

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

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

abhandenkommen, ist dies umgehend dem Vorgesetzten zu melden.	
Zusätzliche Informationen zum Thema IT-Sicherheit im Privathaushalt finden Sie unter: <a href="https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold">https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold</a>	Altre informazioni riguardanti la sicurezza informatica a casa Vostra trovate sotto: <a href="https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold">https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold</a>
<b>4. KONTROLLEN</b>	<b>4. VERIFICHE</b>
<p>4.1. Die Tätigkeiten der Mitarbeiter für den Arbeitgeber/Verantwortlichen, welche mittels Privatgeräten abgewickelt werden, werden nicht systematisch und kontinuierlich überwacht, die Systemadministratoren des Arbeitgebers/Verantwortlichen (auch in Zusammenarbeit mit der EDV-Abteilung des Gemeindenverbandes) können die Tätigkeiten auf den Servern des Arbeitgebers/Verantwortlichen (z.B. die erzeugten Logfiles; die Privatgeräte selbst werden klarerweise nicht kontrolliert) aber überwachen oder untersuchen; dies geschieht nur, um die Einhaltung der relevanten Richtlinien zu bestätigen und mögliche Sicherheitsverletzungen, unbefugte Zugriffe, technische Probleme, usw. zu untersuchen und nicht für die Zwecke der Überwachung der Arbeitstätigkeit. Die Verwendung von Logfiles erfolgt immer mit einer festgelegten zeitlichen Begrenzung (kurze Frist) und Tracing-Tätigkeit erfolgt nur bei allfälligen Verdachtsmomenten, in manueller Form und üblicherweise in direkter Zusammenarbeit mit dem betroffenen Nutzer.</p> <p>Die Kontrollen können wie folgt zusammengefasst werden:</p> <ol style="list-style-type: none"> <li>1) Kontrolle/Einschränkung auf der Grundlage der IP der Region, aus welcher der Verbindungszugriff erfolgt (ev. auch für weitere Dienste)</li> <li>2) Kontrolle/Einschränkung auf der Grundlage der IP für den E-Mail-Zugang</li> <li>3) Befähigung bestimmter IP's in Zusammenhang mit kritischen Diensten (z.B. Meldedaten an die Polizeikräfte)</li> <li>4) mobile device management (betrifft nur die mobilen Betriebsgeräte)</li> <li>5) zusätzliche Kontrollformen, die im Laufe der Zeit, zur best practice des Sektors zählen werden (z.B. conditional access und multifactor authentication, usw.)</li> </ol>	<p>4.1 Le attività dei dipendenti, svolte per datore di lavoro/Titolare utilizzando dispositivi propri, non sono soggetti a una sorveglianza sistematica e continua, ma gli amministratori di sistema del datore di lavoro/Titolare (anche in collaborazione con la Ripartizione EDP del Consorzio dei Comuni) possono monitorare o indagare le attività sui server dell' datore di lavoro/Titolare (p.es. i logfile 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 logfile è limitato a tempistiche prefissate (breve termine) e l'attività di tracing viene espletata solo nei casi di dubbio, in forma manuale e di regola in collaborazione diretta con l'utente interessato.</p> <p>Le attività di controllo possono essere così riassunte:</p> <ol style="list-style-type: none"> <li>1) controllo/restrizione su base IP della regione di accesso per collegamento VPN (ev. anche per altri servizi)</li> <li>2) controllo/restrizione su base IP per l'accesso alle e-mail</li> <li>3) abilitazione su IP specifici dei servizi critici (es. anagrafe alle forze dell'ordine)</li> <li>4) mobile device management (riguarda solo i dispositivi mobili aziendali)</li> <li>5) ulteriori forme di controllo che costituiranno, nel continuo, la best practice di settore (p.es. conditional access e multifactor authentication, ecc.)</li> </ol>
<b>5. RECHT AUF NICHTERREICHBARKEIT</b>	<b>5. DIRITTO ALLA DISCONNESSIONE</b>
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;
<b>BEI ZWEIFELN KONTAKTIEREN SIE UNS GERNE!</b>	<b>IN CASO DI DUBBI NON ESITATE A CONTATTARCI!</b>
Version 01.02.2022	Versione 01.02.2022
Letzte Abänderung: 01.02.2022	Ultima modifica: 01.02.2022
<b>DIE VORLIEGENDE ARBEITSANWEISUNG WIRD ALLEN MITARBEITERN VOM GENERALSEKRETARIAT AUF DEREN ZUGEWIESENE E-MAIL-ADRESSE ÜBERMITTELT. DIE ÜBERMITTLUNG WIRD PROTOKOLLIERT.</b>	<b>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.</b>

