1. AUSGABE 2023

EBNER STOLZ

novus

INFORMATIONSTECHNOLOGIE

Die IT-Prüfung im Rahmen der Jahresabschlussprüfung nach neuen Regeln? Der ISA [DE] 315 (Revised 2019)

Deutsche Regelung zum Arbeitnehmerdatenschutz nicht EU-rechtskonform?

Künstliche Intelligenz: Die dunkle Seite der IT? – Zwischen Chancen, Risiken und Regularien –

Editorial

Sehr geehrte Leserin, sehr geehrter Leser,

wagen wir mit der ersten Ausgabe des novus IT 2023 einen Blick in die bunte und vielseitige Welt der IT.

Die IT-Prüfung im Rahmen der Jahresabschlussprüfung wird aufgrund des ISA (DE) 315 (2019 Revised) neuen (?) Regeln folgen müssen – und ist zwingend in die Jahresabschlussprüfung zu integrieren.

Der Finanzsektor muss seit 16.01.2023 den Digital Operational Resilience Act (DORA) beachten. Wir geben in dieser Ausgabe des novus IT einen Überblick, worauf es dabei ankommt.

Für Unternehmen, die elektronische Kassensysteme verwenden, besteht möglicherweise dringender Handlungsbedarf. Sie sollten überprüfen, ob bei ihnen als Zertifizierte Technische Sicherheitseinrichtung die Bundesdruckerei D-Trust TSE Version 1.0 der cv cryptovision GmbH eingesetzt wird. Für dieses Modul ist die Zertifizierung zum 01.01.2023 abgelaufen. Eine Übergangslösung besteht bis 31.07.2024 – jedoch nur, wenn bestimmte Vorkehrungen getroffen wurden. Um welche es sich hierbei handelt, lesen Sie in dieser Ausgabe!

Die Personalabteilungen werden sich aufgrund der aktuellen Rechtsprechung des EuGH darum kümmern müssen, wie sie den Arbeitnehmerdatenschutz ausgestalten, da zu befürchten steht, dass die nationalen Regelungen nicht EU-konform sind. Einzelheiten zur EuGH-Entscheidung und den Auswirkungen in nationalen Datenschutzrecht haben wir für Sie zusammengestellt.

Die fortschreitende Entwicklung der Künstlichen Intelligenz birgt zahlreiche Chancen und Risiken und ist spätestens mit ChatGPT in den Fokus der gesellschaftlichen und ethischen Auseinandersetzung gerückt. Wir setzen uns mit dieser Fragestellung in einem umfassenden Beitrag grundsätzlich auseinander – und lassen dabei auch die KI selbst zu Wort kommen. Auch richten wir den Blick auf die in diesem Zusammenhang zu erwartende Regulatorik.

Im Bereich der Kritischen Infrastrukturen sind Anfang des Jahres mit der NIS 2.0 und der RCE zwei zentrale Direktiven in Kraft getreten, wodurch die Anforderungen an die betroffenen Unternehmen deutlich steigen. Mehr dazu und über weitere Entwicklungen im Bereich der Informationstechnologie lesen Sie in dieser Ausgabe.

Wir wünschen Ihnen eine anregende Lektüre und stehen bei eventuellen Fragen gerne zur Verfügung.

Ihr GBIT

IT & WIRTSCHAFTSPRÜFUNG

Die IT-Prüfung im Rahmen der Jahresabschlussprüfung nach neuen Regeln? Der ISA [DE] 315 (Revised 2019) 4

Der Digital Operational Resilience Act (DORA): Eine Zusammenfassung des Status Quo 5

Dringender Handlungsbedarf bei Kassen mit D-TRUST TSE-Modul/cv cryptovision GmbH 8

Wie aus einer Kassennachschau eine Außenprüfung werden kann 9

Ordnungsmäßigkeitskriterien bei Navision aus Sicht des WPs 10

IT-RECHT

Digitale Produkte nachhaltig gestalten – ESG in IT- und Datenschutzrecht 12

Deutsche Regelung zum Arbeitnehmerdatenschutz nicht EU-rechtskonform? 13

Wer haftet für DSGVO-Verstöße in Unternehmen? 15

IT-SICHERHEIT

Künstliche Intelligenz: Die dunkle Seite der IT? – Zwischen Chancen, Risiken und Regularien – 16

NIS 2.0 und RCE – Next Level KRITIS 23

Die IT-Prüfung im Rahmen der Jahresabschlussprüfung nach neuen Regeln? Der ISA [DE] 315 (Revised 2019)

Im Dezember 2019 hat das International Auditing and Assurance Standards Board (IAASB), das sich um weltweit einheitliche Standards für Wirtschaftsprüfer bemüht, den überarbeiteten International Standard on Auditing (ISA) 315 „Identification and Assessing the Risks of Material Misstatement" veröffentlicht.

Durch das Institut der Wirtschaftsprüfer in Deutschland e. V. (IDW) wurde dieser internationale Standard ins Deutsche übersetzt sowie um nationale Besonderheiten ergänzt und als Prüfungsstandard „Identifizierung und Beurteilung der Risiken wesentlicher falscher Darstellungen" ISA [DE] 315 (Revised 2019) (im Folgenden kurz „ISA [DE] 315") veröffentlicht.

Dieser Standard ersetzt den aus dem Jahr 2002 stammenden IDW-Prüfungsstandard (IDW PS 330) „Abschlussprüfung bei Einsatz von Informationstechnologie". Er ist verpflichtend anzuwenden für Prüfungen von Abschlüssen, die am oder nach dem 15.12.2022 beginnen.

Kurz zusammengefasst: Die wesentliche Änderung besteht darin, dass die IT-Prüfung als Teil der Jahresabschlussprüfung deutlich an Bedeutung gewinnt, da die IT in unternehmerischen und damit natürlich auch in buchhalterischen Prozessen einen höheren Stellenwert einnimmt.

Der IDW PS 330 geht in die verdiente Rente

Das IDW legte mit dem IDW PS 330 bereits früh das Regelwerk fest, nach dem sich seither „Generationen" von IT-Prüferinnen und IT-Prüfern zu richten hatten, wenn eine IT-Systemprüfung im Rahmen der Jahresabschlussprüfung anstand. Der IDW PS 330 wurde am 24.09.2022 in der WPg 2002, S. 1167 ff. veröffentlicht. Wenn man bedenkt, wie die meisten ERP-Systeme im Jahr 2002 ausgestaltet waren – einzelne Modulbausteine mit minimaler (wenn überhaupt vorhandener) Integration – war der IDW PS 330 mehr als zeitgemäß und hat seine Zweckmäßigkeit über Jahre hinweg bewiesen und tut es im Grundsatz noch heute. Doch zwanzig Jahre sind eine lange Zeit – im IT-Umfeld tatsächlich sogar eher eine Ewigkeit. Angesichts der stetig wachsenden Bedeutung und der immer größer werdenden Komplexität der Unternehmen und Anzahl an Daten und damit der Einsatz von IT als integraler, weil steuernder Bestandteil von Prozessen und Abläufen, musste auch der Prüfungsansatz in der Jahresabschlussprüfung angepasst werden. Oder doch nur der Fokus?

Nicht alles neu, aber zeitgemäß

Der IDW PS 330 sieht die Beurteilung des IT-gestützten Rechnungslegungssystems hinsichtlich der Erfüllung gesetzlicher Anforderungen (Ordnungsmäßigkeits- sowie Sicherheitsanforderungen) vor, um eine Aussage über die Ordnungsmäßigkeit der Buchführung treffen zu können.

Dabei basiert dieser alte Standard auf den allgemeinen Anforderungen an die Prüfung des internen Kontrollsystems (IKS-Prüfung) durch den Abschlussprüfer, die wiederum im IDW PS 261 „Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken" dargestellt sind. Die IT-Systemprüfung gemäß PS 330 stellt also einen Ausschnitt aus der Prüfung des internen Kontrollsystems dar.

Auch mit dem Prüfungsstandard ISA [DE] 315 ist die IT-Prüfung ein Bestandteil der IKS-Prüfung, aber nun als ein integraler, nicht trennbarer Bestandteil. Der ISA [DE] 315 ist nicht der Prüfungsstandard für die IT-Prüfung im Rahmen der Jahresabschlussprüfung, sondern dient eben zentral der Risikoidentifikation durch den Abschlussprüfer.

Der Fokus liegt allgemein auf der Identifizierung und Beurteilung von Risiken wesentlicher falscher Darstellungen im Jahresabschluss.

In der Grundausrichtung entspricht der überarbeitete Standard den alten Prüfungsstandards 261 und 330. Allerdings wird hier

berücksichtigt, dass heute nahezu keine nicht IT-bezogenen Prozesse in den Unternehmen mehr vorhanden sind, weshalb die IT in aller Regel einen wesentlichen Risikobereich in den Unternehmen selbst, und nicht nur in der Jahresabschlussprüfung, darstellt.

Wie wird die IT-Prüfung in die Jahresabschlussprüfung heute „integriert"?

Zu Beginn der Jahresabschlussprüfung identifiziert der Wirtschaftsprüfer die für die Rechnungslegung sowie den Jahresabschluss relevanten Geschäftsprozesse. Hieraus ergeben sich dann die rechnungslegungsrelevanten IT-Systeme. Im nächsten Schritt werden die Risiken für die Jahresabschlussprüfung resultierend aus dem Einsatz dieser IT-Systeme identifiziert. Abhängig von dieser Risikobeurteilung werden die notwendigen IT-Prüfungshandlungen geplant.

Sowohl bei der Risikobeurteilung als auch im Rahmen der eigentlichen Prüfung erfolgt eine Betrachtung auf zwei Ebenen:

- Die Basis bilden die IT General Controls (kurz: ITGC). Im Wesentlichen betrachtet der Wirtschaftsprüfer dabei folgende Prüffelder:
  - Access Management
  - Change Management
  - IT-Betrieb
  - Outsourcing, sofern relevant.
- Die eigentlichen – auf das zu prüfende Zahlenwerk bezogenen – Prüfungshandlungen betreffen die applikations- und geschäftsprozessbezogenen Kontrollen (kurz: ITAC (IT Application Controls)).

Ziel der Prüfung ist es, für die ITACs festzustellen, inwieweit durch vorhandene Maßnahmen bzw. ITGCs sichergestellt wird, dass in dem jeweiligen Prozess keine Fehler entstehen (vorgelagerte Kontrollen) bzw. entstandene Fehler rechtzeitig entdeckt werden können (nachgelagerte Kontrollen).

Exemplarisch seien hier Freigabekonzepte, Liefersperren oder Abstimmreports genannt.

Voraussetzung dafür, dass die ITACs überhaupt Sicherheit für die Abschlussprüfung generieren, ist die Funktionsfähigkeit bzw. Ordnungsmäßigkeit des jeweiligen IT-Systems. Diese Ordnungsmäßigkeit wird durch die Funktionsfähigkeit oben genannter ITGCs und der damit einhergehenden Funktionsfähigkeit der IT-Prozesse sichergestellt.
So wird im Rahmen der ITGCs z. B. das Berechtigungskonzept sowie der Berechtigungsvergabeprozess geprüft. Nur wenn die Konzeption und der Prozess angemessen sind, ist eine Prüfung von Freigabeworkflows sinnvoll, da falsch vergebene Berechtigungen den Freigabeprozess konterkarieren würden.
Im Ergebnis wird festgestellt, ob auf die rechnungslegungsrelevanten IT-Systeme hinreichender Verlass ist und von einem Jahresabschluss ohne wesentliche Fehler ausgegangen werden kann. Nicht funktionierende Kontrollen bedeuten im ersten Schritt einen deutlich höheren Prüfaufwand, da kompensierend aufwendigere manuelle aussagebezogene Prüfungshandlungen durchgeführt werden müssen. Im schlimmsten Fall kann keine hinreichende Prüfungssicherheit erlangt werden. Beispielsweise kann bei Vorliegen von Massendaten im Geschäftsprozess eine rein aussagebezogene Prüfung nicht möglich sein, mit der Konsequenz, dass das Testat eingeschränkt oder versagt werden muss.

Was bedeutet das für die Unternehmens-IT?

Die IT ist heute kein schmückendes Beiwerk mehr, sondern ein zentrales Thema – und das nicht nur für das Unternehmen, sondern auch ganz explizit in der Jahresabschlussprüfung. Eine funktionierende IT ist eben nicht nur für die Abschlussprüfung relevant, sondern wird durch andere Compliance-Gebiete (z. B. Datenschutz oder GoBD) ebenso gefordert. Gerade auch im Bereich der steuerlichen Betriebsprüfung werden vermehrt IT-Themen aufgegriffen.

Daher empfehlen wir, sich intensiv mit den eigenen IT-Prozessen zu befassen.

Der Digital Operational Resilience Act (DORA): Eine Zusammenfassung des Status Quo

Am 27.12.2022 haben das Europäische Parlament und der Rat die Verordnung zur digitalen operationalen Resilienz, kurz DORA, verabschiedet. Diese ist bereits am 16.01.2023 in Kraft getreten. Sie hat zum Ziel, einheitliche Anforderungen für die Sicherheit von Netzwerk- und Informationssystemen festzulegen, die die Geschäftsprozesse von Finanzunternehmen unterstützen. Die betroffenen Unternehmen des Finanzsektors und die Behörden haben nun bis zum 17.01.2025 Zeit, die Verordnung umzusetzen und ein hohes Niveau an digitaler operationaler Resilienz sicherzustellen.

Fast zeitgleich mit der DORA-Verordnung wurde die Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie) veröffentlicht. Die DORA-Verordnung hat als lex specialis Anwendungsvorrang vor der NIS-2-Richtlinie. Ähnliches gilt in Bezug auf die ebenfalls Anfang 2023 in Kraft getretene Richtlinie (EU) 2022/2557 (REC-Richtlinie).

