COMUNE DI MALLES VENOSTA

PIANO INTEGRATIVO DI ATTIVITÀ ED ORGANIZZA-ZIONE (PIAO) 2022-2024

Approvato von delibera della Giunta comunale n. 568 del 20.12.2022

Contenuto

PREMESSA ..... Fehler! Textmarke nicht definiert.

1. SCHEDA ANAGRAFICA DELL'AMMINISTRAZIONE **4**

2. VALORE PUBBLICO, PERFORMANCE E ANTICORRUZIONE **4**

3. ORGANIZZAZIONE **6**

4. MONITORAGGIO **9**

Allegati **9**

PREMESSA

L'articolo 6 del decreto-legge 9 giugno 2021, n. 80, convertito, con modificazioni, dalla legge 6 agosto 2021, n. 113 ha previsto che le pubbliche amministrazioni con più di cinquanta dipendenti, con esclusione delle scuole di ogni ordine e grado e delle istituzioni educative, adottino, entro il 31 gennaio di ogni anno, il Piano integrato di attività e organizzazione (di seguito PIAO). Il successivo decreto-legge 30 dicembre 2021, n. 228 "Disposizioni urgenti in materia di termini legislativi" ha differito, in sede di prima applicazione, al 30 aprile 2022, il termine per l'adozione del PIAO. Da ultimo, l'art. 7 comma 1 lett. a) del D.L. 30/04/2022, n. 36, ha ulteriormente spostato il termine di approvazione del PIAO al 30/06/2022.

Con il DPR n° 81 del 24 giugno 2022 (G.U. 151 del 30 giugno 2022) la data di prima adozione del PIAO è stata differita di 120 giorni dalla data di approvazione del bilancio di previsione.

Il Piano ha l'obiettivo di assorbire, razionalizzandone la disciplina in un'ottica di massima semplificazione, molti degli atti di pianificazione cui sono tenute le amministrazioni.

Il Piano ha durata triennale e, per le Amministrazioni con meno di 50 dipendenti è aggiornato annualmente solo in presenza di fatti corruttivi, modifiche organizzative rilevanti o ipotesi di disfunzioni amministrative significative intercorse ovvero di aggiornamenti o modifiche degli obiettivi di performance a protezione del valore pubblico (art. 6, comma 2, DPR 81/2022).

Il PIAO sostituisce alcuni altri strumenti di programmazione, in particolare:

- Piano del Fabbisogno del personale;
- Piano delle Performance;
- Piano Triennale Anticorruzione;
- Piano del Lavoro Agile;
- Piano delle Dotazioni strumentali;
- Piano delle Azioni positive e Azioni concrete

Il principio che guida la definizione del PIAO risponde alla volontà di superare la molteplicità degli strumenti di programmazione introdotti in diverse fasi dell'evoluzione normativa e di creare un piano unico di governance. In quest'ottica, il Piano Integrato di Attività e Organizzazione rappresenta una sorta di "testo unico" della programmazione.

Nella sua redazione, oltre alle Linee Guida per la compilazione del Piano Integrato di Attività e Organizzazione (PIAO) pubblicate dal Dipartimento della Funzione Pubblica ed agli Orientamenti ANAC del 2 febbraio 2022, è stata tenuta in considerazione anche la normativa precedente e non ancora abrogata riguardante la programmazione degli Enti Pubblici.

Nello specifico, è stato rispettato il quadro normativo di riferimento, ovvero:

- per quanto concerne la Performance, il decreto legislativo n. 150/2009 e s.m.i, la L.R. n. 22/2010 e s.m.i. e le Linee Guida emanate dal Dipartimento della Funzione Pubblica;
- riguardo ai Rischi corruttivi ed alla trasparenza, il Piano nazionale anticorruzione (PNA) e gli atti di regolazione generali adottati dall'ANAC ai sensi della legge n. 190 del 2012, il decreto legislativo n. 33 del 2013;
- in materia di Organizzazione del lavoro agile, Linee Guida emanate dal Dipartimento della Funzione Pubblica e tutte le ulteriori specifiche normative di riferimento delle altre materie relative al Piano delle azioni positive, al Piano triennale dei fabbisogni di personale ed alla Formazione.
- Il presente documento è stato predisposto dalla Segretaria Comunale (RPCT) ed adottato dalla Giunta Comunale, in ottemperanza a quanto previsto dalla normativa sopra riportata.

Per gli Enti con non più di cinquanta dipendenti sono previste modalità semplificate.

Questa Amministrazione ha un organico di meno di cinquanta dipendenti.

Il calcolo del numero dei dipendenti di questa Amministrazione è stato effettuato secondo le indicazioni contenute nel Quaderno ANCI n° 36 del luglio 2022 (modalità di calcolo utilizzate per compilare la tabella 12 del Conto Annuale).

Con Circolare 6/EL/2022 la Regione Trentino-Alto Adige ha precisato:

“Con riferimento al contenuto del PIAO, si evidenzia che l’art. 4 della l.r. n. 7/2021 (Legge regionale collegata alla legge regionale di stabilità 2022) dispone che: 1. La Regione e gli enti pubblici a ordinamento regionale, ai sensi dell’articolo 18-bis del decreto-legge 9 giugno 2021, n. 80 (Misure urgenti per il rafforzamento della capacità amministrativa delle pubbliche amministrazioni funzionale all’attuazione del Piano nazionale di ripresa e resilienza (PNRR) e per l’efficienza della giustizia), convertito, con modificazioni, dalla legge 6 agosto 2021, n. 113, applicano gradualmente le disposizioni recate dall’articolo 6 del decreto stesso. Per l’anno 2022, salvo differimento del termine, sono obbligatorie la compilazione delle parti del Piano integrato di attività e organizzazione relative alle lettere a) e d) dell’articolo 6, comma 2, compatibilmente con gli strumenti di programmazione previsti alla data del 30 ottobre 2021 per gli enti stessi, e la definizione delle relative modalità di monitoraggio. Rimane salva la facoltà di integrare il Piano con gli altri contenuti previsti dall’articolo 6, comma 2.

Alla luce della normativa regionale sopra citata, per il 2022, le sezioni del PIAO da ritenersi di compilazione obbligatoria per gli enti ad ordinamento regionale sono dunque le seguenti:

- Scheda anagrafica;
- Sezione Valore pubblico, Performance e Anticorruzione (art. 3 del decreto ministeriale che definisce lo schema tipo);
- Sezione Monitoraggio (art. 5 del decreto ministeriale che definisce lo schema tipo), limitatamente alle parti compilate”.

A prescindere dalla normativa regionale sopra indicata, il Comune di Malles Venosta ritiene di compilare, sin dalla sua prima attuazione (triennio 2022-2024), il PIAO integrale per le parti di pertinenza delle Amministrazioni con meno di 50 dipendenti.

SEZIONE DI PROGRAMMAZIONE	DESCRIZIONE SINTETICA DELLE AZIONI/ATTIVITÀ OGGETTO DI PIANIFICAZIONE	AMMINISTRAZIONI CON PIÙ DI 50 DIPENDENTI	AMMINISTRAZIONI CON MENO DI 50 DIPENDENTI
1. SCHEDA ANAGRAFICA DELL'AMMINISTRAZIONE	Nome: Comune di Malles Venosta Indirizzo: 39024 Malles, via Stazione 19 Sito web: www.comune.malles.bz.it Sindaco: THURNER Josef Numero di dipendenti al 31/12/2021: 41 (27,6 posti a tempo pieno) Popolazione al 31/12/2021: 5277 Telefono: 0473 831117 E-mail: info@comune.malles.bz.it PEC: mals.malles@legalmail.it Codice fiscale: 82006550212 Partita IVA: 00827900218	SI	SI
2. VALORE PUBBLICO, PERFORMANCE E ANTICORRUZIONE			
2.1 Valore pubblico	La compilazione della presente sezione non è dovuta per I Comuni con meno di 50 dipendenti.	SI	NO
2.2. Performance	La compilazione della presente sezione non è dovuta per I Comuni con meno di 50 dipendenti.	SI	NO
2.3 Rischi corruttivi e trasparenza	**Valutazione di impatto del contesto esterno** L'analisi del contesto esterno ha come obiettivo quello di evidenziare come le caratteristiche dell'ambiente nel quale l'Ente è chiamato ad operare, con riferimento, ad esempio, a variabili culturali, criminologiche, sociali ed economiche del territorio possano favorire il verificarsi di fenomeni corruttivi al proprio interno. A tal fine, sono stati considerati sia i fattori legati al territorio della Provincia di Bolzano, sia le relazioni e le possibili influenze esistenti con i portatori e i rappresentanti di interessi esterni. Comprendere le dinamiche territoriali di riferimento e le principali influenze e pressioni a cui un Ente locale struttura è sottoposto consente infatti di indirizzare con maggiore efficacia e precisione la strategia di gestione del rischio. Ricercando precisi indicatori di contesto, utili risultano i dati pubblicati nel 2016 da ASTAT, Istituto di statistica Provinciale, in occasione della giornata mondiale contro la corruzione, dati relativi all'opinione degli altoatesini sulla corruzione e su comportamenti che attengono al senso civico e che, più o meno direttamente, fungono da indicatori di legalità di un territorio. Il 44,4% dei cittadini altoatesini rifiuta nettamente l'affermazione secondo cui la corruzione sarebbe un qualcosa di naturale e caratterizzante la vita	SI	SI

SEZIONE DI PROGRAMMAZIONE	DESCRIZIONE SINTETICA DELLE AZIONI/ATTIVITÀ OGGETTO DI PIANIFICAZIONE	AMMINISTRAZIONI CON PIÙ DI 50 DIPENDENTI	AMMINISTRAZIONI CON MENO DI 50 DIPENDENTI
	sociale ed economica. Quasi un quarto (24,3%) degli altoatesini si trova poco d'accordo con la stessa affermazione mentre quasi un terzo (31,3%) della popolazione è abbastanza o molto concorde nel ritenere che non sia possibile evitare e combattere la pratica corruttiva. Il 60% degli altoatesini considera molto o abbastanza pericoloso denunciare fatti di corruzione. Quanto una società sia "resistente" alla corruzione può essere misurato anche attraverso il dato relativo alla propensione alla denuncia. Nello specifico, il rischio legato alla decisione di denunciare è indicatore della "libertà percepita" nel cui ambito il cittadino può far valere i propri diritti. In Alto Adige esiste un 15,0% di cittadini che è molto concorde nel ritenere pericolosa la denuncia della corruzione ed un ulteriore 44,3% ritiene comunque che la denuncia di fatti di corruzione comporti ancora qualche pericolo. Viceversa, il 17,0% dei residenti in provincia di Bolzano considera la denuncia dei fatti di corruzione assolutamente non pericolosa. Nell'analisi del contesto esterno, questa Amministrazione terrà conto anche dell'impatto causato dalla pandemia Covid 19 sul tessuto economico e sociale. Da una parte, Covid 19, ha impoverito la popolazione, dall'altra ha bloccato o ridimensionato le attività delle imprese operanti sui territori con il rischio che le organizzazioni criminali si infiltrino nel tessuto sociale ed economico. Ciò vale soprattutto per l'eccesso al credito. **Valutazione di impatto del contesto interno** Nel processo di costruzione del presente Piano si è tenuto conto degli elementi di conoscenza sopra sviluppati relativi al contesto ambientale di riferimento, ma anche delle risultanze dell'ordinaria vigilanza costantemente svolta all'interno dell'Amministrazione sui possibili fenomeni di deviazione dell'agire pubblico dai binari della correttezza e dell'imparzialità. Nel corso dei monitoraggi sinora effettuati, non sono emerse irregolarità attinenti al fenomeno corruttivo, né a livello di personale dipendente / collaboratore, né a livello di organi di indirizzo politico amministrativo. Si segnala inoltre: - **Sistema di responsabilità**: ruoli responsabilità e deleghe sono preventivamente e		

SEZIONE DI PROGRAMMAZIONE	DESCRIZIONE SINTETICA DELLE AZIONI/ATTIVITÀ OGGETTO DI PIANIFICAZIONE	AMMINISTRAZIONI CON PIÙ DI 50 DIPENDENTI	AMMINISTRAZIONI CON MENO DI 50 DIPENDENTI
	dettagliatamente definiti e formalizzati, così come i processi decisionali - **Politiche, obiettivi e strategie**: sono definiti di concerto da Giunta comunale e Segretario Comunale - **Risorse, conoscenze, sistemi e tecnologie**: l'Amministrazione è dotata di una sede efficiente, di una rete infrastrutturale ed informatica recente, con formazione continua del suo Personale - **Cultura organizzativa**: a partire dall'assunzione tutti gli impiegati sono valutati e valorizzati per la loro capacità di interpretare in modo etico il raggiungimento delle finalità dell'ente - **Flussi informativi**: la trasparenza interna è considerata un pilastro fondante la capacità dell'ente di porsi come Organizzazione in grado di apprendere e di sviluppare il valore delle risorse ad esso affidate. - **Denunce, segnalazioni o altre indagini in corso**: non risultano agli atti, né si riscontrano procedimenti disciplinari pregressi o pendenti. Si può quindi fondatamente ritenere che il contesto interno è sano e non genera particolari preoccupazioni. Vedasi allegato: Mappatura dei processi, Identificazione e valutazione dei rischi corruttivi potenziali e concreti, Progettazione di misure organizzative per il trattamento del rischio.		
3. ORGANIZZAZIONE			
3.1 STRUTTURA ORGANIZZATIVA	Il modello organizzativo dell'ente contiene: • organigramma; • livelli di responsabilità organizzativa, numero di Dirigenti e numero di Posizioni Organizzative, sulla base di quattro dimensioni: o inquadramento contrattuale (o categorie); o profilo professionale (possibilmente non ingessato sulle declaratorie da CCNL); o competenze tecniche (saper fare); o competenze trasversali (saper essere - soft skill); o numero dei dipendenti medi per ciascuna unità organizzativa; Si veda l'organigramma allegato, i regolamenti	SI	SI

SEZIONE DI PROGRAMMAZIONE	DESCRIZIONE SINTETICA DELLE AZIONI/ATTIVITÀ OGGETTO DI PIANIFICAZIONE	AMMINISTRAZIONI CON PIÙ DI 50 DIPENDENTI	AMMINISTRAZIONI CON MENO DI 50 DIPENDENTI
	dell'ufficio e la tabella dell'organico, estratto dal rapporto DUP e sulla struttura del personale.		
3.2. ORGANIZZAZIONE DEL LAVORO AGILE	Nelle more della regolamentazione del lavoro agile, ad opera dei contratti collettivi nazionali di lavoro che disciplineranno a regime l'istituto del Lavoro Agile per gli aspetti non riservati alla fonte unilaterale, così come indicato nelle premesse delle "Linee guida in materia di lavoro agile nelle amministrazioni pubbliche", adottate dal Dipartimento della Funzione Pubblica il 30 novembre 2021 e per le quali è stata raggiunta l'intesa in Conferenza Unificata, ai sensi dell'articolo 9, comma 2, del decreto legislativo 28 agosto 1997, n. 281, in data 16 dicembre 2021, l'istituto del lavoro agile presso il Comune di Sluderno, rimane regolato dalle disposizioni di cui alla vigente legislazione In data 3/12/2020 è stato sottoscritto dalle parti contrattuali il secondo accordo stralcio per il rinnovo del contratto collettivo intercompartimentale per il triennio 2019 – 2021. Gli articoli 7 e 8 del predetto accordo stralcio definiscono la disciplina quadro sul lavoro agile ordinario per il periodo posto Covid-19. L'epidemia Covid-19 ha posticipato l'entrata in vigore delle disposizioni del predetto nuovo accordo. Per tutta la durata della pandemia, il comune di Sluderno ha promosso e implementato il più ampio utilizzo possibile dello smart working nelle aree in cui ciò era possibile. A partire dal 01.04.2022 il lavoro agile è possibile unicamente - come previsto dal predetto accordo stralcio come anche dalla normativa nazionale – previa sottoscrizione di un accordo individuale ad hoc. Gli articoli 7 e 8 del contratto collettivo intercompartimentale prevedono specificamente quanto segue: - il lavoro agile è una modalità volontaria di esecuzione del rapporto di lavoro ovvero è sottoposto alla volontà delle parti; - il lavoro agile può avere durata determinata o indeterminata; - il lavoro agile si basa sul raggiungimento di obiettivi e/o di una performance concordati; - le attività lavorative di norma vengono effettuate nella fascia oraria giornaliera compresa tra le ore 6.00 e le ore 20.00, secondo un orario liberamente gestito; - in base alle esigenze di servizio possono		

SEZIONE DI PROGRAMMAZIONE	DESCRIZIONE SINTETICA DELLE AZIONI/ATTIVITÀ OGGETTO DI PIANIFICAZIONE	AMMINISTRAZIONI CON PIÙ DI 50 DIPENDENTI	AMMINISTRAZIONI CON MENO DI 50 DIPENDENTI
	comunque concordati vincoli di orario o precise fasce di reperibilità; - è garantito il diritto alla disconnessione nei periodi di riposo; - il lavoro agile non prevede la prestazione di lavoro straordinario e non dà diritto alla fruizione di buoni pasto; - il datore di lavoro garantisce la corretta e completa informazione rispetto alla sicurezza sul lavoro. Con l'accordo individuale, il quale deve essere compilato e sottoscritto tra il singolo dipendente ed il relativo responsabile del servizio rispettivamente delle strutture secondo il fac-simile elaborato dall'amministrazione, vengono per es. definiti la durata temporale dell'accordo, la descrizione generale delle attività da svolgere e gli obiettivi da raggiungere, la previsione delle giornate/mezze giornate da svolgersi in modalità agile o il numero delle giornate fruibili in modo flessibile con riferimento ad un periodo, le fasce orarie di svolgimento dell'attività lavorativa e quelle di rintracciabilità e la strumentazione tecnologica da utilizzare. L'accesso al lavoro agile è privilegiato nei seguenti casi: - Fragilità personali o situazioni di disagio familiare; - Distanza chilometrica dal posto di lavoro; - Idoneità dell'ambiente domestico; - Eventuale ripresentarsi di situazioni pandemiche; Si allegano: - Accordo di intercomparto; - Istruzioni per il lavoro con dispositivi privati o aziendali; - Linee guida per l'utilizzo delle soluzioni cloud aziendali.		
3.3 PIANO TRIENNALE DEI FABBISOGNI DI PERSONALE	Il numero dei dipendenti al 31 dicembre dellePreseè calcolato sulla base della sezione Personale del Documento Strategico Unico 2022 – 2024, approvata con delibera del Consiglio Comunale n. 62 del 29.12.2021. Si allega la sezione Risorse umane del Documento di Strategia Unica 2022 – 2024. Il Piano Triennale dei fabbisogni di personale illustra i seguenti elementi:	SI	SI

SEZIONE DI PROGRAMMAZIONE	DESCRIZIONE SINTETICA DELLE AZIONI/ATTIVITÀ OGGETTO DI PIANIFICAZIONE	AMMINISTRAZIONI CON PIÙ DI 50 DIPENDENTI	AMMINISTRAZIONI CON MENO DI 50 DIPENDENTI