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

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

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

Angestellten u.a. die Ruhepausen mit Anrecht auf Unterbrechung der Verbindung vor.	prevede, tra l'altro, i tempi di riposo con diritto alla disconnessione;
<b>BEI ZWEIFELN KONTAKTIEREN SIE UNS GERNE!</b>	<b>IN CASO DI DUBBI NON ESITATE A CONTATTARCI!</b>
Version 01.02.2022	Versione 01.02.2022
Letzte Abänderung: 01.02.2022	Ultima modifica: 01.02.2022
<b>DIE VORLIEGENDE ARBEITSANWEISUNG WIRD ALLEN MITARBEITERN VOM GENERALSEKRETARIAT AUF DEREN ZUGEWIESENE E-MAIL-ADRESSE ÜBERMITTELT. DIE ÜBERMITTLUNG WIRD PROTOKOLLIERT.</b>	<b>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.</b>



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

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;

<ul style="list-style-type: none"> <li>• Schützen Sie Ihre Konten besagter Cloud-Lösungen und Ihre Passwörter vor Offenlegung. Zugangspasswörter sind geheim zu halten.</li> <li>• Verwenden Sie sichere Passwörter und ändern Sie Passwörter, wenn Sie den Verdacht haben, dass jemand sie kennt.</li> <li>• Beachten Sie die Versuche Dritter, Kennwörter oder andere Anmeldeinformationen zu erhalten, z. B. per E-Mail oder Telefon.</li> <li>• Aktivieren Sie den Bildschirmschoner oder das Sperrsystem, wenn Sie sich nicht in der Nähe von Arbeitsstationen oder Geräten befinden.</li> <li>• Seien Sie vorsichtig bei der Verbindung mit öffentlichen oder unbekanntem Wi-Fi-Netzwerken. Seien Sie sich stets bewusst, dass Verbindungen zwischen dem Remote-Standort und Cloud-Lösungen ein potenzielles Risiko darstellen.</li> <li>• Beachten Sie, dass alle elektronischen Kommunikationsaktivitäten des Unternehmens Eigentum des Arbeitgebers/Verantwortlichen sind/werden.</li> <li>• Seien Sie sich bewusst, dass Sie für die Folgen verantwortlich sind, wenn der Fernzugriff missbraucht wird.</li> <li>• Benachrichtigen Sie sofort den Systemadministrator bei Verdacht auf Diebstahl oder Missbrauch Ihres Kontos.</li> <li>• 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.</li> <li>• Melden Sie sich nach Gebrauch jeder einzelnen verwendeten Cloud-Lösung immer sofort und ordnungsgemäß ab.</li> <li>• Auf dem für den Zugang zur Cloud-Lösung verwendeten Gerät sind keine Dokumente, Informationen und personenbezogenen Daten zu speichern.</li> </ul>	<ul style="list-style-type: none"> <li>• Proteggere i propri account delle soluzioni cloud e le relative password dalla divulgazione. Le password di accesso devono essere tenute segrete. <ul style="list-style-type: none"> <li>• Utilizzare password complesse e modificare le password se si sospetta che qualcuno le conosca.</li> </ul> </li> <li>• Essere consapevoli di tentativi da parti terze di ottenere password o altre credenziali di accesso, ad esempio tramite e-mail o truffe telefoniche.</li> <li>• Attivare lo screen saver o il sistema di blocco se si è lontani da workstation o dispositivi.</li> <li>• 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</li> <li>• Tenere presente che tutte le attività di comunicazione elettronica aziendale sono/diventano proprietà del datore di lavoro/Titolare.</li> <li>• Comprendere che hanno la responsabilità delle conseguenze nel caso in cui l'accesso remoto venga utilizzato in modo improprio.</li> <li>• Avvisare immediatamente l'amministratore di sistema in caso di sospetto furto o uso improprio del proprio account di accesso remoto.</li> <li>• 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.</li> <li>• Disconnettersi sempre regolarmente ed immediatamente da tutte le singole soluzioni cloud al termine dell'uso.</li> <li>• Sul dispositivo utilizzato per l'accesso alla soluzione cloud documenti, informazioni e dati personali non devono mai essere salvati.</li> </ul>
<p><b>KONTROLLEN</b></p> <p>1.5. Der Arbeitgeber/Verantwortliche hat die Aufsicht über die Cloud-Lösungen, einschließlich der etwaigen Aufzeichnung von Kommunikationen. Der Zugriff auf die Cloud-Lösungen wird nicht systematisch und kontinuierlich überwacht, die Systemadministratoren des Arbeitgebers/Verantwortlichen (auch in Zusammenarbeit mit der EDV-Abteilung des Gemeindenverbandes) können die Nutzung aber überwachen oder untersuchen; dies geschieht nur, um die Einhaltung der relevanten Richtlinien zu bestätigen und mögliche Sicherheitsverletzungen, unbefugte</p>	<p><b>VERIFICHE</b></p> <p>1.5. Il datore di lavoro/Titolare ha la supervisione in relazione alle soluzioni cloud, inclusa l'eventuale registrazione di comunicazioni aziendali. Non si procede ad una sorveglianza sistematica e continua dell'accesso alle soluzioni cloud, ma gli amministratori di sistema del datore di lavoro/Titolare (anche in collaborazione con la Ripartizione EDP del Consorzio dei Comuni) possono monitorare o indagare sull'utilizzo; ciò si verificherà solo per confermare la conformità ai requisiti della politica pertinente e per indagare su possibili violazioni della sicurezza, accessi</p>