Anwendungsbereich der DORA-Verordnung

Der Geltungsbereich der DORA-Verordnung umfasst insgesamt 21 Unternehmenstypen; darunter fallen beispielsweise Banken, Wertpapierfirmen und Versicherungen. Eine Besonderheit von DORA ist, dass auch IKT-Drittdienstleister, d. h. Unternehmen, die digitale und Datendienste anbieten, einschließlich Anbieter von Cloud-Computing-Diensten, Software, Datenanalysediensten und Rechenzentren, in den Geltungsbereich der

Verordnung fallen. Zuvor waren IKT-Drittdienstleister nur indirekt über ihr Dienstleistungsverhältnis mit Finanzunternehmen von der aufsichtlichen Regulierung betroffen.

Dagegen fallen anders als in der Entwurfsfassung zunächst vorgesehen, Abschlussprüfer und Prüfungsgesellschaften erst einmal nicht unter den Geltungsbereich von DORA. Diesbezüglich wird es bis zum 17.01.2026 eine Evaluierung geben.

Zielsetzung

Mit der DORA-Verordnung werden im Wesentlichen die nachstehenden Zielsetzungen verfolgt:

- die Harmonisierung der Regelwerke,
- die Regelung der Zusammenarbeit zwischen den Behörden,
- die systematische Erhebung von IKT-Risiken, IKT-Störungen und Cyberbedrohungen.

Zur Zielerreichung sind in den insgesamt neun Kapiteln der Verordnung entsprechende Vorgaben definiert, die im Rahmen von weiteren Leitlinien, technischen Regulierungsstandards sowie technischen Umsetzungsstandards in den kommenden zwölf bis 18 Monaten, insb. durch die European Supervisory Authorities (ESA), noch präzisiert werden müssen.

Übersicht über die Kapitel der DORA-Verordnung

- Kapitel I: Allgemeine Bestimmungen
- Kapitel II: IKT-Risikomanagement
- Kapitel III: Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle
- Kapitel IV: Testen der digitalen operationalen Resilienz
- Kapitel V: Management des IKT-Drittparteienrisikos
- Kapitel VI: Vereinbarungen über den Austausch von Informationen
- Kapitel VII: Zuständige Behörden
- Kapitel VIII: Delegierte Rechtsakte
- Kapitel IX: Übergangs- und Schlussbestimmungen

In Bezug auf die Umsetzung der Vorgaben – insb. der Kapitel II, III, IV und V – gilt, wie bereits aus den Rundschreiben der Finanzaufsicht bekannt, der Grundsatz der Verhältnismäßigkeit. Zugleich gibt es für sog. „Kleinstunternehmen" Erleichterungen sowie weitere abgestufte Regelungen, wie bspw. einen vereinfachten IKT-Risikorahmen für bestimmte Unternehmen. Hier bietet es sich an, individuell zu prüfen, welche Vorgaben das eigene Unternehmen betreffen und in welchem Umfang diese umzusetzen sind.

Die für Finanzunternehmen und IKT-Drittdienstleister wesentlichsten Kapitel sind neben dem Kapitel I, das grundsätzliche Bestimmungen enthält, die Kapitel II, III, IV und VI.

Kapitel II – IKT-Risikomanagement

Kapitel II zum IKT-Risikomanagement enthält Vorgaben in Bezug auf den Aufbau eines internen Governance- und Kontrollrahmens für das Management von IKT-Risiken und einen damit verbundenen IKT-Risikomanagementrahmen für Finanzunternehmen. Auf der Governance- und Organisationsebene werden hierbei Aufgaben und Verantwortlichkeiten der Leitungsebene definiert. Diese bestehen neben der Einführung von Leitlinien u. a. auch in der Festlegung und Genehmigung einer Strategie für die digitale operationale Resilienz und der Genehmigung, Überwachung und Überprüfung der Umsetzung einer IKT-Geschäftsfortführungsleitlinie. Weiterhin stehen die Meldekanäle für die Leitungsebene hinsichtlich des Bezugs von IKT-Drittdienstleistungen im Fokus der Regelungen. Die Leitungsebene wird zudem verpflichtet, die eigenen Kenntnisse und Fähigkeiten in Bezug auf IKT-Risiken, anhand geeigneter Schulungen auf dem neuesten Stand zu halten.

Der gemäß der DORA-Verordnung umzusetzende IKT-Risikomanagementrahmen entspricht im Wesentlichen den klassischen Risikomanagementsystemen, wie sie bereits aus Best-Practice Standards (wie bspw. der ISO 270XX-Reihe) bekannt sind. Dabei bilden die Informations- und IKT-Assets die Grundlage. Für das Management der IKT-Risiken sind entsprechende Strategien, Leit- und Richtlinien, Verfahren sowie IKT-Protokolle und Tools zu implementieren. Die Funktionsweise des IKT-Risikomanagementsystems muss hierbei durch geeignete Überwachungs- sowie Lessons-Learned-Prozesse sichergestellt werden. Das Verfahren zum Management der IKT-Risiken besteht aus den einzelnen Verfahrensschritten

- Identifikation,
- Schutz und Prävention,
- Erkennung,
- Reaktion und Wiederherstellung,
- Lernprozesse und Weiterentwicklung sowie
- Kommunikation.

Dies entspricht dem bekannten Plan-Do-Check-Act (PDCA)-Zyklus. Die in den einzelnen Verfahren verordneten Vorgaben entsprechen im Wesentlichen den Anforderungen aus den XAIT (Informationsrisikomanagement, ((Operatives) Informationssicherheitsmanagement, IT-Notfallmanagement (inklusive Datensicherungs- und Wiederherstellungsverfahren)). Damit sind bereits jetzt viele der zukünftigen Vorgaben gelebte Praxis bei den Finanzunternehmen. An dieser Stelle ist hervorzuheben, dass das Finanzunternehmen mindestens jährlich, beim Auftreten von schwerwiegenden IKT-Vorfällen sowie nach aufsichtlichen Anweisungen oder Feststellungen eine Überprüfung und Dokumentation des IKT-Risikomanagementrahmens durchführen muss. Der Bericht ist auf Anfrage der zuständigen Behörde im Anschluss bereitzustellen.

Kapitel III – Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle

Nach Kapitel III der Verordnung haben Finanzunternehmen zwingend Prozesse für die Erkennung, Behandlung und Meldung von IKT-bezogenen Vorfällen und optional für Cyberbedrohungen einzurichten. Für die Klassifizierung der IKT-bezogenen Vorfälle werden in der Verordnung bereits spezielle Kriterien genannt. Dies sind:

- Anzahl und/oder Relevanz betroffener Kunden/Gegenparteien/Transaktionen und ob ein Reputationsschaden verursacht wurde,
- Dauer des IKT-bezogenen Vorfalls,
- Geografische Ausbreitung,
- Verbundener Verfügbarkeits-, Authentitäts-, Integritäts- oder Vertraulichkeitsverlust von Daten,
- Kritikalität der betroffenen Dienste,
- Wirtschaftliche Auswirkungen.

Entsprechende Wesentlichkeitsschwellenwerte, insb. zur Klassifizierung schwerwiegender IKT-bezogener Vorfälle, müssen noch in Form

eines technischen Regulierungsstandards durch die ESA definiert werden (die Frist für den Entwurf ist der 17.01.2024). Meldungen von identifizierten schwerwiegenden IKT-Vorfällen haben an die jeweils zuständige Behörde zu erfolgen. Dabei wird zwischen Erstmeldung, Zwischenmeldung und Abschlussmeldung unterschieden. Auch bzgl. Inhalt und Frist für die Meldeprozesse schwerwiegender IKT-Vorfälle sowie der Ausgestaltung der Meldeformulare und Verfahren sind noch durch die ESA technische Regulierungsstandards und technische Durchführungsstandards zu erarbeiten (die Frist für den Entwurf ist der 17.07.2024).

Kapitel IV – Testen der digitalen operationalen Resilienz

Kapitel IV der Verordnung verpflichtet Finanzunternehmen, ein Testprogramm für das Testen der digitalen operationalen Resilienz zu erstellen und umzusetzen. Das Testprogramm für Tests soll unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit erstellt werden und kann hierbei u. a. folgende Testverfahren konkret beinhalten:

- Schwachstellenbewertung und -scans,
- Open-Source-Analysen,
- Netzwerksicherheitsbewertungen,
- Lückenanalysen,
- Überprüfungen der physischen Sicherheit
- Fragebögen und Scans von Softwarelösungen,
- Quellcodeprüfungen,
- Szenariobasierte Tests,
- Kompatibilitätstests, Leistungstests,
- End-to-End-Tests und Penetrationstests.

Finanzunternehmen müssen im Rahmen der Testplanung sicherstellen, dass bei allen IKT-Systemen und -Anwendungen, die kritische oder wichtige Funktionen unterstützen, mindestens einmal jährlich angemessene Tests durchgeführt werden. Hierbei können die Tests durch unabhängige interne oder externe Parteien erfolgen.

Weiterhin müssen bestimmte Finanzunternehmen, die zuvor von den zuständigen Behörden anhand festgelegter Kriterien ermittelt und benannt worden sind, erweiterte Tests auf Basis von Threat-Led Penetration Tests (TLPT) durchführen. Dies sind sog. Red-Team-Tests, bei denen auf der Grundlage einer vorangegangenen Bedrohungsanalyse (nicht nur technische) Angriffsszenarien am Live-Produktionssystem getestet werden. Entsprechende Tests sind mindestens alle drei Jahre durch die betroffenen Finanzunternehmen durchzuführen. Zur Präzisierung der Test müssen zuvor durch die ESA im Einvernehmen mit der EZB und im Einklang mit dem TIBER-EU-Rahmen noch technische Regulierungsstandards erarbeitet werden (die Frist für den Entwurf ist der 17.07.2024).

Kapitel V – Management des IKT-Drittparteienrisikos

Kapitel V der Verordnung umfasst insb. zwei Anforderungsbereiche. Zum einen geht es um Vorgaben in Bezug auf das Management von IKT-Drittparteienrisiken im Sinne von (Risiko-) Steuerungsprozessen und dem Vertragsmanagement für ausgelagerte IKT-Drittdienstleistungen. Zum anderen geht es um die Überwachung sog. „kritischer" IKT-Drittdienstleister direkt durch die europäische Finanzaufsicht.

Der erste Anforderungsbereich entspricht im Wesentlichen den bereits bestehenden Anforderungen der AT 9 MaRisk zum Umgang mit (wesentlichen) Auslagerungen mit Erweiterungen insb. zur Berichterstattung von bezogenen IKT-Drittdienstleistungen an die zuständige Behörde.

Weitaus spannender ist der zweite Anforderungsbereich. Die Vorgaben richten sich direkt an IKT-Drittdienstleister. Nach der Verordnung erfolgt zukünftig eine Einstufung der IKT-Drittdienstleister durch die zuständigen Behörden. Hierzu existiert bereits ein entsprechender Kriterienkatalog, der im Rahmen eines delegierten Rechtsaktes bis zum 17.07.2024 durch die Europäische Kommission präzisiert werden muss. Erst im Anschluss darf eine Einstufung der IKT-Drittdienstleister erfolgen. Wird ein IKT-Drittdienstleister als „kritisch" eingestuft, hat dies eine Überwachung durch eine der drei europäischen Finanzaufsichtsbehörden (federführende Überwachungsbehörde) zum Ergebnis. Die Überwachung erfolgt nach einer Bewertung auf der Basis eines jährlich anzupassenden Überwachungsplans und in Abstimmung mit weiteren Aufsichtsbehörden. Hierzu sind entsprechende Foren zur Zusammenarbeit und Koordination vorgesehen. Im Rahmen ihrer Überwachungstätigkeit verfügt die federführende Überwachungsbehörde u. a. auch über das Recht, Empfehlungen auszusprechen, die in Form von Maßnahmen durch den „kritischen" IKT-Drittdienstleister umzusetzen sind. Bei Nicht-Folgeleistung können empfindliche Zwangsgelder festgelegt werden. Die Kosten für die Überwachung muss der „kritische" IKT-Drittdienstleister selbst tragen.

Kapitel VI – Vereinbarungen über den Austausch von Informationen

Kapitel VI der Verordnung zielt darauf ab, Hürden zu überwinden, um den Finanzunternehmen sowie ggf. weiteren Adressaten (z. B. IKT-Drittdienstleister) hinsichtlich Cyberbedrohungen und dem Umgang mit Cyberbedrohungen einen Austausch untereinander zu ermöglichen. Hierzu sollen entsprechende Vereinbarungen zum Austausch von Informationen geschaffen werden. Dies soll auf freiwilliger Basis erfolgen.

Fazit

Zusammenfassend kann festgehalten werden, dass nicht alle Vorgaben der DORA-Verordnung neu sind, sondern spätestens seit der Veröffentlichung der XAIT existieren und bereits umgesetzt wurden (z. B. IKT-Risikomanagementrahmen). Gleichzeitig bringt die Verordnung aber auch Erweiterungen sowie Harmonisierungen von z. T. bestehenden Vorgaben mit sich (z. B. Meldeprozessen), die noch umzusetzen sind. Wesentlichste Neuerung ist die teilweise verpflichtende Durchführung von TPLT-Tests für Finanzunternehmen sowie die direkte Überwachung von „kritischen IKT-Drittdienstleistern" durch die europäische Finanzaufsicht.

Grundsätzlich gilt, dass die Uhr bereits tickt und sich jedes Finanzunternehmen bzw. die betroffenen IKT-Drittdienstleister mit der Umsetzung der Vorgaben spätestens jetzt beschäftigen sollten, auch wenn in den nächsten Monaten noch einige Präzisierungen – inklusive der Harmonisierung der bestehenden europäischen und nationalen gesetzlichen und aufsichtlichen Regelungen – folgen werden.

