Grundwissen

Compliance goes Digital - Was versteckt sich hinter Digital Compliance?

Isabel Ecker

Open Peer Review

Dieser Beitrag wurde lektoriert von: Julia Keselj und Maria Osmakova

Isabel hat Jura an der Universität zu Köln studiert. Sie schreibt derzeit ihre Promotion im Bereich des Wirtschaftsstrafrechts u.a. zur Criminal Compliance bei Herrn Professor Waßmer und ist Promotionsstipendiatin der Studienstiftung des deutschen Volkes. Zudem ist sie Co-Head und Head of People des Legal Tech Lab Cologne e.V.

Wer aufmerksam die Berichterstattung der letzten Jahre verfolgt hat, kommt an dem Begriff der Compliance nicht vorbei. Karriere macht Compliance immer dann, wenn der nächste große Unternehmensskandal vor der Tür steht. Früher war es ***Siemens***, heute steht ***Volkswagen*** mit einem uferlos anmutenden Abgasskandal im Mittelpunkt der medialen Aufmerksamkeit. Offenbart sich ein jahrelang andauernder Unternehmensskandal, stellt sich oftmals insbesondere bei großen Unternehmen die Frage, wie konnte es so weit kommen, ohne dass jemand das Fehlverhalten bemerkt hat? Jeder, der sich diese Frage stellt, trifft den Kernpunkt, warum wir heute Vorbeugungsmaßnahmen unter dem Stichwort Compliance diskutieren.

A. Grundbegriff Compliance

Compliance zielt auf die Beherrschung von Risiken in einem Unternehmen ab, um Rechtsverstöße zu verhindern. Die verantwortlichen Führungskräfte müssen dafür sorgen, dass die (internationalen) Rechtsnormen und Vorgaben eingehalten werden, um wirtschaftliche Risiken von dem eigenen Unternehmen fernzuhalten, indem Fehlverhalten vermieden wird. Die rechtlichen Grenzen werden durch die öffentliche und private Regulierung der speziellen Bereiche festgelegt. Praktisch soll dieses Ziel durch den Einsatz vorbeugender Unternehmensorganisation wie Kontrollsysteme, Schulungs- und Meldemechanismen erreicht werden. Hierdurch sollen Regelverstöße durch Mitarbeiter und Leitungspersonen vorgebeugt werden, die zu einer ‚Strafe' führen können.

Hierbei ist Strafe nicht herkömmlich strafrechtlich zu verstehen, denn bisher gibt es in Deutschland (noch) kein Verbandssanktionenrecht. Vielmehr liegt der Fokus der Schadensvermeidung bisher vor allem in den Bereichen des Kartellrechts sowie der Vermeidung von Betrugs- und Finanzkriminalität. Dabei haftet etwa auch der Vorstand für ein mangelndes Compliance-System nach § 93 I AktG, wenn er deshalb seiner Überwachungspflichten über die unteren Ebenen des Unternehmens nicht nachgekommen ist. Eine allgemeine Legaldefinition des Compliance-Begriffs existiert bisher nicht. Allerdings hat sich die Definition aus dem Deutschen Corporate Governance Kodex zu einer allgemein anerkannten Leitlinie für den Compliance-Begriff entwickelt.

Grundsatz 4 und 5 des DCGK 2022:
Für einen verantwortungsvollen Umgang mit den Risiken der Geschäftstätigkeit bedarf es eines geeigneten und wirksamen internen Kontroll- und Risikomanagementsystems.
Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der internen Richtlinien zu sorgen und wirkt auf deren Beachtung im Unternehmen hin (Compliance).[1]

DCGK: Der Deutsche Corporate Governance Kodex ist ein von der Regierungskommission Deutscher Corporate Governance Kodex beschlossenes Sammelwerk an besten Vorgehensweisen (engl. Best Practices) für börsennotierte Aktiengesellschaften, die oft über die Anforderungen des Aktiengesetzes hinausgehen. Dabei ist die Regierungskommission ein politisch unabhängiges Gremium von Personen mit Wirtschaftserfahrung wie Vorstands-, Aufsichtsratsmitgliedern und Wirtschaftsprüfern. Da es politisch unabhängig ist, handelt es sich bei dem DCGK mangels demokratischer Legitimation nicht um ein bindendes Gesetz. Jedoch wird die Bindung der Unternehmen indirekt durch § 161 Abs. 1 AktG herbeigeführt, wonach börsennotierte Gesellschaften eine jährliche Entsprechenserklärung abgeben müssen. In dieser Erklärung müssen sie den Anteilseignern mitteilen, wenn sie einer Empfehlung nicht entsprachen und weshalb (Comply-or-Explain-Prinzip). Damit soll eine Selbstbindung ohne Rechtsbindung bewirkt werden, weshalb der DCGK häufig auch als Soft Law bezeichnet wird.