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

<p><b>2.A) Anweisung für die politischen Vertreter und andere körperschaftsexterne Personen (z.B. Mitglieder von Kommissionen, usw.) mit Privatgeräten</b></p>	<p><b>2.A) Istruzioni per i referenti politici e altre persone esterne all'ente (p.es. membri di commissioni, ecc.) con dispositivi propri</b></p>
<p>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.</p>	<p>Le presenti istruzioni hanno lo scopo di contribuire a garantire il rispetto delle disposizioni di legge sul trattamento dei dati personali e della sicurezza informatica e, in particolare, che possa essere garantita la riservatezza, l'integrità e la disponibilità di documenti e informazioni aziendali/d'ufficio e dei collegati dati personali, sia all'interno dell'ente, sia in sede di telelavoro/al di fuori dell'ente.</p>
<p><i>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</i></p>	<p><i>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</i></p>
<p><b>1. VORGABEN PRIVATGERÄTE</b></p>	<p><b>1. DIRETTIVE PER L'UTILIZZO DI DISPOSITIVI PROPRI</b></p>
<p><b>UPDATES</b> 1.1. Die Betriebssysteme und Programme auf PCs und Laptops sind immer auf dem aktuellen Stand zu halten. Deshalb muss regelmäßig geprüft werden, ob Updates zur Verfügung stehen. Diese sind zu installieren. Mit Updates werden meist Sicherheitsschwachstellen behoben.</p>	<p><b>UPDATES</b> 1.1. I sistemi operativi e i programmi su PC, e PC portatili/laptops devono essere sempre tenuti aggiornati. Pertanto, deve essere controllato regolarmente se sono disponibili aggiornamenti. Questi devono essere installati. Gli aggiornamenti vengono solitamente utilizzati per correggere le vulnerabilità della sicurezza.</p>
<p><b>PASSWÖRTER</b> 1.2. Starke Passwörter schützen Systeme und Daten vor dem Zugriff durch Unberechtigte. Die Passwörter müssen den gängigen Sicherheitsstandards entsprechen.</p>	<p><b>PASSWORD</b> 1.2. Password complesse proteggono sistemi e dati da accessi non autorizzati. Le password devono corrispondere agli standard attuali.</p>
<p><b>2. NUTZUNG DER VPN-VERBINDUNG</b></p>	<p><b>2. UTILIZZO DELLA CONNESSIONE VPN</b></p>
<p><b>VPN VERBINDUNG</b> 2.1. Der Zugriff auf Daten der Körperschaft darf <b>ausschließlich</b> 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.</p>	<p><b>CONNESSIONE VPN</b> 2.1. È possibile accedere ai dati dell'ente <b>solo</b> 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.</p>
<p><b>SICHERE IDENTIFIKATION</b></p>	<p><b>IDENTIFICAZIONE SICURA</b></p>