	• Rappresentazione della consistenza di personale al 31 dicembre dell'anno precedente;
	• Programmazione strategica delle risorse umane, valutata sulla base dei seguenti fattori:
	  ○ capacità di assunzione calcolata sulla base dei vigenti vincoli di spesa;
	  ○ stima del trend delle cessazioni, sulla base dei pensionamenti;
	  ○ stima dell'evoluzione dei bisogni, in funzione di scelte legate, alla digitalizzazione dei processi, alle esternalizzazioni o internalizzazioni o a potenziamento, dismissione di Servizi, attività, funzioni o ad altri fattori interni o esterni che richiedono una discontinuità nel profilo delle risorse umane in termini di profili di competenze e/o quantitativi.
	Si allega il Piano triennale di fabbisogno del personale 2022-2024.
	Il Comune di Malles Venosta ritiene di fondamentale importanza strategica la formazione dei propri dipendenti.
	• Privacy;
	• anticorruzione e amministrazione trasparente;
	• sicurezza sul lavoro;
	• Diritto degli appalti pubblici;
	• Licenze
	• Imposte e tributi
	• Finanza
	• Ufficio anagrafe e anagrafe
	• Biblioteconomia
	• Sicurezza pubblica
	• Edilizia
	• Alimenti (intolleranze)		

4. MONITORAGGIO	La compilazione della presente sezione non è dovuta per I Comuni con meno di 50 dipendenti.	SI	NEIN

Allegati

1. Catalogo rischi prevenzione alla corruzione

2. Organigramma, Regolamento Uffici, pianta organica
3. Estratto ESD Auszug ESD situazione personale
4. Rapporto annuale struttura personale
5. Contratto collettivo intercompartimentale Smart-Working

GEMEINDE MALS

INTEGRIERTER TÄTIGKEITS- UND ORGANISATIONSPLAN
(PIAO) 2022-2024

Genehmigt mit Beschluss des Gemeindeausschusses Nr. 568 vom 20.12.2022

Inhalt

VORWORT **2**

1.DATENÜBERSICHT DER VERWALTUNG **4**

2. ÖFFENTLICHER WERT, PERFORMANCE UND KORRUPTIONS-VORBEUGUNG **4**

3. ORGANISATION UND HUMANRESSOURCEN **6**

4. ÜBERPRÜFUNGEN **10**

Anlagen **10**

VORWORT

Artikel 6 des Gesetzesdekrets Nr. 80 vom 9. Juni 2021, umgewandelt in das Gesetz Nr. 113 vom 6. August 2021, sieht vor, dass öffentliche Verwaltungen mit mehr als fünfzig Mitarbeitern, mit Ausnahme von Schulen aller Arten und Ausbildungsstufen und Bildungseinrichtungen, bis zum 31. Januar eines jeden Jahres den Integrierten Plan der Tätigkeiten und der Organisation (in der Folge PIAO genannt) verabschieden müssen. Durch das nachfolgende Gesetzesdekret Nr. 228 vom 30. Dezember 2021 "Dringende Bestimmungen zu Gesetzgebungsfristen" wurde die Frist für die Verabschiedung des PIAO auf den 30. April 2022 verschoben, als es erstmals zur Anwendung kam. Schließlich wurde in Artikel 7 Absatz 1 Buchstabe a) des Gesetzesdekrets Nr. 36 vom 30.04.2022 die Frist für die Genehmigung des PIAO weiter auf den 30.06.2022 verschoben.

Mit dem Dekret des Präsidenten der Republik Nr. 81 vom 24. Juni 2022 (G.U. 151 vom 30. Juni 2022) wurde das Datum der ersten Verabschiedung des PIAO um 120 Tage ab dem Datum der Genehmigung des Haushalts verschoben.

Ziel des Plans ist es, durch die Vereinfachung der Materie einen Großteil der von den Verwaltungen durchzuführenden Planungsmaßnahmen zu übernehmen.

Der Plan hat eine Laufzeit von drei Jahren und wird bei Verwaltungen mit weniger als 50 Mitarbeitern - wie der vorliegenden - nur dann jährlich aktualisiert, wenn Korruptionsfälle, bedeutende organisatorische Veränderungen oder Hypothesen über aufgetretene erhebliche Verwaltungsmängel oder Aktualisierungen oder Änderungen der Leistungsziele zum Schutz des öffentlichen Wertes vorliegen (Artikel 6 Absatz 2 des Dekrets des Präsidenten der Republik Nr. 81/2022).

Der PIAO ersetzt einige andere Planungsmittel, nämlich:

- Personalbedarfsplan;
- Leistungsplan;
- Dreijahresplan zur Korruptionsbekämpfung;
- Plan für Smart-Working;
- Plan für die Zuweisung von Betriebsmitteln;
- Maßnahmenplan

Das Prinzip, das der Definition des PIAO zugrunde liegt, entspricht dem Wunsch, die Vielzahl von Planungsinstrumenten zu überwinden, die in den verschiedenen Phasen der Gesetzgebungsentwicklung eingeführt wurden, und einen einzigen Plan zu erstellen. In diesem Sinne stellt der Integrierte Tätigkeits- und Organisationsplan eine Art "Einheitstext" der Planung dar.

Bei der Ausarbeitung wurden neben den Richtlinien für die Erstellung des Integrierten Tätigkeits- und Organisationsplans (PIAO), die vom Ministerium für öffentliche Verwaltung veröffentlicht wurden, und den ANAC-Richtlinien vom 2. Februar 2022 auch die früheren und noch nicht aufgehobenen Rechtsvorschriften über die Planung öffentlicher Einrichtungen berücksichtigt.

Insbesondere wurde der Bezugsrechtsrahmen eingehalten, d. h:

- in Bezug auf die Leistung (Performance) das Gesetzesdekret Nr. 150/2009 und nachfolgende Änderungen und Ergänzungen, das Regionalgesetz Nr. 22/2010 und nachfolgende Änderungen und Ergänzungen, sowie die von der Abteilung für öffentliche Verwaltung herausgegebenen Richtlinien;
- im Hinblick auf Korruptionsrisiken und Transparenz, den Nationalen Korruptionsbekämpfungsplan (PNA) und die Allgemeinen Vorschriften, die von der ANAC gemäß dem Gesetz Nr. 190 von 2012, Gesetzesdekret Nr. 33 von 2013, erlassen wurden;
- zum Thema "Organisation des Smart-Working", die vom Ministerium für den

öffentlichen Dienst herausgegebenen Richtlinien und alle anderen spezifischen Bezugsvorschriften zu anderen Fragen im Zusammenhang mit dem Maßnahmenplan, dem dreijährigen Personalbedarfsplan und der Ausbildung.

- dieses Dokument wurde vom Gemeindesekretär (RPCT) erstellt und vom Gemeindeausschuss in Übereinstimmung mit den oben genannten Vorschriften angenommen.

Vereinfachte Verfahren sind für Einrichtungen mit nicht mehr als fünfzig Beschäftigten vorgesehen.

Diese Verwaltung hat weniger als fünfzig Mitarbeiter.

Die Berechnung der Zahl der Beschäftigten dieser Verwaltung erfolgte gemäß den Angaben im ANCI-Heft Nr. 36 vom Juli 2022 (Berechnungsmethoden zur Erstellung von Tabelle 12 des Jahresberichtes zur Personalstruktur).

Im Rundschreiben 6/EL/2022 hat die Region Trentino Südtirol festgelegt:

“In Bezug auf den Inhalt des PIAO wird betont, dass im Art. 4 des RG Nr. 7/2021 (Regionales Begleitgesetz zum Stabilitätsgesetz 2022 der Region) Nachstehendes vorgesehen wird: „(1) Gemäß Art. 18-bis des Gesetzesdekrets vom 9. Juni 2021, Nr. 80 (Dringende Maßnahmen zur Stärkung der Verwaltungstätigkeit der öffentlichen Verwaltungen zwecks Umsetzung des nationalen Plans für Aufbau und Resilienz (PNRR) und für die Effizienz der Justiz), das mit Änderungen mit dem Gesetz vom 6. August 2021, Nr. 113 in Gesetz umgewandelt worden ist, wenden die Region und die öffentlichen Körperschaften, für deren Ordnung die Region zuständig ist, die Bestimmungen laut Art. 6 desselben Gesetzesdekrets schrittweise an. Für das Jahr 2022 müssen – vorbehaltlich einer Fristaufschiebung – die laut Buchst. a) und d) des Art. 6 Abs. 2 vorgesehenen Abschnitte des Integrierten Tätigkeits- und Organisationsplans entsprechend den zum 30. Oktober 2021 für die Körperschaften selbst vorgesehenen Planungsinstrumenten erstellt und die diesbezüglichen Monitoring-Verfahren festgelegt werden. Die Möglichkeit, den Plan um die weiteren im Art. 6 Abs. 2 vorgesehenen Inhalte zu ergänzen, bleibt davon unberührt.“.

Im Lichte der oben genannten Regionalbestimmungen müssen demnach die Körperschaften, für deren Ordnung die Region zuständig ist, für das Jahr 2022 nachstehende Abschnitte des PIAO erstellen:

- Datenübersicht;
- Abschnitt Public Value, Performance und Korruptionsvorbeugung (Art. 3 des Ministerialdekrets zur Festlegung der Vorlage);
- Abschnitt Monitoring (Art. 5 des Ministerialdekrets zur Festlegung der Vorlage), beschränkt auf die erstellten Teile.”.

Unabhängig von den oben genannten regionalen Bestimmungen beabsichtigt die Gemeinde Mals, ab der ersten Umsetzung (Dreijahreszeitraum 2022-2024) den integralen PIAO für die Bereiche, die Verwaltungen mit weniger als 50 Mitarbeitern betreffen, zu erstellen.

PLAUNUNG-ABSCHNITT	KURZBESCHREIBUNG DER DER PLANUNG UNTERLIEGENDEN BEREICHE/TÄTIGKEITEN	VERWALTUNGEN MIT MEHR ALS 50 BESCHÄFTIGTEN	VERWALTUNGEN MIT WENIGER ALS 50 BESCHÄFTIGTEN
1.DATEN-ÜBER-SICHT DER VERWAL-TUNG	Bezeichnung: Gemeinde Mals Adresse: 39024 Mals, Bahnhofstr. 19 Internetseite: www.gemeinde.mals.bz.it Bürgermeister/in: THURNER Josef Beschäftigte zum 31/12/2021: 41 (27,60 Vollzeit-äquivalente) Einwohner zum 31/12/2021: 5277 Telefon: 0473 831117 E-mail: info@gemeinde.mals.bz.it PEC: mals.malles@legalmail.it Steuernummer: 82006550212 MWSt. Nummer: 00827900218	JA	JA
2. ÖFFENTLICHER WERT, PERFORMANCE UND KORRUPTIONS-VORBEUGUNG			
2.1 Öffentlicher Wert	Dieser Abschnitt muss für Gemeinden mit weniger als 50 Beschäftigten nicht ausgefüllt werden.	JA	NEIN
2.2. Performance	Dieser Abschnitt muss für Gemeinden mit weniger als 50 Beschäftigten nicht ausgefüllt werden.	JA	NEIN
2.3 Korruptionsrisiken und Transparenz	**Folgenabschätzung für den externen Kontext** Ziel der Analyse des externen Kontextes ist es, aufzuzeigen, wie die Merkmale des Umfelds, in dem die Behörde tätig ist, z. B. kulturelle, kriminologische, soziale und wirtschaftliche Variablen in dem Gebiet, das Auftreten korrupter Phänomene in der Behörde begünstigen können. Zu diesem Zweck wurden sowohl die Faktoren, die mit dem Gebiet der Provinz Bozen zusammenhängen, als auch die Beziehungen und möglichen Einflüsse, die mit externen Akteuren und Interessensvertretern bestehen, berücksichtigt. Das Verständnis der territorialen Bezugsdynamik und der wichtigsten Einflüsse und Belastungen, denen eine kommunale Struktur ausgesetzt ist, ermöglicht eine effizientere und präzisere Ausrichtung der Risikomanagementstrategie. Auf der Suche nach präzisen Kontextindikatoren sind die 2016 vom ASTAT, dem Landesinstitut für Statistik, anlässlich des Weltkorruptionsbekämpfungstages veröffentlichten Daten nützlich, die sich auf die Meinung der Südtirolerinnen und Südtiroler zur Korruption und zu Verhaltensweisen beziehen, die den Bürgersinn betreffen und mehr oder weniger direkt als Indikatoren für die Legalität eines Gebiets dienen. 44,4 % der Südtirolerinnen und Südtiroler lehnen	JA	JA

PLAUNUNG-ABSCHNITT	KURZBESCHREIBUNG DER DER PLANUNG UNTERLIEGENDEN BEREICHE/TÄTIGKEITEN	VERWALTUNGEN MIT MEHR ALS 50 BESCHÄFTIGTEN	VERWALTUNGEN MIT WENIGER ALS 50 BESCHÄFTIGTEN
	die Aussage, dass Korruption etwas Natürliches ist und das gesellschaftliche und wirtschaftliche Leben prägt, klar ab. Fast ein Viertel (24,3 %) der Südtirolerinnen und Südtiroler ist mit dieser Aussage überhaupt nicht einverstanden, während fast ein Drittel (31,3 %) der Bevölkerung ziemlich oder sehr zustimmt, dass es nicht möglich ist, korrupte Praktiken zu verhindern und zu bekämpfen. Sechzig Prozent der Südtirolerinnen und Südtiroler halten es für sehr oder ziemlich gefährlich, Korruptionsfälle zu melden. Wie "resistent" eine Gesellschaft gegen Korruption ist, lässt sich auch an der Meldebereitschaft messen. Insbesondere das Risiko, das mit der Entscheidung, Anzeige zu erstatten, verbunden ist, ist ein Indikator für die "gefühlte Freiheit", in der die Bürger ihre Rechte geltend machen können. In Südtirol sind 15,0 % der Bürger der Meinung, dass die Meldung von Bestechungsfällen gefährlich ist, und weitere 44,3 % glauben, dass die Meldung von Bestechungsfällen immer noch eine gewisse Gefahr darstellt. Umgekehrt halten 17,0 % der Einwohner der Provinz Bozen die Meldung von Bestechung für überhaupt nicht gefährlich. Bei der Analyse des externen Kontextes wird diese Verwaltung auch die Auswirkungen der Covid 19-Pandemie auf das wirtschaftliche und soziale Gefüge berücksichtigen. Einerseits hat Covid 19 die Bevölkerung verarmen lassen, andererseits hat es die Aktivitäten der in den Gebieten tätigen Unternehmen blockiert oder eingeschränkt, so dass die Gefahr besteht, dass kriminelle Organisationen in das soziale und wirtschaftliche Gefüge eindringen. Dies gilt insbesondere für die Kreditklemme. **Folgenabschätzung für den internen Kontext** Bei der Ausarbeitung dieses Plans wurden nicht nur die oben angeführten Erkenntnisse über die örtlichen Gegebenheiten berücksichtigt, sondern auch die Ergebnisse der Überwachung, die innerhalb der Verwaltung ständig über mögliche Phänomene der Abweichung beim öffentlichen Handeln von den Unkorrektheit und Unparteilichkeit durchgeführt wird. Im Rahmen der bisherigen Überwachung sind keine Unregelmäßigkeiten im Zusammenhang mit dem Phänomen der Korruption aufgetreten, weder auf der Ebene der Angestellten/Mitarbeiter		

PLAUNUNG-ABSCHNITT	KURZBESCHREIBUNG DER DER PLANUNG UNTERLIEGENDEN BEREICHE/TÄTIGKEITEN	VERWALTUN-GEN MIT MEHR ALS 50 BESCHÄFTIG-TEN	VERWALTUN-GEN MIT WE-NIGER ALS 50 BESCHÄFTIG-TEN
	noch auf der Ebene der politischen Verwaltungs-organe. **Es wird auch darauf hingewiesen:** - System der Zuständigkeiten: Rollen, Zuständigkeiten und Delegationen werden im Voraus und im Detail definiert und formalisiert, ebenso wie die Entscheidungsprozesse. - Politik, Ziele und Strategien: Diese werden gemeinsam vom Gemeinderat und dem Gemeindesekretär festgelegt. - Ressourcen, Wissen, Systeme und Technologien: Die Verwaltung verfügt über einen effizienten Hauptsitz, eine moderne Infrastruktur und ein IT-Netz sowie eine kontinuierliche Schulung des Personals. - Organisationskultur: Von der Einstellung an werden alle Mitarbeiter nach ihrer Fähigkeit beurteilt und bewertet, wie sie die Erreichung der Ziele der Organisation ethisch interpretieren. - Informationsfluss: Interne Transparenz wird als ein Eckpfeiler der Fähigkeit der Organisation angesehen, sich als eine Organisation zu positionieren, die in der Lage ist, zu lernen und den Wert der ihr anvertrauten Ressourcen zu entwickeln. - Beschwerden, Berichte oder andere laufende Untersuchungen: Es sind keine früheren oder laufenden Disziplinarverfahren aktenkundig. Es kann daher davon ausgegangen werden, dass das interne Umfeld gesund ist und keinen Anlass zu besonderen Bedenken gibt. Aufnahme von Prozessen, Identifizierung und Bewertung potenzieller und tatsächlicher Korruptionsrisiken, Entwurf organisatorischer Maßnahmen zur Bewältigung des Risikos. Siehe Anlage 1 Risikokatalog		
3. ORGANISATION UND HUMANRESSOURCEN			
3.1 ORGANI-SATIONS-STRUKTUR	Das Organisationsmodell der Körperschaft enthält: • Organigramm; • Ebenen der organisatorischen Verantwortung, Anzahl der Führungskräfte und Anzahl der organisatorischen Positionen, basierend auf vier Dimensionen:	JA	JA

PLAUNUNG-ABSCHNITT	KURZBESCHREIBUNG DER DER PLANUNG UNTERLIEGENDEN BEREICHE/TÄTIGKEITEN	VERWALTUN-GEN MIT MEHR ALS 50 BESCHÄFTIG-TEN	VERWALTUN-GEN MIT WE-NIGER ALS 50 BESCHÄFTIG-TEN
	○ vertragliche Einstufung (oder Kategorien); ○ Berufsprofil (wenn möglich, nicht auf CCNL-Erklärungen festgelegt); ○ technische Kompetenzen (Wissen, wie es geht) ○ transversale Kompetenzen (Wissen, wie man ist - Soft Skills); ○ die durchschnittliche Anzahl der Beschäftigten pro Organisationseinheit; Siehe beiliegendes Organigramm, Ämterordnung und Stellenplan, Auszug aus dem ESD und Jahresbericht Personalstruktur.		
3.2. ORGANISATION DES AGILEN ARBEITENS	In Erwartung der Regelung der agilen Arbeit durch die nationalen Tarifverträge, die die Einrichtung der agilen Arbeit für die Aspekte regeln werden, die nicht einseitigen Quellen vorbehalten sind, wie in der Einführung der "Leitlinien zur agilen Arbeit in den öffentlichen Verwaltungen" angegeben, die vom Ministerium für öffentliche Verwaltung am 30. November 2021 angenommen wurden und für die auf der Einheitskonferenz gemäß Artikel 9, Absatz 2, des Gesetzesdekrets Nr. 281 vom 28. August 1997 am 16. Dezember 2021 eine Einigung erzielt wurde, bleibt die Einrichtung der agilen Arbeit in der Gemeinde Mals durch die Bestimmungen der geltenden Gesetzgebung geregelt. Am 03.12.2020 wurde der zweite Vertragsentwurf für die Erneuerung des bereichsübergreifenden Tarifvertrags für den Dreijahreszeitraum 2019 - 2021 von den Vertragsparteien unterzeichnet. In den Artikeln 7 und 8 des oben genannten Vereinbarungsentwurfs wird die Rahmendisziplin für die gewöhnliche agile Arbeit für den Zeitraum nach dem Covid-19 festgelegt. Durch die Covid-19-Epidemie wurde das Inkrafttreten der Bestimmungen des oben genannten neuen Abkommens verschoben. Für die Dauer der Pandemie hat die Gemeinde Mals in den Bereichen, in denen dies möglich war - die weitestgehende Nutzung von Smart-Working gefördert und umgesetzt. Ab dem 01.04.2022 ist agiles Arbeiten - wie im oben genannten bereichsübergreifenden Abkommen sowie in der nationalen Gesetzgebung vorgesehen - nur noch durch den Abschluss einer individuellen Ad-hoc-Vereinbarung möglich. In den Artikeln 7 und 8 des bereichsübergreifenden Tarifvertrags heißt es ausdrücklich, dass - agiles Arbeiten eine freiwillige Form der		