1 Grundsatz 4 und 5 des Deutschen Corporate Governance Kodex in der aktuellen Fassung von 2020, hier abrufbar (Stand: 14.06.22). Aktuell gibt es eine neue Fassung des Deutschen Corporate Governance Kodex 2022, die dem BMJ zur Prüfung vorliegt, hier abrufbar (Stand: 14.06.22). Dort sollen der 4. und 5. Grundsatz vereinigt werden, sodass es unter dem Grundsatz 5 n.F. künftig heißen soll: *„Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der internen Richtlinien zu sorgen und wirkt auf deren Beachtung im Unternehmen hin (Compliance). Das interne Kontrollsystem und das Risikomanagementsystem umfassen auch ein an der Risikolage des Unternehmens ausgerichtetes Compliance Management System."*

Um die Compliance-Risiken zu beherrschen, wird gerade in größeren Unternehmen oftmals ein Compliance-Management-System (***CMS***) implementiert. Dieses CMS besteht grundsätzlich aus mehreren Kernelementen, beginnend mit der Einschätzung des Risikos, gefolgt von der Organisation der möglichen Vorbeugungsmaßnahmen, die das Risiko beherrschen und Fehlverhalten vermeiden sollen. Hinzu kommt die kommunikative Weitergabe der Regularien an die Mitarbeiter und die Schaffung einer integren Unternehmenskultur mit gelebter Compliance.

Zu den Compliance-Maßnahmen können ganz einfache Regularien für das Verhalten von Mitarbeitern gehören, wie Vorgaben zur Annahme von Geschenken. Hinzu kommen Mechanismen, um Indizien für Fehlverhalten zu sammeln, wie etwa die Einrichtung eines Hinweisgebersystems für Whistleblower oder regelmäßige Interviews mit Mitarbeitern. Darin erschöpft sich der Bereich der Compliance jedoch bei Weitem nicht. Compliance ist vielschichtig und gestaltet sich individuell je nach Aufbau, Rechtsform und Größe eines Unternehmens. Schnittmenge der Compliance-Systeme sind die einzuhaltenden Gesetze und Regelungen.

> „Compliance zielt darauf ab, Risiken von vornherein zu minimieren und Verstöße zu vermeiden.“

Im Hinblick auf die verschiedenen zu beherrschenden Risiken lässt sich festhalten, dass die Aufgabe und das Ziel der Compliance ganz überwiegend in der Prävention liegt. Compliance-Management zielt also darauf ab, Risiken von vornherein zu minimieren und Verstöße bereits bevor es zu ihnen kommt, zu vermeiden. Hierneben gibt es einen repressiven Teil der Compliance, also Mechanismen, die greifen, sobald ein Verstoß vorliegt und aufgedeckt wurde. Darunter fallen insbesondere die unternehmensinternen Ermittlungen (engl. ***Internal Investigations***).

B. Compliance und Digitalisierung

Allerdings zeigt sich, dass die präventive Zielsetzung der Schadensvermeidung praktisch schwer umsetzbar ist. Oftmals werden trotz eingerichteter Compliance-Maßnahmen Indizien für Verstöße zu spät erkannt. Die Folge ist, dass es nicht wie geplant zu einer präventiven Aktion kommt, sondern lediglich nachgelagert zu einer Reaktion auf den Verstoß. Grund hierfür ist die Komplexität und Vielschichtigkeit der Prozesse in den Unternehmen, auf die ein analoges Compliance-Programm nicht in Echtzeit reagieren kann. Für die Überwindung des zeitlichen Auseinanderfallens von Fehlverhalten und Reaktion birgt die Digitalisierung eine Lösungsmöglichkeit.