<p>2.2. Die im vorhergehenden Punkt beschriebenen Zugriffe sind als streng persönlich einzustufen und die entsprechenden Passwörter dürfen niemals an Dritte weitergegeben werden.</p>	<p>2.2. Gli accessi descritti al punto precedente sono da intendersi come strettamente personali e le relative password non devono mai essere comunicate a terzi.</p>
<p><b>3. WEITERE VORGABEN</b></p>	<p><b>3. ALTRE PRESCRIZIONI</b></p>
<p><b>GESCHÄFTLICHE INFORMATIONEN UND DATEN SCHÜTZEN</b></p> <p><b>DOKUMENTE, PERSONENBEZOGENE DATEN SCHÜTZEN</b></p> <p>3.1. Dokumente, Informationen und personenbezogene Daten sind zu schützen, auch im Homeoffice/außerhalb der Körperschaft:</p> <ul style="list-style-type: none"> <li>- 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;</li> <li>- Zugangspasswörter sind geheim zu halten;</li> <li>- Interne Informationen und personenbezogene Daten sind vor Unberechtigten, auch Familienmitgliedern, zu schützen;</li> <li>- Der Bildschirm ist vor Einsicht zu schützen;</li> <li>- Auf dem privaten Gerät sind keine Dokumente, Informationen und personenbezogenen Daten zu speichern;</li> <li>- Papierdossiers und Ausdrücke sind vor unberechtigtem Zugriff zu schützen;</li> <li>- Nicht mehr benötigte Papierunterlagen sind zu schreddern oder sicher aufzubewahren, bis sie in der Körperschaft vernichtet werden können.</li> </ul>	<p><b>PROTEGGERE I DATI PERSONALI E SEGRETI D'UFFICIO (DOCUMENTI, INFORMAZIONI)</b></p> <p>3.1. Documenti, informazioni e dati personali devono essere protetti, anche durante il telelavoro/al di fuori dell'ente:</p> <ul style="list-style-type: none"> <li>- 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;</li> <li>- Le password di accesso devono essere tenute segrete;</li> <li>- Le informazioni interne e i dati personali devono essere protetti da persone non autorizzate, compresi i familiari;</li> <li>- Lo schermo deve essere protetto dalla vista di terzi,</li> <li>- Sul dispositivo privato documenti, informazioni e dati personali non devono mai essere salvati;</li> <li>- I fascicoli cartacei e le stampe devono essere protetti dall'accesso non autorizzato;</li> <li>- 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.</li> </ul>
<p><b>E-MAIL SICHER EINSETZEN</b></p> <p>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.</p>	<p><b>UTILIZZO SICURO DELLE MAIL</b></p> <p>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.</p>
<p><b>KOMMUNIKATIONS-TOOLS AUSWÄHLEN</b></p> <p><b>GEZIELT</b></p> <p>3.3. Neben dem Telefon und den E-Mails werden auch Messengers und Videokonferenzdienste eingesetzt. Informationen zu den Diensten erhalten Sie auf Anfrage beim IT-Verantwortlichen der Körperschaft.</p>	<p><b>SELEZIONE MIRATA DEGLI STRUMENTI DI COMUNICAZIONE</b></p> <p>3.3. Oltre al telefono e alla posta elettronica, vengono utilizzati anche servizi di messaggistica e videoconferenza. Le informazioni sui servizi sono disponibili su richiesta presso il responsabile del reparto informatico dell'ente.</p>
<p><b>SICH VOR PHISHING UND ANDEREN BEDROHUNGEN SCHÜTZEN</b></p> <p>3.4. Verdächtige E-Mails dürfen nicht geöffnet werden. Anhänge in Mails von unbekanntem Absendern dürfen nicht angeklickt werden. Im Zweifel ist die Absenderin oder der Absender per Telefon zu kontaktieren, damit sie oder er den Inhalt der E-Mail bestätigen kann.</p>	<p><b>PROTEGGETEVI DAL PHISHING E DA ALTRE MINACCE</b></p> <p>3.4. Le e-mail sospette non devono essere aperte. Non fare clic sugli allegati nelle e-mail di mittenti sconosciuti. In caso di dubbio, il mittente deve essere contattato telefonicamente in modo che possa confermare il contenuto dell'e-mail.</p>
<p><b>DATENSCHUTZVERLETZUNGEN MELDEN</b></p> <p><b>SOFORT</b></p>	<p><b>SEGNALARE IMMEDIATAMENTE I DATA BREACH</b></p>