PLAUNUNG-ABSCHNITT	KURZBESCHREIBUNG DER DER PLANUNG UNTERLIEGENDEN BEREICHE/TÄTIGKEITEN	VERWALTUN-GEN MIT MEHR ALS 50 BESCHÄFTIG-TEN	VERWALTUN-GEN MIT WE-NIGER ALS 50 BESCHÄFTIG-TEN
	Durchführung des Arbeitsverhältnisses ist oder es unterliegt dem Willen der Parteien; - agile Arbeit kann von fester oder unbestimmter Dauer sein; - agile Arbeit basiert auf dem Erreichen von vereinbarten Zielen und/oder Leistungen; - die Arbeitstätigkeiten werden in der Regel in dem täglichen Zeitfenster zwischen 7 und 20 Uhr nach einem frei gestaltbaren Zeitplan durchgeführt; - je nach den Erfordernissen des Dienstes, können zeitliche Beschränkungen oder genaue Bereitschaftszeiten vereinbart werden; - das Recht auf Unterbrechung der Verbindung während der Ruhezeiten ist gewährleistet; - agiles Arbeiten sieht keine Überstunden vor und gibt keinen Anspruch auf Essensgutscheine; - der Arbeitgeber garantiert korrekte und vollständige Informationen über die Sicherheit am Arbeitsplatz. In der individuellen Vereinbarung, die von dem einzelnen Arbeitnehmer und dem Leiter der betreffenden Abteilung oder Struktur gemäß der von der Verwaltung erstellten Vorlage unterzeichnet werden muss, werden z. B. die Dauer der Vereinbarung, die allgemeine Beschreibung der auszuführenden Tätigkeiten und der zu erreichenden Ziele, die Anzahl der Tage/Halbe Tage, die im agilen Modus ausgeführt werden sollen, oder die Anzahl der Tage, die in einem bestimmten Zeitraum flexibel genutzt werden können, die Zeitfenster für die Arbeit und die Überwachungszeiten sowie die zu verwendenden technologischen Instrumente festgelegt. Der Zugang zu agiler Arbeit ist in folgenden Fällen vorgesehen: - Persönliche Gebrechlichkeit oder familiäre Härtefälle; - Entfernung in Kilometern vom Arbeitsplatz; - Angemessenheit der häuslichen Umgebung; - Mögliches Wiederauftreten von Pandemien; Es wird beigefügt: - Bereichsübergreifender Kollektivvertrag; - Anweisungen für die Arbeit mit privaten oder Firmengeräten;		

PLAUNUNG-ABSCHNITT	KURZBESCHREIBUNG DER DER PLANUNG UNTERLIEGENDEN BEREICHE/TÄTIGKEITEN	VERWALTUNGEN MIT MEHR ALS 50 BESCHÄFTIGTEN	VERWALTUNGEN MIT WENIGER ALS 50 BESCHÄFTIGTEN
	- Leitlinien für die Nutzung von Cloud-Lösungen für Unternehmen.		
3.3 DREIJÄHRIGER PLAN DES PERSONALBEDARFES	Der Personalstand zum 31. Dezember des Vorjahres wird anhand des Abschnittes Personal aus dem Einheitlichen Strategiedokument 2022 – 2024, genehmigt mit Beschluss des Gemeinderates Nr. 33 vom 16.12.2021, nachgewiesen. Beigefügt wird der Abschnitt Personal aus dem Einheitlichen Strategiedokument 2022 – 2024. Der Dreijahresplan des Personalbedarfs weist folgende Elemente auf: • Darstellung des Personalbestands zum 31. Dezember des Vorjahres; • Strategische Personalplanung, die auf der Grundlage folgender Faktoren bewertet wird: ○ Einstellungskapazitäten, die auf der Grundlage der derzeitigen Ausgabenbeschränkungen berechnet werden; ○ geschätzte Entwicklung der Abgänge auf der Grundlage der Pensionierungen; ○ Abschätzung der Bedarfsentwicklung in Abhängigkeit von Entscheidungen im Zusammenhang mit der Digitalisierung von Prozessen, dem Outsourcing oder der Internalisierung oder dem Ausbau, der Veräußerung von Dienstleistungen, Tätigkeiten, Funktionen oder anderen internen oder externen Faktoren, die eine Diskontinuität des Personalprofils in Bezug auf die Qualifikations- und/oder Mengenprofile erfordern. Es wird der Jahresbericht zur Personalstruktur beigelegt. Die Gemeinde Mals misst der Ausbildung ihrer Mitarbeiter eine grundlegende strategische Bedeutung bei. Im Dreijahreszeitraum 2022-2024 sind Schulungen in den folgenden Bereichen geplant: • Datenschutz; • Antikorruption und transparente Verwaltung; • Sicherheit am Arbeitsplatz; • Vergaberecht; • Lizenzwesen • Steuerwesen • Finanzwesen	JA	JA

PLAUNUNG-ABSCHNITT	KURZBESCHREIBUNG DER DER PLANUNG UNTERLIEGENDEN BEREICHE/TÄTIGKEITEN	VERWALTUN-GEN MIT MEHR ALS 50 BESCHÄFTIG-TEN	VERWALTUN-GEN MIT WE-NIGER ALS 50 BESCHÄFTIG-TEN
	• Meldeamt und Standesamt • Bibliothekswesen • Öffentliche Sicherheit • Bauwesen • Lebensmittel(unverträglichkeiten)		
4. ÜBER-PRÜFUN-GEN	Dieser Abschnitt muss für Gemeinden mit weni-ger als 50 Beschäftigten nicht ausgefüllt werden.	JA	NEIN

Anlagen

1. Risikokatalog Korruptionsprävention
2. Organigramm, Ämterordnung, Stellenplan
3. Auszug ESD Personalstand
4. Jahresbericht Personalstruktur

Area	Ambito	Processi con indice di rischio elevato	Pesatura rischio: probabilità x impatto	Rischi	Azioni o misure preventive previste	output/indicatori	tempistica	responsabile dell'azione o misura preventiva	note/eventuali oneri finanziari
Area Gestione del territorio	Edilizia Privata	Gestione degli atti abilitativi (concessioni edilizie, permessi di costruire, autorizzazioni paesaggistiche, agibilità edilizia, ecc.)	4	**Disomogeneità delle valutazioni**	Rischio "Disomogeneità delle valutazioni" 1. Esplicitazione della documentazione necessaria per l'attivazione delle pratiche e delle richieste di integrazione 2. Codificazione dei criteri di controlli sulle dichiarazioni 3. Compilazione di check list puntuale per istruttoria	**monitoraggio annuale del rispetto delle misure**	Già in atto	Responsabile Ufficio Edilizia Privata	
				Non rispetto delle scadenze temporali	Rischio "Non rispetto delle scadenze temporali" 1. Pubblicizzazione del calendario sedute commissione e tempi minimi per la presentazione o integrazione delle pratiche 2. Procedura formalizzata e informatizzata che garantisca la tracciabilità delle istanze e tiene conto dell'ordine cronologico di arrivo salve motivate eccezioni 3. Rispetto dei tempi di evasione istanze, per tipologia di procedimento				Si rileva che il sistema territoriale provinciale e il presidio del territorio anche grazie ai contributi economici erogati dalla Provincia sia particolarmente efficiente sia nella vigilanza su eventuali abusi che in genere nel rispetto della normativa e dei tempi
Area Gestione del territorio	Edilizia Privata	Controllo della segnalazione di inizio di attività edilizie	4	**Assenza di criteri di campionamento**	Rischio "Assenza di criteri di campionamento" 1. Formalizzazione dei criteri statistici per la creazione del campione di pratiche da controllare, con priorità per alcune tipologie di pratiche	**Report annuale**	Già in atto	Responsabile Ufficio Edilizia Privata	Sorteggio di almeno 6% dei procedimenti
				Disomogeneità delle valutazioni	Rischio "Disomogeneità delle valutazioni" 1. Creazione di supporti operativi per la effettuazione dei controlli	**Check list**	Già in atto		
				Non rispetto delle scadenze temporali	Rischio "Non rispetto delle scadenze temporali" 1. Procedura formalizzata e informatizzata che garantisca la tracciabilità dell'operato 2. Realizzazione dei controlli secondo procedura	**monitoraggio annuale del rispetto delle misure**	Già in atto		In fase di approvazione una nuova legge urbanistica provinciale, dopodichè si rielaborerà il regolamento edilizio
Area Gestione del territorio	Edilizia Privata	Gestione degli abusi edilizi (pratiche sanatoria, segnalazioni di parte, ecc.)	6	**Discrezionalità nell'intervenire**	Rischio "Discrezionalità nell'intervenire" 1. Procedura formalizzata a livello di Ente per la gestione delle segnalazioni esterne o di uffici interni ed effettuazione dei relativi controlli per i provvedimenti conseguenti 2. Formalizzazione di criteri per la verifica di ufficio	**monitoraggio annuale del rispetto delle misure**	Già in atto	Responsabile Ufficio Edilizia Privata	
				Disomogeneità dei comportamenti	Rischio "Disomogeneità dei comportamenti" 1. Formalizzazione degli elementi minimi da rilevare nell'eventuale sopralluogo per la definizione del verbale 2. Istruttoria sistematica sullo storico delle pratiche edilizie presentate relative all'edificio verificato				Presenza garantita di agente della Polizia Municipale (in caso di necessità)
				Non rispetto delle scadenze temporali	Rischio "Non rispetto delle scadenze temporali " 1. Rispetto dei tempi di realizzazione dei controlli 2. Differenziazione delle modalità di intervento a seconda della gravità potenziale dell'abuso (urgenza)	**monitoraggio annuale del rispetto delle misure**			
Area Gestione del territorio	Edilizia Privata	Idoneità alloggiativa	2	**Disomogeneità delle valutazioni**	Rischio "Disomogeneità delle valutazioni" 1. Procedura formalizzata a livello di Ente 2. Formalizzazione degli elementi minimi da rilevare nell'istruttoria e nell'eventuale sopralluogo		Già in atto	Responsabile Ufficio Edilizia Privata	Collegamento con Polizia Municipale
Area Gestione del territorio	Pianificazione territoriale	Rilascio dei pareri urbanistici preventivi	4	**Disomogeneità delle valutazioni**	Rischio "Disomogeneità delle valutazioni" 1. Esplicitazione della documentazione necessaria per l'attivazione delle richieste di parere 2. Procedura formalizzata di gestione dell'iter con individuazione delle casistiche sottoponibili a parere 3. evasione istanze secondo procedura 4. Individuazione di FAQ e risposte già predefinite alle questioni più significative	**monitoraggio annuale del rispetto delle misure**	Già in atto	Responsabile Ufficio Edilizia Privata	Uff. Provinciale ambito e natura
Area Gestione del territorio	Ambiente	Controlli amministrativi o sopralluoghi	6	**Discrezionalità nell'intervenire**	Rischio "Discrezionalità nell'intervenire" 1. Procedura formalizzata a livello di Ente per la gestione delle segnalazioni esterne o di uffici interni ed effettuazione dei relativi controlli per i provvedimenti conseguenti 2. Formalizzazione di criteri per la verifica di ufficio	**monitoraggio annuale del rispetto delle misure**	Già in atto		Già certificato EMAS
				Disomogeneità dei comportamenti	Rischio "Disomogeneità dei comportamenti" 1. Formalizzazione degli elementi minimi da rilevare nell'eventuale sopralluogo per la definizione del verbale 2. Istruttoria puntuale dello storico delle pratiche edilizie presentate relative all'edificio verificato				
				Non rispetto delle scadenze temporali	Rischio "Non rispetto delle scadenze temporali " 1. Differenziazione delle modalità di intervento a seconda della gravità potenziale dell'abuso (urgenza)				
Area Gestione Licenze	Commercio/attività produttive	Controllo delle DIA/SCIA	4	**Controlli addomesticati per assenza di criteri di campionamento**	Rischio "Assenza di criteri di campionamento" 1. Formalizzazione dei criteri statistici per la creazione del campione di pratiche da controllare, con priorità per alcune tipologie di pratiche	**monitoraggio annuale del rispetto delle misure**	già in atto	Il responsabile del procedimento	controllo come da L.P. n. 17/1993 (min 6%)
				Disomogeneità delle valutazioni	Rischio "Disomogeneità delle valutazioni" 1. Creazione di supporti operativi per la effettuazione dei controlli				
				Non rispetto delle scadenze temporali	Rischio "Non rispetto delle scadenze temporali" 1. Procedura formalizzata e informatizzata che garantisca la tracciabilità dell'operato 2. Supervisione sul rispetto dei tempi di realizzazione dei controlli				SUAP

Area Gestione Lavori pubblici	Lavori Pubblici/manutenzione /mobilità	Gare d'appalto per lavori ed incarichi progettazione e D.L.	4	**Scarsa trasparenza dell'operato/alterazione della concorrenza**	Rischio "Scarsa trasparenza/alterazione della concorrenza" 1. Utilizzo di bandi tipo per requisiti e modalità di partecipazione 2. Monitoraggio per tipologia delle modalità utilizzate per l'effettuazione delle gare 3. Stesura di un atto di indirizzo che regolamenti la rotazione dei concorrenti	**1. e 2. Monitoraggio 3. Creazione di un vademecum per la rotazione**	già in atto	RUP	
				Disomogeneità di valutazione nella individuazione del contraente	Rischio "Disomogeneità delle valutazioni nella individuazione del contraente" 1. Definizione dei tempi di nomina e di criteri per la composizione delle commissioni e verifica che chi vi partecipa non abbia interessi o legami parentali con le imprese concorrenti	**monitoraggio annuale**	Già in atto		
				Scarso controllo del possesso dei requisiti dichiarati	Rischio "Scarso controllo del possesso dei requisiti dichiarati" 1. Definizione preventiva dei criteri di selezione dei partecipanti per i controlli sui requisiti				Controllo puntuale
Area Gestione Lavori pubblici	Lavori Pubblici	Controllo esecuzione contratto (DL e coord sicurezza)	4	**Assenza di controlli**	Rischio "Assenza di un piano dei controlli" 1. Formalizzazione di un programma di controlli/direzioni lavori da effettuare in relazione alle fasi di esecuzione dell'opera, con evidenza di un report per ogni controllo da parte del DL e coord sicurezza 2. Inserimento nei capitolati tecnici della Direzione Lavori o nelle richieste di offerte della qualità e quantità della prestazione attesa 3. Visita mensile da parte dell'UT + DL al cantiere per verificare di persona le situazioni rilevate con stesura di report	**monitoraggio annuale - presenza del RUP sui cantieri**	Già in atto	RUP	
				Disomogeneità delle valutazioni	Rischio "Disomogeneità delle valutazioni" 1. Procedura formalizzata per la gestione dell'attività (varianti, richieste subappalti, ecc.) 2. Periodico reporting dei controlli realizzati e di tutte le varianti richieste, per ogni opera	**Verbale delle riunioni di coordinamento interni**	Già in atto		
	Manutenzione immobili, strade e giardini	Controllo dei servizi appaltati (manutenzione caldaie, manutenzione ascensori, illuminazione, verde, ecc.)	4	**Assenza di criteri di campionamento**	Rischio "Assenza di criteri di campionamento" 1. Inserimento nei capitolati tecnici o nelle richieste di offerte della qualità e quantità della prestazione attesa 2. Inserire delle modalità di segnalazioni di eventuali disservizi	**Check list**	Già in atto	RUP	controllo puntuale

Area Gestione Lavori pubblici	Tutti i Servizi che effettuano acquisti	Acquisto di beni e servizi e controllo forniture	4	**Scarsa trasparenza dell'operato/alterazione della concorrenza**	Rischio "Scarsa trasparenza/alterazione della concorrenza" 1. Formalizzazione dei criteri di rotazione fornitori 2. Istituzione di un "albo di fornitori" interno	**Monitoraggio annuale dell'attuazione**	Già in atto	Il responsabile del procedimento	Ricorso alla piattaforma elettronica del sistema Provinciale
				Disomogeneità di valutazione nella individuazione del contraente	Rischio "Disomogeneità delle valutazioni nella individuazione del contraente" 1. Definizione di criteri per la composizione delle commissioni e verifica che chi vi partecipa non abbia interessi o legami parentali con le imprese concorrenti 2. Creazione di griglie per la valutazione delle offerte	**Monitoraggio annuale**	Già in atto		
				Scarso controllo del possesso dei requisiti dichiarati	Rischio "Scarso controllo del possesso dei requisiti dichiarati" 1. Creazione di supporti operativi per la effettuazione dei controlli dei requisiti dei partecipanti				Attraverso l'albo dei fornitori interno ha la funzione di garantire anche il controllo dei requisiti dichiarati
				Scarso controllo del servizio erogato	Rischio "Scarso controllo del servizio erogato" 1. Stesura di capitolati di gara che prevedono la qualità e la quantità delle prestazioni attese 2. Creazione di supporti operativi per la effettuazione dei controlli del servizio erogato				
Area Segreteria	Segreteria Generale	Gestione di segnalazioni e reclami	2	**Discrezionalità nella gestione**	Rischio "Discrezionalità nella gestione" 1. Procedura formalizzata a livello di Ente per la gestione delle segnalazioni esterne scritte e dei reclami	**Monitoraggio annuale**	Già in atto	Segretario Generale	Nell'anno 2017 non sono entrate alcuni reclami o segnalazioni
Area Servizi demografici	Servizi demografici	Gestione archivio servizi demografici	2	**Fuga di notizie di informazioni riservate**	**Rischio "Fuga di notizie di informazioni riservate"** 1. Formalizzazione di una linea guida che identifica le modalità di richiesta di accesso a dati anagrafici	**Monitoraggio annuale**	Già in atto	Responsabile dei Servizi demografici	Tracciabilità e sicurezza accessi verificate Piano della sicurezza dei dati informatici
	Servizi demografici	Gestione degli accertamenti relativi alla residenza	2	**Assenza di criteri di campionamento**	Rischio "Assenza di criteri di campionamento" 1. Formalizzazione dei controlli di tutte le situazioni	**Monitoraggio annuale**	Già in atto	Responsabile dei Servizi demografici	concordare tempi di intervento della polizia municipale - D.L. n. 35 del 4.4.2012
				Mancato presidio delle ricadute fiscali	Rischio "Mancato presidio delle ricadute fiscali" 1. Formalizzazione delle modalità di comunicazione delle migrazioni a Tributi e Ufficio Tecnico				
				Non rispetto delle scadenze temporali	Rischio "Non rispetto delle scadenze temporali" 1. Essere notiziati rispetto ai tempi di evasione				
	Servizi cimiteriali	Rilascio di autorizzazioni e concessioni cimiteriali	2	**Disomogeneità delle valutazioni**	Rischio "Disomogeneità delle valutazioni" 1. Formalizzazione del regolamento cimiteriale	**Monitoraggio annuale**	Già in atto	Responsabile dei Servizi demografici	
Area Servizi finanziari	Servizi finanziari	Pagamento fatture fornitori	2	**Disomogeneità delle valutazioni**	Rischio "Disomogeneità delle valutazioni" 1. Esplicitazione della documentazione necessaria per effettuare la liquidazione 2. Definizione del campione dei controlli della regolarità contributiva per importi inferiori ad€ 20.000,00 (o effettuazione puntuale dei controlli)	**Monitoraggio annuale dell'attuazione**	Già in atto	Responsabile dell'Unità Organizzativa	avviene tramite sistema digitale
				Non rispetto delle scadenze temporali	Rischio "Non rispetto delle scadenze temporali" 1. Monitoraggio dell'ordine cronologico dei tempi di liquidazione, per tipologia di fattura	**Monitoraggio semestrale**			
Area	Patrimonio	Acquisti e alienazioni patrimoniali (immobili) e di diritti reali	4	**Disomogeneità delle valutazioni**	Rischio "Disomogeneità delle valutazioni" 1. Formalizzazione della procedura di alienazione	**Bandi tipo**	Già in atto	Responsabile dell'Unità Organizzativa	
				Scarsa trasparenza/poca pubblicità dell'opportunità	Rischio "Scarsa trasparenza/poca pubblicità dell'opportunità" (solo per alienazioni) 1. Formalizzazione delle attività di pubblicizzazione da effettuare				

