| **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*<br>*Präventionsrichtlinien der ENISA*<br>*Präventionsrichtlinien von EUROPOL* | *Norme applicabili: Regolamento (UE) 2016/679, Art. 32, nonché specifiche dell'Autorità Garante per la protezione dei dati personali*<br>*Linee guida ENISA*<br>*Linee guida EUROPOL* |
| **1. VORGABEN BETRIEBSGERÄTE** | **1. DIRETTIVE PER L'UTILIZZO DI DISPOSITIVI AZIENDALI** |
| **UPDATES**<br>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**<br>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**<br>1.2. Starke Passwörter schützen Systeme und Daten vor dem Zugriff durch Unberechtigte. Die Passwörter müssen den gängigen Sicherheitsstandards der Körperschaft entsprechen. | **PASSWORD**<br>1.2. Password complesse proteggono sistemi e dati da accessi non autorizzati. Le password devono corrispondere alle prescrizioni dell'Ente. |
| **VPN VERBINDUNG**<br>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**<br>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.<br>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**<br>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**<br>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**<br>2.1. Dokumente, Informationen und personenbezogene Daten sind zu schützen, auch im Homeoffice/außerhalb der Körperschaft:<br>- 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;<br>- Zugangspasswörter sind geheim zu halten;<br>- Interne Informationen und personenbezogene Daten sind vor Unberechtigten, auch Familienmitgliedern, zu schützen;<br>- Der Bildschirm ist vor Einsicht zu schützen;<br>- Auf dem Betriebsgerät sind keine personenbezogenen Daten privater Natur zu speichern;<br>- Papierdossiers und Ausdrucke sind vor unberechtigtem Zugriff zu schützen;<br>- 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)**<br>2.1. Documenti, informazioni e dati personali devono essere protetti, anche durante il telelavoro/al di fuori dell'ente:<br>- 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;<br>- Le password di accesso devono essere tenute segrete;<br>- Le informazioni interne e i dati personali devono essere protetti da persone non autorizzate, compresi i familiari;<br>- Lo schermo deve essere protetto dalla vista di terzi,<br>- Sul dispositivo aziendale non devono essere salvati dati di natura privata;<br>- I fascicoli cartacei e le stampe devono essere protetti dall'accesso non autorizzato;<br>- 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**<br>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**<br>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**<br>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**<br>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**<br>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**<br>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**<br>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**<br>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.<br>Die Kontrollen können wie folgt zusammengefasst werden:<br>1) Kontrolle/Einschränkung auf der Grundlage der IP der Region, aus welcher der Verbindungszugriff erfolgt (ev. auch für weitere Dienste)<br>2) Kontrolle/Einschränkung auf der Grundlage der IP für den E-Mail-Zugang<br>3) Befähigung bestimmter IP's in Zusammenhang mit kritischen Diensten (z.B. Meldedaten an die Polizeikräfte)<br>4) mobile device management für die mobilen Betriebsgeräte<br>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.<br>Le attività di controllo possono essere così riassunte:<br>1) controllo/restrizione su base IP della regione di accesso per collegamento VPN (ev. anche per altri servizi)<br>2) controllo/restrizione su base IP per l'accesso alle e-mail<br>3) abilitazione su IP specifici dei servizi critici (es. anagrafe alle forze dell'ordine)<br>4) mobile device management per i dispositivi mobili aziendali<br>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 |