Dringender Handlungsbedarf bei Kassen mit D-TRUST TSE-Modul/cv cryptovision GmbH

Allen Unternehmen, die elektronische Kassen einsetzen, wird dringend empfohlen zu überprüfen, ob bei ihnen als sog. Zertifizierte Technische Sicherheitseinrichtung („TSE") die „Bundesdruckerei D-TRUST TSE, Version 1.0" der cv cryptovision GmbH verwendet wird.

Für dieses in der Praxis weit verbreitete TSE-Modul ist die Zertifizierung zum 07.01.2023 abgelaufen. Eine Übergangsregelung bis spätestens 31.07.2024 besteht, allerdings nur, wenn man jetzt richtig handelt.

Hintergrund

Seit dem 01.01.2020 müssen elektronische Aufzeichnungssysteme mit Kassenfunktion gemäß § 146a AO sowie den Bestimmungen der Kassensicherungsverordnung mit einer TSE ausgestattet sein. Jede TSE-Variante muss nach § 146a Abs. 3 Satz 2 AO durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert sein.

Hinweis: Technisch basiert die Zertifizierung auf mehreren einzelnen Zertifizierungsnormen entsprechend der jeweiligen Komponente:

- TR-Zertifizierung nach der Technischen Richtlinie BSI TR-03153
- CC-Zertifizierung nach dem Schutzprofil BSI-CC-PP-0105-2019 (SMA-ERS)
- CC-Zertifizierung nach dem Schutzprofil BSI-CC-PP-0104-2019 (CSP) in der Konfiguration nach BSI-CC-PP-0107 (Time Stamp Service and Audit) oder BSI-CC-PP-0108 (Time Stamp Service, Audit and Clustering).

Befristung der Zertifizierung

Die erteilten Zertifikate sind auf acht Jahre befristet und beinhalten die Auflage, nach fünf Jahren eine Neubewertung durchzuführen.

Im Rahmen der Einführungsphase der TSE bestand eine Übergangsregelung, wonach nicht alle Teilzertifikate in Gänze erfüllt sein mussten, sondern – unter bestimmten Umständen – vereinfachte Begutachtungen durch das BSI stattfinden konnten. Die Gültigkeit dieser Zertifikate war auf 15 Monate befristet. Für das von der Bundesdruckerei über die D-TRUST GmbH vertriebene, D-TRUST TSE-Modul Version 1 der Firma cv cryptovision GmbH lag eine solche Zertifizierung i. S. d. Übergangsregelung vor. Diese ist nun mit Wirkung zum 07.01.2023 abgelaufen.

Aufgrund der großen Verbreitung dieses TSE-Moduls hat das Bundesfinanzministerium (BMF) bereits mit Schreiben vom 13.10.2022 (BStBl. 2022 I, S. 1436) eine Übergangsregelung bis zum 31.07.2023 gewährt. Mit Schreiben vom 16.03.2023 (Az. IV A 4 – S 0319/20/10002 :009) wurde diese Übergangsregelung bis zum 31.07.2024 verlängert.

Voraussetzung für die Inanspruchnahme der Übergangsregelung ist, dass die Inanspruchnahme dem zuständigen Finanzamt schriftlich oder elektronisch mitgeteilt wird bzw. aufgrund des ersten Schreibens vom 13.10.2022 bereits mitgeteilt wurde. Spätestens ab dem Zeitpunkt, ab dem die Zertifizierung der TSE Version 2 der Firma cv cryptovision GmbH vorliegt, ist aber der Austausch der TSE bei allen Kassen umgehend durchzuführen.

Darüber hinaus ist die Einhaltung dieser Voraussetzungen, also

- das Vorliegen des betreffenden TSE-Moduls,
- das Schreiben an die Finanzverwaltung sowie
- die Maßnahmen, die sicherstellen, dass der Austausch der TSE umgehend erfolgen wird, sobald die Version 2 zertifiziert ist,

in der Verfahrensdokumentation zur Kassenführung darzulegen und entsprechend den gesetzlichen Aufbewahrungsfristen aufzubewahren.

Lösungsansätze

Weder von Seiten der D-Trust GmbH noch von Seiten der Herstellerfirma wurden bisher konkrete Informationen bzgl. des Standes der neuen Version veröffentlicht; man arbeite wohl an einer Lösung.

Da das erste Schreiben des BMF vom 13.10.2022 nur allgemein von einem Austausch – im Zweifel auch gegen eine andere TSE eines anderen Herstellers – ausging, musste sowohl technisch als auch finanziell von einem größeren Aufwand ausgegangen werden. Nachdem im zweiten Schreiben vom 16.03.2023 nun aber die 2. Version der gleichen Herstellerfirma konkret angesprochen wurde, besteht die leise Hoffnung, dass das BMF hier tiefergehende Informationen besitzt und tatsächlich eine (einfache) technische Lösung fristgerecht erfolgen kann.

Gleichwohl empfehlen wir, dass betroffene Unternehmen – soweit noch nicht geschehen – unverzüglich die Meldung an das Finanzamt vornehmen und Entsprechendes in der Verfahrensdokumentation ergänzen.

Des Weiteren raten wir, dass die Unternehmen möglichst frühzeitig mit dem jeweiligen Kassenhersteller Kontakt aufnehmen, um das weitere Vorgehen abzustimmen (und dieses Vorgehen ebenfalls in der Verfahrensdokumentation abbilden).

Wie aus einer Kassennachschau eine Außenprüfung werden kann

Mit dem Gesetz zum Schutz vor Manipulation an digitalen Grundaufzeichnungen vom 22.12.2016 wurde die Möglichkeit der sog. Kassen-Nachschau in die Abgabenordnung aufgenommen (§ 146b AO; anwendbar seit 01.01.2018).

Seither darf die Finanzverwaltung unangekündigte Kassenprüfungen bei Steuerpflichtigen vornehmen.

Das Prüfrecht der Finanzverwaltung umfasst insb. die folgenden Bereiche:

- Zutrittsrecht zu den Geschäftsräumen und Beobachtung von Kassenvorgängen,
- Möglichkeit zur Durchführung anonymer Testkäufe,
- Verlangen eines Kassensturzes, d. h.,
  - Zählen des tatsächlich vorhandenen Kassenbestandes,
  - Einfordern der Mitwirkung von Personen mit ausreichenden Zugriffs- und Benutzerrechten,
- Vorlage der Verfahrensdokumentation zu den Kassen bzw. zu dem Kassenprozess.

Werden im Rahmen einer solchen Nachschau Feststellungen getroffen, können die Folgen weitreichend sein.

Nach der Kassenprüfung ist vor der Außenprüfung

Werden im Rahmen einer Kassennachschau bestimmte Feststellungen getroffen, kann dies für die Finanzbehörde gemäß § 146b Abs. 3 AO Anlass genug sein, direkt zu einer Außenprüfung („Betriebsprüfung") nach § 193 AO überzugehen.

Bisher war jedoch der Wortlaut des Gesetzes, insb. der Begriff „Anlass", noch nicht konkretisiert und damit Auslegungssache. Nunmehr hat jedoch das FG Hamburg gemäß Urteil vom 30.08.2022 (Az. 6 K 47/22) der Finanzverwaltung einen großen Ermessensspielraum bei der Anordnung einer Außenprüfung zugestanden.

Mit dem genannten Urteil des FG Hamburg gibt es jetzt erstmals eine finanzgerichtliche Konkretisierung, bei welchen Anlässen die Finanzverwaltung nach einer Kassennachschau zu einer Außenprüfung übergehen kann.

Im Streitfall konnte die Steuerpflichtige im Rahmen einer Kassennachschau die angeforderten Unterlagen nicht zeitnah aushändigen. Daraufhin wurde – 3 ½ Wochen nach der Kassennachschau – der Übergang zur Außenprüfung nach § 146b Abs. 3 AO vollzogen. Obwohl die Steuerpflichtige zwei Wochen nach der Nachschau die relevanten Unterlagen noch aushändigen konnte, wurde entschieden, dass aus Sicht des Finanzgerichtes die nicht zeitnahe Zurverfügungstellung der Nachweise innerhalb der kurzen Frist von zwei Wochen ein alleiniger und ausreichender Anlass für die Finanzbehörde darstellen kann, direkt zur regulären Außenprüfung übergehen zu dürfen.

Im betreffenden Fall wurde von der Finanzbehörde zusätzlich noch angeführt, dass es aus ihrer Sicht inhaltliche Unstimmigkeiten bei den erfassten Kassenbelegen gab. Dies wurde von der Steuerpflichtigen bestritten. Hierzu führte das Finanzgericht Folgendes aus: „Demnach handelt es sich bei der Anordnung des Übergangs zur Außenprüfung um eine Ermessensentscheidung der Finanzbehörde. Die Möglichkeit einer gerichtlichen Überprüfung beschränkt sich deshalb lediglich auf mögliche Ermessensfehler der Finanzbehörde. Diese wurden im vorliegenden Fall nicht gesehen."

Die Konsequenzen

Für die Praxis bedeutet dies, dass jeder Verstoß gegen die formale Ordnungsmäßigkeit sowie jeder vermutete inhaltliche Fehler ausreichend sein können, um begründet zu einer regulären Betriebsprüfung überzugehen. Eine Grenze sei nach dem Finanzgericht lediglich dann erreicht, wenn die Feststellungen des Prüfers greifbar gesetzeswidrig sind.

Hinweis: Gegen das Urteil wurde Nichtzulassungsbeschwerde beim BFH eingelegt. Es bleibt abzuwarten, ob der BFH die Meinung des Finanzgerichts teilt.

In jedem Fall ist Kassenbetreibern dringend zu empfehlen, sich auf mögliche Kassennachschauen vorzubereiten. Insb. sollten angemessene Prozesse etabliert und entsprechende Dokumentationen angefertigt werden, sofern dies noch nicht erfolgt ist. Vor allem sollte sichergestellt werden, dass das anwesende Personal vor Ort bei der Kasse im Fall einer unangekündigten Kassenprüfung, mit den entsprechenden Zugriffs- und Benutzerrechten ausgestattet und auch in der Lage ist, direkte Einsicht in die Kassendaten zu ermöglichen oder die Daten auf Verlangen herausgeben zu können. Eine ausreichende Information bzw. Schulung des Personals sollte nicht außer Acht gelassen werden.

Daneben kann auch die Vorlage der Verfahrensdokumentation zu den Kassen bzw. dem Kassenprozess im Rahmen der Nachschau gefordert werden. Diese sollte also in aktueller Fassung vor Ort bei der Kasse vorliegen und unverzüglich herausgegeben werden können.

Ordnungsmäßigkeitskriterien bei Navision aus Sicht des Wirtschaftsprüfers

In der Jahresabschlussprüfung ist es unerlässlich, die Ordnungsmäßigkeitskriterien und die sachgerechte Integration eines Enterprise Resource Planning (ERP) Systems zu bewerten, da das ERP-System eine zentrale Rolle bei der Rechnungslegung, der Unterstützung der finanziellen Berichterstattung und der Gestaltung der internen Kontrollen eines Unternehmens einnimmt. Die finanzielle Berichterstattung ist von der Richtigkeit und Vollständigkeit der im ERP-System hinterlegten Daten abhängig. Um diese Risiken zu minimieren, evaluieren Wirtschaftsprüfer die Funktionsfähigkeit und sachgerechte Integration des ERP-Systems, um sicherzustellen, dass es den gesetzlichen und regulatorischen Anforderungen entspricht sowie eine verlässliche finanzielle Berichterstattung unterstützt.

Gemäß Prüfungsstandard ISA [DE] 315 (Revised 2019) hat der Wirtschaftsprüfer die Ordnungsmäßigkeitskriterien und Risiken in Bezug auf die elektronische Buchführung zu identifizieren und zu bewerten. Hierzu gehört auch die Beurteilung der IT-Systeme und ihrer Kontrollen. Konkret bedeutet dies, dass Wirtschaftsprüfer bei der Prüfung von Unternehmen beurteilen müssen, ob das IT-System und die IT-Prozesse des Unternehmens geeignet sind, um die Risiken im Zusammenhang mit den Jahresabschlüssen des Unternehmens zu minimieren.

Möglichkeiten zur Beurteilung der Ordnungsmäßigkeit

Bei einer vorliegenden Softwarebescheinigung nach dem Prüfungsstandard IDW PS 880 („Prüfung von Softwareprodukten") wird dem Softwarehersteller oder -anwender vor Implementierung im jeweiligen Unternehmensumfeld bestätigt, dass die Software bei sachgerechter Anwendung eine Rechnungslegung ermöglicht, die den Grundsätzen ordnungsmäßiger Buchführung entspricht. Die Prüfung bezieht sich gemäß IDW PS 880 auf folgende Bereiche:

- Softwareentwicklungsverfahren,
- Angemessenheit der Programmfunktionen,
- Dokumentation,
- Funktionsfähigkeit der Programmfunktionen.

Um im Rahmen der Jahresabschlussprüfung die Funktionsfähigkeit und die sachgerechte Integration des ERP-Systems in die prozessuale Infrastruktur des Unternehmens zu bewerten, wird geprüft, ob die im organisatorischen Umfeld des Programmsystems geltenden handels- und steuerrechtlichen Vorschriften eingehalten werden und ob das interne Kontrollsystem beim Anwender eine zuverlässige und sichere Anwendung der Software gewährleistet. Dabei werden u. a. folgende Aspekte betrachtet:

- Anforderungen und Einstellungen bezüglich der Systemkonfiguration,
- Protokollierung von Systemaktivitäten,
- Rechtevergabe an Nutzer und Gruppen,
- Funktionalitäten und individuelle Anpassungen,
- Verarbeitungs- und Buchungskontrollen,
- Datensicherung und -wiederherstellung.