<p>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.</p>	<p>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.</p>
<p>Zusätzliche Informationen zum Thema IT-Sicherheit im Privathaushalt finden Sie unter:  <a href="https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold">https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold</a></p>	<p>Altre informazioni riguardanti la sicurezza informatica a casa Vostra trovate sotto:  <a href="https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold">https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold</a></p>
<p><b>4. KONTROLLEN</b></p>	<p><b>4. VERIFICHE</b></p>
<p>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 Logfiles; die Privatgeräte selbst werden klarerweise nicht kontrolliert) aber überwachen oder untersuchen; dies geschieht nur, um die Einhaltung der relevanten Richtlinien zu bestätigen und mögliche Sicherheitsverletzungen, unbefugte Zugriffe, technische Probleme, usw. zu untersuchen und nicht für die Zwecke der Überwachung der Arbeitstätigkeit. Die Verwendung von Logfiles erfolgt immer mit einer festgelegten zeitlichen Begrenzung (kurze Frist) und Tracing-Tätigkeit erfolgt nur bei allfälligen Verdachtsmomenten, in manueller Form und üblicherweise in direkter Zusammenarbeit mit dem betroffenen Nutzer.  Die Kontrollen können wie folgt zusammengefasst werden:</p> <ol style="list-style-type: none"> <li>1) Kontrolle/Einschränkung auf der Grundlage der IP der Region, aus welcher der Verbindungszugriff erfolgt (ev. auch für weitere Dienste)</li> <li>2) Kontrolle/Einschränkung auf der Grundlage der IP für den E-Mail-Zugang</li> <li>3) Befähigung bestimmter IP's in Zusammenhang mit kritischen Diensten (z.B. Meldedaten an die Polizeikräfte)</li> <li>4) mobile device management (betrifft nur die mobilen Betriebsgeräte)</li> <li>5) zusätzliche Kontrollformen, die im Laufe der Zeit, zur best practice des Sektors zählen werden (z.B. conditional access und multifactor authentication, usw.)</li> </ol>	<p>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.</p> <p>Le attività di controllo possono essere così riassunte:</p> <ol style="list-style-type: none"> <li>1) controllo/restrizione su base IP della regione di accesso per collegamento VPN (ev. anche per altri servizi)</li> <li>2) controllo/restrizione su base IP per l'accesso alle e-mail</li> <li>3) abilitazione su IP specifici dei servizi critici (es. anagrafe alle forze dell'ordine)</li> <li>4) mobile device management (riguarda solo i dispositivi mobili aziendali)</li> <li>5) ulteriori forme di controllo che costituiranno, nel continuo, la best practice di settore (p.es. conditional access e multifactor authentication, ecc.)</li> </ol>

<b>BEI ZWEIFELN KONTAKTIEREN SIE UNS GERNE!</b>	<b>IN CASO DI DUBBI NON ESITATE A CONTATTARCI!</b>
Version 01.02.2022	Versione 01.02.2022
Letzte Abänderung: 01.02.2022	Ultima modifica: 01.02.2022
<b>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.</b>	<b>LE PRESENTI ISTRUZIONI VENGONO INVIAE 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.</b>

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 dati personali



<p>2.B) Anweisung für die politischen Vertreter und andere körperschaftsexterne Personen (z.B. Mitglieder von Kommissionen, usw.) mit Betriebsgeräten</p>	<p>2.B) Istruzioni per i referenti politici e altre persone esterne all'ente (p.es. membri di commissioni, ecc.) con dispositivi aziendali</p>
<p>Diese Arbeitsanweisung soll dazu beitragen, dass die Rechtsvorschriften zur Verarbeitung personenbezogener Daten und zum Schutz der informationstechnischen Systeme eingehalten werden und insbesondere die Vertraulichkeit, Integrität und Verfügbarkeit von betrieblichen/geschäftlichen Dokumenten und Informationen sowie damit zusammenhängenden personenbezogenen Daten gewährleistet werden kann, sowohl in der Körperschaft Büro als auch im Homeoffice/außerhalb der Körperschaft.</p>	<p>Le presenti istruzioni di lavoro hanno lo scopo di contribuire a garantire il rispetto delle disposizioni di legge sul trattamento dei dati personali e della sicurezza informatica e, in particolare, che possa essere garantita la riservatezza, l'integrità e la disponibilità di documenti e informazioni aziendali/d'ufficio e dei collegati dati personali, sia all'interno dell'ente, sia in sede di telelavoro/al di fuori dell'ente.</p>
<p>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</p>	<p>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</p>
<p><b>1. VORGABEN BETRIEBSGERÄTE</b></p>	<p><b>1. DIRETTIVE PER L'UTILIZZO DI DISPOSITIVI AZIENDALI</b></p>
<p><b>UPDATES</b> 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.</p>	<p><b>UPDATES</b> 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.</p>
<p><b>PASSWÖRTER</b> 1.2. Starke Passwörter schützen Systeme und Daten vor dem Zugriff durch Unberechtigte. Die Passwörter müssen den gängigen Sicherheitsstandards der Körperschaft entsprechen.</p>	<p><b>PASSWORD</b> 1.2. Password complesse proteggono sistemi e dati da accessi non autorizzati. Le password devono corrispondere alle prescrizioni dell'Ente.</p>
<p><b>VPN VERBINDUNG</b> 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 – <b>ausschließlich</b> 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.</p>	<p><b>CONNESSIONE VPN</b> 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) – <b>solo</b> 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,</p>