Area Segreteria	Patrimonio	Alienazione di beni mobili e di diritti	2	**Dismogeneità delle valutazioni**	Rischio "Disomogeneità delle valutazioni" 1. Formalizzazione della procedura di alienazione (trasparenza)	**Procedura**	Già in atto	Responsabile dell'Unità Organizzativa	
				Scarsa trasparenza/poca pubblicità dell'opportunità	Rischio "Scarsa trasparenza/poca pubblicità dell'opportunità" (solo per alienazioni) 1. Formalizzazione delle attività di pubblicizzazione da effettuare				
Area Segreteria	Trasversale	Assegnazione/concessione beni comunali	4	**Scarsa trasparenza/ poca pubblicità dell'opportunità**	Rischio "Scarsa trasparenza/poca pubblicità dell'opportunità" 1. Formalizzazione delle attività di pubblicizzazione da effettuare 2. Definizione criteri per assegnazione dei beni e modalità di accessc	**Monitoraggio annuale**	Già in atto	Il responsabile del procedimento	
				Disomogeneità delle valutazioni nella verifica delle richieste	Rischio "Disomogeneità delle valutazioni nella verifica delle richieste" 1. Creazione dell'elenco delle associazioni o altri soggetti potenzialmente beneficiari 2. Stesura del regolamento di assegnazione sale e spazi pubblici 3. Esplicitazione della documentazione necessaria per l'ottenimento del beneficic				
Area Servizi finanziari	Tributi e entrate patrimoniali	Controlli/accertamenti sui tributi/entrate pagati	2	**Assenza di criteri di campionamento**	Rischio "Assenza di criteri di campionamento" 1. Controllo puntuale delle situazioni come da regolamento o definizione di criteri predeterminati per il controllo a campione	**Report annuale**	già in atto	Responsabile dei Servizi finanziari	
				Non rispetto delle scadenze temporali	Rischio "Non rispetto delle scadenze temporali" 1. Monitoraggio dei tempi di evasione dei controlli				
Area Personale	Personale	Selezione/reclutamento del personale	2	**Disomogeneità delle valutazioni durante la selezione**	Rischio "Disomogeneità delle valutazioni durante la selezione" 1. Definizione di criteri stringenti per le diverse tipologie di chiamate a termine 2. Creazione di griglie per la valutazione dei candidati 3. Definizione di criteri per la composizione delle commissioni e verifica che chi vi partecipa non abbia legami parentali con i concorrenti 4. Ricorso a criteri statistici casuali nella scelta dei temi o delle domande	**Monitoraggio annuale**	già in atto	Responsabile dei Servizi finanziari	
				Comportamenti opportunistici nell'utilizzo delle graduatorie	Rischio "Disomogeneità delle valutazioni durante la selezione" 1. Definizione di criteri stringenti per le diverse tipologie di chiamate a termine 2. Creazione di griglie per la valutazione dei candidati 3. Definizione di criteri per la composizione delle commissioni e verifica che chi vi partecipa non abbia legami parentali con i concorrenti 4. Ricorso a criteri statistici casuali nella scelta dei temi o delle domande	**Monitoraggio annuale**	già in atto	Responsabile dei Servizi finanziari	
				illecito trattamento di dati personali	Rischio illecito trattamento di dati personali Revisione modulistica Valutazione sicurezza banca dati del personale	**Registro dei trattamenti** **Audit DPO**	già in atto	DPO	
				Disomogeneità nel controllo del possesso dei requisiti dichiarati	Rischio "Disomogeneità nel controllo del possesso dei requisiti dichiarati" 1. Creazione di supporti operativi per la effettuazione dei controlli dei requisiti		già in atto		
Area Personale	Personale	Vigilanza di contrasto agli illeciti	4	**sviluppo di clima omertoso e non etico**	**Rischio "sviluppo di clima omertoso e non etico" 1. attivazione procedura di tutela del segnalante interno 2. formazione etica al personale**	**1) n° segnalazioni/numero istruttorie 2. personale formato>80% per almeno 2 h**	1.già in atto 2. entro 30 /11/ 2022	responsabile del personale	
		contrasto comportamenti opportunistici (L.104, malattie, mancato lavoro in smart working)	4	**danno erariale e di immagine**	**1.Controllo periodico uso permessi L.104 2. Visite fiscali per malattie a ridosso di giorni non lavorativi 3. Controllo puntuale del rispetto degli obiettivi assegnati nel lavoro a distanza**	**1. monitoraggio 2. almeno 60% 3. monitoraggio**	già in atto	responsabile del personale	
		contrasto attività extraistituzionali non autorizzate	2	**danno di immagine** **conflitto di interessi latente**	**1. Verifica posizioni individuali in rete (controllo P.Iva) 2. Circolare di richiamo**	**1. Controllo a campione (6%) 2. nuova circolare**	entro il 30/11/2022	1. responsabili di servizio 2. responsabile del personale	
		salute e sicurezza sul lavoro	2	**danno alla salute pubblica** **danno erariale**	**1. adozione protocollo covid 19 2. sviluppo dello smartworking durante emergenza sanitaria**	**1. protocollo 2. 30% dei dipendenti smartw.**	1. in atto 2.entro il 30/11/2022	1. RSPP 2. Responsabile del personale	
		alterazione attestazioni di presenza	4	**danno erariale e di immagine**	**1. Controlli a campione presenze in servizio 2. Sanzioni per reiterate mancate timbrature**	**1. verbali 2.n.sanzioni irrogate**	30.11.2022	1. ufficio ispettivo 2. Responsabile UPD	

Area Personale	Personale	Mobilità tra enti	2	**Scarsa trasparenza/poca pubblicità della opportunità**	Rischio "Scarsa trasparenza/poca pubblicità dell'opportunità" 1. Pubblicazione dei bandi di selezione	**Pubblicazione sul "mercato del lavoro" della Provincia e sulla pagina internet**	già in atto	Responsabile dei Servizi finanziari	
				Disomogeneità delle valutazioni durante la selezione	Rischio "Disomogeneità delle valutazioni durante la selezione" 1. Creazione di griglie per la valutazione dei candidati	**Schema di verbale commissione**			
				Comportamenti opportunistici nell'utilizzo delle graduatorie di altri enti"	Rischio "Comportamenti opportunistici nell'utilizzo delle graduatorie di altri enti" 1. Formalizzazione preventiva di criteri (es. vicinanza territoriale), per l'utilizzo	**linee di indirizzo**			
	Personale	Progressioni di carriera	2	**Disomogeneità delle valutazioni durante la selezione**	Rischio "Disomogeneità delle valutazioni durante la selezione" 1. Creazione di griglie per la valutazione dei candidati 2. Definizione di criteri per la composizione delle commissioni e verifica che chi vi partecipa non abbia legami parentali con i concorrenti	**Schema di verbale commissione**	già in atto	Responsabile dei Servizi finanziari	
				Disomogeneità nel controllo del possesso dei requisiti dichiarati	Rischio "Disomogeneità nel controllo del possesso dei requisiti dichiarati" 1. Creazione di supporti operativi per la effettuazione dei controlli dei requisiti	**Check list**			
Area Segreteria	Sociale/Cultura/Sport/ Tempo libero	Erogazione di contributi e benefici economici a associazioni	6	**Scarsa trasparenza/ poca pubblicità dell'opportunità**	Rischio "Scarsa trasparenza/poca pubblicità dell'opportunità" 1. Pubblicizzazione delle modalità di accesso al contributo e della tempistica	**Monitoraggio**	Già in atto	Responsabile dei Servizi finanziari	
				illecito trattamento di dati personali	Rischio illecito trattamento di dati personali Revisione modulistica Valutazione correttezza pubblicazioni sul sito Amministrazione trasparente	**Registro dei trattamenti** **Audit DPO**	già in atto in sede audit annuale	DPO	
				Disomogeneità delle valutazioni nella verifica delle richieste	Rischio "Disomogeneità delle valutazioni nella verifica delle richieste" 1. Rispetto regolamento per l'erogazione dei contributi con esplicitazione dei criteri 2. Trasparenza dei requisiti e della documentazione necessaria per l'ottenimento del beneficio	**monitoraggio**	Già in atto	Assessore competente Responsabile del Servizio/ufficio	procedura secondo regolamento comunale
				Scarso controllo del possesso dei requisiti dichiarati e della rendicontazione Controllo a campione sulla rendicontazione delle spese	Rischio "Scarso controllo del possesso dei requisiti dichiarati" 1. Controllo puntuale dei requisiti e della documentazione consegnata e della rendicontazione, oppure controllo del campione previsto dalla norma (6%) (L.P. n. 17/1993)	**Verbale controlli**	Già in atto	Assessore competente Responsabile del Servizio/ufficio	
Area Segreteria	Sociale/Cultura/Sport/ Tempo libero	Utilizzo di sale, impianti e strutture di proprietà comunale	2	**Scarsa trasparenza/ poca pubblicità dell'opportunità**	Rischio "Scarsa trasparenza/poca pubblicità dell'opportunità" 1. Pubblicizzazione delle strutture disponibili e delle modalità di accesso	**Monitoraggio**	Già in atto	Il responsabile del procedimento	
				Disomogeneità delle valutazioni nella verifica delle richieste	Rischio "Disomogeneità delle valutazioni nella verifica delle richieste" 1. Stesura regolamento per la gestione delle sale e strutture 2. Esplicitazione della documentazione necessaria per la concessione	**Monitoraggio**			
Area Segreteria	Segreteria Generale	Gestione accesso agli atti	2	**illecito trattamento di dati personali**	Rischio illecito trattamento di dati personali Istruttoria preventiva con DPO per richieste di accesso inerenti dati "particolari" Formazione agli addetti interessati in tema Privacy	**n° richieste / n° consulenze interne= 1** **2 ore di formazione pro capite**	già in atto	Segretario Generale	Vedasi Regolamento, completato il percorso per adeguarsi alla nuova direttiva europea sulla privacy
				Disomogenità nella valutazione delle richieste	**Rischio "Disomogeneità nella valutazione delle richieste"** 1. Standardizzazione della modulistica con particolare riferimento all'esplicitazione della motivazione della richiesta e del procedimento amministrativo cui si riferisce	Modulo	Già in atto	Il responsabile del procedimento	
				Violazione della privacy	**Rischio "Violazione privacy"** 1. Tracciabilità informatica di accessi e interrogazioni alle banche dati con elementi sensibili	Monitoraggio			
Area Segreteria	Tutti i servizi che affidano incarichi	Incarichi e consulenze professionali	4	**Scarsa trasparenza dell'affidamento dell'incarico/consulenza**	**Rischio "Scarsa trasparenza"** 1. Pubblicazione di richieste di offerta/bandi 2. Predisposizione di indirizzi per l'affidamento di incarichi di consulenza e collaborazione	linee di indirizzo	Già in atto	Segretario Generale	
				Scarso controllo del possesso dei requisiti dichiarati	**Rischio "Scarso controllo del possesso dei requisiti dichiarati"** 1. Creazione di supporti operativi per la effettuazione dei controlli dei requisiti	Check list		Il responsabile del procedimento	
Area servizio polizia locale	Polizia locale	Gestione della videosorveglianza del territorio	4	**Violazione della privacy**	Rischio "Violazione della privacy " 1. Stesura regolamento per accesso alle banche dati 2. Stesura regolamento e tracciabilità informatica di accessi e interrogazioni ai sistemi di videosorveglianza o a banche dati con elementi sensibili	**Monitoraggio annuale**	Già in atto	Comandante della Polizia Municipale	Regolamento comunale
				Fuga di notizie verso la stampa di informazioni riservate	Rischio "Fuga di notizie verso la stampa di informazioni riservate" 1. Formalizzazione di una linea guida che identifica le sole persone abilitate a comunicare con la stampa	**Istruttoria**			

Area servizio polizia locale	Polizia locale	Controlli annonaria/commercio	4	**Assenza di criteri di campionamento**	Rischio "Assenza di criteri di campionamento" 1. Formalizzazione dei controlli delle attività	**Verbale controlli**	Già in atto	Comandante della Polizia Municipale	Comunità comprensoriale Val Venosta - convenzione Collaborazione sovracomunale
				Disomogeneità delle valutazioni	Rischio "Disomogeneità delle valutazioni" 1. Creazione di supporti operativi per la effettuazione dei controlli	**Istruttoria**			Comunità comprensoriale Val Venosta - convenzione Collaborazione sovracomunale
				Non rispetto delle scadenze temporali	Rischio "Non rispetto delle scadenze temporali" 1. Monitoraggio e semestrali reporting dei tempi di realizzazione dei controlli	**Report**			
Area servizio polizia locale	Polizia locale	Controlli edilizi e ambientali	4	**Assenza di criteri di campionamento**	Rischio "Assenza di criteri di campionamento" 1. Formalizzazione dei controlli delle situazioni	**Verbale controlli**	già in atto	Comandante della Polizia Municipale	In collaborazione con l'ufficio tecnico
				Disomogeneità delle valutazioni	Rischio "Disomogeneità delle valutazioni" 1. Creazione di supporti operativi per la effettuazione dei controlli	**Check list**			
				Non rispetto delle scadenze temporali	Rischio "Non rispetto delle scadenze temporali" 1. Monitoraggio e reporting dei tempi di realizzazione dei controlli	**Monitoraggio**	Già in atto		
Area servizio polizia locale	Polizia locale	Gestione dell'iter dei verbali per infrazioni al codice della strada	4	**Disomogeneità dolosa delle valutazioni**	Rischio "Disomogeneità dolosa delle valutazioni" 1. Monitoraggio dei verbali annullati 2. Monitoraggio dei ricorsi e al loro esito	**Monitoraggio**	Già in atto	Comandante della Polizia Municipale	Comunità comprensoriale Val Venosta - convenzione Collaborazione sovracomunale
				Non rispetto delle scadenze temporali	Rischio "Non rispetto delle scadenze temporali" 1. Monitoraggio dei verbali che per motivi temporali risultano prescritti				Comunità comprensoriale Val Venosta - convenzione Collaborazione sovracomunale
Area servizio polizia locale	Polizia locale	Accertamenti relativi alla residenza	4	**Assenza di criteri di campionamento**	Rischio "Disomogeneità delle valutazioni" 1. Creazione di supporti operativi per la effettuazione dei controlli	**Check list**	Già in atto	Comandante della Polizia Municipale	In collaborazione con i Servizi demografici
				Non rispetto delle scadenze temporali	Rischio "Non rispetto delle scadenze temporali" 1. Monitoraggio dei tempi di evasione 2. Monitoraggio del numero di procedimenti che superano i tempi del silenzio assenso	**Monitoraggio**			
Area Segreteria	contratti e appalti	affidamenti diretti	**6**	**alterazione della concorrenza tramite utilizzo artificioso della motivazione di assenza di concorrenza per motivi tecnici**	**Rischio "alterazione della concorrenza tramite affidamento diretto"** Esplicitare nel provvedimento di affidamento diretto i presupposti per i quali si è ricorsi a questo tipo di procedura	**Monitoraggio**	Già in atto	Responsabile ufficio contratti/Segretario Comunale	
		procedure d'urgenza	3	**alterazione della concorrenza tramite ricorso ad una procedura in deroga per ragioni di estrema urgenza in mancanza dei previsti presupposti**	**Rischio "alterazione della concorrenza tramite procedura in deroga"** Esplicitare nel provvedimento dettagliatamente i presupposti per i quali si è ricorsi a ragioni di estrema urgenza	**Monitoraggio**	Già in atto	Responsabile ufficio contratti e appalti/Segretario Comunale	
	contratti e appalti	difformità nell'esecuzione di un contratto	4	**alterazione della concorrenza tramite omessa verifica circa la corrispondenza tra quanto dichiarato dall'operatore economico in sede di offerta e quanto dallo stesso adempiuto in fase di esecuzione del contratto d'appalto**	**Rischio "alterazione della concorrenza tramite omessa verifica"** a) Prevedere a chiusura di un contratto una valutazione sintetica delle difformità rispetto alle condizioni proposte in sede di offerta. b) Definire dei parametri di allarme per avviare una eventuale istruttoria più puntuale.	**Monitoraggio**	30.11.2022	a) RUP/Direttore dell'esecuzione b) Responsabile ufficio contratti e appalti/Segretario Comunale	