Die genannten Anforderungen ergeben sich aus dem Handels- und Steuerrecht (HGB und AO) und werden durch die Grundsätze ordnungsmäßiger Buchführung, GoBD, weiter konkretisiert.

Hinweis: Als Verwaltungsanweisung stellen die GoBD eine Meinungsäußerung des Ministeriums dar, die gegenüber den nachgeordneten Dienststellen Verbindlichkeitscharakter hat.

Prüfungshandlungen zur Feststellung der Ordnungsmäßigkeit am Beispiel des Einsatzes von Microsoft D365 Business Central

Für das ERP-System Microsoft Dynamics 365 Business Central (nachfolgend D365 BC) bietet sich ein tabellenorientierter Prüfungsansatz an. Hierbei werden definierte Tabellen und Felder aus D365 BC mittels der Standardfunktion „Datenexporte" aus dem System exportiert. Anschließend werden die auf diese Weise gewonnenen Informationen durch einen qualifizierten Prüfer ausgewertet.

Zunächst erfolgt die Beurteilung der Angemessenheit kritischer Systemparameter. Hierzu zählen u. a. die Auswertung spezieller Parameter in den Einrichtungstabellen

- „Finanzbuchhaltung Einrichtung",
- „Benutzer Einrichtung",
- „Lager Einrichtung",
- „Debitoren & Verkauf Einrichtung",
- „Kreditoren & Einkauf Einrichtung" und
- „Anlageneinrichtung".

Hier wird beispielsweise dem Risiko begegnet, dass die Einrichtung für das Finanzmanagement den gesetzlichen und organisatorischen Regelungen widersprechen, welche falsche bzw. nicht nachvollziehbare Bilanzansätze zur Folge haben können.

Der Zugang zu Programmfunktionen und Daten wird mittels einer Analyse der aktiven Authentifizierungsmethoden und der systemseitig vergebenen Berechtigungen, den sog. Rollen, gegen das vom Mandanten erstellte Berechtigungskonzept und Best-Practice-Erfahrungswerte abgeglichen. Beispielsweise müssen Datenbanken mit vertraulichen Daten vor nicht autorisiertem Systemzugriff geschützt werden.

Aus einer generellen Compliance-Sicht kommt dem Thema Zugriffschutz und Informationssicherheit eine herausragende Bedeutung zu. Im Fokus der Berechtigungsprüfung steht die Identifizierung von Benutzern mit weitreichenden Berechtigungen im System, wie beispielsweise der Rolle „SUPER". Mit der Rolle SUPER hat ein Benutzer uneingeschränkte Zugriffsrechte in einem D365 BC System und damit weit über das hinaus, was für seinen regulären Tätigkeitsbereich zulässig und notwendig sein sollte. Sofern Benutzer mit dem Berechtigungsobjekt „ÄNDPROT-LÖSCHEN" (Änderungsprot.-Posten löschen) vorhanden sind, kann dies einen Verstoß insb. gegen die Grundsätze der Nachvollziehbarkeit, Unveränderlichkeit und Funktionstrennung darstellen.

Bei der Prüfung in der Änderungsprotokoll-Einrichtung wird sichergestellt, dass für die rechnungslegungsrelevanten Tabellen die Protokollierung aktiviert ist. Ist dies nicht der Fall, können Änderungen an diesen Tabellen nicht nachvollzogen werden. Dies stellt einen Verstoß gegen den Grundsatz der Unveränderlichkeit der Daten und der Nachvollziehbarkeit dar.

Um die Funktionsfähigkeit und die sachgerechte Integration des ERP-Systems in die prozessuale Infrastruktur des Unternehmens zu bewerten, werden bei der Prüfung auch allgemeine Aspekte, wie die (Weiter-)Entwicklung des Systems im Rahmen des allgemeinen Entwicklungs- und Change-Prozesses des Unternehmens, berücksichtigt. Hierzu werden die vorgenommenen Changes analysiert und mittels einer Stichprobe die Wirksamkeit der etablierten Kontrollen validiert.

Die Anforderungen an die Funktionalität der Beleg- und Kontenfunktionen werden anhand von Systemeinstellungen und (Buchungs-)Logiken im System betrachtet. Der sog. Journal Entry Test kann die Ergebnisse der Prüfung weiter unterstützen.

Hinweis: Hierbei handelt es sich um eine datenbasiere Analyse des Hauptbuches um sicherzustellen, dass Buchungen des Unternehmens ordnungsgemäß dokumentiert und gebucht werden.

Im Rahmen der Jahresabschlussprüfung ergeben sich somit hohe Anforderungen an die verwendeten Systeme, die Organisation und die IT-Infrastruktur des Unternehmens. Die Prüfung der technischen Parameter hinsichtlich Sicherheit, ordnungsgemäßer und GoB-konformer Einrichtung auf Ebene vom ERP-System selbst und darüber hinaus auch auf Betriebssystem- und Datenbankebene stehen verstärkt im Fokus der Prüfung.

Neben der Bewertung der Ordnungsmäßigkeit und der sachgerechten Integration des ERP-Systems in die (prozessuale) Infrastruktur des Unternehmens sind die Einhaltung von handels- und steuerrechtlichen Vorschriften und die Gewährleistung einer zuverlässigen und sicheren Anwendung der Software zu beurteilen. Die Prüfungshandlungen erfolgen risikoorientiert und beziehen sich auf die Kontrolle der IT-Systeme sowie der Implementierung systembezogener Kontrollen.

Digitale Produkte nachhaltig gestalten – ESG in IT- und Datenschutzrecht

Die Bereiche Umwelt, Soziales und Governance (ESG) haben in den letzten Jahren deutlich an Bedeutung gewonnen. Bei der Datenverarbeitung und der Nutzung von IT-Systemen stellen sich zahlreiche Nachhaltigkeitsfragen. Um den Energie- und Ressourcenverbrauch zu reduzieren, kann der Einsatz umweltschonender Hard- und Software im Rahmen von Beschaffungsverträgen in Betracht gezogen werden. Besonders effektiv können zudem die längere Nutzungsdauer sowie die Möglichkeit zur Reparatur elektronischer Produkte sein. Doch auch der Datenschutz und die Datensicherheit sind wesentliche ESG-Themen.

ESG im Bereich IT-Recht

Bekanntermaßen verursachen digitale Dienste, die Herstellung von Endgeräten sowie weitere Bereiche in der IT wesentliche Emissionen. Physische Bestandteile digitaler Produkte sowie die darauf installierte Software weisen häufig eine verhältnismäßig kurze Nutzungsdauer auf. Oft liegt dies an irreparablen, defekten Einzelteilen, fehlender Kompatibilität mit dem Betriebssystem oder daran, dass die Hersteller keine Aktualisierungen der Software mehr zur Verfügung stellen. Zunehmend stellt sich bei der Nutzung elektronischer Produkte die Frage nach deren Lebensdauer und dem Umgang mit veralteten Vorgängerprodukten. Häufig müssen die Produkte neu beschafft werden.

Die Defizite in Sachen Nachhaltigkeit haben sowohl der nationale Gesetzgeber als auch die EU erkannt. Mit der Einführung des digitalen Vertragsrechts im BGB hat der nationale Gesetzgeber umfassende und langfristige Updatepflichten geschaffen. Bei der Bereitstellung digitaler Produkte und Waren mit digitalen Elementen müssen diese für die erwartete Nutzungsdauer aktuell gehalten werden. Des Weiteren sind Bestrebungen des nationalen Gesetzgebers sowie der EU erkennbar, die darauf abzielen, ein gesetzlich geregeltes wirksames „Recht auf Reparatur" zu begründen. Durch die langfristige Bereitstellung von Ersatzteilen sollen Hersteller dazu verpflichtet werden, ihre Produkte nachhaltiger nutzbar zu machen.

In diesem Zusammenhang hat die EU-Kommission am 30.03.2022 den Entwurf einer neuen Ökodesign-Verordnung für nachhaltige Produkte vorgelegt. Mit diesem Vorschlag möchte sie die derzeit geltende Ökodesign-Richtlinie (RL 2009/125/EG) ersetzen und für eine Vermarktung umweltfreundlicherer und kreislauforientierter Produkte innerhalb der EU sorgen. Die seit 2009 bestehende alte Richtlinie legte nur einen Rahmen für die Festlegung von Anforderungen in Bezug auf die umweltgerechte Gestaltung energieverbrauchsrelevanter Produkte fest. Der Anwendungsbereich des neuen Regelungsrahmens erstreckt sich auf alle physischen Waren, die in Verkehr gebracht werden sollen, mit wenigen Ausnahmen bei Lebens- oder Arzneimitteln. Die Regelungen betreffen etwa die Haltbarkeit, Wiederverwendbarkeit, Energie- und Ressourceneffizienz von Produkten oder die Menge deren voraussichtlicher Abfallstoffe. Ziel ist es, Energieeffizienz, Kreislaufwirtschaft und Recycling im Produkthandel durch erhöhte Ökodesign-Anforderungen zu verbessern. Auf diese Weise sollen Produkte mit einem geringen Klima- und Umweltfußabdruck EU-weit zur „Norm" werden. Eine Gemeinsamkeit der Richtlinie und der Verordnung besteht darin, dass die EU-Kommission dazu ermächtigt wird, für bestimmte Kategorien von Produkten delegierte Rechtsakte zu erlassen, in denen dann erst die konkreten Anforderungen an die spezifischen Produktgruppen geregelt werden. Bei diesen Rechtsakten wird es sich in der Regel um Durchführungsverordnungen handeln, die in allen Mitgliedsstaaten unmittelbare Geltung entfalten. So wurden bereits Anforderungen an Haushaltswaschmaschinen und Haushaltstrockner oder an Server und Datenspeicherprodukte erlassen. Im August 2022 wurde zudem ein Regulierungsvorschlag zu Anforderungen an die umweltgerechte Gestaltung von Handys, schnurlosen Telefonen und Tablets veröffentlicht.

Datensicherheit und Datenschutz als wesentliche ESG-Elemente

Ist von ESG die Rede, denkt man zuerst an die Komponente Environmental. Häufig wird vergessen, dass sich Aufsichtsbehörden auch auf den Datenschutz und die Datensicherheit, als zwei wesentliche ESG-Themen, konzentrieren. So werden derzeit im Rahmen von ESG zahlreiche Kennzahlen entwickelt, anhand derer Unternehmen künftig beurteilt werden sollen. Beispiele für solche Kennzahlen sind u. a. die Wahrscheinlichkeit von Sicherheitsvorfällen wie Datenschutzverletzungen oder das von einem Unternehmen verarbeitete Volumen der personenbezogenen Daten. Der Datenschutz ist aber nicht nur eine gesetzliche Vorgabe, die es einzuhalten gilt. Er bietet auch die Chance für Unternehmen, Punkte im Rahmen von ESG zu sammeln.

Im Rahmen der Datenwirtschaft ist für viele Unternehmen die ESG-Komponente Governance der einfachste Ausgangspunkt. Aufgrund der zunehmenden Bedeutung von Mitarbeiter- und Verbraucherdaten für Unternehmen in sämtlichen Branchen ist das Aufzeigen der wirksamen Governance Aufgabe der Geschäftsleitung. Denkbar ist, dass in nicht allzu ferner Zukunft formelle Bescheinigungen von Datenschutzmanagementsystemen oder die Einführung verbindlicher Unternehmensrichtlinien zur Governance-Komponente der ESG-Wertungen beitragen.

Je nach Branche und Geschäftsmodell eines Unternehmens kann die Wertung auch mit Blick auf die ESG-Komponente Social verbessert werden. Hier spielt auch der Datenschutz eine wichtige Rolle. Bei der Implementierung datenintensiver Technologien und künstlicher Intelligenz benötigen Unternehmen Programme für Datenschutz und Datenethik. Dabei muss nicht nur die datenschutzrechtliche Regulatorik gewährleistet werden. Die Modelle müssen und können auch positive soziale Ergebnisse erzielen, wie etwa den Abbau von Ungleichheiten zwischen Geschlechtern sowie ethnischen und sozioökonomischen Gruppen.

Unternehmen aller Größen betroffen

Sowohl die bereits bestehenden Vorgaben als auch die noch in den Startlöchern stehenden Regelwerke haben große Auswirkungen auf Unternehmen, die digitale Produkte beziehen, vertreiben oder mit der Verarbeitung personenbezogener Daten befasst sind. Nachhaltigkeitsfragen sind längst kein Thema von morgen mehr und betreffen Unternehmen aller Größenordnungen. Unternehmen sollten sich mit der sich fortlaufend ändernden Rechtslage vertraut machen und erforderliche Maßnahmen ergreifen. Die gesetzlichen Anforderungen an digitale Produkte müssen ebenso umgesetzt werden, wie auch die Prüfung von Lieferanten und Dienstleistern erfolgen muss. Zudem ist eine Datenschutz-Compliance im Sinne des nachhaltigen und rechtssicheren Umgangs mit personenbezogenen Daten unumgänglich.

Deutsche Regelung zum Arbeitnehmerdatenschutz nicht EU-rechtskonform?

Der EuGH hat Ende März in einer aktuellen Entscheidung klargestellt, dass spezifischere Vorschriften zur Datenverarbeitung im Beschäftigungskontext nur in dem durch die DSGVO vorgegebenen Rahmen zulässig sind. Wird dieser Rahmen nicht eingehalten, sind nationale Regelungen unwirksam und es gelten die Grundsätze der DSGVO. Ob der in Deutschland geregelte Arbeitnehmerdatenschutz dem vollumfänglich gerecht wird, darf bezweifelt werden.

Was lag dem EuGH zur Entscheidung vor?

