Virtuelle Datenräume: Vertrauen und Komfort durch datenschutzkonforme Cloud-Dienste

Wie erhalten Wirtschaftsprüfer, Ärzte oder Anwälte das Vertrauen ihrer Kunden? Diese Frage stellt sich angesichts des im April verabschiedeten Bundesdatenschutzgesetzes, das die Datenschutzkontrolle für Berufsgeheimnisträger einschränkt. Wir zeigen eine mögliche Lösung – und worauf die Betroffenen unbedingt achten sollten.

Bisher unterliegen sämtliche Berufsgruppen, die personenbezogene Daten erheben oder verarbeiten, der vollen Kontrolle durch die Datenschutzbehörden. Das soll sich ändern: Am 12. Mai 2017 hat der Bundesrat das Bundesdatenschutzgesetz (BDSG) beschlossen, das am 25. Mai 2018 parallel zur EU-Datenschutz-Grundverordnung (DSGVO) in Kraft tritt. Ab diesem Datum wird auch eine neue Regelung wirksam, die Berufsgeheimnisträger betrifft – also Personen, die gemäß StGB §203 einer Schweigepflicht unterliegen. Datenschutzbehörden sollen ab dann weder Zugang zu den Geschäftsräumen noch zu den Datenverarbeitungsanlagen bekommen, in denen Berufsgeheimnisse gespeichert sind. Auch sollen sie keine Daten und Informationen darüber erhalten. Das gilt unter anderem für Ärzte, Anwälte, Apotheker, Krankenkassen, Wirtschaftsprüfer und Sozialarbeiter – für Berufsgruppen also, die das Vertrauen ihrer Kunden genießen bzw. darauf angewiesen sind

Für Berufsgeheimnisträger heißt das konkret: Sie müssen die Daten ihrer Kunden zwar weiterhin effizient schützen, wissen jedoch meist wesentlich weniger darüber Bescheid als Datenschutzbeauftragte und IT-Sicherheitsbeauftragte, welche technischen Risiken die neuen Technologien bergen.

Wie können sie also ihren Kunden die gewohnte Datensicherheit bieten? Indem sie auf technische Lösungen setzen, die ihrerseits höchste Datenschutzstandards garantieren. Geeignete Dienste sind an einer entsprechenden Zertifizierung erkennbar, die in der Regel vom TÜV oder anderen akkreditierten Organisationen vergeben wird. Ein möglicher Ansatz wäre die Verwendung revisionssicherer virtueller Datenräume für den Datenaustausch mit Kunden: diese bieten nicht nur – je nach Anbieter – erstklassigen Datenschutz, sondern sind auch einfach einzurichten, günstig, jederzeit zugänglich und verfügen darüber hinaus über unbestechliche Kontrollinstanzen.

Doch so vielfältig der Markt für Datenräume ist, so unterschiedlich sind auch die Angebote. Für welchen Datenraum Sie sich entscheiden, hängt letztlich von Ihren Anforderungen ab: Welche Features und Funktionen benötigen Sie, worauf können Sie verzichten – und was wollen Sie auf keinen Fall in Kauf nehmen?

Wir haben einige Punkte zusammengetragen, die einen virtuellen Datenraum unserer Meinung nach unbrauchbar oder zumindest übermäßig umständlich in der Handhabung machen.

Die folgenden zehn Mängel sollten Berufsgeheimnisträger bei der Wahl eines Datenraums nicht tolerieren:

- **Lange Wartezeiten bei der Einrichtung**
  Es gibt keinen guten Grund, 12 Stunden oder länger auf einen virtuellen Datenraum zu warten. Bei den meisten Anbietern steht Ihnen der Datenraum sofort zur Verfügung. So sollte das auch sein.

- **Nach oben oder unten begrenzte Teilnehmerzahl**
  Sie bestimmen selbst, wie viele Teilnehmer Sie in Ihren Datenraum einladen wollen. Datenräume, die erst ab zehn Teilnehmern oder für maximal 50 Teilnehmer geeignet sind, sind zwar selten – aber auch unnötig.

