VERWENDUNGSVORGABEN FÜR DIE ANGESTELLTEN IN BEZUG AUF BETRIEBLICH ZUGELASSENE CLOUD-LÖSUNGEN (MITTELS VERSCHLÜSSELUNG GESICHERTE VERBINDUNGEN, Z.B. SSL, IPSEC, ECC.)

LINEE GUIDA PER DIPENDENTI PER L'UTILIZZO DI SOLUZIONI CLOUD AUTORIZZATE DALL'AZIENDA (TRAMITE CONNESSIONI CRITTOGRAFATE, P.ES. SSL, IPSEC, ECC.)

Diese Vorgaben sollen dazu beitragen, dass die Rechtsvorschriften zur Verarbeitung personenbezogener Daten und zum Schutz der informationstechnischen Systeme eingehalten werden und insbesondere die Vertraulichkeit, Integrität und Verfügbarkeit von betrieblichen/geschäftlichen Dokumenten und Informationen sowie damit zusammenhängenden personenbezogenen Daten gewährleistet werden kann, sowohl am Arbeitsplatz im Büro als auch im Homeoffice.

Le presenti istruzioni hanno lo scopo di contribuire a garantire il rispetto delle disposizioni di legge sul trattamento dei dati personali e della sicurezza informatica e, in particolare, che possa essere garantita la riservatezza, l'integrità e la disponibilità di documenti e informazioni aziendali/d'ufficio e dei collegati dati personali, sia sul posto di lavoro in ufficio, sia in sede di telelavoro.

Anwendbare Normen: Verordnung (EU) 2016/679, Art. 32, sowie Vorgaben der Autorità Garante per la protezione dei dati personali

Norme applicabili: Regolamento (UE) 2016/679, Art. 32, nonché specifiche dell'Autorità Garante per la protezione dei dati personali

ANWENDUNGSBERICHT

1.1. Alle Mitarbeiter müssen diese Richtlinien bei jeder Verwendung von betrieblich zugelassenen Cloud-Lösungen befolgen, um die einschlägigen Richtlinien und Gesetze einzuhalten. Mitarbeiter müssen immer daran denken, dass sie bei der Verwendung dieser Cloud-Lösungen einen Service nutzen, der ihnen für geschäftliche Zwecke zur Verfügung gestellt wird.

Die Bereitstellung von Cloud-Lösungen zielt darauf ab, die Produktivität durch den Einsatz moderner Bürotechnologien zu verbessern, die eine größere Mobilität sowie eine effiziente Zusammenarbeit und Kommunikation zwischen Mitarbeitergruppen ermöglichen.

Es ist wichtig, dass die Verwendung von Cloud-Lösungen so verwaltet wird, dass eine ordnungsgemäße Verwendung gewährleistet ist.

APPLICABILITÀ

1.1. Tutti i dipendenti devono seguire queste linee guida ogni volta che utilizzano le soluzioni cloud autorizzate dall'azienda, al fine di conformarsi alla politica e alla legislazione pertinenti. I dipendenti devono sempre ricordare che quando utilizzano queste soluzioni cloud, stanno utilizzando un servizio fornito loro per scopi lavorativi.

La fornitura delle soluzioni cloud mira a migliorare la produttività attraverso l'uso di moderne tecnologie per l'ufficio che consentono una maggiore mobilità e una collaborazione e comunicazione efficiente tra gruppi di personale.

È essenziale che l'uso di soluzioni cloud sia gestito per garantire che venga utilizzato in modo appropriato.

ZUGRIFFE AUF DIE CLOUD-LÖSUNGEN

1.2. Der Zugriff auf Daten des Arbeitgebers/Verantwortlichen darf ausschließlich;

ACCESSO ALLE SOLUZIONI CLOUD

1.2. È possibile accedere ai dati del datore di lavoro/Titolare di trattamento solo direttamente tramite:

a) über das Informatiknetzwerk der Gemeinde;

b) über eine sichere VPN Verbindung erfolgen. Die Zugangsdaten werden Ihnen vorab mitgeteilt.

Es ist keine Verwendung von anderen VPN- oder anderen - z.B. Tor oder ähnlichen Diensten zur Verschleierung des Standortes, ob beabsichtigt oder nicht, zulässig.

a) la rete informatica del Comune

b) tramite una connessione sicura VPN. Le verranno forniti le credenziali di accesso in anticipo.

Non è ammesso l'utilizzo intenzionale o meno, di altri servizi VPN- o altro – p.es. Tor – funzionali ad occultare la localizzazione.

REGELN

1.3. Alle Mitarbeiter sind verpflichtet, die Vertraulichkeit personenbezogener Daten oder anderer Informationen, die ihnen im Laufe ihrer Arbeitstätigkeit zur Verfügung stehen, zu wahren und die Informationen nur zur Erfüllung ihrer 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

REGOLE

1.3. Tutti dipendenti hanno il dovere di mantenere la riservatezza su dati personali o informazioni di altro tipo che diventa loro disponibile nel corso del loro impiego e di utilizzare le informazioni solo per lo svolgimento della loro prestazione lavorativa. Quando 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.

Personendaten während einer Cloud-Videokonferenz (z.B. Hochladen eines Dokuments in den Chatverlauf, usw.) stellt eine nicht zu unterschätzende informatische Risikoquelle da.

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.