Gegenstand des Streits war die Verarbeitung der personenbezogenen Daten von Lehrerinnen und Lehrern während der COVID-19-Pandemie bei der Durchführung von Videokonferenz-Livestreams für den hybriden Schulunterricht. In der vom EuGH entschiedenen Rechtssache ging es konkret um eine hessische Regelung im Landesdatenschutzgesetz zum Arbeitnehmerdatenschutz. Auf Basis dieser Regelung sah es das Hessische Kultusministerium nicht für erforderlich an, von Lehrerinnen und Lehrern eine datenschutzrechtliche Einwilligung für die Videokonferenz-Livestreams einzuholen. Schüler hingegen wurden um deren Einwilligung, ggf. vertreten durch die Eltern, gebeten. Sowohl das Hessische Kultusministerium als auch das zuständige Verwaltungsgericht sahen auf die Klage des Hauptpersonalrats der Lehrerinnen und Lehrer in der hessischen Regelung zum Arbeitnehmerdatenschutz eine „spezifischere Vorschrift" im Sinne des Art. 88 Abs. 1 DSGVO, die die Verarbeitung vorrangig erlaubt und damit vorsieht, dass eine Einwilligung der Lehrerinnen und Lehrer nicht benötigt wird. Nach Art. 88 DSGVO sind Mitgliedstaaten ermächtigt, spezifischere, nationale Regelungen zur Gewährleistung des Schutzes der Rechte und Freiheiten von Beschäftigten hinsichtlich der Verarbeitung ihrer personenbezogenen Daten im Beschäftigungskontext zu fassen. Allerdings zweifelte das Verwaltungsgericht die Vereinbarkeit der hessischen Regelung mit den Voraussetzungen des Art. 88 Abs. 2 DSGVO an und ersuchte deshalb den EuGH um eine Vorabentscheidung.

Zu welchem Ergebnis kam der EuGH?

In seinem Urteil vom 30.03.2023 (Rs. C-34/21, Hauptpersonalrat der Lehrerinnen und Lehrer) führt der EuGH zunächst aus, dass der Videokonferenz-Livestream des öffentlichen Schulunterrichts grundsätzlich in den sachlichen Anwendungsbereich der DSGVO fällt. Die Übertragung der Kamerabilder sowie Namensangaben im Rahmen der Videokonferenz sind eine Verarbeitung personenbezogener Daten im Sinne der DSGVO. Hinsichtlich der hessischen Regelung zum Arbeitnehmerdatenschutz, woraus das Hessische Kultusministerium gefolgert hatte, dass keine ausdrückliche datenschutzrechtliche Einwilligung der Lehrerinnen und Lehrer erforderlich sei, urteilt der EuGH, dass es sich nur dann um eine nach Art. 88 Abs. 1 DSGVO „spezifischere Vorschrift" handeln kann, wenn diese auch die Vorgaben des Art. 88 Abs. 2 DSGVO erfüllt.

Als „spezifischere Vorschriften" gefasste Regelungen eines Mitgliedstaats dürfen sich dabei aber nicht auf eine bloße Wiederholung der Bestimmungen der DSGVO zur Verarbeitung personenbezogener Daten beschränken. Vielmehr ist erforderlich, dass sich die Regelungen von dem allgemeinen Regelungsgehalt der DSGVO unterscheiden und auf den zusätzlichen Schutz der Rechte und Freiheiten der Beschäftigten abzielen müssen. Zudem ist gemäß Art. 88 Abs. 2 DSGVO erforderlich, dass die „spezifischeren Vorschriften" geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insb. im Hinblick auf die Transparenz der Verarbeitung, der Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe sowie der Überwachungssysteme am Arbeitsplatz treffen. Nur wenn diese beiden Anforderungen erfüllt sind, finden nationale Regelungen zum Beschäftigtendatenschutz Anwendung. Sind die Anforderungen nicht oder nur teilweise erfüllt, sind die Regelungen nicht anwendbar und es verbleibt beim gesetzlichen Rahmen der DSGVO.

Ob die gegenständlichen Normen diese Anforderungen erfüllen, muss nun das vorlegende Gericht, hier das zuständige Verwaltungsgericht, beurteilen. Sofern das nationale Gericht dies verneint, seien die Bestimmungen nicht anwendbar.

Was bedeutet das für den Arbeitnehmerdatenschutz in Deutschland?

Im Rahmen der Einführung der DSGVO haben der Bundesgesetzgeber und die Länder vermeintlich von ihrer Befugnis aus Art. 88 DSGVO Gebrauch gemacht und gesonderte Regelungen zum Beschäftigtendatenschutz im BDSG und den Landesdatenschutzgesetzen aufgenommen. Die Gesetzgeber haben dabei jedoch entweder die bisherigen Regelungen (etwa § 32 BDSG alt) nahezu wortgleich übernommen oder in Anlehnung an die Regelungen der DSGVO formuliert.

Mit seinem Urteil stellt der EuGH nun klar, dass es für die vorrangige Anwendung von nationalen Regelungen im Beschäftigtendatenschutz nicht allein darauf ankommt, dass der nationale Gesetzgeber eigene Regelungen erlassen hat, sondern er muss auch sicherstellen, dass diese Regelungen einen eigenen, über die Regelungen der DSGVO hinausgehenden Schutzbereich haben. Ist dies nicht der Fall, bleibt es beim Vorrang der DSGVO.

Gerade im Rahmen der Regelungen zur Begründung, Durchführung und Beendigung des Arbeitsverhältnisses bestehen nunmehr erhebliche Zweifel, ob § 26 BDSG oder die vergleichbaren Regelungen in den Landesdatenschutzgesetzen weiterhin angewandt werden können, da diese keinen zusätzlichen Schutz zu den Regelung der DSGVO für die Betroffenen bieten. Diese Einschätzung teilt nun auch der Hamburgische Beauftragte für den Datenschutz. Er hält die Regelungen zum Arbeitnehmerdatenschutz im BDSG und den jeweiligen Landesgesetzen für unanwendbar.

Die Verarbeitung von Beschäftigtendaten wird dadurch nicht unzulässig, sodass kein Grund zu Panik besteht, aber Arbeitgeber müssen erneut die einschlägigen Rechtsgrundlagen bei der Verarbeitung personenbezogener Daten von Mitarbeiterinnen und Mitarbeitern überprüfen und insb. Datenschutzhinweise anpassen. Auch die allgemeinen Regelungen der DSGVO bieten ausreichend Grundlage für die Verarbeitung von Mitarbeiterdaten, wie sich auch in anderen Mitgliedstaaten der EU zeigt. Deutschland war eines der wenigen Länder, das von der Öffnungsklausel in Art. 88 DSGVO Gebrauch gemacht hat. Im Einzelfall kann auch der Abschluss zusätzlicher Betriebsvereinbarungen hilfreich sein, wenn die Verarbeitung nicht auf die allgemeinen Regelungen der DSGVO gestützt werden kann.

Ob die nationalen Regelungen nun vollständig unwirksam sind, bleibt jedoch abzuwarten. Zunächst ist darauf zu achten, zu welchem Ergebnis das zuständige Verwaltungsgericht für die hessische Regelung kommt. Sollte das Verwaltungsgericht die Regelungen für unwirksam halten, wird man davon ausgehen können, dass auch die Regelungen des BDSG und der übrigen Landesgesetze nicht anwendbar sind. Der Gesetzgeber wird seine Regelungen anpassen müssen, sollte er einen weitergehenden Schutz als nach der DSGVO beabsichtigen.

Unternehmen bleiben bis dahin aber gut beraten, stets zu prüfen, auf welcher Rechtsgrundlage nach der DSGVO sie die personenbezogenen Daten ihrer Mitarbeiter verarbeiten, und ggf. erforderliche Anpassungen zu treffen.

Wer haftet für DSGVO-Verstöße in Unternehmen?

Am 27.04.2023 hat der Generalanwalt am Europäischen Gerichtshof (EuGH) Manuel Campos Sánchez-Bordona seine Schlussanträge im Verfahren der Deutsche Wohnen SE gegen die Berliner Staatsanwaltschaft bekannt gegeben und sich darin gegen eine verschuldensunabhängige Bebußung bei DSGVO-Verstößen ausgesprochen (Rs. C-807/21). Das erst in einigen Monaten zu erwartende Urteil verspricht, grundsätzliche Fragen bei der Bebußung von Unternehmen wegen DSGVO-Verstößen zu klären.

Ausgangsfall und Vorlagefragen

Gegenstand des Verfahrens sind zwei Vorlagefragen, die das Kammergericht (KG) Berlin dem EuGH im Dezember 2021 in Zusammenhang mit einem von der Berliner Datenschutzbehörde gegenüber der Deutsche Wohnen SE verhängten Bußgeld wegen vermeintlicher DSGVO-Verstöße einer Tochtergesellschaft vorgelegt hatte. Als Grund für das Bußgeld von über 14 Mio. Euro gibt die Berliner Datenschutzbehörde die fortgesetzte Speicherung personenbezogener Mieterdaten in mindestens 15 Fällen an, obwohl eine Speicherung nicht (mehr) erforderlich gewesen sei.

Mit den Vorlagefragen wollte das KG Berlin erfahren,

1. ob ein DSGVO-Bußgeldverfahren unmittelbar gegen ein Unternehmen geführt werden darf, ohne dass es einer durch eine identifizierte natürliche Person begangenen Ordnungswidrigkeit bedarf und

2. sofern dies der Fall ist, ob es für eine Bebußung des Unternehmens im Grundsatz bereits ausreicht, wenn ein dem Unternehmen zuzuordnender objektiver Pflichtenverstoß vorliegt (sog. „strict liability") oder ob ein durch den Mitarbeiter des Unternehmens schuldhaft begangener Verstoß erforderlich ist.

Der Generalanwalt hat sich nun dafür ausgesprochen, dass Geldbußen grundsätzlich gegen juristische Personen als Verantwortliche im Sinne der DSGVO verhängt werden können. Nichtsdestotrotz bedürfe es dafür aber eines vorsätzlichen oder fahrlässigen Verstoßes. Ein rein objektiver Pflichtenverstoß genügt damit nach Ansicht des Generalanwalts nicht.

Was bedeuten die Schlussanträge des Generalanwalts für Unternehmen?

Die Schlussanträge des unparteiischen Generalanwalts sind für die Entscheidung des EuGH nicht verbindlich. Erfahrungsgemäß sind die Aussagen des Generalanwalts als Gutachten zur Unterstützung des EuGH bei der Entscheidungsfindung aber eine erste Tendenz für das zu diesem Zeitpunkt noch ausstehende Urteil.

Der Generalanwalt fordert zwar einen vorsätzlichen oder fahrlässigen Verstoß gegen die DSGVO, betont aber auch, dass dieser im Zweifel auf einen Mangel des Kontroll- und Überwachungssystems innerhalb eines Unternehmens zurückgehen kann. Das Aufstellen, Einhalten und die Kontrolle von Datenschutz-Compliance-Maßnahmen sind in ihrer Bedeutung für das bei DSGVO-Verstößen im Raum stehende Verschulden des Unternehmens als Bußgeldadressat deshalb nicht zu unterschätzen.

Klarstellung zur Höhe der Bußgeldbemessung in Konzernstrukturen

Bereits vor Bekanntgabe des Urteils dürfte für Unternehmen sowohl in der datenschutzrechtlichen Risikobewertung als auch im Konfliktfall außerdem besonders interessant sein, wie sich der Generalanwalt in seinen Schlussanträgen zur Bußgeldbemessung in Konzernstrukturen geäußert hat. Diese können laut DSGVO bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres betragen. Bisher ist nicht abschließend geklärt, ob laut DSGVO für die Bußgeldbemessung der Konzernumsatz oder der jeweilige Umsatz der einzelnen konzernangehörigen Unternehmen heranzuziehen ist. Der Generalanwalt spricht sich nun für eine Bußgeldbemessung anhand des Konzernumsatzes aus, wie es auch im europäischen Wettbewerbsrecht gehandhabt wird. Gleichzeitig betont er aber, dass die DSGVO nur bezüglich der Bußgeldbemessung auf die wettbewerbsrechtlichen Grundsätze verweist. Offen lässt er explizit, ob das gleiche Verständnis des Unternehmensbegriffs hinsichtlich der Haftung der Muttergesellschaft für Datenschutzverstöße der Tochtergesellschaft heranzuziehen ist.

Mangelhafte Datenschutz-Compliance kann teuer werden

Es bleibt abzuwarten, ob der EuGH in seinem Urteil die Chance ergreift und neben der Beantwortung der konkreten Vorlagefragen zur datenschutzrechtlichen Verantwortlichkeit und Haftung im Konzern grundsätzliche Aussagen treffen wird. Die Schlussanträge des Generalanwalts unterstreichen aber bereits jetzt das finanzielle Risiko, das mangelhafte Datenschutz-Compliance für konzernangehörige Unternehmen seit Inkrafttreten der DSGVO darstellt.

Künstliche Intelligenz: Die dunkle Seite der IT? – Zwischen Chancen, Risiken und Regularien

Die fortschreitende Entwicklung von Technologien wie Künstlicher Intelligenz (KI) birgt sowohl Chancen als auch Risiken für unsere Gesellschaft. Auf der einen Seite kann KI dazu beitragen, komplexe Probleme schneller und effektiver zu lösen, Arbeitsprozesse zu automatisieren und die Lebensqualität der Menschen zu verbessern. Auf der anderen Seite gibt es auch Bedenken, dass KI unvorhergesehene Konsequenzen haben und zu sozialen Ungleichheiten und ethischen Herausforderungen führen könnte. Es ist daher von entscheidender Bedeutung, sich eingehend mit den Chancen und Risiken von KI auseinanderzusetzen und eine verantwortungsvolle Nutzung dieser Technologien zu fördern.

