Cloud Compliance Spezialisten: Datenschutz in der Cloud durch den Brückenschlag zwischen IT und Regulierung

Geschrieben von Joshua Bucheli, Talent Community Manager bei cyberunity, in Zusammenarbeit mit Aljaz Galof, Senior Risk and Compliance Manager und Data Protection Officer bei Aveniq, und Peter Kosel, Gründer von cyberunity

In einem viel beachteten Artikel des Economist aus dem Jahr 2017 heisst es, "data is the new oil", d. h., dass dieser digitale Rohstoff zum Eckpfeiler unserer modernen Wirtschaft geworden ist. Mit dieser treffenden Analogie im Hinterkopf überrascht es nicht, dass nicht nur die Nutzung der Daten sondern auch deren Schutz ein zentrales Anliegen sowohl für moderne Unternehmen als auch für Behörden ist.

Betrachtet man Daten als Unternehmensvermögen, so werden sie in erster Linie durch Cybersicherheit geschützt. Personenbezogene Daten unterliegen dem Datenschutz, welcher zum Ziel hat, den Missbrauch mit unseren persönlichen Daten zu verhindern und unsere Persönlichkeitsrechte zu schützen.

Da die Cloud jedoch ihre Position als weltweit vorherrschende Datenspeicherlösung weiter festigt, entstehen neue Herausforderungen für die Cybersicherheit aber insbesondere auch für den Datenschutz - Herausforderungen, die aber auch neue Chancen für Spezialisten darstellen, die die Kluft zwischen rechtlichen Vorschriften und den technischen Aspekten der Cloud überbrücken können.

Wo steht das Thema Cloud Compliance heute?

"Wenn man heutzutage online ist, sei es als Privatperson, als Mitarbeitender oder als Unternehmen, hat man so gut wie immer mindestens einen Fuss in der Cloud", sagt Aljaz Galof, Senior Risk and Compliance Manager und Data Protection Officer bei Aveniq.

Im Jahr 2015 wurden 30 % aller Unternehmensdaten in der Cloud gespeichert, und diese Zahl ist seitdem stetig gestiegen. Da ab 2022 bis zu 60 % der Daten in der Geschäftswelt extern gespeichert werden, ist die Cloud eindeutig die dominierende Lösung für alle, die

versuchen, die Kosten zu senken und die Effizienz ihrer Datenspeicherung zu erhöhen. Ausserdem, so Aljaz, "integrieren Unternehmen häufig ihre On-Premise- und cloud-basierten Datenprozesse so, dass die Unterscheidung zwischen den beiden in der Praxis immer mehr verschwimmt".

Dies wirft die Frage auf, ob bei dieser digitale Massenmigration in die Cloud von Anfang an die Einhaltung von datenschutzrechtlichen Vorschriften berücksichtigt wird oder ob die Unternehmen “einfach” auf den Zug aufspringen und sich erst im Nachhinein mit den damit verbundenen Risiken befassen - wenn überhaupt.

Die Speicherung und Verarbeitung von Daten, insbesondere von personenbezogenen Daten, ist mit klar definierten Verantwortlichkeiten und Pflichten verbunden welche in den jeweils anwendbaren Datenschutzvorschriften wie der DSGVO, HIPAA oder dem DSG, um nur einige zu nennen, kodifiziert sind. Auch wenn man die Datenbearbeitung an Dritte (d.h die Cloud-Provider) auslagert, bleiben diese Vorschriften bestehen, oft mit erhöhter Komplexität in Bezug auf deren Umsetzung und Aufrechterhaltung.

Die Herausforderung besteht zu einem grossen Teil darin, dass die Cloud-Nutzung aus datenschutzrechtlicher Sicht einer Bearbeitung durch Dritte (d.h. Outsourcing) entspricht und somit per se keine Cloud-spezifischen Regelungen bestehen. Dies gilt insbesondere in Hinblick auf die länderübergreifende Cloud-Nutzung und die dazu notwendigen technischen und organisatorischen Massnahmen. Dieser Mangel an praxisnaher ‘Guidance’ in Verbindung mit der (technischen) Komplexität eines Cloud-Setups hat dazu geführt, dass viele Unternehmen in Bezug auf die Cloud eine negative Haltung “geht aus Compliance-Gründen nicht“ entwickelt haben oder schlicht auf "Wir wollen das Beste hoffen" setzen.