- **Server-Standort außerhalb der BRD**
  Deutschland hat weltweit die strengsten Gesetze und höchsten Standards in Sachen Datenschutz und Datensicherheit. Wir empfehlen daher, einen Anbieter zu suchen, dessen Server in Deutschland stehen.

- **Kostenpflichtiger Support**
  Der Support sollte mindestens an den Wochentagen zu den üblichen Geschäftszeiten erreichbar sein – und einen kostenlosen Rückrufservice bieten. Teure Hotlines sind heutzutage nicht mehr zeitgemäß.

- **Keine Datenschutz-Zertifizierung**
  Achten Sie auf eine aussagekräftige Datenschutz-Zertifizierung des TÜV,nach dem Trusted Cloud Datenschutzprofil (TCDP) oder auf das Europäische Datenschutzsiegel (EuroPriSe). So können Sie sich auch rechtlich absichern: Wenn Sie einen TCDP-zertifizierten Dienst wählen, haben Sie automatisch Ihre Kontrollpflicht nach dem Bundesdatenschutzgesetz erfüllt.

- **Fehlende Betreibersicherheit**
  Bei vielen Cloud-Anbietern haben der Betreiber und seine Angestellten die Möglichkeit, auf die Server – und damit theoretisch auch auf die Daten ihrer Kunden – zuzugreifen. Suchen Sie sich einen Anbieter, bei dem der Betreiberzugriff durch entsprechende Maßnahmen ausgeschlossen ist.

- **Ungeschützte Metadaten**
  Dass Daten und Passwörter verschlüsselt übertragen werden, ist heutzutage Standard. Aber nicht alle Anbieter schützen auch die Metadaten. Aus diesen lassen sich erstaunlich viele Informationen ableiten – Berufsgeheimnisträger müssen dies ebenfalls berücksichtigen.

- **Keine (optionale) Zwei-Faktor-Authentifizierung**
  Eine Zwei-Faktor-Authentifizierung ist zwar kein absolutes Muss, aber ein sehr nützliches Feature, das entscheidend dazu beitragen kann, das Sicherheitsniveau des Datenraums zu erhöhen. Das für Berufsgeheimnisträger erforderliche Schutzniveau wird tatsächlich nur mit Zwei-Faktor-Authentisierung erreicht.

- **Kein Browserzugang**
  Sicherer Zugang direkt über den Browser ist heutzutage Standard. Dienste, bei denen man sich ausschließlich über einen herunterladbaren Client einloggen kann, sind nicht mehr zeitgemäß und erschweren die Arbeit mit dem Datenraum unnötig. Apps für mobile Geräte meinen wir damit natürlich nicht – diese sind eine sinnvolle Ergänzung zum Browserzugang.

- **Keine kostenlose Testphase**
  Bevor Sie sich für einen Datenraum entscheiden, sollten Sie ihn ausgiebig testen. Meist gibt es eine 14- oder 30-tägige Testphase – so können Sie auch mehrere Anbieter direkt vergleichen. Kaufen Sie auf keinen Fall die Katze im Sack!

Weiterführende Informationen zu diesem Thema finden Sie außerdem im Whitepaper „Anforderungen an einen virtuellen Datenraum" – hier geht es zum kostenlosen Download.

Wenn Sie Fragen haben, wenden Sie sich bitte an presse@uniscon.de.

Über Uniscon GmbH

Die Uniscon GmbH ist Technologieführer im Bereich Cloud Security. Als Experte für versiegelte Cloud-Technologien bieten sie auf Basis der international patentierten Sealed Cloud Technologie technische Lösungen und eigene Cloud Services an. Die Sealed Cloud repräsentiert einen technischen Durchbruch bei der Realisierung hochsicherer Rechenzentren: Sie schützt Daten auf so hohem Niveau, dass selbst der Anbieter mit ausschließlich technischen Maßnahmen vom Zugriff auf die Daten bei der Speicherung UND während der Verarbeitung ausgeschlossen ist. Weitere Informationen zu Partnern und Produkt: www.uniscon.de und www.idgard.de

Pressekontakt

Uniscon GmbH, Claudia Seidl
Agnes-Pockels-Bogen 1
80992 München
E-Mail: presse@uniscon.de
Internet: www.uniscon.de
Telefon: 089 / 41 615 988 103