In diesem Artikel werden wir uns sowohl mit den potenziellen Vorteilen als auch den möglichen Risiken von KI beschäftigen und untersuchen, wie wir sicherstellen können, dass die Technologie unser Leben auf positive Weise beeinflusst.

Hat Ihnen die Einleitung für unseren Artikel gefallen? Wir haben uns erlaubt, die Einleitung von der aktuell wohl meist diskutierten Künstlichen Intelligenz, dem Chatbot ChatGPT des Unternehmens OpenAI, schreiben zu lassen.

Einführung

Unter KI versteht man von Menschen entwickelte Anwendungen, Systeme und Maschinen, die Probleme und Aufgaben lösen, indem sie menschliche (kognitive) Fähigkeiten wie logisches Denken, Urteilen oder Lernen imitieren.

Viele KI-Systeme basieren auf „Maschinellem Lernen". Sie werden mit (Trainings-) Daten gefüttert und lernen aus diesen, um Aufgaben zunehmend besser ausführen zu können. KI-Systeme erkennen anhand der eingespielten Daten und Algorithmen Muster, auf Basis derer sie Modelle erstellen, um das Gelernte auf andere Daten zu übertragen und so Vorhersagen und Entscheidungen treffen zu können.

Indem sie die Folgen früherer Entscheidungen und (Re-)Aktionen analysieren und eigenständig verarbeiten, ist es KI-Systemen möglich, ihr Vorgehen anzupassen.

Im Unternehmenskontext betrachtet ist KI ein wesentlicher Treiber für die digitale Transformation. Der Einsatz dieser maschinell lernenden Systeme bringt eine Vielzahl an Möglichkeiten, aber auch Herausforderungen mit sich. Dabei werden wir vereinzelt auch ChatGPT zur Illustration zu Wort kommen lassen bzw. als Beispiel verwenden.

Hinweis: Über den Unternehmenskontext hinausgehende Aspekte von KI für die Wissenschaft und Gesellschaft bzw. ethische Aspekte, werden nur am Rande in die Betrachtung miteinbezogen.

Chancen von KI

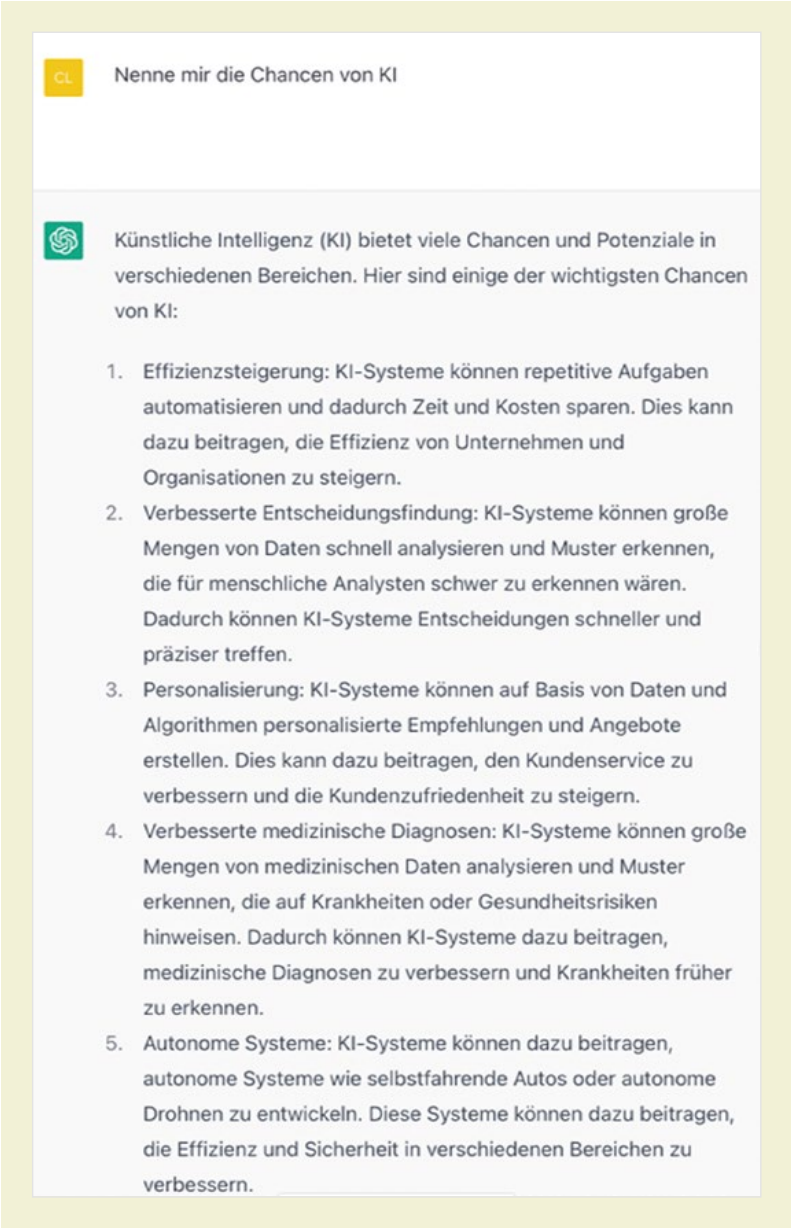
KI-Systeme können Unternehmen und der Wirtschaft eine Reihe von Vorteilen bieten. Es ist möglich, Aufgaben am Arbeitsplatz zu automatisieren, welche sonst von Menschen ausgeführt werden. Dies reduziert aus Unternehmenssicht nicht nur die anfallenden Kosten für Mitarbeitende, sondern kann dazu beitragen die Effizienz und Produktivität bis 2035 um 11-37 % zu steigern (offizielle Seite des Europaparlaments nach EP Think Tank 2020).

Gleichzeitig wird z. B. durch den Einsatz von KI-gesteuerten Robotern bei gefährlichen Arbeitsschritten zur Arbeitssicherheit beigetragen. Zusätzlich kann KI eingesetzt werden, um Arbeiten auszuführen, die für menschliche Mitarbeitende sehr monoton, repetitiv und wenig fordernd sind. Als Gegenpart können die durch KI gewonnenen Ressourcen zur Weiterentwicklung genutzt und neue Arbeitsplätze geschaffen werden.

Die folgenden Anwendungsbeispiele konkretisieren, wie der Einsatz von KI zum Unternehmenserfolg und zur Effizienzsteigerung beitragen kann.

Verbesserte Entscheidungsfindung

Mithilfe von KI-Anwendungen werden sowohl Daten als auch gewonnene Erkenntnisse gesammelt, um anschließend durch KI-gestützte Analysen Trends schneller erkennen und Entscheidungen fundierter treffen zu können.



Im Personalmanagement kommt KI bei der Bewertung von Bewerbungsunterlagen zum Einsatz und verschlankt den Auswahlprozess.

Im Kundenservice ermöglicht es die Nutzung von KI den Unternehmen, den Service durch personalisierte Werbung zu verbessern. Und nicht zuletzt kann durch den vermehrten Einsatz von Chatbots oder anderen digitalen Assistenten, z. B. gegenüber den Kunden, zeitunabhängige Unterstützung geleistet werden.

Hinweis: Ein weit verbreiteter Einsatz von KI, der nicht nur in der Wirtschaft, sondern auch im privaten Umfeld Erleichterungen bringt, sind Navigationssysteme genauso wie Text- und Spracherkennung, die auf Smartphones, in Unternehmen und in Fahrzeugen zum Einsatz kommen.

Doch je weiter die Entwicklung der KI voranschreitet, desto größer werden die Bedenken über die potenziellen Risiken, die mit ihrem Einsatz verbunden sind.

Risiken von KI

Die Risiken von KI variieren je nach Anwendungsfall und müssen stets individuell bewertet und gesteuert werden.

Ein grundlegendes Risiko liegt in einer ungenügenden Leistung eines KI-Systems. Dies kann zu Ausfällen oder Fehlentscheidungen führen. Grund dafür können mangelhafte Daten sein. Sind diese unvollständig oder inkorrekt, können fehlerhafte Analysen zu falschen Ergebnissen oder Entscheidungen der KI führen und immer wieder reproduziert werden. Dies kann zu schwerwiegenden Folgen führen. Im Fall einer Fehlentscheidung ist das resultierende Risiko eines autonom fahrenden Autos wesentlich höher einzustufen als bspw. bei einer Kaufempfehlung für ein Produkt.

In diesem Zusammenhang stellt sich auch die Frage nach der Verantwortungsübernahme. Wer haftet, wenn die KI eigenständig agiert und zu ungewollten und kritischen Ergebnissen führt? Je autonomer KI-Systeme agieren, desto schwieriger wird die

Verantwortungsregulation. Diese Frage nach der Verantwortungsübernahme sollte deshalb in jedem Fall geklärt werden und gesetzlich klar geregelt sein.

Risikobehaftet sind selbstlernende Verfahren außerdem insoweit, als sie unbemerkte Änderungen in Prozessen oder Verfahren vornehmen können. Dies verringert die Erklärbarkeit und Nachvollziehbarkeit der KI-Anwendung und kann zu einem Kontrollverlust führen. Zudem sind schwer verständliche KI-Anwendungen für Anwender und Betroffene nur bedingt nachvollziehbar (siehe auch nachfolgend). Sie haben keinen Einfluss darauf, wie die Systeme funktionieren, auf die ggf. ungerechtfertigten, personenbezogenen Ergebnisse und wo sie angewandt werden.

Ein hohes Risiko besteht auch im Bereich der Cybersicherheit. Mangelnde Sicherheit und Robustheit machen die KI-Anwendung anfällig für Störungen, Manipulationen und Hackerangriffe, die den Schutz vertraulicher Daten gefährden können. Im Falle der Nutzung für unerwünschte Zwecke kann dies einen enormen wirtschaftlichen, politischen oder persönlichen Schaden hervorrufen.

Sollten die eingespielten Trainingsdaten verzerrt oder unvollständig sein, bewirkt dies auch potenziell Verzerrungen in den Ergebnissen. Im Falle der Verarbeitung von personenbezogenen Informationen könnte dies etwa eine ungerechtfertigte Diskriminierung der Betroffenen bewirken. Als Beispiel führt die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) in der Hambacher Erklärung zur Künstlichen Intelligenz den Fall eines Unternehmens an, welches einen Bewerbungsprozess frei von Benachteiligung und Vorurteilen durchführen möchte. Das KI-System wird mit Daten von erfolgreichen Bewerbungen trainiert, ohne dass das Geschlecht ein Bewertungskriterium darstellt. Die Tatsache, dass bisher allerdings hauptsächlich männliche Bewerber eingestellt wurden, deren Bewerbungen als Trainingsgrundlage für das KI-System dienten, führte dazu, dass nicht-männliche Personen im Bewerbungsprozess schlechter bewertet und folglich benachteiligt werden. Solche Verzerrungen in den Trainingsdaten verfestigen sich oftmals unbemerkt und können auch ein Reputationsrisiko für das jeweilige Unternehmen bedeuten.

Nicht zuletzt sollte KI-nutzenden Unternehmen bewusst sein, dass der Einsatz von KI eine Abhängigkeit hervorrufen kann. Je mehr sich die Menschen auf die KI verlassen, desto mehr können sie die Fähigkeiten verlieren, entsprechende Aufgaben eigenständig auszuführen. Die zunehmende Automatisierung von Prozessen kann zudem laut der Vermutung einiger Experten zukünftig zu einem Beschäftigungsverlust vor allem in repetitiven Tätigkeitsbereichen führen.

> Auch hier haben wir es uns nicht nehmen lassen, auch einmal ein KI-System selbst über seine Risiken zu befragen. So erwähnt auch der Chatbot ChatGPT alle der hier bereits genannten Risikobereiche. Risiken lägen im Arbeitsplatzverlust, in der Abhängigkeit von Technologie und Anfälligkeit für Störungen, im Bereich Bias und Diskriminierung, in der Transparenz und Verantwortlichkeit oder im Bereich Ethik und Sicherheit: „Diese Herausforderungen und Risiken zeigen, dass es wichtig ist, KI-Systeme auf ethische und sichere Weise zu entwickeln und einzusetzen, um die Vorteile von KI zu maximieren und potenzielle Schäden zu minimieren."

Um eine sichere und transparente Nutzung der KI-Systeme zu gewährleisten, müssen diese individuell risikoorientiert geprüft und kontrolliert werden. Dafür sollten gewisse Qualitätskriterien an KI-Anwendungen gestellt werden. Dazu zählen beispielsweise

- Verlässlichkeit,
- Zweckmäßigkeit,
- Vertrauenswürdigkeit,
- Sicherheit,
- Nachvollziehbarkeit bzw.
- Resilienz.

Diese Kriterien sowie ihre Priorisierung variieren je nach Anwendungsfall und müssen mit den jeweiligen Risiken abgewogen werden. Eine erhöhte Leistungsfähigkeit der Anwendung kann durch eine gesteigerte Komplexität beispielsweise eine geringere Nachvollziehbarkeit bewirken.