<p>Es ist keine Verwendung von VPN- oder anderen – z.B. Tor – ähnlichen Diensten zur Verschleierung des Standortes, ob beabsichtigt oder nicht, zulässig.</p>	
<p><b>SICHERE IDENTIFIKATION</b> 1.4. Die im vorhergehenden Punkt beschriebenen Zugriffe sind als streng persönlich einzustufen und die entsprechenden Passwörter dürfen niemals an Dritte weitergegeben werden.</p>	<p><b>IDENTIFICAZIONE SICURA</b> 1.4. Gli accessi descritti al punto precedente sono da intendersi come strettamente personali e le relative password non devono mai essere comunicate a terzi.</p>
<p><b>2. WEITERE VORGABEN</b></p>	<p><b>2. ALTRE PRESCRIZIONI</b></p>
<p><b>GESCHÄFTLICHE DOKUMENTE, INFORMATIONEN UND PERSONENBEZOGENE DATEN SCHÜTZEN</b> 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 Ausdrücke sind vor unberechtigtem Zugriff zu schützen; - Nicht mehr benötigte Papierunterlagen sind zu schreddern oder sicher aufzubewahren, bis sie in der Körperschaft vernichtet werden können.</p>	<p><b>PROTEGGERE I DATI PERSONALI E SEGRETI D'UFFICIO (DOCUMENTI, INFORMAZIONI)</b> 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.</p>
<p><b>E-MAIL SICHER EINSETZEN</b> 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.</p>	<p><b>UTILIZZO SICURO DELLE MAIL</b> 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.</p>
<p><b>KOMMUNIKATIONS-TOOLS GEZIELT AUSWÄHLEN</b> 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.</p>	<p><b>SELEZIONE MIRATA DEGLI STRUMENTI DI COMUNICAZIONE</b> 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.</p>
<p><b>SICH VOR PHISHING UND ANDEREN BEDROHUNGEN SCHÜTZEN</b> 2.4. Verdächtige E-Mails dürfen nicht geöffnet werden. Anhänge in Mails von unbekanntem Absender dürfen nicht angeklickt werden. Im Zweifel ist die Absenderin oder der Absender per Telefon zu kontaktieren, damit sie oder er den Inhalt der E-Mail bestätigen kann.</p>	<p><b>PROTEGGETEVI DAL PHISHING E DA ALTRE MINACCE</b> 2.4. Le e-mail sospette non devono essere aperte. Non fare clic sugli allegati nelle e-mail di mittenti sconosciuti. In caso di dubbio, il mittente deve essere contattato telefonicamente in modo che possa confermare il contenuto dell'e-mail.</p>

<p><b>DATENSCHUTZVERLETZUNGEN SOFORT MELDEN</b></p> <p>2.5. Wenn Arbeitsmittel wie Dokumente oder auch Ihr PC verloren gehen oder abhandenkommen, ist dies umgehend dem IT-Verantwortlichen der Körperschaft zu melden.</p>	<p><b>SEGNALARE IMMEDIATAMENTE I DATA BREACH</b></p> <p>2.5. In caso di smarrimento di documenti o apparecchiature di lavoro è necessario segnalarlo immediatamente al responsabile del reparto informatico dell'ente.</p>
<p>Zusätzliche Informationen zum Thema IT-Sicherheit im Privathaushalt finden Sie unter:  <a href="https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold">https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold</a></p>	<p>Altre informazioni riguardanti la sicurezza informatica a casa Vostra trovate sotto:  <a href="https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold">https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold</a></p>
<p><b>3. KONTROLLEN</b></p>	<p><b>3. VERIFICHE</b></p>
<p>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 Logfiles; Überprüfung anhand des installierten mobile device managements; bei Bedarf auch direkte Überprüfung des Betriebsgerätes selbst; usw.) aber überwachen oder untersuchen; dies geschieht nur, um die Einhaltung der relevanten Richtlinien zu bestätigen und mögliche Sicherheitsverletzungen, unbefugte Zugriffe, technische Probleme, usw. zu untersuchen und nicht für die Zwecke der Überwachung der Arbeitstätigkeit. Die Verwendung von Logfiles erfolgt immer mit einer festgelegten zeitlichen Begrenzung (kurze Frist) und Tracing-Tätigkeit erfolgt nur bei allfälligen Verdachtsmomenten, in manueller Form und üblicherweise in direkter Zusammenarbeit mit dem betroffenen Nutzer.</p> <p>Die Kontrollen können wie folgt zusammengefasst werden:</p> <ol style="list-style-type: none"> <li>1) Kontrolle/Einschränkung auf der Grundlage der IP der Region, aus welcher der Verbindungszugriff erfolgt (ev. auch für weitere Dienste)</li> <li>2) Kontrolle/Einschränkung auf der Grundlage der IP für den E-Mail-Zugang</li> <li>3) Befähigung bestimmter IP's in Zusammenhang mit kritischen Diensten (z.B. Meldedaten an die Polizeikräfte)</li> <li>4) mobile device management für die mobilen Betriebsgeräte</li> <li>5) zusätzliche Kontrollformen, die im Laufe der Zeit, zur best practice des Sektors zählen werden (z.B. conditional access und multifactor authentication, usw.)</li> </ol>	<p>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 logfile 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 logfile è limitato a tempistiche prefissate (breve termine) e l'attività di tracing viene espletata solo nei casi di dubbio, in forma manuale e di regola in collaborazione diretta con l'utente interessato.</p> <p>Le attività di controllo possono essere così riassunte:</p> <ol style="list-style-type: none"> <li>1) controllo/restrizione su base IP della regione di accesso per collegamento VPN (ev. anche per altri servizi)</li> <li>2) controllo/restrizione su base IP per l'accesso alle e-mail</li> <li>3) abilitazione su IP specifici dei servizi critici (es. anagrafe alle forze dell'ordine)</li> <li>4) mobile device management per i dispositivi mobili aziendali</li> <li>5) ulteriori forme di controllo che costituiranno, nel continuo, la best practice di settore (p.es. conditional access e multifactor authentication, ecc.)</li> </ol>

