2022</p>	<p>Ultima modifica: 01.02.2022</p>
<p>DIE VORLIEGENDE ARBEITSANWEISUNG WIRD ALLEN MITARBEITERN VOM GENERALSEKRETARIAT AUF DEREN ZUGEWIESENE E-MAIL-ADRESSE ÜBERMITTELT. DIE ÜBERMITTLUNG WIRD PROTOKOLLIERT.</p>	<p>LE PRESENTI ISTRUZIONI DI LAVORO VENGONO INVIATE DALLA SEGRETERIA GENERALE A TUTTI I DIPENDENTI SULL'INDIRIZZO E-MAIL A LORO ASSEGNATO. L'INVIO VIENE PROTOCOLLATO.</p>