Regulierungen und Richtlinien

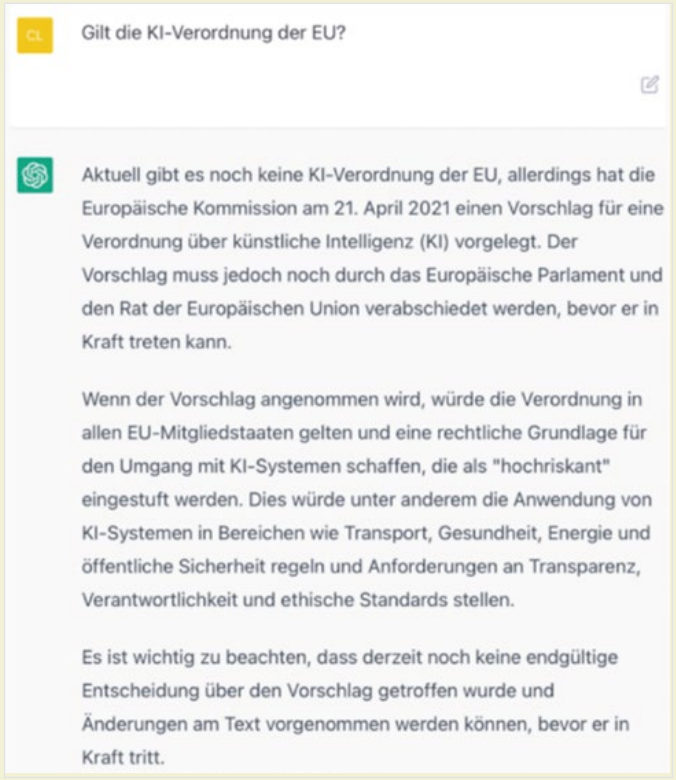
Bereits jetzt existieren einige Regularien und Leitfäden an denen sich bei der Entwicklung, Implementierung, Prüfung und Kontrolle von KI-Anwendungen sowie der Beurteilung von Risiken orientiert werden muss bzw. kann.

EU-AI-Act

Auf europäischer Ebene wird dazu derzeit der EU Artificial Intelligence Act, EU-AI-Act, entwickelt, der verpflichtende Anforderungen an Unternehmen stellt, die KI in ihren Unternehmensprozessen nutzen.

Mit dem AI-Act, auch KI-Verordnung (KI-VO) genannt, veröffentlicht die EU-Kommission einen Verordnungsentwurf mit regulatorischen Überwachungsfunktionen für KI-Systeme in Forschung und Wirtschaft. Dabei geht es weniger um die technische Komponente des KI-Systems, sondern vielmehr um den tatsächlichen Einsatz. Die KI-VO sollte Anfang 2023 in Kraft treten. Dies ist jedoch bis zur Erstellung dieses Artikels nicht erfolgt. Aktuell ist vorgesehen, dass nach Inkrafttreten der Verordnung eine 24-monatige Umsetzungsfrist für die Unternehmen besteht.

ChatGPT konnte sich hinsichtlich der Gültigkeit der KI-Verordnung nicht sicher entscheiden und hat innerhalb von zehn Minuten zwei unterschiedliche Meinungen zum bisherigen Inkrafttreten der Verordnung ausgegeben. Es stellt sich die Frage, ob die Rechtschreibung der Fragestellung dabei eine Rolle spielt:



Mit der KI-VO soll möglichen Risiken von KI, wie dem Missbrauch von personenbezogenen Daten, der Diskriminierung und allgemeinen Auswirkungen auf die Gesellschaft, vorgebeugt werden. Der Act wird die Unternehmen verpflichten, ihre eingesetzten KI-Tools und die damit verbundenen Risiken zu bewerten und zu dokumentieren.

Der Verordnungsentwurf verfolgt einen risikobasierten Ansatz. Die KI-Tools werden je nach Anwendungsbereich in vier Risiko-Kategorien unterteilt und unterliegen je nach Einstufung unterschiedlich strengen Anforderungen.

1. KI-Systeme, die den ethischen Grundsätzen der EU widersprechen, eine Bedrohung für die Sicherheit, die Lebensgrundlage und Rechte der Menschen bedeuten und ein unakzeptables Risiko darstellen, sollen verboten werden. Verbotene KI-Systeme fallen unter Art. 5 Nr. 1 KI-VO. Hierzu zählen Anwendungen, die

   - menschliches Verhalten manipulieren und Menschen schaden könnten,
   - aufgrund von sozialem Verhalten oder persönlicher Charakteristik eine nachteilige Bewertung ermöglichen,
   - die biometrische Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen verwenden. Hier bestehen Ausnahmen im Zusammenhang mit der Abwehr von Terrorismus oder um schwere Straftaten aufzuklären.

2. Hochrisiko-KI-Systeme" sollen künftig strengen Anforderungen und der Überwachung durch Menschen unterliegen. Sie erfordern ein umfassendes Qualitäts- und Risikomanagementsystem, in dem u. a. Entscheidungsvorgänge, Datenqualität und Transparenz dokumentiert und nachgewiesen werden müssen.

Für KI-Systeme mit (3) geringem Risiko sind Transparenzpflichten vorgesehen, für Systeme mit (4) minimalem Risiko sollen keine zusätzlichen rechtlichen Verpflichtungen bestehen.

Diese Risikoabschätzung muss von den Nutzenden selbst vorgenommen werden und verpflichtet sie, eine Eintragung in der EU-Datenbank für Hochrisiko-KI-Systeme vorzunehmen, sollte ein System dieser Risikokategorie (2) verwendet werden.

U. a. gelten KI-basierte Anwendungen im Personalmanagement, in der Justiz oder mit Sicherheitsfunktionen als Hochrisikoanwendung, aber auch die automatische biometrische Identifizierung sowie Systeme zur Verwaltung und zum Betrieb kritischer Infrastruktur (z. B. Sicherheitskomponenten im Rahmen der Wasser- und Stromversorgung).

Tritt der EU-AI-Act in Kraft, wird auf die Hersteller und Verwender von KI-Systemen ein deutlicher Aufwand zukommen oder bestimmte Anwendungen wird es voraussichtlich in ihrer derzeitigen Form nicht mehr geben.

Wenn der aktuelle Entwurf des EU-AI-Acts verabschiedet wird, kann es auch für den von uns im Rahmen der Artikelerstellung verwendeten Chatbot ChatGPT eng werden. Die Liste der Hochrisiko-KI-Systeme wurde um textgenerierende KI erweitert, sofern der generierte Text fälschlicherweise für von Menschen verfasst gehalten werden könnte. Dies kommt nur in dem Fall nicht zum Tragen, wenn der generierte Text von Menschen überprüft wird und eine Person oder Organisation rechtlich dafür verantwortlich ist.

Um die Umsetzung der Verordnung durchzusetzen, können für Verstöße gegen die Anforderungen des AI-Act Bußgelder verhängt werden. Diese richten sich nach der Art und Schwere des jeweiligen Verstoßes und können bis zu 30 Mio. Euro bzw. 6 % des weltweiten Jahresumsatzes des Unternehmens betragen.

Hinweis: Momentan befindet sich der EU-AI-Act noch in der Entwurfsphase. Es können noch Anpassungen und Konkretisierungen erfolgen. Trotzdem sollten sich Unternehmen bereits jetzt auf die rechtlichen Anforderungen der neuen EU-Verordnung vorbereiten und prüfen, ob die eingesetzten oder geplanten KI-Systeme, die internen Prozesse sowie Governance-Strukturen den Vorgaben des AI-Acts genügen. Sollten in den Unternehmen noch keine Richtlinien zum Umgang mit KI verschriftlicht worden sein, ist es ratsam, diese bereits jetzt zu erstellen.

Weitere Leitfäden

Darüber hinaus existieren bereits Prüfkataloge und Umsetzungshinweise, die Empfehlungen, Anforderungen, Implikationen und Konkretisierungen von rechtlichen Anforderungen an KI-Anwendungen abbilden, um diese sicher und vertrauenswürdig zu gestalten, zu steuern und zu kontrollieren.

1. Der Artificial Intelligence Cloud Service Compliance Criteria Catalogue (AIC4) des Bundesamts für Sicherheit und Informationstechnik (BSI) fokussiert sich auf KI-Services, die auf maschinellem Lernen beruhen und ihre Leistung durch die Nutzung von Trainingsdaten stetig verbessern. Der Katalog stellt Mindestanforderungen an ihre sichere Verwendung. Dabei wird sich auf den gesamten Lebenszyklus der KI von der Entwicklung über die Erprobung und Validierung bis zum eigentlichen Betrieb bezogen. Die Risikoanalyse der Bereiche Sicherheit und Robustheit, Performance und Funktionalität, Zuverlässigkeit, Datenqualität, Datenmanagement, Erklärbarkeit, Bias ermöglichen ein grundlegendes Level an Sicherheit sowie die Beurteilung, ob der KI-Service und die damit verbunden Methoden für den jeweiligen Anwendungsfall angemessen sind.

2. Der Leitfaden zur Gestaltung vertrauenswürdiger Künstlicher Intelligenz des Fraunhofer-Instituts für Intelligente Analyse- und Informationssysteme (IAIS) bietet einen praxisorientierten Ansatz zur Beurteilung von KI-Risiken. Der Fokus liegt ebenfalls auf Anwendungen des maschinellen Lernens und beinhaltet den gesamten KI-Lebenszyklus. Der Katalog enthält einen Leitfaden, mit dem Risiken im Hinblick auf die sechs Dimensionen Fairness, Autonomie und Kontrolle, Transparenz, Verlässlichkeit, Sicherheit und Datenschutz identifiziert werden können. Zudem beinhaltet er eine Anleitung zur Entwicklung von KI-Prüfkriterien sowie eine Anleitung zur Dokumentation der eingesetzten technischen und organisatorischen Maßnahmen.

3. Das Positionspapier der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen bezieht sich auf KI-Anwendungen des maschinellen Lernens primär im Hinblick auf den Datenschutz. Eine Betrachtung erfolgt auf allen Ebenen des Lebenszyklus einer KI-Anwendung: Design und Veredelung, Training und Validierung sowie Einsatz, Rückkopplung und Selbstveränderung. Anforderungen an die Systeme zur risikoarmen Verwendung werden mit Fokus auf die sieben Gewährleistungsziele Transparenz, Datenminimierung, Nichtverkettung, Intervenierbarkeit, Verfügbarkeit, Integrität und Vertraulichkeit gestellt. Außerdem geht das Positionspapier auf (datenschutz-) rechtliche Bezüge hinsichtlich der KI-Systeme aus technischer Sicht ein.

4. Der Entwurf des Prüfungsstandards: Prüfung von KI-Systemen (IDW EPS 861) des Instituts der Wirtschaftsprüfer in Deutschland e. V. (IDW) wurde im Februar 2022 veröffentlicht. Durch diesen Prüfungsstandard, welcher noch nicht in endgültiger Version vorliegt, verdeutlicht das IDW die Anforderungen an freiwillige Prüfungen von KI-Systemen auf Basis geeigneter Kriterien.

5. Das Prinzipienpapier Big Data und künstliche Intelligenz: Prinzipien für den Einsatz von Algorithmen in Entscheidungsprozessen der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) wurde am 15.06.2021 publiziert. Der verantwortungsvolle Einsatz von KI und Big Data sowie die Kontrolle der inhärenten Risiken sind das Ziel dieser aufsichtlichen Prinzipien.

Datenschutz

KI nutzt Unmengen von Daten, aus denen sie lernt und sich weiterentwickelt. Wenn dafür z. B. technische oder anonyme Daten verwendet werden, kommt zukünftig voraussichtlich der EU-AI-Act (KI-VO) zum Tragen. Sobald diese Daten einen Personenbezug haben, greift parallel dazu der Datenschutz, so dass die Vorgaben der Datenschutz-Grundverordnung (DSGVO) bzw. des Bun-

desdatenschutzgesetzes (BDSG) angewendet werden müssen. Sie dienen dem Schutz der Grundrechte und Grundfreiheiten natürlicher Personen. Je nach Einsatzgebiet der KI erhöhen sich die Risiken für die Rechte und Freiheiten der Menschen. Beispielsweise ist das Erkennen von Krankheitsmustern durch KI für Patient und Arzt ein großer Fortschritt, doch sollten derartige Möglichkeiten nur unter kontrollierten Bedingungen ausgeschöpft werden, um negative Auswirkungen auf die Betroffenen zu vermeiden.

In der Praxis bedeutet dies, dass schon bei der Beschaffung der personenbezogenen Daten (pbD) die rechtliche Grundlage für deren Verarbeitung geprüft werden muss. KI darf pbD nur verarbeiten, wenn der Grundsatz der Zweckbindung gegeben ist. Das heißt pbD müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden – und zwar auch nicht zu Trainingszwecken einer KI.

Eine weitere datenschutzrechtliche Herausforderung, nicht ganz zur Natur von KI passend, ist der Grundsatz der Datenminimierung, wonach die Verarbeitung von pbD dem Zweck angemessen und auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein muss. Für die Nutzung im Rahmen der KI muss hinterfragt werden, ob die entsprechenden personenbezogenen Daten tatsächlich gebraucht werden oder die Verarbeitung anonymer Daten ausreicht. Die pbD müssen mit dem Wegfall der Zweckbindung gelöscht werden, wenn keine rechtliche Grundlage mehr besteht – Stichwort Löschkonzept. Datenminimierung sollte unter der Prämisse des Betroffenenrechts auf Löschung frühzeitig betrachtet werden, da einmal zu Trainingszwecken verarbeitet pbD ggf. im Fall eines Löschanspruchs nicht ohne Weiteres entfernt werden können, ohne die KI zurücksetzen und neu trainieren zu müssen.

Ein Erfolgskriterium für KI, um valide Ergebnisse zu bringen, wird durch eine Datenschutzanforderung unterstützt: Es dürfen nur aktuelle und inhaltlich richtige personenbezogene Daten verarbeitet werden. Durch fehlerhafte oder unvollständige Daten darf es nicht zu diskriminierenden Ergebnissen kommen. Wenn die Verarbeitung personenbezogener Daten durch KI voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen birgt, was bei automatisierten Entscheidungen häufig der Fall sein kann, muss eine Datenschutz-Folgenabschätzung durchgeführt werden.