Dieses digitale Spielfeld eröffnet sich durch die Symbiose der Begriffe ‚Compliance‘ und ‚Digitalisierung‘, im Ergebnis ‚Digital Compliance‘, wobei sich die Oberkategorie der Digital Compliance in zwei Themenblöcke unterteilen lässt: In einem ersten Schritt stellt sich die Frage, wie ein Compliance-System durch technische Tools umgesetzt werden kann (***Digitalisierte Compliance***). Ist dies beantwortet, so muss sichergestellt werden, dass das digitale Compliance-System selbst auf die eigene Compliance überprüft werden kann (***Compliance der Digitalisierung***).

I. Digitalisierung der Compliance durch technische Tools (Digitalisierte Compliance)

1. Technische Einsatzfelder

Unter den Begriff der Digital Compliance fällt der Einsatz technischer Tools in einem Compliance-Prozess. Es geht im Kern unmittelbar um die Digitalisierung von Abläufen. Während Vorbeugemaßnahmen überwiegend analog durchgeführt wurden, etwa durch Mitarbeiterschulungen und menschliche Risikobewertung, können diese Maßnahmen in vielen Bereichen technisiert und hierdurch verbessert werden. Begonnen werden kann mit einer Technisierung der Risikobewertung. Der Einsatz von Big-Data-Technologie und Algorithmen bietet die Möglichkeit, durch umfangreiche Dateneingabe Risikowahrscheinlichkeiten zu bestimmen. Eine detaillierte

Vorhersage des Risikos führt aus Unternehmenssicht zu einer besseren Skalierbarkeit und ‚Bilanzierbarkeit' des Risikos. Hierdurch können Kosten durch gezielten Einsatz in Hochrisikobereichen kanalisiert und in der Gesamtheit sinnvoll eingespart werden. Durch die ergänzende Einspeisung neuronaler Daten in das System kann die Eintrittswahrscheinlichkeit bestimmter menschlicher Verhaltensweisen anhand ausgewählter Parameter prognostiziert werden (***Predictive Analytics***[1]). Diese Ergänzung führt zu einer noch genaueren Berechnung des Risikos. Insgesamt ermöglicht eine schnelle Risikobewertung für das Unternehmen eine finanzielle Skalierbarkeit bestimmter Risikobereiche und ermöglicht die Kategorisierung der Risikogruppen für ein CMS.

Geht es um starre regulatorische Vorgaben, also beispielsweise feste Werte, die bei der Produktion eingehalten werden müssen, könnte deren Einhaltung unmittelbar durch (algorithmische) Analysetools überprüft werden. So können mehrere Daten aus parallelen Prozessen in Echtzeit erfasst, abgeglichen und bewertet sowie visualisiert und zusammengefasst werden. Wird eine Vorgabe verfehlt, kann das Analysetool den Prozess kurzzeitig unterbrechen und auf den Fehler hinweisen. Die Transparenz eines komplexen Prozesses steigt hierdurch enorm an und der Prozess lässt sich zu jeder Zeit nachverfolgen. Eine Nachverfolgbarkeit des Prozesses würde auch eine Datenspeicherung z.B. in der Blockchain garantieren.

Problematisch kann es bei dem Einsatz solcher Tools jedoch werden, sobald sich regulatorische Vorgaben des Gesetzgebers (sowohl national als auch international) ändern. In diesem Fall müssen die Daten in dem verwendeten Compliance-Tool unmittelbar angepasst werden. Durch die Vielzahl an Regelungen, die es zu beachten gilt und die stetigen inhaltlichen Weiterentwicklungen der Normen sowie der Europäisierung der Gesetze, sind die betroffenen Unternehmen ständig angehalten, ihre Compliance-Vorgaben und Systeme anzupassen. Es kommt zu immer höheren Compliance-Ausgaben für die Unternehmen.

Allerdings bietet der Einsatz digitaler Lösungen auch in diesem Bereich einen Vorteil: Für die regulatorischen Anwendungsfälle werden Softwarelösungen zur Unterstützung der Compliance entwickelt, deren Ziel es ist, sich ändernde Regularien in Echtzeit in bereits bestehende Compliance-Systeme zu integrieren (‚Regulatory Technology', kurz: ‚RegTech'). Die Vorteile einer solchen technischen Lösung liegen vor allem in der extremen Zeitersparnis. Hinzu kommt die Tatsache, dass keine Lücke im bestehenden CMS besteht. Durch die zeitliche Kohärenz zwischen einer neuen Regel und der Einbettung in das bestehende CMS wird nahtlos neuen Verstößen vorgebeugt.