	basso rischio
	medio rischio
	alto rischio

Beilage A zum Ratsbeschluss Nr. 31 vom 03.12.2020

Allegato A alla delibera consiliare n. 31 del 03.12.2020

STELLENPLAN DER GEMEINDE MALS

PIANTA ORGANICA DEL COMUNE DI MALLES VENOSTA

Pos.	Berufsbild	profilo professionale	F.E. Q.F.	Zweisprachigkeitsgrad / grado di bilinguismo	Zugangsvoraussetzung von außen *)	requisiti culturali per l'accesso dall'esterno *)	Aufnahmeverfahren	modalità di accesso	Stellenanzahl nr. posti	Aufgabenbeschreibung *)	descrizione mansioni *)
1	Generalsekretär Berufsbild Nr. **80**	segretario generale profilo prof. n. **80**	IX	A	siehe Berufsbild Nr. **80**	vedi profilo prof. n. **80**	Wettbewerb nach Titeln aufgrund der im DPRA vom 26.8.93, Nr. 15/L festgesetzten Kriterien	concorso per titoli sulla base dei criteri stabiliti dal D.P.G.R. del 26.08.1993, n. 15/L	1	siehe Berufsbild **Nr. 80**	vedi profilo professionale **n. 80**
2	Vizegeneralsekretär Berufsbild Nr. **82**	Vicesegretario generale profilo prof. n. **82**	IX	A	siehe Berufsbild Nr. **82**	vedi profilo prof. n. **82**	Wettbewerb nach Titeln und Prüfungen	concorso per titoli ed esami	1	siehe Berufsbild **Nr. 82**	vedi profilo professionale **n. 82**
3	Funktionär der Verwaltung oder des Rechnungswesens Berufsbild Nr. **72**	Funzionario amministrativo o contabile profilo prof. n. **72**	VIII	A	siehe Berufsbild Nr. **72**	vedi profilo prof. n. **72**	Wettbewerb nach Titeln und Prüfungen	concorso per titoli ed esami	2	siehe Berufsbild Nr. **72**	vedi profilo professionale n. **72**
4	Techniker mit Berufsbefähigung Berufsbild Nr. **56 + 57**	Tecnico con abilitazione all'esercizio della professione Profilo prof. n. **56 + 57**	VII	B	siehe Berufsbild Nr. **56** bzw. **57**	vedi profilo prof. n. **56** risp. **57**	Wettbewerb nach Titeln und Prüfungen	concorso per titoli ed esami	2	siehe Berufsbild **Nr. 56** bzw. **57**	vedi profilo professionale **n. 56** risp. **57**
5	Verwaltungsassistent Berufsbild Nr. **43; 50**	assistente amm.vo profilo prof. n. **43; 50**	VI	B	siehe Berufsbild Nr. **43** bzw. **50**	vedi profilo prof. n. **43** e/o **50**	öffentlicher Wettbewerb nach Titeln und Prüfungen	concorso pubblico per titoli ed esami	13,50	siehe Berufsbilder Nr. **43** , **50**	vedi profilo professionale n. **43, 50**
6	Bibliothekar Berufsbild Nr. **46**	bibliotecario profilo prof. n. **46**	VI	B	siehe Berufsbild Nr. **46**	vedi profilo prof. n. **46**	öffentlicher Wettbewerb nach Titeln und Prüfungen	concorso pubblico per titoli ed esami	2 (1,2)	siehe Berufsbild Nr. **46**	vedi profilo professionale n. **46**
7	Inspektor der Gemeindepolizei Berufsbild Nr. **45**	Ispettore di polizia municipale ed annonaria profilo prof. n. **45**	VI	B	siehe Berufsbild Nr. **45**	vedi profilo prof. n. **45**	öffentlicher Wettbewerb nach Titeln und Prüfungen	concorso pubblico per titoli ed esami	1	siehe Berufsbild Nr. **45**	vedi profilo professionale n. **45**
8	Gemeinde- und Lebensmittelpolizist Berufsbild Nr. **32 + 35**	vigile comunale e annonario profilo prof.	V	C	siehe Berufsbild **Nr. 32 + 35**	vedi profilo prof. **n. 32 + 35**	öffentlicher Wettbewerb nach Titeln und Prüfungen	concorso pubblico per titoli ed esami	2	siehe Berufsbild **Nr. 32 + 35**	vedi profilo professionale **n. 32 + 35**

Pos.	Berufsbild	profilo professionale	F.E. Q.F.	Zweisprachigkeitsgrad / grado di bilinguismo	Zugangsvoraussetzung von außen *)	requisiti culturali per l'accesso dall'esterno *)	Aufnahmeverfahren	modalità di accesso	Stellenanzahl nr. posti	Aufgabenbeschreibung *)	descrizione mansioni *)
		n. **32+35**									
9	Verwaltungsbeamter Berufsbild Nr. **31**	operatore amministrativo profilo prof. n. **31**	V·	C	siehe Berufsbild Nr. **31**	vedi profilo prof. n. **31**	*Vorbehalt für Personal der geschützten Kategorien*	*Riservato alle persone appartententi alle categorie protette*	(1)	siehe Berufsbild Nr. **31**	vedi profilo professionale n. **31**
10	Koch / Diätetisch geschulter koch Berufsbild Nr. **19 + 19/bis**	Cuoco / cuoco dietista specializzato profilo prof. n. **19 + 19/bis**	**IV**	D	siehe Berufsbild Nr. **19 + 19/bis**	vedi profilo prof. n. **19 + 19/bis**	öffentlicher Wettbewerb nach Titeln und theoretisch-prak-tischer Prüfung	consorso pubblico per titoli e esame teorico-pratico	6 (3,75)	siehe Berufsbild Nr. **19 + 19/bis**	vedi profilo professionale n. **19 + 19/bis**
11	qualifizierter Koch Berufsbild Nr.**13 + 2**	cuoco qualificato profilo prof. n. **13 e 2**	**III** (II)	D	siehe Berufsbild **Nr.13 + 2**	profilo prof. **n. 13 e 2**	*Auslaufstelle*	*Posto a scadenza*	--		
12	spezialisierter Arbeiter Berufsbild Nr. **15**	operaio specia-lizzato profilo prof. n. **15**	IV	D	siehe Berufsbild Nr. **15**	vedi profilo prof. **n. 15**	öffentlicher Wettbewerb nach Titeln und theoretisch-prak-tischer Prüfung	concorso pubblico per titoli ed esami teorico-pratico	5	siehe Berufsbild Nr. **15**	vedi profilo professionale n. **15**
13	Qualifizierter Arbeiter Berufsbild Nr. **9**	operaio qualifcato profilo prof. n. **9**	III	D	siehe Berufsbild Nr. **9**	vedi profilo prof. **n. 9**	öffentlicher Wettbewerb nach Titeln und theoretisch-prak-tischer Prüfung	concorso pubblico per titoli ed esami teorico-pratico	2	siehe Berufsbild Nr. **9**	vedi profilo professionale n. **9**
14	qualifiziertes Reinigungspersonal Berufsbild Nr. **2**	addetto alle pulizie qualificato profilo prof. n. **2**	**II** (I)	D	siehe Berufsbild Nr. **2**	vedi profilo prof. **n. 2**	öffentliche Rangordnung nach Titeln und Eignungsprüfung	graduatoria pubblica per titoli e prova selettiva	1 (0,45)	siehe Berufsbild Nr. **2**	vedi profilo professionale **n. 2**
							INSGESAMT in Vollzeitstellen umgerechnete Stellen	**TOTALE posti trasformati in posti ad orario pieno**	38,5 **34,9**		
							max. mögliche Stellen lt. LAB Nr. 429 vom 11.04.2017	**n. posti massimi ai sensi della DGP n. 429 del 11.04.2017**	**42,50**		

DER BÜRGERMEISTER/ IL SINDACO
Thurner Josef

DIE GENERALSEKRETÄRIN/ petraLA SEGRETARIA GENERALE
Dr. Monika Platzgummer

3. Disponibilità e gestione delle risorse umane

La pianta organica vigente del Comune Malles Venosta comprende 34,90 posti di lavoro considerati come unità a tempo pieno (38 ore). Di questi sono occupati 27,30 posti a tempo pieno. 41 collaboratrici e collaboratori hanno un rapporto di lavoro dipendente con il Comune, di cui 30 donne e 11 uomini. 35 persone hanno un rapporto di lavoro indeterminato.

	2017	%	2018	%	2019	%	2020	%	2021	%
Dipendenti a tempo indeterminato	26,04	90,45%	26,53	94,65%	26,66	91,33%	27,65	82,93%	29,63	84,88%
Dipendenti a tempo determinato	2,75	9,55%	1,50	5,35%	2,53	8,67%	5,69	17,07%	5,28	15,12%
Totale Dipendenti	**28,79**	**100,00%**	**28,03**	**100,00%**	**29,19**	**100,00%**	**33,34**	**100,00%**	**34,91**	**100,00%**

3. Personal

Der geltende Stellenplan der Gemeinde Mals umfasst 34,90 Stellen bemessen in Vollzeitarbeitseinheiten (38 Stunden). Davon sind 27,30 Vollzeiteinheiten besetzt. 41 Mitarbeiterinnen (davon 6 in Mutterschaft) und Mitarbeiter stehen in einem abhängigen Arbeitsverhältnis mit der Gemeinde, davon sind 30 Frauen und 11 Männer. 35 Personen haben ein unbefristetes Arbeitsverhältnis.

	2017	%	2018	%	2019	%	2020	%	2021	%
Bedienstete mit unbefristeten Arbeitsverhältnis	26,04	90,45%	26,53	94,65%	26,66	91,33%	27,65	82,93%	29,63	84,88%
Bedienstete mit befristeten Arbeitsverhältnis	2,75	9,55%	1,50	5,35%	2,53	8,67%	5,69	17,07%	5,28	15,12%
Summe Bedienstete	**28,79**	**100,00%**	**28,03**	**100,00%**	**29,19**	**100,00%**	**33,34**	**100,00%**	**34,91**	**100,00%**

Stampa Intero Modello in data : 7/12/2022

Tipo Rilevazione : CONSUNTIVAZIONE SPESE	Anno : 2021
Tipo Istituzione : COMUNI	Contratto : PROV. AUTONOMA DI BOLZANO
Istituzione : 4034 - MALLES VENOSTA	
Organo di Controllo di Primo Livello : RTS BOLZANO	

	T1	T1a	T1b	T1c	T1c bis	T1d	T1e	T1f	T1g	T1sd	T2	T2a	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15	S1	S1A	SICI	Tab. Ric.
Tenute	X										X	X	X	X	X	X	X	X	X		X	X	X	X		X	X		X
Dichiarate	X										X	X		X	X	X	X	X	X		X	X	X	X		X	X		X
Inviate	X										X	X		X	X	X	X	X	X		X	X	X	X		X	X		X
Risultano inviati i dati dell'appendice SI1A Convenzioni																													

Il Modello inviato risulta certificato in data : 17/11/2022

Il Modello inviato è stato certificato la prima volta in data : 11/08/2022

188293

Kollektivabkommen und -verträge - 1. Teil - Jahr 2019

Autonome Provinz Bozen - Südtirol

KOLLEKTIVABKOMMEN UND -VERTRAG

vom 4. Dezember 2019

Teilvertrag für die Erneuerung des bereichsübergreifenden Kollektivvertrages für den Dreijahreszeitraum 2019 - 2021

Fortsetzung >>>

Accordi e contratti collettivi - Parte 1 - Anno 2019

Provincia Autonoma di Bolzano - Alto Adige

ACCORDO - CONTRATTO COLLETTIVO

del 4 dicembre 2019

Accordo stralcio per il rinnovo del contratto collettivo intercompartimentale per il triennio 2019 - 2021

Continua >>>

Unterzeichnet am 4. Dezember 2019 aufgrund des Beschlusses der Landesregierung Nr. 1030 vom 03.12.2019

Sottoscritto in data 4 dicembre 2019 in base della deliberazione della Giunta Provinciale del 03/12/2019, n. 1030

Teilvertrag für die Erneuerung des bereichsübergreifenden Kollektivvertrages für den Dreijahreszeitraum 2019 - 2021

Accordo stralcio per il rinnovo del contratto collettivo intercompartimentale per il triennio 2019 - 2021

Vorspann

Mit Beschluss Nr. 352 vom 14/05/2019 hat die Landesregierung die Richtlinien für die Verhandlungen des bereichsübergreifenden Kollektivvertrages für den normativen und wirtschaftlichen Dreijahreszeitraum 2019-2021 erlassen. Mit dem gleichen Beschluss wurde die öffentliche Delegation ermächtigt, Teilverträge abzuschließen.

Nach umfassenden Verhandlungen mit den Gewerkschaftsorganisationen und der öffentlichen Verhandlungsdelegation wurde es als notwendig erachtet, einen Teilvertrag (nachstehend „Abkommen" genannt) über die Anpassung an die Inflation, die Produktivität, die Aufwertung der Sprachkenntnisse sowie der Berufszulagen abzuschließen.

Das vorliegende Abkommen wird wesentlicher und integrierender Bestandteil des bereichsübergreifenden Kollektivvertrages für den Dreijahreszeitraum 2019-2021.

Premessa

Con deliberazione n. 352 del 14/05/2019 la Giunta Provinciale ha emanato le direttive riguardanti la contrattazione collettiva per il rinnovo del contratto collettivo intercompartimentale per il triennio giuridico ed economico 2019-2021. Con la medesima deliberazione, la delegazione pubblica è stata autorizzata alla stipulazione di accordi stralcio.

A seguito di articolate trattative con le organizzazioni sindacali e la delegazione pubblica trattante si è ritenuto necessario procedere ad un accordo stralcio (di seguito "accordo") relativamente ad un adeguamento all'inflazione, alla produttività e alla valorizzazione delle competenze linguistiche, nonché della retribuzione professionale.

Il presente accordo sarà parte essenziale ed integrante del contratto collettivo intercompartimentale per il triennio 2019-2021.

Art. 1

Anwendungsbereich

1. Das vorliegende Abkommen gilt für das Personal folgender Bereiche:
   a) Landesverwaltung,
   b) Landesgesundheitsdienst,
   c) Gemeinden, Seniorenwohnheime und Bezirksgemeinschaften,
   d) Institut für sozialen Wohnbau,
   e) Verkehrsamt Bozen und Kurverwaltung Meran.

Art. 1

Ambito di applicazione

1. Il presente accordo si applica al personale dei seguenti comparti:
   a) Amministrazione provinciale;
   b) Servizio sanitario provinciale;
   c) Comuni, Residenze per anziani e Comunità comprensoriali;
   d) Istituto per l'edilizia sociale;
   e) Azienda di soggiorno e turismo di Bolzano e Azienda di soggiorno, cura e turismo di Merano.

Art. 2

Dauer, Gültigkeit und Verfahren für die Anwendung

1. Das vorliegende Abkommen betrifft den Zeitraum vom 1. Januar 2019 bis zum 31.

Art. 2

Durata, decorrenza e procedure di applicazione

1. Il presente accordo riguarda il periodo 1° gennaio 2019 – 31 dicembre 2021. Esso

Dezember 2021. Dieses bleibt so lange in Kraft, bis es durch den nächsten bereichsübergreifenden Kollektivvertrag ersetzt wird. Die wirtschaftlichen Auswirkungen laufen ab dem jeweiligen Fristbeginn, der in den einzelnen Vertragsbestimmungen angegeben ist.

rimane comunque in vigore fino a quando non sarà sostituito dal successivo contratto collettivo intercompartimentale. Gli effetti economici decorrono dalle specifiche decorrenze indicate nelle singole disposizioni contrattuali.

Art. 3

Erhöhung der Entlohnung

1. Die jährlichen Anfangsbruttogehälter der in den verschiedenen Besoldungsstufen der einzelnen Funktionsebenen laut Artikel 6 Absatz 1 des bereichsübergreifenden Kollektivvertrages vom 15. November 2011 werden bestätigt.

2. Die jährliche Bruttosonderergänzungszulage der einzelnen Funktionsebenen wird mit Wirkung 1. Januar 2019 wie folgt festgelegt (+0,9 Prozent berechnet auf das Anfangsgehalt der oberen Besoldungsstufe mit vier Gehaltsvorrückungen und die Sonderergänzungszulage der jeweiligen Funktionsebenen):

Funktionsebene	Jahresbruttobetrag	
1	11.074,07	Euro
2	11.123,95	Euro
3	11.171,73	Euro
4	11.238,85	Euro
5	11.301,38	Euro
6	11.388,95	Euro
7	11.491,05	Euro
7 ter	11.546,93	Euro
7 bis	11.596,32	Euro
8	11.616,75	Euro
9	11.732,96	Euro
einheitliche Leitungsebene der sanitären Führungskräfte	11.755,36	Euro
1. Leitungsebene im Auslaufrang der Gemeinden	12.096,00	Euro

3. Die jährliche Bruttosonderergänzungszulage der einzelnen Funktionsebenen wird mit Wirkung 1. Januar 2020 wie folgt festgelegt (+1,0 Prozent berechnet auf das Anfangsgehalt der oberen Besoldungsstufe mit vier Gehaltsvorrückungen und die Sonderergänzungszulage der jeweiligen Funktionsebenen):

Art. 3

Aumento della retribuzione

1. Sono confermati gli stipendi annui lordi iniziali dei livelli retributivi delle qualifiche funzionali di cui all'articolo 6, comma 1 del contratto collettivo intercompartimentale del 15 novembre 2011.

2. L'indennità integrativa speciale annua lorda delle singole qualifiche funzionali è determinata, con decorrenza 1° gennaio 2019, come segue (+0,9 per cento calcolato sullo stipendio iniziale del livello retributivo superiore con quattro scatti e sull'indennità integrativa speciale delle singole qualifiche funzionali):

qualifica funzionale	importo annuo lordo	
1	11.074,07	Euro
2	11.123,95	Euro
3	11.171,73	Euro
4	11.238,85	Euro
5	11.301,38	Euro
6	11.388,95	Euro
7	11.491,05	Euro
7 ter	11.546,93	Euro
7 bis	11.596,32	Euro
8	11.616,75	Euro
9	11.732,96	Euro
qualifica unica dirigenza sanitaria	11.755,36	Euro
1° qualifica dirigenti comunali ad esaurimento	12.096,00	Euro

3. L'indennità integrativa speciale annua lorda delle singole qualifiche funzionali è determinata, con decorrenza 1° gennaio 2020, come segue (+1,0 per cento calcolato sullo stipendio iniziale del livello retributivo superiore con quattro scatti e sull'indennità integrativa speciale delle singole qualifiche funzionali):

Funktionsebene	Jahresbruttobetrag		qualifica funzionale	importo annuo lordo	
1	11.287,03	Euro	1	11. 287,03	Euro
2	11.361,08	Euro	2	11.361,08	Euro
3	11.421,12	Euro	3	11.421,12	Euro
4	11.500,93	Euro	4	11.500,93	Euro
5	11.582,84	Euro	5	11.582,84	Euro
6	11.694,32	Euro	6	11.694,32	Euro
7	11.832,99	Euro	7	11.832,99	Euro
7ter	11.898,52	Euro	7 ter	11.898,52	Euro
7bis	11.961,97	Euro	7 bis	11.961,97	Euro
8	12.005,32	Euro	8	12.005,32	Euro
9	12.184,54	Euro	9	12.184,54	Euro
einheitliche Leitungsebene der sanitären Führungskräfte	12.293,27	Euro	qualifica unica dirigenza sanitaria	12.293,27	Euro
1. Leitungsebene im Auslaufrang der Gemeinden	12.627,24	Euro	1° qualifica dirigenti comunali ad esaurimento	12.627,24	Euro

4. Nach vorheriger Einigung über die neue Regelung der Lohnstruktur gemäß Titel I des bereichsübergreifenden Kollektivvertrages vom 12. Februar 2008 werden das Grundgehalt und die Sonderergänzungszulage mit Wirkung 1. Januar 2021 zu einem einzigen Gehaltselement als Grundentlohnung zusammengefasst, welche mit gleicher Wirkung um 1,1 Prozent erhöht wird.