<b>BEI ZWEIFELN KONTAKTIEREN SIE UNS GERNE!</b>	<b>IN CASO DI DUBBI NON ESITATE A CONTATTARCI!</b>
Version 01.02.2022	Versione 01.02.2022
Letzte Abänderung: 01.02.2022	Ultima modifica: 01.02.2022
<b>DIE VORLIEGENDE ANWEISUNG WIRD ALLEN POLITISCHEN VERTRETEREN UND DEN ANDEREN KÖRPERSCHAFTSEXTERNEN PERSONEN VOM GENERALSEKRETARIAT AUF DEREN ZUGEWIESENE ODER MITGETEILTE E-MAIL-ADRESSE ÜBERMITTELT. DIE ÜBERMITTLUNG WIRD PROTOKOLLIERT.</b>	<b>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.</b>

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 dati personali

<p>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.)</p>	<p>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.)</p>
<p>Diese Vorgaben sollen dazu beitragen, dass die Rechtsvorschriften zur Verarbeitung personenbezogener Daten und zum Schutz der informationstechnischen Systeme eingehalten werden und insbesondere die Vertraulichkeit, Integrität und Verfügbarkeit von betrieblichen/geschäftlichen Dokumenten und Informationen sowie damit zusammenhängenden personenbezogenen Daten gewährleistet werden kann, sowohl in der Körperschaft Büro als auch im Homeoffice/außerhalb der Körperschaft.</p>	<p>Le presenti istruzioni hanno lo scopo di contribuire a garantire il rispetto delle disposizioni di legge sul trattamento dei dati personali e della sicurezza informatica e, in particolare, che possa essere garantita la riservatezza, l'integrità e la disponibilità di documenti e informazioni aziendali/d'ufficio e dei collegati dati personali, sia all'interno dell'ente, sia in sede di telelavoro/al di fuori dell'ente.</p>
<p><i>Anwendbare Normen: Verordnung (EU) 2016/679, Art. 32, sowie Vorgaben der Autorità Garante per la protezione dei dati personali</i></p>	<p><i>Norme applicabili: Regolamento (UE) 2016/679, Art. 32, nonché specifiche dell'Autorità Garante per la protezione dei dati personali</i></p>
<p><b>ANWENDUNGSBEREICH</b></p> <p>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.</p> <p>Die Bereitstellung von Cloud-Lösungen zielt darauf ab, die Produktivität durch den Einsatz moderner Bürotechnologien zu verbessern, die eine größere Mobilität sowie eine effiziente Zusammenarbeit und Kommunikation zwischen den politischen Vertretern bzw. den anderen körperschaftsexternen Personen und der Körperschaft ermöglichen.</p> <p>Es ist wichtig, dass die Verwendung von Cloud-Lösungen so verwaltet wird, dass eine ordnungsgemäße Verwendung gewährleistet ist.</p>	<p><b>APPLICABILITÀ</b></p> <p>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.</p> <p>La fornitura delle soluzioni cloud mira a migliorare la produttività attraverso l'uso di moderne tecnologie per l'ufficio che consentono una maggiore mobilità e una collaborazione e comunicazione efficiente tra i referenti politici rispettivamente le altre persone esterne all'ente e l'ente stesso.</p> <p>È essenziale che l'uso di soluzioni cloud sia gestito per garantire che venga utilizzato in modo appropriato.</p>
<p><b>ZUGRIFFE AUF DIE CLOUD-LÖSUNGEN</b></p> <p>1.2. Der Zugriff auf Daten der Körperschaft darf <u>ausschließlich</u> a) direkt über dessen Netzwerk oder b) über eine sichere Verbindung erfolgen. Die Zugangsdaten werden Ihnen vorab mitgeteilt. Es ist keine Verwendung von VPN- oder anderen – z.B. Tor – ähnlichen Diensten zur Verschleierung des Standortes, ob beabsichtigt oder nicht, zulässig.</p>	<p><b>ACCESSO ALLE SOLUZIONI CLOUD</b></p> <p>1.2. È possibile accedere ai dati dell'ente <u>solo</u> direttamente tramite a) la sua rete oppure b) tramite una connessione sicura. Le verranno forniti le credenziali di accesso in anticipo. Non è ammesso l'utilizzo intenzionale o meno, di VPN- o altri servizi – p.es. Tor – funzionali ad occultare la localizzazione.</p>