Wichtig sind jedoch nicht nur die technischen Mechanismen zur Gesamtrisikominimierung im Unternehmen. Das zweite elementare Standbein einer effektiven Compliance ist das Verständnis und das Mindset der Mitarbeiter. Bisher beschränkt sich die Vermittlung der Compliance-Richtlinien oftmals entweder auf dicke Papierstapel, die nicht gelesen werden bzw. schwer verständlich sind oder auf Schulungen, die eine Bandbreite von Compliance-Themen in Form von Frontalunterricht abdecken. Hinzu kommt, dass die Zeiten für Schulungen oft starr sind und es dementsprechend an der regelmäßigen Auffrischung der wichtigen bereichsbezogenen Compliance-Vorgaben fehlt.

An dieser Stelle bietet der Einsatz von on demand E-Learning Angeboten eine Chance, den Mitarbeitern individualisiert, interaktiv und regelmäßig das für sie wichtige Wissen zu vermitteln. Durch einen enger getakteten Schulungsrhythmus kann zudem erreicht werden, dass die Thematik Compliance jederzeit fest in den Köpfen der Mitarbeiter verankert ist, was das generelle Compliance-Mindset bestärkt. Für die textuelle Aufbereitung der Richtlinien sollte auf zwei Säulen gebaut werden. Erstens müssen die Informationen kanalisiert und individualisiert werden, sodass jeder Mitarbeiter die für seinen Bereich wichtigen Informationen erhält. Ein Mitarbeiter, der beispielsweise in einem internen Verwaltungsbereich mit geringem Risiko arbeitet, benötigt nicht dieselben Compliance-Informationen, wie ein Mitarbeiter, der in einem Hochrisikobereich arbeitet, wie dem Vertrieb. Zudem sollten situationsbe-

1 Für weitere Ausführungen zu Predictive Analytics, insb. zu der Verwendung durch die deutschen Polizeibehörden, vgl. *Scholz*, CTRL 2/21, 110 ff.

zogene Compliance-Richtlinien angezeigt werden können. So könnte etwa bei einer Geschäftsreise eine automatisierte, auf das Zielland zugeschnittene, Compliance-Übersicht auf das Smartphone oder Tablet eines Mitarbeiters geschickt werden. Dieser kann sich dann auf einen Blick ins Gedächtnis rufen, was er im Folgenden zu beachten hat.

Zweitens sollte an der Darstellung der Information gearbeitet werden. Hier muss zwar eine präzise, aber dennoch verständliche Darstellung nach dem Legal-Design-Thinking-Ansatz[2] das Ziel sein. Ergänzend zu der allgemeinen Darstellung könnten in Hochrisikobereichen bei der täglichen Arbeit technische Checklisten installiert werden, die einem Mitarbeiter verständlich, übersichtlich und schnell anzeigen, welche Punkte er bedenken und beachten muss, um Verstößen bereits im Arbeits- bzw. Produktionsprozess zu begegnen.

All dies lässt sich durch die Big-Data-Technologie umsetzen. Durch Einspeisung interner Compliance-Daten sowie repräsentativer Mitarbeiterdaten, deren Bedürfnisse in verschiedenen Situationen erfasst werden, ließen sich individuelle Risikoprofile erstellen. Diese Profile können wiederum situationsabhängig eingestuft werden. Funktioniert die digitalisierte Compliance einfach, verständlich und schnell, wird die Akzeptanz der Maßnahmen durch die Mitarbeiter weiter ansteigen.

2. Vorteile des Einsatzes neuer Technologien

Die genannten Beispiele verdeutlichen einen Teil der möglichen Einsatzmöglichkeiten digitaler Compliance-Tools. Sie bieten den Unternehmen die Chance, ihre Compliance zu vereinfachen und effizienter, verständlicher sowie verlässlicher zu gestalten. Der Einsatz digitaler Technologien verhilft der Compliance letztlich erst zur Erreichung ihres tatsächlichen Ziels, nämlich der Antizipation des drohenden-Risikos verbunden mit der präventiven Vermeidung von Fehlern oder Verstößen im Gegensatz zu einer erst nachgelagerten Reaktion auf einen Verstoß.

Analoge Compliance-Mechanismen arbeiten trotz präventiver Ausrichtung oftmals zu langsam. Es fehlt an der Möglichkeit, Indizien für die Gefahr eines drohenden Verstoßes im Vorfeld zu erkennen und zu verhindern. Durch die Implementierung der neuen Technologie in bestehende CMS kann eine Überwachung in Echtzeit ablaufen und schon während des laufenden Geschäftsprozesses korrektive Wirkung entfalten.