Unternehmen, die die Vorteile von Cloud-Diensten (selbst so etwas Banales wie Office 365) nutzen und gleichzeitig die Datenschutzvorschriften einhalten wollen, müssen den Schutz über den gesamten Lebenszyklus ihrer Daten gewährleisten können. Dies beinhaltet z. B. die Art der Daten, die gespeichert und verarbeitet werden, den Ort, an dem diese Speicherung und Verarbeitung stattfindet, die Personen, die in den verschiedenen Phasen der Bearbeitung Zugriff auf diese Daten haben, und so weiter. Dies ist eine äusserst anspruchsvolle Aufgabe, und selbst wenn all diese Elemente berücksichtigt werden, ist die Einhaltung der Vorschriften aufgrund mangelnder Transparenz beim Cloud-Provider oft nicht garantiert. Das Ergebnis: "Obwohl solche Fragen absolut unerlässlich sind, werden sie allzu oft überhaupt nicht erst gestellt", sagt Aljaz.

Abgesehen von den datenschutzrechtlichen Herausforderungen bestehen natürlich auch die Aufgaben, die allgemein mit der Auslagerung von Geschäftsprozessen verbunden sind. Dazu gehört insbesondere die Datensicherheit. Wie wir in unserem Artikel zum Thema Cloud-Sicherheit Datenwächter der Zukunft erfahren haben, geht die Auslagerung der Datenspeicherung mit dem Nachteil einher, dass man die Kontrolle darüber aufgibt, wie diese digitalen Kronjuwelen gegen die aktuelle vielfältigen Bedrohungen geschützt werden. Auch im Falle des Datenschutzes stellt sich eine ähnliche Frage: Wie kann ich sicherstellen, dass die Sicherheit der Personendaten, für die ich verantwortlich bin, intakt bleibt, wenn ich nicht derjenige bin, der diese Daten "hält"? Insbesondere bei Daten unter Geheimnisschutz (z. B. Patienten- oder Bankkundendaten) ist die Gewährleistung der Datensicherheit und des Datenschutzes zentral.

Und schliesslich ist die Frage des Auslandsbezugs zentral. Erfolgt eine Auslagerung in ein Land ohne adäquates Datenschutzniveau müssen damit einhergehenden datenschutz- oder aufsichtsrechtlichen Risiken beurteilt und entsprechend weitergehende vertragliche, organisatorische und technische Massnahmen umgesetzt werden. Letztlich zeigt jedes dieser Szenarien den Bedarf an Compliance-Spezialisten, die im Namen von Cloud-

Anbietern und ihren Kunden die Verbindung zwischen der theoretischen Welt der Vorschriften und der praktischen Welt der Datenverarbeitung herstellen können.

Wohin bewegt sich das Thema Cloud Compliance?
Was die allgemeine Richtung betrifft, in die sich der Bereich der Cloud-Compliance entwickeln wird, kristallisieren sich drei Hauptoptionen heraus. Die erste besteht darin, dass die Gesetzgeber neue Rahmenwerke ausarbeiten, in denen umfassend dargelegt wird, wie der Datenschutz in der Cloud gewährleistet werden sollte (siehe z. B. die jüngsten Bemühungen des EDPB). Option 2: Bestehende Verordnungen werden so geändert, dass ihr Anwendungsbereich um spezielle Bestimmungen für den Datenschutz in der Cloud erweitert wird. Die dritte Option, die Aljaz für die wahrscheinlichste hält, besteht darin, dass die Regulierungs- und Überwachungsbehörden mehr Leitlinien für die Anwendung der bestehenden Vorschriften auf die Cloud bereitstellen werden.

