Checkliste zu technischen Aspekten bei der Nutzung einer Cloud-Lösung zur Arbeit im Homeoffice im Bereich Rechts- & Steuerwesen

Bevor Sie Ihre Mitarbeiter ins Homeoffice schicken, sollten Sie die wichtigsten IT-Sicherheitsfragen und Datenschutzbestimmungen klären. Darum haben wir gemeinsam mit Partnern aus dem Bereich Rechts- & Steuerwesen eine Checkliste erstellt. So sehen Sie auf einen Blick, worauf Sie bei der Arbeit in den eigenen vier Wänden aus technischer und datenschutzrechtlicher Sicht achten müssen.

Checkpoint	Erläuterung	Check	Erfüllt idgard® diese Anforderung?
Ist die Internetverbindung schnell genug?	Für das effiziente Arbeiten in den eigenen vier Wänden ist eine ausreichend schnelle (Breitband-) Internetverbindung unverzichtbar – für den Datenaustausch, aber auch für Online-Meetings oder Video-Calls mit den Kollegen.		Bei schlechter Netzabdeckung können Sie über die idgard®-Apps trotzdem auf Ihren mobilen Arbeitsplatz zugreifen. Die Daten stehen Ihnen offline zur Verfügung und bearbeitete Dokumente werden synchronisiert, sobald eine Internetverbindung vorhanden ist.
Funktioniert der Cloud-Dienst ohne Installation?	Manche Dienste zur sicheren Datenübertragung lassen sich nur nutzen, wenn der Anwender vorher eine Client-Software installiert hat.		Der Cloud-Dienst idgard® ist ohne Installation, schnell und einfach als Web-App nutzbar und benötigt daher keine Installation oder Konfiguration. Für iOS und Android stehen Apps zur Verfügung, die zusätzliche Funktionen bieten.
Ist die Daten-verbindung zum Home Office sicher?	Der Zugriff auf das Firmennetzwerk sollte nur verschlüsselt erfolgen. Dies erfordert häufig eine Verbindung über VPN (Virtual Private Network).		Bei idgard® erfolgt die Verbindung ausschließlich verschlüsselt und ohne VPN-Zugang. Der Zugriff ist direkt über den Browser oder per Mobile-App (Android & iOS) möglich.

Checkliste zu technischen Aspekten bei der Nutzung einer Cloud-Lösung zur Arbeit im Homeoffice im Bereich Rechts- & Steuerwesen

Checkpoint	Erläuterung	Check	Erfüllt idgard® diese Anforderung?
Haben nur berechtigte Nutzer Zugang zum System?	Nicht nur im Homeoffice muss sichergestellt sein, dass unbefugte Nutzer keinen Zugang zum System haben. Authentifizierungssysteme erhöhen den Datenschutz zusätzlich. Hier empfiehlt sich eine Zwei-Faktor-Identifizierung, bei der z. B. ein zweites Gerät für die Feststellung der Identität eines Nutzers herangezogen wird.		Bei idgard® wird Ihnen zum Log-In eine Zwei-Faktor-Authentifizierung angeboten. Diese hilft dabei, Ihren Account und vertrauliche Daten zu schützen. Die Anmeldung erfolgt entweder über Passwort und SMS-Passcode oder über die idgard®-Login-Card (Tan-Generator im Scheckkartenformat). In idgard® arbeiten Sie mit virtuellen Projekt-arbeitsbereichen, sogenannten Boxen. In jeder Box können Sie individuelle Nutzer-Rechte vergeben, sodass sichergestellt ist, dass nur berechtigte Personen Zugriff auf die Daten in der Box haben.
Ist die IT der Mitarbeiter technisch geschützt?	Virenscanner und Firewall sollten bei Remote Work selbstverständlich sein. Ebenso tragen regelmäßige Updates relevanter Systeme zur Sicherheit bei.		In idgard® können Sie den Service „Sealed Cloud Anti-Virus“ auf Wunsch hinzubuchen. Hier erfolgt eine Überprüfung der Dateien innerhalb der versiegelten Infrastruktur. Auf die gescannten Daten haben weder der Betreiber des Rechenzentrums noch die Administratoren des Dienstes Zugriff. Auch privilegierter Zugriff, etwa durch uniscon-Mitarbeiter, ist technisch ausgeschlossen.