> „Funktioniert die digitalisierte Compliance einfach, verständlich und schnell, wird die Akzeptanz der Maßnahmen durch die Mitarbeiter ansteigen.“

Zudem ist eine digitalisierte Compliance finanziell für die Unternehmen von Vorteil, da Verstöße mit immer härteren Bußgeldern einhergehen, die schlimmstenfalls in die Insolvenz führen können. Doch nicht nur die im Falle eines Verstoßes drohende finanzielle Gefahr stellt für die betroffenen Unternehmen eine Belastungsprobe dar. Hinzu kommt der drohende, erhebliche Reputationsschaden, der durch das Fehlverhalten ausgelöst wird. Es ist somit von höchstem Unternehmensinteresse, Verstöße effektiv zu vermeiden. Genau dieses Ziel kann mit einer digitalisierten Compliance besser erreicht werden.

3. Einsatzgrenzen neuer Technologien

Neben zahlreichen Vorteilen birgt eine digitalisierte Compliance allerdings neue Risiken und Hürden, die es zu bewältigen gilt. Zuvorderst bedarf es für die meisten Systemideen einer großen Menge an Trainingsdaten. Ohne diese Trainingsdaten wird die Digitalisierung im Compliance-Bereich in ihrem Keim ersticken. Die Nutzung großer Datenmengen bringt als Folge Fragen des Datenschutzrechts mit sich.

2 Zu den Hintergründen, Vorteilen und Vorgehensweisen bei Legal Design Thinking, s. *Bayzat,* CTRL 2/21, 178 ff.

Ob Big Data, Blockchain oder Algorithmen: Daten sind die Grundlage eines erfolgreichen Gelingens der Digitalisierung. Umso wichtiger wird es für Unternehmen sein, sich frühzeitig mit den komplexen Vorschriften rund um den Schutz der Daten zu befassen. Zu datenschutzrechtlichen Vorgaben kommen jedoch eine Vielzahl weiterer Vorschriften, die es zu beachten gilt. Die sich stark im Wandel befindliche, komplexe gesetzliche Struktur macht eine ständige Anpassung notwendig, was sicher eine Herausforderung für die Unternehmen darstellen wird. Die Komplexität der Regelungsmaterie wird durch die Unterschiede zwischen den Rechtsordnungen noch verstärkt, insbesondere für ein international operierendes Unternehmen. Zuletzt besteht die Gefahr von Angriffen auf die eigene IT-Sicherheit und Infrastruktur. Wer sich digital aufstellt, muss jederzeit mit Hacking-Angriffen rechnen. Diese Angriffe können neben anderen sensiblen Bereichen ebenso eine digitalisierte Compliance betreffen.

II. Compliance der eingesetzten Tools (Compliance der Digitalisierung)

Die Risiken, die der Einsatz digitaler Tools mit sich bringt, ist unmittelbarer Grund für den zweiten Themenkomplex, der unter dem Stichwort Digital Compliance diskutiert wird. Dieser erfasst solche Compliance-Maßnahmen, die Risiken managen, welche erst durch den Einsatz eines technischen Tools entstehen. Wird also z.B. Blockchain eingesetzt, müssen die Risiken, die ein Blockchain-Einsatz mit sich bringt, wiederum eingeschätzt und beherrscht werden. Überspitzt gesagt, könnte es eine Compliance für ein technisches Compliance-Tool geben. Dass für den Einsatz von Technologien selbst wiederum ein gutes Compliance-Management gefragt ist, zeigt die Auswirkung von Fehlern in diesem Bereich. Kommt es zu einem Cyber-Angriff auf das Unternehmen, ist der daraus resultierende Schaden oftmals verheerend.[3] Zudem werden für den Einsatz neuer Technologien zunehmend eigenständige Regularien geschaffen. Insbesondere der europäische Gesetzgeber ist aktiv geworden und möchte weitere Auflagen und Vorschriften für verschiedene Technologien schaffen, so zum Beispiel der Artificial Intelligence Act[4] als Regulierung Künstlicher Intelligenz. Wird somit algorithmische Analyse im Unternehmen eingesetzt, gilt es, die gesetzlichen Anforderungen an die Nutzung des Systems sicherzustellen.