Abgesehen von dieser allgemeinen Entwicklung gibt es jedoch noch einige andere Schlüsselfragen im Bereich der Cloud-Compliance, die noch Klärungspotential mit sich bringen - Fragen, die künftige Cloud-Compliance-Spezialisten aktiv mitgestalten werden. Dazu gehört insbesondere das Thema des Auslandsbezugs, bzw. des potentiellen Datenzugriffs durch Sicherheitsbehörden. Hier stellen sich interessante Fragen in Bezug auf den Einsatz von nahtlosen Verschlüsselungstechniken welche die Vorteile der Cloud-Nutzung nicht gefährden. Interessant ist auch die Einführung von “Data Boundaries” bei den Cloud-Providern (siehe z. B. Microsofts EU Data Boundary) welche das Vertrauen in Cloud-Dienstleistungen stärken sollen. Schliesslich lohnt sich auch der Blick auf die staatliche Ebene unter dem Aspekt der digitalen Unabhängigkeit oder Souveränität (siehe die Pläne Russlands oder Chinas zur Entwicklung eines eigenen Internets).

Cloud Compliance Spezialisten – Gefragte Fähigkeiten und Ausbildungen
Wie wir erfahren haben, befindet sich die Cloud-Compliance am Scheideweg zwischen der Welt der Technik und der Welt der Verwaltung und Regulierung. Dementsprechend müssen Cloud-Compliance-Spezialisten vor allem die Kluft zwischen diesen beiden Dimensionen des Datenschutzes überbrücken.

In erster Linie ist ein grundlegendes Verständnis und eine Affinität zu den rechtlichen Grundlagen der Compliance - idealerweise des IT-Rechts - die wichtigste Voraussetzung für eine Karriere in der Cloud Compliance. Das soll nicht heissen, dass solche Karrieren auf Juristen oder Anwälte beschränkt sind. Vielmehr ist es wichtig, dass angehende Cloud-Compliance-Spezialisten auf Augenhöhe mit Rechtswissenschaftlern und Wirtschaftsprüferinnen kommunizieren, mit Verträgen umgehen können und die Nuancen der Vorschriften verstehen, die sie umsetzen sollen (z.B. DSGVO)", so Aljaz.

Darüber hinaus müssen sie auch die technischen Aspekte im Zusammenhang mit solchen Vorschriften verstehen. Sie müssen wissen, welche Arten von Daten gespeichert und verarbeitet werden, wo diese Speicherung und Verarbeitung stattfindet, wer in den verschiedenen Phasen der Aufbewahrungskette Zugang zu diesen Daten hat usw.

Nehmen wir zum Beispiel die Löschung von Daten, ein kritisches Thema in der Welt des Datenschutzes. Cloud-Compliance-Spezialisten müssen nicht nur in der Lage sein, auf Vorschriften zu verweisen und zu beraten, wann Daten gelöscht werden müssen - sie müssen auch mit den technischen Prozessen vertraut sein, die mit dieser Löschung verbunden sind, um zu beraten und zu überwachen, ob diese Daten tatsächlich gelöscht wurden. Denn in einer Zeit, in der Informationen überwiegend virtuell (digital) und online (in der Cloud) gespeichert werden, reicht ein Praktikant mit einem Schredder nicht mehr aus, um sensible Informationen sauber zu vernichten.

Aufgrund des interdisziplinären Charakters der Cloud-Compliance ist es ein Bereich, der sich gut für Quereinsteiger eignet. "Personen mit juristischem Hintergrund, Informatiker, IT-Governance-Fachleute, Qualitäts- und Risikomanagement-Spezialisten - jeder, der Erfahrung im Umgang mit Assurance-Prozessen, der Umsetzung interner Vorschriften oder der Durchführung interner Audits hat, verfügt über eine gute Grundlage, auf der eine Karriere in der Cloud-Compliance aufgebaut werden kann", erklärt Aljaz.

Abschlüsse, Diplome und Zertifikate

Gab es bis anhin eher wenige Studiengänge, die die technischen und rechtlichen Aspekte des Datenschutzes miteinander verbinden, so tut sich nun auch im Weiterbildungsbereich etwas (siehe z.B. das LLM in Compliance und Unternehmenssicherheit der Fachhochschule Köln oder die CAS Data Privacy Officer von der HSLU, Digital Compliance Officer von der HWZ und Managing Privacy and Data Security von der USG). Bis solche Studiengänge auf der Ebene des Grundstudiums zugänglicher werden, bietet eine universitäre Ausbildung in Informatik oder Wirtschaftsinformatik in Verbindung mit praktischer IT-Erfahrung die beste Grundlage für angehende Cloud-Compliance-Profis.

