GeschGehG - Interview mit Hagen Albus, Rechtsanwalt und Geschäftsführer jurcons GmbH (l.)

12.04.2019 12:20 CEST

GeschGehG - Digitaler Safe für Geschäftsgeheimnisse wird Gesetz

Interview mit Hagen Albus, Rechtsanwalt und Geschäftsführer jurcons GmbH

Leipzig, 12. April 2019: Soeben hat der Bundesrat das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) gebilligt. Damit ist nun die ‚Richtlinie (EU) 2016/943 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung' in deutsches Recht umgesetzt. Was sich genau hinter diesem neuen Gesetz verbirgt, beantwortet Hagen Albus, Geschäftsführer der jurcons GmbH in einem Interview:

F: Sie beschäftigen sich seit langem mit den Gesetzgebungen zu Datenschutz und Informationssicherheit. Warum ist das GeschGehG für Sie interessant?

HA: Nun, Kern meiner Betrachtung sind vorrangig die Auswirkungen des Gesetzes auf Unternehmen aus Sicht der Informationssicherheit. Aus juristischer Sicht wird hier eine Lücke geschlossen, auf die wir in der Praxis des Öfteren gestoßen sind.

Lassen Sie mich das an einem Beispiel veranschaulichen. Ein Firmeninhaber, der sich um das besondere und einzigartige Wissen seiner Firma sorgt, hat in der Vergangenheit Know-How, wie Rezepturen, Konstruktionszeichnungen aber auch die firmeninterne Kalkulation in einem Safe gelagert. Dieser stand nicht selten auch noch im Chef-Zimmer. Mitarbeiter, die auf diese Unterlagen Zugriff hatten, wurden sorgfältig ausgewählt und zu besonderer Verschwiegenheit verpflichtet. Heute finden sich solche Geschäftsgeheimnisse oftmals ungesichert auf irgendwelchen Servern oder in der Cloud. Mitarbeiter jeglicher Couleur können sie einsehen oder kopieren. Nicht selten werden vertrauliche Unterlagen unverschlüsselt in einer E-Mail an Geschäftspartner oder Kunden geschickt. Ob man dann noch von Geheimnissen sprechen kann ist also fraglich. Aus juristischer Sicht stellt sich dann die Frage: kann ich jemanden zur Rechenschaft ziehen, der eine öffentlich zugängliche Information weiter gibt? Oder knapp formuliert: kein Schutz, kein Geheimnis.

Genau hier ist für mich eine Motivation der Gesetzgebung zu sehen. Es werden die rechtlichen Rahmenbedingungen für die Digitalisierung in der Industrie und Mittelstand in Sachen Verantwortung und Strafbarkeit definiert. Im übertragenen Sinn kann man auch sagen, wir reden über digitales Hausrecht und den digitalen Hausfriedensbruch.

F: Nicht alle Medien teilen Ihre Meinung zur Motivation des Gesetzes. Oft liest man jetzt, dass das Gesetz primär dazu dient, potentielle Whistleblower zu privilegieren?

Moralische Kategorien spielen bei mir im Rahmen der rechtlichen Bewertung hier eine untergeordnete Rolle. Ob es sich beim Whistleblowing um eine Offenlegung von Geschäftsgeheimnissen, eine begründbare, wertvolle Information für die Öffentlichkeit handelt oder überspitzt formuliert nur um eine Denunziation, werden die jeweiligen Einzelfälle zeigen und letztendlich die Gerichte entscheiden müssen. Bei vernünftigem Vorgehen bietet das

inzwischen diskutierte dreistufige Meldesystem die Chance, eine Eskalation zu vermeiden. Ich hoffe doch sehr, dass sich dieses so bezeichnete 3-Stufen-Modell auch durchsetzen wird. Damit wäre einem großen Teil der Debatte aus meiner Sicht die Schärfe genommen. Die eingangs dargestellten Betrachtungen werden bei den aktuellen und emotional geführten Debatten hierzu leider mitunter übersehen.

Andreas Liefeith von procilon (r.) im Interwiew mit RA Hagen Albus, Geschäftsführer der jurcons GmbH (l.)

F: Damit drängt sich ja geradezu die Frage auf, ob Sie die Informationssicherheit ausreichend im Gesetz berücksichtigt sehen?