• Schützen Sie Ihre Konten besagter Cloud-Lösungen und Ihre Passwwörter vor Offenlegung. Zugangspasswörter sind geheim zu halten.

• Verwenden Sie sichere Passwörter und ändern Sie Passwörter, wenn Sie den Verdacht haben, dass jemand sie kennt.

• Beachten Sie die Versuche Dritter, Kennwörter oder andere Anmeldeinformationen zu erhalten, z. B. per E-Mail oder Telefon.

• Aktivieren Sie den Bildschirmschoner oder das Sperrsystem, wenn Sie sich nicht in der Nähe von Arbeitsstationen oder Geräten befinden.

• Seien Sie vorsichtig bei der Verbindung mit öffentlichen oder unbekannten Wi-Fi-Netzwerken. Seien Sie sich stets bewusst, dass Verbindungen zwischen dem Remote-Standort und Cloud-Lösungen ein potenzielles Risiko darstellen.

• Beachten Sie, dass alle elektronischen Kommunikationsaktivitäten des Unternehmens Eigentum des Arbeitgebers/Verantwortlichen sind/werden.

• Seien Sie sich bewusst, dass Sie für die Folgen verantwortlich sind, wenn der Fernzugriff missbraucht wird.

• Benachrichtigen Sie sofort den Systemadministrator bei Verdacht auf Diebstahl oder Missbrauch Ihres Kontos.

• Melden Sie sich in Bezug auf die Cloud-Lösungen immer direkt an: stellen Sie sicher, dass

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;

• Proteggere i propri account delle soluzioni cloud e le relative password dalla divulgazione. Le password di accesso devono essere tenute segrete.

• Utilizzare password complesse e modificare le password se si sospetta che qualcuno le conosca.

• Essere consapevoli di tentativi da parti terze di ottenere password o altre credenziali di accesso, ad esempio tramite e-mail o truffe telefoniche.

• Attivare lo screen saver o il sistema di blocco se si è lontani da workstation o dispositivi.

• Diffidare della connessione a reti Wi-Fi pubbliche o sconosciute. Rimanere costantemente consapevoli del fatto che le connessioni tra la posizione remota e le soluzioni cloud determinano un potenziale rischio

• Tenere presente che tutte le attività di comunicazione elettronica aziendale sono/diventano proprietà del datore di lavoro/Titolare.

• Comprendere che hanno la responsabilità delle conseguenze nel caso in cui l'accesso remoto venga utilizzato in modo improprio.

• Avvisare immediatamente l'amministratore di sistema in caso di sospetto furto o uso improprio del proprio account di accesso remoto.

• Per quanto riguarda le soluzioni cloud, accedi sempre direttamente: assicurati di non accedere

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.

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.

• Melden Sie sich nach Gebrauch jeder einzelnen verwendeten Cloud-Lösung immer sofort und ordnungsgemäß ab.

• Disconnettersi sempre regolarmente ed immediatamente da tutte le singole soluzioni cloud al termine dell'uso.

• Auf dem für den Zugang zur Cloud-Lösung verwendeten Gerät sind keine Dokumente, Informationen und personenbezogenen Daten zu speichern.

• Sul dispositivo utilizzato per l'accesso alla soluzione cloud documenti, informazioni e dati personali non devono mai essere salvati.

KONTROLLEN

1.5. Der Arbeitgeber/Verantwortliche hat die Aufsicht über die Cloud-Lösungen, einschließlich der etwaigen Aufzeichnung von Kommunikationen. Der Zugriff auf die Cloud-Lösungen wird nicht systematisch und kontinuierlich überwacht, die System-administratoren des Arbeitgebers/ Verantwortlichen (auch in Zusammenarbeit mit der EDV-Abteilung) können die Nutzung aber überwachen oder untersuchen; dies geschieht nur, um die Einhaltung der relevanten Richtlinien zu bestätigen und mögliche Sicherheits-verletzungen, 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.

VERIFICHE

1.5. Il datore di lavoro/Titolare ha la supervisione in relazione alle soluzioni cloud, inclusa l'eventuale registrazione di comunicazioni aziendali. Non si procede ad una sorveglianza sistematica e continua dell'accesso alle soluzioni cloud, ma gli amministratori di sistema del datore di lavoro/Titolare (anche in collaborazione con la Ripartizione CED) 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.

Die Kontrollen können wie folgt zusammengefasst werden:

Le attività di controllo possono essere così riassunte:

1) Kontrolle/Einschränkung auf der Grundlage der IP der Region, aus welcher der Verbindungszugriff erfolgt (ev. auch für weitere Dienste)

1) controllo/restrizione su base IP della regione di accesso per collegamento VPN (ev. anche per altri servizi)

2) Kontrolle/Einschränkung auf der Grundlage der IP für den E-Mail-Zugang

2) controllo/restrizione su base IP per l'accesso alle e-mail

3) Befähigung bestimmter IP's in Zusammenhang mit kritischen Diensten (z.B. Meldedaten an die Polizeikräfte)

3) abilitazione su IP specifici dei servizi critici (es. anagrafe alle forze dell'ordine)

4) zusätzliche Kontrollformen, die im Laufe der Zeit, zur best practice des Sektors zählen

4) ulteriori forme di controllo che costituiranno, nel continuo, la best practice di settore (p.es.

werden (z.B. conditional access und multifactor autentication, usw.)

conditional access e multifactor autentication, ecc.)