5. Die in diesem Artikel vorgesehenen Erhöhungen werden in gleicher Weise dem Personal der Führungskräfte sowie der sanitären Leiter des Landesgesundheitsdienstes ausbezahlt.

6. Die Erhöhungen laut Absatz 2 bis 4 gelten nicht für die Ergänzung der Ruhestandsbehandlung im Sinne von Artikel 46 des Landesgesetzes vom 19. Mai 2015, Nr. 6.

4. Previo accordo relativo alla nuova disciplina della struttura retributiva di cui al titolo I del contratto collettivo intercompartimentale del 12 febbraio 2008, lo stipendio base e l'indennità integrativa speciale sono unificati con decorrenza 1° gennaio 2021 in un'unica voce stipendiale, quale retribuzione fondamentale; tale retribuzione fondamentale verrà aumentata con la stessa decorrenza dell'1,1 per cento.

5. Gli aumenti previsti dal presente articolo sono corrisposti con le medesime modalità al personale della dirigenza e della dirigenza sanitaria del Servizio Sanitario Provinciale.

6. Gli aumenti di cui ai commi 2 fino a 4 non trovano applicazione per l'integrazione provinciale della pensione di cui all'articolo 46 della legge provinciale 19 maggio 2015, n. 6.

Art. 4

Wirkungen der Erhöhungen der Entlohnung

1. Die aus der Anwendung der vorangehenden Artikel resultierenden Erhöhungen finden

Art. 4

Effetti degli aumenti della retribuzione

1. I benefici economici risultanti dall'applicazione dei precedenti articoli hanno effetto

volle Berücksichtigung bei der Festlegung des Ruhegehaltes für das im Zeitraum der Gültigkeit dieses Abkommens aus dem Dienst ausgeschiedenen Personal mit Anrecht auf das Ruhegehalt, zu den Fälligkeiten und in dem Ausmaß, die von den in diesem Artikel angeführten Bestimmungen vorgesehen sind. Zu diesem Zwecke werden die Erhöhungen der Sonderergänzungszulage neu festgelegt; dazu wird die Erhöhung in Bezug auf das Jahr des Dienstaustrittes für jene Monate, in denen die betreffende Person voll gearbeitet hat, in Zwölfteln angerechnet.

integralmente sulla determinazione del trattamento di quiescenza del personale cessato dal servizio, con diritto a pensione, nel periodo di vigenza del presente accordo alle scadenze e negli importi previsti dalle disposizioni richiamate nel presente articolo. A tale fine gli aumenti dell'indennità integrativa speciale sono rideterminati calcolando l'aumento relativo all'anno di cessazione dal servizio in dodicesimi, in relazione ai mesi interi di servizio.

2. Die in diesem Abkommen vorgesehene Erhöhung der Sonderergänzungszulagen gilt für Überstunden, die ab dem ersten Tag des Monats geleistet werden, der auf den Monat der Veröffentlichung dieses Vertrages im Amtsblatt der Region folgt.

2. Gli aumenti dell'indennità integrativa speciale di cui al presente accordo trovano applicazione per il lavoro straordinario prestato con decorrenza dal primo giorno del mese successivo alla data di pubblicazione del presente contratto sul Bollettino Ufficiale della Regione.

3. Die in diesem Abkommen vorgesehenen Erhöhungen, mit Ausnahme der Bestimmung des Absatzes 2, haben keine Auswirkungen auf die wirtschaftlichen Institute, für deren Berechnung sich die geltenden Bestimmungen auf die entsprechenden Gehaltselemente beziehen. Für deren Berechnung wird, in Erwartung der neuen Bestimmung laut Artikel 3, Absatz 4, auf die zum 31.12.2018 gültigen Gehaltselemente zurückgegriffen.

3. Gli aumenti previsti dal presente accordo, escluso quanto previsto al comma 2, non producono effetti sugli istituti di carattere economico per il cui calcolo le disposizioni vigenti rinviano ai relativi elementi retributivi. Per il calcolo, in attesa di nuova disciplina ai sensi del comma 4 dell'articolo 3, si fa riferimento, agli elementi retributivi in vigore al 31/12/2018.

Art. 5

Inflationsanpassung

Art. 5

Adeguamento all'inflazione

1. Nach Absprache mit den Vertragspartnern wird am Ende der dreijährigen Vertragslaufzeit eine Überprüfung der vorgesehenen und der tatsächlich dokumentierten Inflation durchgeführt. Ein Ausgleich einer eventuellen Abweichung erfolgt innerhalb des ersten Jahres des nächsten Dreijahresverhandlungszeitraumes.

1. Previo confronto tra le parti sarà effettuata alla scadenza del triennio contrattuale una verifica circa eventuali scostamenti tra inflazione prevista e quella reale effettivamente documentata. Il recupero dell'eventuale scostamento avverrà entro il primo anno del successivo triennio contrattuale.

Art. 6

Zweisprachigkeitszulage, Anwendungsbereich, Definition und Festlegung – Zulage für den Gebrauch der ladinischen Sprache

Art. 6

Indennità di bilinguismo – ambito di applicazione, definizione e determinazione – Indennità per l'uso della lingua ladina

1. Das Personal gemäß Artikel 1 des vorliegenden Abkommens, das nach den geltenden Bestimmungen über den öffentlichen Dienst in der Provinz Bozen im Besitze der Bescheinigung über die

1. Al personale di cui all'articolo 1 del presente accordo che, ai sensi della vigente normativa sul pubblico impiego in provincia di Bolzano deve essere in possesso dell'attestato di conoscenza delle lingue italiana e tedesca, è corrisposta a partire dal

Kenntnisse der italienischen und deutschen Sprache sein muss, erhält wie nachstehend angeführt, ab 01.01.2020 die Zweisprachigkeitszulage.

2. Die für das im Absatz 1 betroffene Personal anerkannte Zweisprachigkeitszulage setzt sich aus zwei Quoten zusammen. Die erste Quote, die bereits im Grundgehalt und in der Sonderergänzungszulage enthalten ist, wird dem gesamten Personal gemäß Absatz 4 dieses Artikels und die zweite Quote wird als eigenes Gehaltselement ausbezahlt.

3. Die Zweisprachigkeitszulage, als Teil des Grundgehalts wird monatlich ausbezahlt. Die erste Quote unterliegt in jeder Hinsicht derselben Regelung wie das Gehalt und wird bei der Berechnung der individuellen beruflichen Entwicklung der/des Bediensteten berücksichtigt. Beide Quoten der Zulage wirken sich auf das dreizehnte Monatsgehalt aus.

4. Die monatliche Bruttozweisprachigkeitszulage wie folgt festgelegt:

Quote 1 bereits im Grundgehalt und in der Sonderergänzungszulage enthalten	Quote 2 Zweisprachigkeitszulage als neues und eigenes Lohnelement
Zweisprachigkeitsnachweis A2 (ehem. Niveau D)	
€ 121,00	€ 51,50
Zweisprachigkeitsnachweis B1 (ehem. Niveau C)	
€ 142,00	€ 56,65
Zweisprachigkeitsnachweis B2 (ehem. Niveau B)	
€ 161,00	€ 79,31
Zweisprachigkeitsnachweis C1 (ehem. Niveau A)	
200,00	€ 88,58

5. Der Zweisprachigkeitsnachweis der italienischen und deutschen Sprache, welcher von der eigenen Kommission in Anwendung des

01/01/2020 l'indennità di bilinguismo così come di seguito definita.

2. Per il personale di cui al comma 1 l'indennità di bilinguismo riconosciuta si compone di due quote. Una prima quota, già ricompresa nello stipendio e nell'indennità integrativa speciale, è corrisposta a tutto il personale in base al comma 4 del presente articolo, ed una seconda quota che viene corrisposta come elemento distinto dello stipendio.

3. L'indennità di bilinguismo quale elemento del salario fondamentale è corrisposta mensilmente. La prima quota è assoggettata ad ogni effetto alla medesima disciplina dello stipendio ed è ricompresa per il calcolo della progressione professionale individuale del/la dipendente. Ambedue le quote dell'indennità hanno effetto sulla tredicesima mensilità.

4. L'indennità di bilinguismo mensile lorda è determinata come segue:

Quota 1 già ricompresa nello e stipendio e nell'indennità integrativa speciale	Quota 2 nuova voce distinta quale indennità di bilinguismo
attestato di bilinguismo A2 (ex livello D)	
€ 121,00	€ 51,50
attestato di bilinguismo B1 (ex livello C)	
€ 142,00	€ 56,65
attestato di bilinguismo B2 (ex livello B)	
€ 161,00	€ 79,31
attestato di bilinguismo C1 (ex livello A)	
200,00	€ 88,58

5. L'attestato di conoscenza della lingua italiana e tedesca, certificato dall'apposita Commissione istituita in applicazione

Artikels 12 der Anlage 2 des Kollektivvertrages für den Bereich des Personals des Landesgesundheitsdienstes mit Ausnahme des Personals des ärztlichen und tierärztlichen Bereiches sowie des leitenden sanitären, verwaltungs-, technischen und berufsbezogenen Bereiches vom 28. August 2001 ausgestellt wird, wird zwecks Anerkennung der Quote 2 des vorliegenden Artikels dem Zweisprachigkeitsnachweis B2 (ehem. Niveau B) gleichgestellt.

dell'articolo 12 dell'allegato 2 del contratto collettivo di comparto per il personale del Servizio Sanitario Provinciale escluso il personale dell'area medica-medico veterinaria e della dirigenza sanitaria, amministrativa, tecnica e professionale del 28 agosto 2001, ai fini del riconoscimento della quota 2 del presente articolo è equiparato all'attestato di bilinguismo B2 (ex livello B).

6. Von der Bestimmung des vorliegenden und nachstehenden Artikels 7 sind die sanitären ärztlichen und tierärztlichen Leiter, die sanitären Leiter, Apotheker, Biologen, Chemiker, Physiker und Psychologen und die Leiter der Pflegeberufe ausgeschlossen.

6. Rimangono esclusi dalla disciplina di cui al presente e al successivo articolo 7 il personale dirigente medico e medico veterinario, i dirigenti sanitari farmacisti, biologi, chimici, fisici e psicologi e la dirigenza delle professioni sanitarie.

7. Von der Bestimmung des vorliegenden und nachstehenden Artikels 7 sind das Landeslehrpersonal, die Kindergärtner/innen, die pädagogischen Mitarbeiter/innen und die Mitarbeiter/innen für Integration ausgeschlossen. Für dieses Personal gelten weiterhin die Bestimmungen bezüglich der Verminderung des Grundgehaltes laut den entsprechenden geltenden Kollektivverträgen.

7. Rimangono esclusi dalla disciplina di cui al presente e al successivo articolo 7 il personale docente delle scuole provinciali, gli/le insegnanti della scuola dell'infanzia, i/le collaboratori/trici pedagogici/che e all'integrazione. Per tale personale rimangono in vigore le discipline concernenti la decurtazione dello stipendio previste nei relativi contratti collettivi vigenti.

8. Zuzüglich zur Zweisprachigkeitszulage laut diesem Artikel wird die Entschädigung für die Verwendung der ladinischen Sprache gemäß Artikel 81 des bereichsübergreifenden Kollektivvertrages vom 12. Februar 2008 für die Berechtigten in dem vorgesehenen Prozentsatz und der vorgesehenen Weise bestätigt.

8. In aggiunta all'indennità di bilinguismo del presente articolo, rimane confermata per gli aventi diritto, nella percentuale e nelle modalità previste, l'indennità per l'uso della lingua ladina così come disciplinata all'articolo 81 del contratto collettivo intercompartimentale del 12 febbraio 2008.

Art. 7

Zweisprachigkeitszulage – Sonderbestimmungen

Art. 7

Indennità di bilinguismo – Norme speciali

1. Nach Inkrafttreten des vorliegenden Abkommens, hat das Personal, welches im Besitz einer Bescheinigung über die Kenntnisse der italienischen und deutschen Sprache ist, die höher als für den Zugang zu seinem Berufsbild erforderlich ist, Anspruch auf die Zulage der Quote 2, welche dem effektiv erworbenen Zweisprachigkeitsnachweis entspricht.

1. Dall'entrata in vigore del presente accordo, al personale in possesso di un attestato di conoscenza delle lingue italiana e tedesca superiore a quello previsto dai requisiti d'accesso al proprio profilo professionale o d'inquadramento, compete l'indennità della quota 2 corrispondente al livello di conoscenza attestata.

2. Es liegt in der Verantwortung der Bediensteten, den Zweisprachigkeitsnachweis der höheren Laufbahn vorzulegen, damit auf Antrag die höhere Quote ab dem ersten Tag des Folgemonats gewährt wird.

2. Compete al dipendente produrre la documentazione attestante il requisito necessario per la quota superiore, che viene riconosciuta, previa domanda, dal primo giorno del mese successivo.

3. Sollten Bedienstete im Besitz eines

3. Qualora l'attestato posseduto sia inferiore a

niedrigeren Zweisprachigkeitsnachweises bezüglich des Zugehörigkeitsberufsbildes sein, so erhalten sie die Quote 2 im Ausmaß des effektiv erworbenen Zweisprachigkeitsnachweises.

4. Dem Personal, das aufgrund von Ausnahmeregelungen ohne Zweisprachigkeitsnachweis eingestellt ist und wird, steht auch weiterhin nur die Quote 1 zu, da es in Bereichen tätig ist, in welchen die zweite Sprache verwendet wird.

5. Um den Erwerb der Kenntnis der italienischen und deutschen Sprache zu fördern, für jene Dienste, in denen derzeit der Zweisprachigkeitsnachweis nicht als Voraussetzung für den Zugang vorgesehen ist, können die Parteien durch spezifisch dezentralisierte Verhandlungen, besondere Anreize vorsehen.

quello previsto dai requisiti d'accesso al profilo professionale di appartenenza, l'indennità della quota 2 è corrisposta nella misura relativa al livello dell'attestato posseduto.

4. Al personale sprovvisto dell'attestato di conoscenza delle lingue italiana e tedesca, assunto in deroga da specifiche discipline, spetta, in quanto opera in ambiti in cui l'utilizzo della seconda lingua è comunque esercitato, la sola quota 1.

5. Al fine di favorire l'acquisizione della conoscenza delle lingue italiana e tedesca, nei servizi in cui oggi non è previsto quale requisito d'accesso, le parti possono, attraverso specifica contrattazione decentrata, individuare particolari incentivi.

Art. 8

Berufszulage für das Landeslehrpersonal, für die Kindergärtnerinnen und Kindergärtner, für die pädagogischen Mitarbeiterinnen/Mitarbeiter, für die Mitarbeiterinnen/Mitarbeiter für die Integration

1. Mit Wirkung 01.01.2020 wird die dem Lehrpersonal der Landesschulen zustehende monatliche Lehrberufszulage um 120,00 Euro brutto erhöht.

2. Mit Wirkung 01.01.2020 wird den Kindergärtnerinnen/Kindergärtnern eine monatliche Berufszulage im Ausmaß von 120,00 Euro brutto ausbezahlt.

3. Mit Wirkung 01.01.2020 wird den pädagogischen Mitarbeiterinnen/Mitarbeitern und den Mitarbeiterinnen/Mitarbeitern für Integration eine monatliche Berufszulage im Ausmaß von 110,00 Euro brutto ausbezahlt.

4. Die, nach Absatz 1 erhöhte Lehrberufszulage und die nach Absatz 2 und 3 vorgesehene Berufszulage werden in zwölf Monatsraten ausbezahlt.

5. Die in diesem Artikel genannten Zulagen unterliegen nicht den allgemeinen Gehaltserhöhungen.

Art. 8

Retribuzione professionale per il personale docente delle scuole provinciali, per gli/le insegnanti della scuola dell'infanzia, per i/le collaboratori/trici pedagogici/che e per i/le collaboratori/trici all'integrazione insegnante della scuola dell'infanzia

1. A decorrere dal 01/01/2020 la retribuzione professionale docente mensile lorda spettante al personale docente delle scuole provinciali è incrementata di euro 120,00 lordi.

2. A decorrere dal 01/01/2020 agli/alle insegnanti della scuola dell'infanzia è corrisposta una retribuzione professionale mensile lorda pari a euro 120,00.

3. A decorrere dal 01/01/2020 ai/alle collaboratori/trici pedagogici/che e ai/alle collaboratori/trici all'integrazione è corrisposta una retribuzione professionale mensile lorda pari a euro 110,00.

4. La retribuzione professionale docente, come incrementata in forza del comma 1 e la retribuzione professionale di cui ai commi 2 e 3 sono corrisposte in dodici rate mensili.

5. Le indennità di cui al presente articolo non seguono gli aumenti generali della retribuzione.

Art. 9

Art. 9

Personal des Behindertensektors

1. Dem Personal, welches erstmals vor dem 01.02.2002 im Behindertensektor gemäß Artikel 4 des Ergänzungsabkommen vom 30.11.2001 zum Bereichsabkommen der Bediensteten der Gemeinden, Bezirksgemeinschaften und Ö.B.P.B. eingesetzt wurde, wird die Aufgabenzulage mit Wirkung 01.01.2020 um 40,00 Euro monatlich brutto, erhöht.

2. Die Zulage laut Absatz 1 wird in 12 Monatsraten ausbezahlt.

Personale del servizio handicap

1. Al personale del servizio handicap di prima assunzione antecedente il 01/02/2002 di cui all'articolo 4 dell'accordo integrativo del 30/11/2001 all'accordo di comparto dei dipendenti Comunali, delle Comunità comprensoriali e delle A.P.S.P., l'indennità d'istituto è aumentata con decorrenza 01/01/2020 di euro 40,00 lordi mensili.

2. L'indennità di cui al comma 1 è corrisposta in 12 rate mensili.

Art. 10

Allgemeine Produktivität

1. Die für die allgemeine Produktivität des Personals gemäß Artikel 79 des bereichsübergreifenden Kollektivvertrages vom 12. Februar 2008 bestehenden Fonds der Körperschaften werden für das Jahr 2019 folgendermaßen erhöht:

   a) Für den Bereich des Personals der Landesverwaltung wird der Fonds für 2019 um 7.204.261,54 Euro brutto inklusive Sozialabgaben erhöht,

   b) Für den Bereich des Personals des Landesgesundheitsdienstes wird der Fonds für 2019 um 4.795.738,46 Euro brutto inklusive Sozialabgaben erhöht,

   c) Die Fonds der anderen Körperschaften laut Artikel 1 werden in analoger Weise wie für den Bereich des Personals der Landesverwaltung und des Landesgesundheitsdienstes und unter Berücksichtigung der besonderen Situation der einzelnen Bereiche, einschließlich der Höhe des bereits bestehenden Fonds, im Vergleich der Fonds des Bereichs des Personals der Landesverwaltung und des Landesgesundheitsdienstes, erhöht.