Cloud-Compliance ist sowohl eine interdisziplinäre als auch eine im Entstehen begriffene Disziplin. Wie wir bereits gesehen haben, erfordert sie die verknüpften Fähigkeiten und Erfahrungen von Juristen und IT-Spezialisten, eine Kombination, die in den Ausbildungsprogrammen noch nicht gut vertreten ist. Somit bleibt die Cloud-Compliance ein Bereich, der Teams aus mehreren Personen mit diversen Fähigkeiten und Hintergründen erfordert.

In Bezug auf professionelle Zertifizierungen empfiehlt Aljaz eine Kombination von Zertifikaten, die einerseits ein grundlegendes Verständnis für die Funktionsweise von Cloud-Plattformen und andererseits für die Informationssicherheit bieten. Programme wie Microsoft Certified Azure Fundamentals, Google Cloud's Grundlagenzertifizierung und AWS' Cloud Practitioner sind ein guter erster Schritt für Fachleute, die in den Bereich der Cloud Compliance einsteigen wollen. Diese können durch Zertifizierungen im Bereich des Datenschutzes wie die CIPP/E und CIPM Programme von IAPP und der Informationssicherheit wie die CISM- oder CRISC-Zertifizierungen von ISACA ergänzt werden.

Für diejenigen, die sich einen zusätzlichen Vorteil gegenüber der Konkurrenz verschaffen wollen, sind praxisorientierte Datenschutzzertifizierungen wie das CDPSE von ISACA ebenfalls eine Überlegung wert.

Personality: über technisches Know-How hinaus

Erfolgreiche Cloud-Compliance-Spezialisten müssen nicht nur die Sprachen von IT- und Rechtsexperten sprechen, sondern auch bestimmte Charaktereigenschaften mitbringen. Zum Beispiel "müssen sie in der Lage sein, das grosse Ganze im Auge zu behalten, während sie sich in einem Bereich bewegen, in dem man sich leicht in Details verstricken kann", sagt Aljaz.

Die Sicherstellung des Datenschutzes im Umgang mit Cloud-Speicherlösungen ist ein komplexer Prozess, der noch nicht klar definiert ist und viel mit der Bewertung und dem Eingehen kalkulierter Risiken zu tun hat. Daher braucht es jemanden mit einem hohen Mass an Pragmatismus - jemanden, der sich damit wohlfühlt, angesichts von Ungewissheit einen Kurs zu setzen und diesen selbstbewusst zu verfolgen.

Eine weitere wichtige Eigenschaft eines effektiven Cloud-Compliance-Spezialisten ist die Affinität zu interdisziplinärer Teamarbeit und ein Händchen für diplomatische horizontale und vertikale Kommunikation. Schliesslich ist die Cloud-Compliance etwas, das die

gemeinsamen Anstrengungen von Technikern, Juristen, Entscheidungsträgern auf Managementebene und Mitarbeitenden erfordert. Zudem ist die Fähigkeit, mit Fingerspitzengefühl zwischen diesen Parteien zu vermitteln unabdingbar.

Alles in allem wird deutlich, dass der Bereich der Cloud-Compliance noch weitgehend unbestimmt ist, fasst Peter Kosel, Gründer der cyberunity AG zusammen. Zwei Tatsachen sind jedoch sicher. Erstens wird die Definition dieses im Entstehen begriffenen Bereichs weitgehend den Cloud-Compliance-Spezialisten überlassen, und zweitens wird künftig der Kampf um die Daten überwiegend in der Cloud ausgetragen werden, aufgrund ihrer zunehmenden Dominanz als Datenspeicherlösung. Vor diesem Hintergrund liegt es auf der Hand, dass in naher Zukunft diejenigen Unternehmen, die frühzeitig Spitzenkräfte für ihre Cloud-Compliance-Teams gewinnen, die Entwicklung der Cloud-Compliance am stärksten mitbestimmen und die besten Chancen haben werden, die mit Datenschutzverstössen verbundenen Konsequenzen zu vermeiden.