Checkliste zu technischen Aspekten bei der Nutzung einer Cloud-Lösung zur Arbeit im Homeoffice im Bereich Rechts- & Steuerwesen

Checkpoints	Erläuterung	Check	Erfüllt idgard® diese Anforderung?
Sind die gespeicherten Daten (und somit auch Berufsgeheimnisse) sicher?	Wer zuhause arbeitet, sollte vertrauliche Daten keinesfalls lokal abspeichern. Nutzen Sie stattdessen eine zentrale Datenablage und achten Sie auf eine verschlüsselte Verbindung. Wenn Sie einen Cloud-Dienst nutzen, sollte der Anbieter die Lösung DSGVO-konform in Deutschland hosten und dies durch entsprechende Zertifikate belegen können. Wichtig ist auch eine gute Erreichbarkeit (etwa per Hotline) bei Problemen.		idgard® erfüllt alle Anforderungen der DSGVO zum Schutz von Berufsgeheimnissen und verhindert mit technischen Mitteln den Zugriff auf Daten durch Unbefugte – auch durch den Cloud-Betreiber. Daher ist der Datenumgang über idgard® datenschutzrechtlich zulässig und auch ohne strafbewehrte Offenbarung von Berufsgeheimnissen möglich. Außerdem ist idgard® in der höchsten Schutzklasse (Schutzklasse III) für Cloud-Dienste zertifiziert nach dem Trusted Cloud Datenschutzprofil (TCDP) zertifiziert. TCDP gilt als Prüfstandard zur Einhaltung der datenschutzrechtlichen Vorschriften.
Hat der Mitarbeiter Zugriff auf seine beruflichen E-Mails?	Nicht nur für die Arbeit zuhause gilt: Berufliche E-Mails dürfen nicht auf private Postfächer umgeleitet werden. Trotzdem muss natürlich sichergestellt sein, dass der Mitarbeiter Zugriff auf berufliche E-Mails hat. Ebenso wichtig: Vertrauliche Dokumente gehören nicht in den E-Mail-Anhang! Besonders dann nicht, wenn es die Vorschriften des Unternehmens aus Gründen der Compliance verbieten.		Dank der integrierten Anwendung von idgard® in Outlook über ein Add-In versenden Sie vertrauliche Anhänge einfach und sicher via Cloud. Die Nachricht inklusive Anhänge landet dann nicht im Postfach des Empfängers, sondern geschützt in der von Ihnen gewählten Privacy Box. Der Adressat wird benachrichtigt, sobald Sie die Dateien abgelegt haben, und kann diese dann über eine verschlüsselte Verbindung herunterladen oder direkt in der Cloud bearbeiten.

Checkliste zu technischen Aspekten bei der Nutzung einer Cloud-Lösung zur Arbeit im Homeoffice im Bereich Rechts- & Steuerwesen

Checkpoint	Erläuterung	Check	Erfüllt idgard® diese Anforderung?
Benötigt der Mitarbeiter weitere Hardware oder Tools, um seine Arbeit zu erfüllen?	Genügt eine schnelle Internetverbindung bereits, oder benötigt der Mitarbeiter beispielsweise ein Firmenhandy, um auch telefonisch erreichbar zu sein? Für die Teilnahme an Calls oder Konferenzen kann sich die Anschaffung eines Headsets oder Mikrofons lohnen. Sind externe Speichergeräte, etwa für vertrauliche Dateien, nötig?		Durch die Nutzung von idgard® können Sie auf externe Speichergeräte und den persönlichen Austausch zwischen Ihnen und Ihren Mandanten vorrübergehend verzichten. Wichtige Dateien und Dokumente werden einfach in eine Box oder einen Datenraum hochgeladen und stehen dort ausgewählten Nutzern mit den entsprechenden Berechtigungen zur Verfügung. Die Chat- und Nachrichtenfunktion erleichtert die Terminabstimmung sowie die effiziente Zusammenarbeit. (Ein Headset für Calls oder Konferenzen benötigen Sie womöglich trotzdem.)

Haben wir einen Aspekt übersehen? Schreiben Sie uns eine E-Mail an marketing@uniscon.de und helfen Sie uns, diese Liste zu ergänzen!