Art. 10

Produttività generale

1. I fondi degli enti già in dotazione per la produttività generale del personale di cui all' art. 79 del contratto collettivo intercompartimentale del 12 febbraio 2008 sono incrementati, per l'anno 2019, come segue:

   a) Per il comparto del personale dell'amministrazione provinciale il fondo per il 2019 viene incrementato di 7.204.261,54 euro lordi compresi gli oneri sociali;

   b) Per il comparto del personale del servizio sanitario provinciale il fondo per il 2019 viene incrementato di 4.795.738,46 euro lordi compresi gli oneri sociali;

   c) I fondi degli altri enti di comparto di cui all'articolo 1 vengono incrementati in analogia a quanto previsto per l'incremento del fondo per il comparto del personale dell'amministrazione provinciale e del comparto del personale del servizio sanitario provinciale, tenendo conto delle particolari situazioni dei singoli comparti, fra cui anche la consistenza del fondo già in dotazione, in comparizione ai fondi dei due comparti, personale dell'amministrazione provinciale e servizio sanitario provinciale.

Art. 11

Aufhebung von Bestimmungen

1. Mit Inkrafttreten des vorliegenden Abkommens und seiner einzelnen Bestimmungen erlischt die Anwendung der Bestimmungen, welche mit diesem unvereinbar sind, und zwar insbesondere

Art. 11

Abrogazione di norme

1. Con l'entrata in vigore del presente accordo e delle singole disposizioni dello stesso cessa l'applicazione delle norme incompatibili con lo stesso, ed in particolare delle seguenti disposizioni:

folgender Bestimmungen:

a) Artikel 12, der Anlage 2 des Kollektivvertrages für den Bereich des Personals des Landesgesundheitsdienstes mit Ausnahme des Personals des ärztlichen und tierärztlichen und des leitenden sanitären, verwaltungs-, technischen- und berufsbezogenen Bereiches vom 28. August 2001.

b) Die Blockierung der Gehaltsentwicklung laut Absatz 2 des Artikels 4 vom Anhang 2 des Kollektivvertrages für den Bereich des Personals des Landesgesundheitsdienstes mit Ausnahme des Personals des ärztlichen und tierärztlichen Bereiches sowie des leitenden sanitären, verwaltungstechnischen und berufsbezogenen Bereiches vom 7. April 2005.

c) Artikel 36 Absatz 3 des Bereichsabkommens für das Lehrpersonal der Berufsschulen des Landes, der Fachschulen für land-, forst- und hauswirtschaftliche Berufsbildung sowie der Musikschulen vom 27. Juni 2013 für den Zeitraum 2005-2008.

a) L'articolo 12, dell'allegato 2 del contratto collettivo di comparto per il personale del Servizio sanitario provinciale, escluso il personale dell'area medica-medico veterinaria e della dirigenza sanitaria, amministrativa, tecnica e professionale del 28 agosto 2001.

b) Il blocco della progressione economica, previsto al comma 2 dell'articolo 4 allegato 2 del contratto collettivo di comparto per il personale del Servizio Sanitario Provinciale, escluso il personale dell'area medica-medico veterinaria e della dirigenza sanitaria, amministrativa, tecnica e professionale del 7 aprile 2005.

c) Il comma 3 dell'articolo 36 del contratto di comparto per il personale docente delle scuole professionali provinciali, della formazione professionale agricola, forestale e di economia domestica e delle scuole di musica del 27 giugno 2013 relativo al periodo 2005-2008.

Bozen, den 4. Dezember 2019

Bolzano, lì 4 dicembre 2019

Der Generaldirektor der Landesverwaltung

Il Direttore Generale della Provincia

Alexander Steiner

(unterzeichnet)

(firmato)

Der Direktor der Landesabteilung Personal

Il Direttore della Ripartizione provinciale Personale

Albrecht Matzneller

(unterzeichnet)

(firmato)

Die Direktorin des Landesamtes für Gesundheitsordnung

La Direttrice dell'Ufficio provinciale Ordinamento Sanitario

Veronika Rabensteiner

(unterzeichnet)

(firmato)

Der Direktor der Betriebsabteilung Personal des Südtiroler Sanitätsbetriebes

Il Direttore della Ripartizione aziendale Personale dell'Azienda Sanitaria dell'Alto Adige

Christian Kofler

(unterzeichnet) (firmato)

Der Referent für das Büro für die Beziehungen zum Personal und den Gewerkschaften im Südtiroler Sanitätsbetrieb

Il referente dell'Ufficio relazioni con il personale ed i sindacati nell'Azienda Sanitaria dell'Alto Adige

Vincenzo Capellupo

(unterzeichnet) (firmato)

Der Präsident des Südtiroler Gemeindeverbandes

Il Presidente del Consorzio dei Comuni della Provincia di Bolzano

Andreas Schatzer

(unterzeichnet) (firmato)

Für den Verhandlungsbereich Gemeinden und Südtiroler Gemeindenverband

Per il comparto comuni e consorzio dei comuni della Provincia

Benedikt Galler

(unterzeichnet) (firmato)

Der Direktor des Personalamtes und Organisation des Institutes für den sozialen Wohnbau des Landes Südtirol

Il Direttore dell'Ufficio Personale e organizzazione dell'Istituto per l'edilizia sociale

Kurt Mair

(unterzeichnet) (firmato)

Der Präsident des Verbandes der Seniorenwohnheime Südtirols

Il Presidente dell'Associazione delle Residenze per Anziani dell'Alto Adige

Moritz Schwienbacher

(unterzeichnet) (firmato)

Die Gewerkschaftsorganisationen **Le Organizzazioni Sindacali**

SAG-GS-AGO

(unterzeichnet)/(firmato)

ASGB

(unterzeichnet)/(firmato)

CGIL/AGB

(nicht unterzeichnet)/(non firmato)

SGB/CISL

(unterzeichnet)/(firmato)

UIL/SGK

(unterzeichnet)/(firmato)

NURSING UP

(unterzeichnet)/(firmato)

1.A) Arbeitsanweisung für Angestellte mit Privatgeräten	1.A) Istruzioni di lavoro per dipendenti con dispositivi propri
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.	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.
Anwendbare Normen: Verordnung (EU) 2016/679, Art. 32, sowie Vorgaben der Autorità Garante per la protezione dei dati personali *Präventionsrichtlinien der ENISA* *Präventionsrichtlinien von EUROPOL*	*Norme applicabili: Regolamento (UE) 2016/679, Art. 32, nonché specifiche dell'Autorità Garante per la protezione dei dati personali* *Linee guida ENISA* *Linee guida EUROPOL*
1. VORGABEN PRIVATGERÄTE	**1. DIRETTIVE PER L'UTILIZZO DI DISPOSITIVI PROPRI**
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.	**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.
PASSWÖRTER 1.2. Starke Passwörter schützen Systeme und Daten vor dem Zugriff durch Unberechtigte. Die Passwörter müssen den gängigen Sicherheitsstandards entsprechen.	**PASSWORD** 1.2. Password complesse proteggono sistemi e dati da accessi non autorizzati. Le password devono corrispondere agli standard attuali.
2. NUTZUNG DER VPN-VERBINDUNG	**2. UTILIZZO DELLA CONNESSIONE VPN**
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.	**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.
SICHERE IDENTIFIKATION 2.2. Die im vorhergehenden Punkt beschriebenen Zugriffe sind als streng persönlich einzustufen und die	**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.

entsprechenden Passwörter dürfen niemals an Dritte weitergegeben werden.	
3. WEITERE VORGABEN	**3. ALTRE PRESCRIZIONI**
GESCHÄFTLICHE DOKUMENTE, INFORMATIONEN UND PERSONENBEZOGENE DATEN SCHÜTZEN 3.1. 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 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 Ausdrucke sind vor unberechtigtem Zugriff zu schützen; - Nicht mehr benötigte Papierunterlagen sind zu schreddern oder sicher aufzubewahren, bis sie im Büro vernichtet werden können.	**PROTEGGERE I DATI PERSONALI E SEGRETI D'UFFICIO (DOCUMENTI, INFORMAZIONI)** 3.1. 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 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;
E-MAIL SICHER EINSETZEN 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.	**UTILIZZO SICURO DELLE MAIL** 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.
KOMMUNIKATIONS-TOOLS GEZIELT AUSWÄHLEN 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.	**SELEZIONE MIRATA DEGLI STRUMENTI DI COMUNICAZIONE** 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.
SICH VOR PHISHING UND ANDEREN BEDROHUNGEN SCHÜTZEN 3.4. Verdächtige E-Mails dürfen nicht geöffnet werden. Anhänge in Mails von unbekannten 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.	**PROTEGGETEVI DAL PHISHING E DA ALTRE MINACCE** 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.
DATENSCHUTZVERLETZUNGEN SOFORT MELDEN 3.5. Wenn Arbeitsmittel wie Dokumente oder auch Ihr PC oder Laptop verloren gehen oder	**SEGNALARE IMMEDIATAMENTE I DATA BREACH** 3.5. In caso di smarrimento di documenti oppure del PC/PC portatile laptop è necessario segnalarlo immediatamente al responsabile di reparto.

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**
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 Logifles; 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. Die Kontrollen können wie folgt zusammengefasst werden: 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 autentication, usw.)	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. Le attività di controllo possono essere così riassunte: 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 autentication, 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 GENERALSEKRETARIAT 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
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.	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.
Anwendbare Normen: Verordnung (EU) 2016/679, Art. 32, sowie Vorgaben der Autorità Garante per la protezione dei dati personali *Präventionsrichtlinien der ENISA* *Präventionsrichtlinien von EUROPOL*	*Norme applicabili: Regolamento (UE) 2016/679, Art. 32, nonché specifiche dell'Autorità Garante per la protezione dei dati personali* *Linee guida ENISA* *Linee guida EUROPOL*
1. VORGABEN BETRIEBSGERÄTE	**1. DIRETTIVE PER L'UTILIZZO DI DISPOSITIVI AZIENDALI**
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.	**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.
PASSWÖRTER 1.2. Starke Passwörter schützen Systeme und Daten vor dem Zugriff durch Unberechtigte. Die Passwörter müssen den gängigen Sicherheitsstandards des Arbeitgebers/Verantwortlichen entsprechen.	**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.
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 Arbeitsgebers 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.	**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.

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.	**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.
2. WEITERE VORGABEN	**2. ALTRE PRESCRIZIONI**
GESCHÄFTLICHE DOKUMENTE, 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 Ausdrucke sind vor unberechtigtem Zugriff zu schützen; - Nicht mehr benötigte Papierunterlagen sind zu schreddern oder sicher aufzubewahren, bis sie im Büro vernichtet werden können.	**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.
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.	**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.
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.	**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.
SICH VOR PHISHING UND ANDEREN BEDROHUNGEN SCHÜTZEN 2.4. Verdächtige E-Mails dürfen nicht geöffnet werden. Anhänge in Mails von unbekannten 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.	**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.
DATENSCHUTZVERLETZUNGEN SOFORT MELDEN	**SEGNALARE IMMEDIATAMENTE I DATA BREACH**

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**
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 Logifles; 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. Die Kontrollen können wie folgt zusammengefasst werden: 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 autentication, usw.)	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.** Le attività di controllo possono essere così riassunte: 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 autentication, 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 GENERALSEKRETARIAT AUF DEREN ZUGEWIESENE E-MAIL-ADRESSE ÜBERMITTELT. DIE ÜBERMITTLUNG WIRD PROTOKOLLIERT.	**LE PRESENTI ISTRUZIONI DI LAVORO VENGONO INVIATE DALLA SEGRETERIA GENERALEA 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.)
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.	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.
Anwendbare Normen: Verordnung (EU) 2016/679, Art. 32, sowie Vorgaben der Autorità Garante per la protezione dei dati personali	*Norme applicabili: Regolamento (UE) 2016/679, Art. 32, nonché specifiche dell'Autorità Garante per la protezione dei dati personali*
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. 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. Es ist wichtig, dass die Verwendung von Cloud-Lösungen so verwaltet wird, dass eine ordnungsgemäße Verwendung gewährleistet ist.	**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. 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. È essenziale che l'uso di soluzioni cloud sia gestito per garantire che venga utilizzato in modo appropriato.
ZUGRIFFE AUF DIE CLOUD-LÖSUNGEN 1.2. Der Zugriff auf Daten des Arbeitgebers/Verantwortlichen darf ausschließlich 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.	**ACCESSO ALLE SOLUZIONI CLOUD** 1.2. È possibile accedere ai dati del datore di lavoro/Titolare di trattamento solo 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.
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	**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

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. 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 offen 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.: rassische 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.	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. 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.
FERNZUGRIFF (unter Einhaltung der Vorgabe laut Punkt 1.2) 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: • 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.	**ACCESSO DA REMOTO (nel rispetto di quanto stabilito al punto 1.2)** 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: • 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;

• Schützen Sie Ihre Konten besagter Cloud-Lösungen und Ihre Passwwörter 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 unbekannten 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.	• 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.
KONTROLLEN 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	**VERIFICHE** 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

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. Die Kontrollen können wie folgt zusammengefasst werden: 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 autentication, usw.)	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. Le attività di controllo possono essere così riassunte: 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 autentication, ecc.)
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 GENERALSEKRETARIAT AUF DEREN ZUGEWIESENE E-MAIL-ADRESSE ÜBERMITTELT. DIE ÜBERMITTLUNG WIRD PROTOKOLLIERT.	**LE PRESENTI ISTRUZIONI DI LAVORO VENGONO INVIATE DALLA SEGRETERIA GENERALEA TUTTI I DIPENDENTI SULL'INDIRIZZO E-MAIL A LORO ASSEGNATO. L'INVIO VIENE PROTOCOLLATO.**

2.A) Anweisung für die politischen Vertreter und andere körperschaftsexterne Personen (z.B. Mitglieder von Kommissionen, usw.) mit Privatgeräten	2.A) Istruzioni per i referenti politici e altre persone esterne all'ente (p.es. membri di commissioni, ecc.) con dispositivi propri
Diese Anweisung 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 in der Körperschaft Büro als auch im Homeoffice/außerhalb der Körperschaft.	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 all'interno dell'ente, sia in sede di telelavoro/al di fuori dell'ente.
Anwendbare Normen: Verordnung (EU) 2016/679, Art. 32, sowie Vorgaben der Autorità Garante per la protezione dei dati personali *Präventionsrichtlinien der ENISA* *Präventionsrichtlinien von EUROPOL*	*Norme applicabili: Regolamento (UE) 2016/679, Art. 32, nonché specifiche dell'Autorità Garante per la protezione dei dati personali* *Linee guida ENISA* *Linee guida EUROPOL*
1. VORGABEN PRIVATGERÄTE	**1. DIRETTIVE PER L'UTILIZZO DI DISPOSITIVI PROPRI**
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.	**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.
PASSWÖRTER 1.2. Starke Passwörter schützen Systeme und Daten vor dem Zugriff durch Unberechtigte. Die Passwörter müssen den gängigen Sicherheitsstandards entsprechen.	**PASSWORD** 1.2. Password complesse proteggono sistemi e dati da accessi non autorizzati. Le password devono corrispondere agli standard attuali.
2. NUTZUNG DER VPN-VERBINDUNG	**2. UTILIZZO DELLA CONNESSIONE VPN**
VPN VERBINDUNG 2.1. Der Zugriff auf Daten der Körperschaft darf **ausschließlich** über eine sichere, von der Körperschaft bereitgestellte, VPN-Verbindung/Remote Desktop erfolgen; davon abgesehen ist der Zugang mittels der von der Körperschaft zugelassenen Cloud-Lösungen/webbasierten Anwendungen erlaubt (vgl. hierzu die eigenen "*Verwendungsvorgaben 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.	**CONNESSIONE VPN** 2.1. È possibile accedere ai dati dell'ente **solo** tramite una connessione VPN sicura/Remote Desktop messa a disposizione dall'ente stesso; oltre a ciò, è ammesso l'accesso tramite soluzioni Cloud/applicazioni basate sul web autorizzate dall'ente (cfr. in merito le specifiche "*Linee guida 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.
SICHERE IDENTIFIKATION	**IDENTIFICAZIONE SICURA**

2.2. Die im vorhergehenden Punkt beschriebenen Zugriffe sind als streng persönlich einzustufen und die entsprechenden Passwörter dürfen niemals an Dritte weitergegeben werden.	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.
3. WEITERE VORGABEN	**3. ALTRE PRESCRIZIONI**
GESCHÄFTLICHE DOKUMENTE, INFORMATIONEN UND PERSONENBEZOGENE DATEN SCHÜTZEN 3.1. Dokumente, Informationen und personenbezogene Daten sind zu schützen, auch im Homeoffice/außerhalb der Körperschaft: - die Inhalte des erteilten Auftrags und der 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 Ausdrucke sind vor unberechtigtem Zugriff zu schützen; - Nicht mehr benötigte Papierunterlagen sind zu schreddern oder sicher aufzubewahren, bis sie in der Körperschaft vernichtet werden können.	**PROTEGGERE I DATI PERSONALI E SEGRETI D'UFFICIO (DOCUMENTI, INFORMAZIONI)** 3.1. Documenti, informazioni e dati personali devono essere protetti, anche durante il telelavoro/al di fuori dell'ente: - I contenuti dell'incarico e delle istruzioni 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 presso l'ente.
E-MAIL SICHER EINSETZEN 3.2. Private und geschäftliche E-Mails (= die Körperschaft betreffend) 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.	**UTILIZZO SICURO DELLE MAIL** 3.2. Le e-mail private e aziendali (= riguardanti l'ente) 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.
KOMMUNIKATIONS-TOOLS GEZIELT AUSWÄHLEN 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 der Körperschaft.	**SELEZIONE MIRATA DEGLI STRUMENTI DI COMUNICAZIONE** 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 dell'ente.
SICH VOR PHISHING UND ANDEREN BEDROHUNGEN SCHÜTZEN 3.4. Verdächtige E-Mails dürfen nicht geöffnet werden. Anhänge in Mails von unbekannten 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.	**PROTEGGETEVI DAL PHISHING E DA ALTRE MINACCE** 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.
DATENSCHUTZVERLETZUNGEN SOFORT MELDEN	**SEGNALARE IMMEDIATAMENTE I DATA BREACH**

3.5. Wenn Arbeitsmittel wie Dokumente oder auch Ihr PC oder Laptop verloren gehen oder abhandenkommen, ist dies umgehend dem IT-Verantwortlichen der Körperschaft zu melden.	3.5. In caso di smarrimento di documenti oppure del PC/PC portatile laptop è necessario segnalarlo immediatamente al responsabile del reparto informatico dell'ente.
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**
4.1. Die Tätigkeiten der politischen Vertreter bzw. der anderen körperschaftsexternen Personen für die Körperschaft, welche mittels Privatgeräten abgewickelt werden, werden nicht systematisch und kontinuierlich überwacht, die Systemadministratoren der Körperschaft (auch in Zusammenarbeit mit der EDV-Abteilung des Gemeindenverbandes) können die Tätigkeiten auf den Servern der Körperschaft (z.B. die erzeugten Logifles; 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. Die Kontrollen können wie folgt zusammengefasst werden: 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 autentication, usw.)	4.1 Le attività dei referenti politici rispettivamente delle altre persone esterne all'ente, svolte per l'ente utilizzando dispositivi propri, non sono soggetti a una sorveglianza sistematica e continua, ma gli amministratori di sistema dell'ente (anche in collaborazione con la Ripartizione EDP del Consorzio dei Comuni) possono monitorare o indagare le attività sui server dell'ente (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. Le attività di controllo possono essere così riassunte: 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 autentication, ecc.)