HA: Bedauerlicherweise wird im Gesetz die Einhaltung der IT-Sicherheit nicht direkt erwähnt. Hier unterscheidet es sich doch erheblich von neueren Gesetzen, wie z.B. dem Bundesdatenschutzgesetz – neu – oder der KRITIS-Verordnung. Allerdings findet sich im GeschGehG die Formulierung „angemessenen Geheimhaltungsmaßnahmen“. Wie eingangs geschildert, legt heute kaum ein Firmeninhaber das besondere Wissen in den Wand-Safe, wie das vielleicht in der Gründerzeit üblich war, denn das Wissen existiert fast ausschließlich digital. Im übertragenen Sinn schreibt das Gesetz also einen digitalen Safe vor. Und nach dem Gesetz sind Geschäftsgeheimnisse nur noch die Daten, die in diesem Safe geschützt abliegen. Den wiederum kann man nur mit Bauplänen aus der Informationssicherheit herstellen. Übertragen heißt das dann, es liegen Daten mit einem hohen Schutzbedarf vor, die man nach ‚dem Stand der Technik‘ durch angemessene technische und organisatorische Maßnahmen (TOM) schützen muss.

F: Das klingt erst einmal sehr generisch. Können Sie da einen praxistauglichen Tipp geben?

HA: Nun in den vergangenen Jahren haben wir gemeinsam mit unseren Kunden aufgrund unterschiedlicher Auslöser eine Reihe von Erfahrungen gesammelt. Nicht zuletzt liegt in einer zunehmend digitalen Welt die Konvergenz von Informationssicherheit und Datenschutz auf der Hand. Hier hilft unsere ganzheitliche Betrachtungsweise der Themen. Am Ende geht es doch darum, Geschäftsgeheimnisse mit der gleichen Sorgfalt wie personenbezogene Daten zu behandeln.

Auf der anderen Seite hat das IT-Sicherheitsgesetz dazu beigetragen, dass

KRITIS-Unternehmen den ISO 2700x als Sicherheitsstandard etabliert haben. Auf demselben Standard, ergänzt um einige Branchenspezifika, etabliert sich in der Automobilindustrie das VDA-ISA (TISAX). Dies ist ein sehr gutes Beispiel, wie die sensiblen Daten von Prototypen = Geschäftsgeheimnis durch einen einheitlichen IT-Sicherheitsstandard besser geschützt werden. Und mit dem BSI-Grundschutz gibt es eine Blaupause für den öffentlichen Dienst.

Unabhängig davon, ob man nur eine Zertifizierung oder ein Testat anstrebt, das Vorgehensmodell zur Erreichung einer besseren Informationssicherheit, also der Bauplan für den digitalen Safe, ist ähnlich. Technologie zur Datenverschlüsselung oder Identity- & Access-Management sind dabei feste Bestandteile.

Herr Albus, vielen Dank für die anregende Beantwortung der Fragen!

Die Fragen stellte Andreas Liefeith, Marketingleiter der procilon GROUP

Seit Jahrzehnten gilt die procilon GROUP als verlässlicher Ansprechpartner, wenn es um den Auf- und Ausbau einer sicheren digitalen Kommunikation im deutschen Rechtsraum geht.

Sowohl Unternehmen als auch Behörden setzen zur sicheren Identifizierung, Übertragung und Aufbewahrung ihrer Daten auf Lösungen der Anbietergruppe. Ihr SaaS- und On-Premises-Portfolio ermöglicht es ihnen, digitale Inhalte sicher, niederschwellig, vertraulich, nachvollziehbar und beweisbar zu signieren, auszutauschen und zu archivieren. Die Stärke der procilon GROUP-Produktpalette basiert dabei zum einen auf der strikten Einhaltung deutscher und europäischer Richtlinien und Vorgaben, zum anderen auf dem Einsatz kryptografischer Spitzentechnologien made in Germany, sowie – last but not least – auf seiner Cloud First-Strategie.

Ein wichtiges Mitglied der Anbietergruppe ist die intarsys GmbH. Sie entwickelt und vertreibt qualitativ hochwertige und technologisch führende Softwareprodukte und -komponenten zur Erzeugung und Prüfung von elektronischen Signaturen, Siegeln und Zeitstempeln sowie zur beweissicheren Langzeitarchivierung von digitalen Dokumenten.

Gemeinsam haben es sich die Mitglieder der Anbietergruppe zum Ziel gesetzt, die procilon GROUP zu einem der führenden deutschen Anbieter elektronischer Vertrauensdienstanwendungen auszubauen.

Sie möchten mehr über die procilon GROUP erfahren? Klicken Sie hier – oder abonnieren Sie den procilon Newsletter.

Kontaktpersonen

Kafka Kommunikation GmbH & Co KG
Pressekontakt
Dr. Torben Gülstorff
procilon@kafka-kommunikation.de
+49 (0) 89 7474705824