## 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 Passwörter vor Offenlegung. Zugangspasswörter sind geheim zu halten.
- Verwenden Sie sichere Passwörter und ändern Sie Passwörter, wenn Sie den Verdacht haben, dass jemand sie kennt.
- Beachten Sie die Versuche Dritter, Kennwörter oder andere Anmeldeinformationen zu erhalten, z. B. per E-Mail oder Telefon.
- Aktivieren Sie den Bildschirmschoner oder das Sperrsystem, wenn Sie sich nicht in der Nähe von Arbeitsstationen oder Geräten befinden.
- Seien Sie vorsichtig bei der Verbindung mit öffentlichen oder unbekanntem Wi-Fi-Netzwerken. Seien Sie sich stets bewusst, dass Verbindungen zwischen dem Remote-Standort und Cloud-Lösungen ein potenzielles Risiko darstellen.
- Beachten Sie, dass alle elektronischen Kommunikationsaktivitäten des Unternehmens Eigentum 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.	
<p><b>KONTROLLEN</b></p> <p>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.</p> <p>Die Kontrollen können wie folgt zusammengefasst werden:</p> <ol style="list-style-type: none"> <li>1) Kontrolle/Einschränkung auf der Grundlage der IP der Region, aus welcher der Verbindungszugriff erfolgt (ev. auch für weitere Dienste)</li> <li>2) Kontrolle/Einschränkung auf der Grundlage der IP für den E-Mail-Zugang</li> <li>3) Befähigung bestimmter IP's in Zusammenhang mit kritischen Diensten (z.B. Meldedaten an die Polizeikräfte)</li> <li>4) mobile device management für die mobilen Betriebsgeräte</li> <li>5) zusätzliche Kontrollformen, die im Laufe der Zeit, zur best practice des Sektors zählen werden (z.B. conditional access und multifactor authentication, usw.)</li> </ol>	<p><b>VERIFICHE</b></p> <p>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.</p> <p>Le attività di controllo possono essere così riassunte:</p> <ol style="list-style-type: none"> <li>1) controllo/restrizione su base IP della regione di accesso per collegamento VPN (ev. anche per altri servizi)</li> <li>2) controllo/restrizione su base IP per l'accesso alle e-mail</li> <li>3) abilitazione su IP specifici dei servizi critici (es. anagrafe alle forze dell'ordine)</li> <li>4) mobile device management per i dispositivi mobili aziendali</li> <li>5) ulteriori forme di controllo che costituiranno, nel continuo, la best practice di settore (p.es. conditional access e multifactor authentication, ecc.)</li> </ol>
<b>BEI ZWEIFELN KONTAKTIEREN SIE UNS GERNE!</b>	<b>IN CASO DI DUBBI NON ESITATE A CONTATTARCI!</b>
Version 01.02.2022	Versione 01.02.2022
Letzte Abänderung: 01.02.2022	Ultima modifica: 01.02.2022
<p><b>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.</b></p>	<p><b>LE PRESENTI ISTRUZIONI VENGONO INVIAE 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.</b></p>



operativer Vermerk:	nota operativa:
<p>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.</p>	<p>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 dati personali</p>