C. Digitalisierte Compliance mit Maß und Verstand

Aus Unternehmenssicht lässt sich also festhalten, dass digitalisierte Compliance eine enorme Effizienzsteigerung bewirken kann. Auch aus Mitarbeitersicht ist der Nutzen digitaler Tools offenkundig. Wer zu jeder Zeit besser verstehen kann, wo sich die gesetzlichen Grenzen befinden, wird effektiv vor Fehlern oder Verstößen geschützt und wendet damit nicht nur schwere Folgen für das Unternehmen ab, sondern ebenso für sich selbst.

> „Digitalisierte Compliance bietet die Chance auf Fortschritt, darf jedoch nicht überbewertet werden.“

Weitet man den Blick, zeigt sich, dass auch die Allgemeinheit ein Interesse an funktionierender präventiver Compliance hat, um Schäden vorzubeugen. Denn von einem Skandal, wie einem solchen rund um die Abgaswerte, ist nicht nur das Unternehmen und dessen Mitarbeiter betroffen, sondern letztlich auch der Verbraucher. Digitalisierte Compliance bietet die Chance auf Fortschritt, darf jedoch

3 Durch derzeit frequentiertere Cyber-Angriffe von russischen Hackergruppen auf deutsche Unternehmen, stellen sich vornehmlich bei der Frage der Lösegeldzahlung, um die erlangten Daten zurückzuerhalten, spannende rechtliche Fragen. So kann die Zahlung von Lösegeld eine Terrorismusfinanzierung nach § 89c StGB oder eine Straftat nach § 18 AWG darstellen, wobei auch die Frage einer etwaigen Rechtfertigung nach § 34 StGB relevant wird.

4 Zum Artificial Intelligence Act im Detail: *Ecker/Mahlow*, CTRL 1/22, 118 ff.

nicht überbewertet werden. Die Komplexität vieler Situationen wird es notwendig machen, weiterhin dispositiven menschlichen Spielraum bei der Risikobewertung und -bewältigung einzuräumen. Es wird demnach weiterhin zu Regelverstößen kommen. Allerdings wird eine Verknüpfung der Digitalisierung mit verbleibenden menschlichen Einschätzungsspielräumen die Fehleranfälligkeit des Risikomanagements minimieren und Fehler bei der Umsetzung und Ausführung vermeiden. Die digitalisierte Compliance trägt hierzu bei, indem sie Fehler in Echtzeit erkennt und von vornherein verhindert. In diesem Sinne: Let's go Digital Compliance!

Weiterführende Hinweise:

Um das Thema Digital Compliance zu vertiefen, bieten sich die im Folgenden genannten Beiträge an, die auch eine Grundlage dieses Beitrags bilden:

Generell zur Compliance s. ***Hauschka/Moosmayer/Lösler***, Corporate Compliance, 3. Auflage 2016; und ***Wieland/Steinmeyer/Grüniger***, Handbuch Compliance-Management, 3. Auflage 2020.

Deutscher Corporate Governance Kodex (Fassung von 2020), hier abrufbar (zuletzt abgerufen am 15.06.22).

Eingehend auf bereits eingesetzte Tools und deren Wirkweise im Rahmen der Digital Compliance: ***Heißner/Schaffer***, CCZ 2018, 147 ff., sowie ***Timmermann,*** Legal-Tech-Anwendungen, Berlin Diss. 2020, S. 118 ff.

Einen guten Überblick über beide Ausprägungen der Digital Compliance bietend: ***Bräutigam/Habbe***, NJW 2022, 809 ff.

Zur technischen Ausgestaltung der Tools s. ***Neufang***, IZR 2017, 249 ff.

Speziell zur digitalen Compliance-Kommunikation für Schulungen von Mitarbeitern: ***Hastenrath***, CCZ 2020, 162 ff.

Weiterführende Hinweise:

Talking Legal Tech – Folge 5

„Was ist die Blockchain, Florian Glatz?"

Talking Legal Tech – Folge 15

„Legal Design – was ist das, Lina Krawietz?"

Zurück zum Inhaltsverzeichnis

CTRL

2/22
2. Jahrgang, 1. Ausgabe
www.legaltechcologne.de/ctrl

Cologne Technology
Review & Law

Hier geht es zur ganzen Ausgabe!

Reise in 15 Beiträgen durch die Legal-Tech-Welt:

Von Kolumbien bis nach Finnland
und von Compliance bis eSport.

LEGAL TECH LAB
COLOGNE