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 ANWEISUNG WIRD ALLEN POLITISCHEN VERTRETERN UND DEN ANDEREN KÖRPERSCHAFTSEXTERNEN PERSONEN VOM GENERALSEKRETARIAT AUF DEREN ZUGEWIESENE ODER MITGETEILTE E-MAIL-ADRESSE ÜBERMITTELT. DIE ÜBERMITTLUNG WIRD PROTOKOLLIERT.	**LE PRESENTI ISTRUZIONI VENGONO INVIATE DALLA SEGRETERIA GENERALE A TUTTI I REFERENTI POLITICI E ALLE ALTRE PERSONE ESTERNE ALL'ENTE SULL'INDIRIZZO E-MAIL LORO ASSEGNATO O DA LORO COMUNICATO. L'INVIO VIENE PROTOCOLLATO.**

operativer Vermerk:	nota operativa:
Es wird daran erinnert, dass neben den politischen Vertretern auch etwaige andere körperschaftsexterne Personen (z.B. Mitglieder von Kommissionen, usw.) personenbezogene Daten im Namen und Auftrag des Verantwortlichen (= Körperschaft) verarbeiten. Daher müssen diese – genau wie dies für die politischen Vertreter gilt (vgl. hierzu GemInfo: „FAQ und operative Hinweise des DPO RA Dr. P. Recla") – vom Bürgermeister/Bezirkspräsidenten einen Auftrag zur Datenverarbeitung gemäß Art. 29 der EU-Verordnung Nr. 679/2016 erhalten.	Si ricorda, che oltre ai referenti politici anche eventuali persone esterne all'ente (p.es. membri di commissioni, ecc.) trattano dati personali in nome e per conto del Titolare (= l'ente). Per questo motivo essi devono – parallelamente a quanto avviene per i referenti politici (cfr. GemInfo: "FAQ e indicazioni operative del DPO Avv. P. Recla") – essere incaricati ex art. 29 del regolamento UE n. 679/2016 dal Sindaco/Presidente della Comunità comprensoriale al trattamento dei dai personali

2.B) Anweisung für die politischen Vertreter und andere körperschaftsexterne Personen (z.B. Mitglieder von Kommissionen, usw.) mit Betriebsgeräten	2.B) Istruzioni per i referenti politici e altre persone esterne all'ente (p.es. membri di commissioni, ecc.) con dispositivi aziendali
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 in der Körperschaft Büro als auch im Homeoffice/außerhalb der Körperschaft.	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 all'interno dell'ente, sia in sede di telelavoro/al di fuori dell'ente.
Anwendbare Normen: Verordnung (EU) 2016/679, Art. 32, sowie Vorgaben der Autorità Garante per la protezione dei dati personali *Präventionsrichtlinien der ENISA* *Präventionsrichtlinien von EUROPOL*	*Norme applicabili: Regolamento (UE) 2016/679, Art. 32, nonché specifiche dell'Autorità Garante per la protezione dei dati personali* *Linee guida ENISA* *Linee guida EUROPOL*
1. VORGABEN BETRIEBSGERÄTE	**1. DIRETTIVE PER L'UTILIZZO DI DISPOSITIVI AZIENDALI**
UPDATES 1.1. Die Körperschaft 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 politischen Vertreter bzw. von der körperschaftsexternen Person regelmäßig geprüft werden, ob Updates zur Verfügung stehen. Diese sind zu installieren. Mit Updates werden meist Sicherheitsschwachstellen behoben.	**UPDATES** 1.1. L'ente 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 referente politico rispettivamente dalla persona esterna all'ente deve essere controllato regolarmente se sono disponibili aggiornamenti. Questi devono essere installati. Gli aggiornamenti vengono solitamente utilizzati per correggere le vulnerabilità della sicurezza.
PASSWÖRTER 1.2. Starke Passwörter schützen Systeme und Daten vor dem Zugriff durch Unberechtigte. Die Passwörter müssen den gängigen Sicherheitsstandards der Körperschaft entsprechen.	**PASSWORD** 1.2. Password complesse proteggono sistemi e dati da accessi non autorizzati. Le password devono corrispondere alle prescrizioni dell'Ente.
VPN VERBINDUNG 1.3. Der Zugriff auf Daten der Körperschaft darf – abgesehen klarerweise von all jenen Fällen, in denen das Betriebsgerät direkt (z.B. mittels Ethernet-Kabel) am Netz der Körperschaft angeschlossen wird – **ausschließlich** über eine sichere, von der Körperschaft bereitgestellte, VPN-Verbindung /Remote Desktop erfolgen; davon abgesehen ist der Zugang mittels der von der Körperschaft zugelassenen Cloud-Lösungen/webbasierten Anwendungen erlaubt (vgl. hierzu die eigenen "*Verwendungsvorgaben in Bezug auf Cloud-Lösungen*"). Die Zugangsdaten werden Ihnen vorab mitgeteilt.	**CONNESSIONE VPN** 1.3. È possibile accedere ai dati dell'ente – e fatti comunque salvi tutti i casi in cui il dispositivo aziendale venga collegato direttamente alla rete dell'ente (p.es. tramite cavo Ethernet) – **solo** tramite una connessione VPN sicura/Remote Desktop messa a disposizione dall'ente; oltre a ciò, è ammesso l'accesso tramite soluzioni Cloud/applicazioni basate sul web autorizzate dall'ente (cfr. in merito le specifiche "*Linee guida 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,

Es ist keine Verwendung von VPN- oder anderen – z.B. Tor – ähnlichen Diensten zur Verschleierung des Standortes, ob beabsichtigt oder nicht, zulässig.	
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.	**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.
2. WEITERE VORGABEN	**2. ALTRE PRESCRIZIONI**
GESCHÄFTLICHE DOKUMENTE, INFORMATIONEN UND PERSONENBEZOGENE DATEN SCHÜTZEN 2.1. Dokumente, Informationen und personenbezogene Daten sind zu schützen, auch im Homeoffice/außerhalb der Körperschaft: - Die Inhalte des erteilten Auftrags und der 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 Ausdrucke sind vor unberechtigtem Zugriff zu schützen; - Nicht mehr benötigte Papierunterlagen sind zu schreddern oder sicher aufzubewahren, bis sie in der Körperschaft vernichtet werden können.	**PROTEGGERE I DATI PERSONALI E SEGRETI D'UFFICIO (DOCUMENTI, INFORMAZIONI)** 2.1. Documenti, informazioni e dati personali devono essere protetti, anche durante il telelavoro/al di fuori dell'ente: - I contenuti dell'incarico e delle istruzioni 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 presso l'ente.
E-MAIL SICHER EINSETZEN 2.2. Die Nutzung privater E-Mail-Konten für die geschäftliche Kommunikation (= die Körperschaft betreffend) ist verboten. Geschäftliche E-Mails dürfen nicht auf private Konten weitergeleitet werden.	**UTILIZZO SICURO DELLE MAIL** 2.2. È vietato utilizzare account di posta elettronica privati per la comunicazione aziendale (= riguardante l'ente). Le e-mail aziendali non devono essere inoltrate ad account personali.
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 der Körperschaft.	**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 dell'ente.
SICH VOR PHISHING UND ANDEREN BEDROHUNGEN SCHÜTZEN 2.4. Verdächtige E-Mails dürfen nicht geöffnet werden. Anhänge in Mails von unbekannten 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.	**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.

DATENSCHUTZVERLETZUNGEN SOFORT MELDEN 2.5. Wenn Arbeitsmittel wie Dokumente oder auch Ihr PC verloren gehen oder abhandenkommen, ist dies umgehend dem IT-Verantwortlichen der Körperschaft zu melden.	**SEGNALARE IMMEDIATAMENTE I DATA BREACH** 2.5. In caso di smarrimento di documenti o apparecchiature di lavoro è necessario segnalarlo immediatamente al responsabile del reparto informatico dell'ente.
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**
3.1. Die Tätigkeiten der politischen Vertreter bzw. der anderen körperschaftsexternen Personen mittels Betriebsgeräten werden nicht systematisch und kontinuierlich überwacht, die Systemadministratoren der Körperschaft (auch in Zusammenarbeit mit der EDV-Abteilung des Gemeindenverbandes) können die Nutzung (= die Tätigkeiten auf den Servern der Körperschaft, so z.B. die erzeugten Logifles; 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. Die Kontrollen können wie folgt zusammengefasst werden: 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 autentication, usw.)	3.1 Le attività dei referenti politici rispettivamente delle altre persone esterne all'ente svolte tramite dispositivi aziendali non sono soggetti a una sorveglianza sistematica e continua, ma gli amministratori di sistema dell'ente (anche in collaborazione con la Ripartizione EDP del Consorzio dei Comuni) possono monitorare o indagare sull'utilizzo (= le attività sui server dell'ente, 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. Le attività di controllo possono essere così riassunte: 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 autentication, ecc.)

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 ANWEISUNG WIRD ALLEN POLITISCHEN VERTRETERN UND DEN ANDEREN KÖRPERSCHAFTSEXTERNEN PERSONEN VOM GENERALSEKRETARIAT AUF DEREN ZUGEWIESENE ODER MITGETEILTE E-MAIL-ADRESSE ÜBERMITTELT. DIE ÜBERMITTLUNG WIRD PROTOKOLLIERT.	**LE PRESENTI ISTRUZIONI VENGONO INVIATE DALLA SEGRETERIA GENERALE A TUTTI I REFERENTI POLITICI E ALLE ALTRE PERSONE ESTERNE ALL'ENTE SULL'INDIRIZZO E-MAIL LORO ASSEGNATO O DA LORO COMUNICATO. L'INVIO VIENE PROTOCOLLATO.**

operativer Vermerk:	nota operativa:
Es wird daran erinnert, dass neben den politischen Vertretern auch etwaige andere körperschaftsexterne Personen (z.B. Mitglieder von Kommissionen, usw.) personenbezogene Daten im Namen und Auftrag des Verantwortlichen (= Körperschaft) verarbeiten. Daher müssen diese – genau wie dies für die politischen Vertreter gilt (vgl. hierzu GemInfo: „FAQ und operative Hinweise des DPO RA Dr. P. Recla") – vom Bürgermeister/Bezirkspräsidenten einen Auftrag zur Datenverarbeitung gemäß Art. 29 der EU-Verordnung Nr. 679/2016 erhalten.	Si ricorda, che oltre ai referenti politici anche eventuali persone esterne all'ente (p.es. membri di commissioni, ecc.) trattano dati personali in nome e per conto del Titolare (= l'ente). Per questo motivo essi devono – parallelamente a quanto avviene per i referenti politici (cfr. GemInfo: "FAQ e indicazioni operative del DPO Avv. P. Recla") – essere incaricati ex art. 29 del regolamento UE n. 679/2016 dal Sindaco/Presidente della Comunità comprensoriale al trattamento dei dai personali

2.C) Verwendungsvorgaben für die politischen Vertreter und andere körperschaftsexterne Personen (z.B. Mitglieder von Kommissionen, usw.) in Bezug auf von der Körperschaft zugelassene Cloud-Lösungen (mittels Verschlüsselung gesicherte Verbindungen, z.B. SSL, IPsec, ecc.)	2.C) Linee guida per i referenti politici e altre persone esterne all'ente (p.es. membri di commissioni, ecc.) per l'utilizzo di soluzioni cloud autorizzate dall'ente (tramite connessioni crittografate, p.es. SSL, IPsec, ecc.)
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 in der Körperschaft Büro als auch im Homeoffice/außerhalb der Körperschaft.	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 all'interno dell'ente, sia in sede di telelavoro/al di fuori dell'ente.
Anwendbare Normen: Verordnung (EU) 2016/679, Art. 32, sowie Vorgaben der Autorità Garante per la protezione dei dati personali	*Norme applicabili: Regolamento (UE) 2016/679, Art. 32, nonché specifiche dell'Autorità Garante per la protezione dei dati personali*
ANWENDUNGSBEREICH 1.1. Die politischen Vertreter bzw. die anderen körperschaftsexternen Personen müssen diese Richtlinien bei jeder Verwendung von von der Körperschaft zugelassenen Cloud-Lösungen befolgen, um die einschlägigen Richtlinien und Gesetze einzuhalten. Sie müssen immer daran denken, dass sie bei der Verwendung dieser Cloud-Lösungen einen Service nutzen, der ihnen für geschäftliche Zwecke der Körperschaft zur Verfügung gestellt wird. 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 den politischen Vertretern bzw. den anderen körperschaftsexternen Personen und der Körperschaft ermöglichen. Es ist wichtig, dass die Verwendung von Cloud-Lösungen so verwaltet wird, dass eine ordnungsgemäße Verwendung gewährleistet ist.	**APPLICABILITÀ** 1.1. I referenti politici rispettivamente le altre persone esterne all'ente devono seguire queste linee guida ogni volta che utilizzano le soluzioni cloud autorizzate dall'ente, al fine di conformarsi alla politica e alla legislazione pertinenti. Loro devono sempre ricordare che quando utilizzano queste soluzioni cloud, stanno utilizzando un servizio fornito loro per scopi lavorativi riferiti all'ente. 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 i referenti politici rispettivamente le altre persone esterne all'ente e l'ente stesso. È essenziale che l'uso di soluzioni cloud sia gestito per garantire che venga utilizzato in modo appropriato.
ZUGRIFFE AUF DIE CLOUD-LÖSUNGEN 1.2. Der Zugriff auf Daten der Körperschaft darf ausschließlich 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.	**ACCESSO ALLE SOLUZIONI CLOUD** 1.2. È possibile accedere ai dati dell'ente solo 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.

REGELN

1.3. Die politischen Vertreter bzw. die anderen körperschaftsexternen Personen sind verpflichtet, die Vertraulichkeit personenbezogener Daten oder anderer Informationen, die ihnen im Laufe ihres politischen Mandats bzw. ihrer Funktion/Aufgabe zur Verfügung stehen, zu wahren und die Informationen nur zur Erfüllung ihrer Rolle zu verwenden. Bei der Verwendung von Cloud-Lösungen müssen die politischen Vertreter bzw. die anderen körperschaftsexternen Personen sicherstellen, dass sie alle Risiken der Offenlegung dieser Informationen über ihren rechtlichen Zweck hinaus berücksichtigen und verwalten.

Die politischen Vertreter bzw. die anderen körperschaftsexternen Personen 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 offen über das Internet für jedermann zugänglich macht. Private Clouds werden hingegen von Unternehmen/der Körperschaft selbst betrieben und ausschließlich den eigenen Nutzern zugänglich gemacht. Die Körperschaft 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.: rassische 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 der Körperschaft 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.

REGOLE

1.3. I referenti politici rispettivamente le altre persone esterne all'ente hanno il dovere di mantenere la riservatezza su dati personali o informazioni di altro tipo che diventa loro disponibile nel corso del loro mandato politico rispettivamente incarico/compito e di utilizzare le informazioni solo per lo svolgimento del loro ruolo. Quando si utilizzano le soluzioni cloud, i referenti politici rispettivamente le altre persone esterne all'ente devono assicurarsi di considerare e gestire qualsiasi rischio di divulgazione di queste informazioni oltre il loro scopo legale.

I referenti politici rispettivamente le altre persone esterne all'ente 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/dagli enti stessi e rese disponibili esclusivamente ai propri utenti. L'ente 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 dell'ente, 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.

FERNZUGRIFF (unter Einhaltung der Vorgabe laut Punkt 1.2)

1.4. Cloud-Lösungen sind von Natur aus von überall zugänglich. Die politischen Vertreter bzw. die anderen körperschaftsexternen Personen, die von zu Hause oder von einem anderen Ort aus, der nicht Teil des Netzwerks der Körperschaft ist, auf Cloud-Lösungen zugreifen, müssen Folgendes beachten:

• Die Inhalte des erteilten Auftrags und der 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.
• Schützen Sie Ihre Konten besagter Cloud-Lösungen und Ihre Passwwörter 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 unbekannten 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 der Körperschaft 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 von der Körperschaft 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,

ACCESSO DA REMOTO (nel rispetto di quanto stabilito al punto 1.2)

1.4. Le soluzioni cloud, per la loro stessa natura, sono accessibili da qualsiasi luogo. I referenti politici rispettivamente le altre persone esterne all'ente che accedono alle soluzioni cloud da casa o da un'altra posizione, che non fa parte della rete dell'ente devono:

• I contenuti dell'incarico e delle istruzioni ex art. 29 regolamento UE n. 679/2016 per il trattamento dei dati personali sono da rispettare anche nell'utilizzo delle soluzioni cloud;

• 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 dell'ente.
• 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 dall'ente), 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.

Informationen und personenbezogenen Daten zu speichern.	
KONTROLLEN 1.5. Die Körperschaft 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 der Körperschaft (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 Zugriffe, technische Probleme, usw. 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. Die Kontrollen können wie folgt zusammengefasst werden: 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 autentication, usw.)	**VERIFICHE** 1.5. L'ente ha la supervisione in relazione alle soluzioni cloud, inclusa l'eventuale registrazione di comunicazioni aziendali. Non si procede ad una verifica una sorveglianza sistematica e continua dell'accesso alle soluzioni cloud, ma gli amministratori di sistema dell'ente (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 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. Le attività di controllo possono essere così riassunte: 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 autentication, ecc.)
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 ANWEISUNG WIRD ALLEN POLITISCHEN VERTRETERN UND DEN ANDEREN KÖRPERSCHAFTSEXTERNEN PERSONEN VOM GENERALSEKRETARIAT AUF DEREN ZUGEWIESENE ODER MITGETEILTE E-MAIL-ADRESSE ÜBERMITTELT. DIE ÜBERMITTLUNG WIRD PROTOKOLLIERT.	**LE PRESENTI ISTRUZIONI VENGONO INVIATE DALLA SEGRETERIA GENERALE A TUTTI I REFERENTI POLITICI E ALLE ALTRE PERSONE ESTERNE ALL'ENTE SULL'INDIRIZZO E-MAIL LORO ASSEGNATO O DA LORO COMUNICATO. L'INVIO VIENE PROTOCOLLATO.**

operativer Vermerk:	nota operativa:
Es wird daran erinnert, dass neben den politischen Vertretern auch etwaige andere körperschaftsexterne Personen (z.B. Mitglieder von Kommissionen, usw.) personenbezogene Daten im Namen und Auftrag des Verantwortlichen (= Körperschaft) verarbeiten. Daher müssen diese – genau wie dies für die politischen Vertreter gilt (vgl. hierzu GemInfo: „FAQ und operative Hinweise des DPO RA Dr. P. Recla") – vom Bürgermeister/Bezirkspräsidenten einen Auftrag zur Datenverarbeitung gemäß Art. 29 der EU-Verordnung Nr. 679/2016 erhalten.	Si ricorda, che oltre ai referenti politici anche eventuali persone esterne all'ente (p.es. membri di commissioni, ecc.) trattano dati personali in nome e per conto del Titolare (= l'ente). Per questo motivo essi devono – parallelamente a quanto avviene per i referenti politici (cfr. GemInfo: "FAQ e indicazioni operative del DPO Avv. P. Recla") – essere incaricati ex art. 29 del regolamento UE n. 679/2016 dal Sindaco/Presidente della Comunità comprensoriale al trattamento dei dai personali