Grundsätzlich gilt es sowohl während der Entwicklung als auch bei dem Einsatz von KI zu beachten, dass neben Zweckbindung und Datenminimierung weitere Datenschutzgrundsätze zu realisieren sind, wie

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz,
- Richtigkeit,
- Speicherbegrenzung ,
- Integrität und Vertraulichkeit (Datensicherheit) und,
- Rechenschaftspflicht.

Im KI-Kontext ist gerade die Transparenzpflicht besonders hervorzuheben. Sie bedingt, dass die Verarbeitung ihrer pbD für die Betroffenen nachvollziehbar, verständlich und leicht zugänglich sein muss, d. h. bei KI-basierten Entscheidungen muss nachvollziehbar sein, wie eine Entscheidung zustande gekommen ist. Die verantwortliche Stelle, die Geschäftsführung, ist dafür rechenschaftspflichtig.

Im Rahmen von KI-Anwendungen werden Massendaten, auch mit Personenbezug, verarbeitet und automatisierte Entscheidungen getroffen. Um den Datenschutz in KI-Systemen zu etablieren und die Rechte und Freiheiten Einzelner zu schützen, sollten bereits bei der Planung und Entwicklung von KI-Systemen technische und organisatorische Maßnahmen von den Verantwortlichen geplant und umgesetzt werden (Privacy by Design) (Positionspapier der DSK, siehe oben).

Auch während der Anwendung von KI-Systemen muss aufgrund der aus neuen Daten fortwährend selbstlernenden Systeme, regelmäßig eine Risikoüberwachung erfolgen. Die Verantwortlichen müssen Maßnahmen ergreifen, um die Rechtmäßigkeit und Sicherheit der Verarbeitung, die Betroffenenrechte und die Beherrschbarkeit des KI-Systems zu gewährleisten.

Entscheidungen mit rechtlicher Wirkung oder ähnlicher erheblicher Beeinträchtigung dürfen gemäß Art. 22 DSGVO nicht allein der Maschine überlassen werden.

Fazit und kritischer Ausblick

KI entwickelt sich rasant. In Wirtschaft, Wissenschaft und Gesellschaft ist KI zunehmend präsent und bietet durch hohe Leistungsfähigkeit sowie Vielfältigkeit der Einsatzgebiete große Chancen, geht aber auch mit neuen Herausforderungen Hand in Hand.

Die Bundesregierung unterstützt die Entwicklung durch eine im Jahr 2018 veröffentlichte KI-Strategie, um den Standort Deutschland in Erforschung, Entwicklung und Anwendung von KI im internationalen Wettbewerb zu stärken: „Für das Bundesministerium für Bildung und Forschung ist zentral: Künstliche Intelligenz muss vom Menschen ausgehend gedacht werden und zu dessen Wohl entwickelt werden".

Neben den bereits aufgeführten Risiken mag sich auch die provokante Frage aufdrängen, ob die nächsten Generationen durch die Verwendung von KI, und hier insb. der selbstlernenden Chatbots, die Fähigkeit zum selbständigen Denken verlernen. Sind wir Mitarbeitende durch den verstärkten Einsatz von KI vielleicht sogar überflüssig? Die Fragen sind nicht neu, bereits die Einführung von EDV-Systemen in Unternehmen und die Verfügbarkeit des Internets haben eine ähnliche Besorgnis hervorgerufen.

Sowohl die Arbeitswelt als auch die technischen Möglichkeiten verändern sich laufend und neue Regulierungen wie der EU-AI-Act sind die logische und notwendige Konsequenz. Für die Unternehmen ist es angebracht, sich frühzeitig mit den neuen Herausforderungen auseinanderzusetzen, um die Chancen und Möglichkeiten von KI sicher und compliant nutzen zu können.

Unabhängig von den rechtlichen Anforderungen ist es sinnvoll, die Verwendung von KI in Unternehmen individuell zu regeln und zu kontrollieren. In Geschäftssoftware eingebundene KI darf keine Black-Box sein, sondern muss hinsichtlich der automatischen Routinen und der generierten Ergebnisse transparent dargestellt werden. Die Entscheidungen, die ein Algorithmus trifft, müssen nachvollziehbar sein. Die unreflektierte Verwendung von KI, beispielsweise von Chatbot-Ergebnissen, ob selbstlernend oder nicht, sollte im Unternehmenskontext stark reguliert oder sogar unterbunden werden.

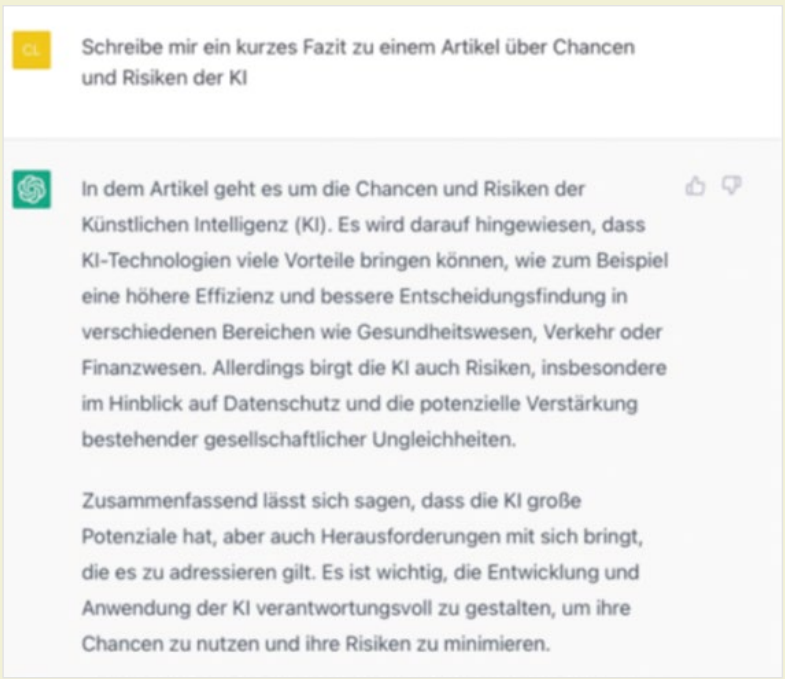
Eine KI ist immer nur so gut, wie die Daten, mit denen sie gefüttert wird. Sowohl Daten als auch Ergebnisse müssen folglich auf Richtigkeit, Aktualität und Vollständigkeit, validiert werden. Die KI-Anwendungen müssen hinsichtlich rechtlicher und allgemeiner Risiken und Kontrollschwächen in die risikoorientierten Prüfungspläne von Compliance, z. B. Datenschutz und der Internen Revision eingebunden werden.

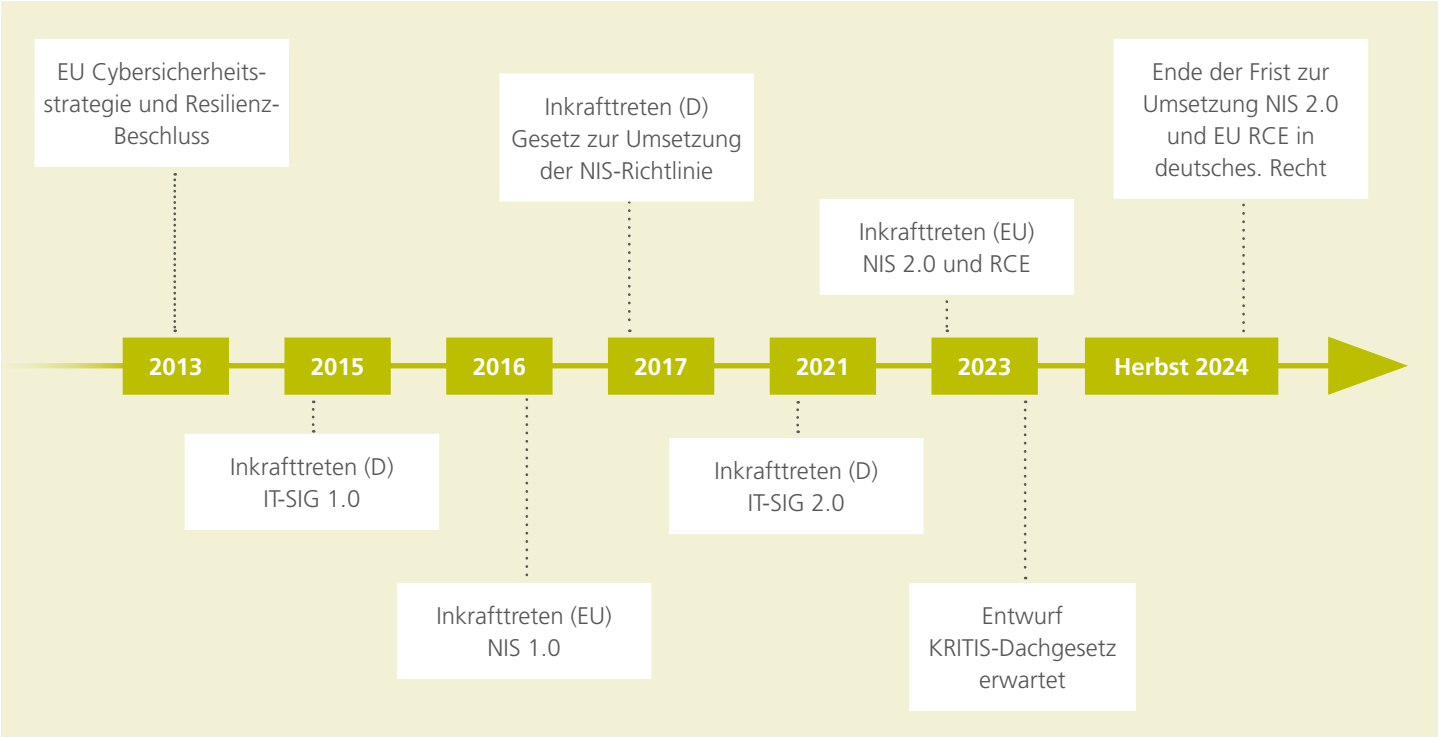
Zum Redaktionsschluss häufen sich die Pressemeldungen und Forderungen aus Wirtschaft und Politik zu KI, z. B.

- Warnt SPD-Chefin Saskia Esken vor den Risiken von KI: Durch Missbrauch von KI können Kriege entstehen (Hamburger Abendblatt vom 17.04.2023) – Stichwort Deepfake.
- SAP-Vorständin, Sabine Bendiek; sie sieht in KI einen Beschleuniger für Wandel der Arbeitswelt (Handelsblatt online vom 16.04.2023).
- Das Bundesinnenministerium von Ressortchefin Nancy Faeser (SPD) hat sich für umfassende Regeln für den Einsatz KI ausgesprochen.
- Digitalminister Volker Wissing (FDP) sieht ebenfalls Regulierungsbedarf und mahnte eine schnelle Regelung auf EU-Ebene an (Handelsblatt online vom 16.04.2023).
- Das Europäische Parlament will die populäre KI ChatGPT offenbar schärfer regulieren. „Es zeichnet sich eine Mehrheit dafür ab, ChatGPT als Hochrisikotechnologie einzustufen“, sagt der CDU-Europaabgeordnete Axel Voss, der das Thema als Berichterstatter betreut. „Das wird höchstwahrscheinlich so kommen.“ (Handelsblatt online vom 17.04.2023).
- Italiens Datenschutzbehörde hat den KI-basierten Chatbot ChatGPT vorerst sperren lassen (Tagesschau online vom 31.03.2023).
- Die rasante Entwicklung bei Künstlicher Intelligenz ruft Kritiker auf den Plan. Mehr als 1.000 Experten aus Tech und Forschung – unter ihnen auch Elon Musk – fordern nun eine Entwicklungspause für neue KI-Modelle. Es brauche erst Sicherheitsstandards (Tagesschau online vom 29.03.2023).

Sicher ist, dass es spannend bleibt und noch nicht alle offenen Fragen beantwortet sind. Wir bleiben für Sie am Ball und werden das Thema KI in unserem novus IT weiterverfolgen, z. B. hinsichtlich der regulatorischen Entwicklung oder weiterer Fragestellungen, beispielsweise zu KI und Urheberecht.

Das letzte Wort hat ChatGPT:





NIS 2.0 und RCE – Next Level KRITIS

Anfang Januar 2023 sind zwei zentrale Direktiven in Kraft getreten, die dafür sorgen, dass sowohl die Anforderungen an sog. Kritische Infrastrukturen (KRITIS), als auch die Anzahl an betroffenen Sektoren und Anlagen selbst deutlich steigen werden. Dies ist zum einen die sog. „The Network and Information Security Directive (NIS) 2.0" (EU 2022/2555) und zum anderen die „Resilience of critical entities and repealing Council Directive" (RCE-Directive) (EU 2022/2557)).

Während NIS 2.0 die Cyber Security reguliert und entsprechende Anforderungen stellt, reguliert RCE die Resilienz von kritischen Infrastrukturen und fordert die Ausfallsicherheit von KRITIS.

Hintergrund der NIS

Durch die europäische Kommission wurde Ende 2015 vor dem Hintergrund einer einheitlichen europäischen Cyber-Sicherheitsstrategie die sog. NIS-Richtlinie finalisiert. Sie ist am 08.08.2016 mit der Vorgabe der länderspezifischen Umsetzung in Kraft getreten (EU-Richtlinie 2016/1148). In Deutschland ist bereits am 25.07.2015 das „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme" (IT-Sicherheitsgesetz, kurz IT-SiG) verabschiedet worden sowie am 30.06.2017 das „Gesetz zur Umsetzung der NIS-Richtlinie" in Kraft getreten. Zum 28.05.2021 erfolgte bereits das Inkrafttreten des IT-Sicherheitsgesetzes 2.0, das u. a. die Befugnisse des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erhöhte, eine Erweiterung der betroffenen Unternehmen als KRITIS-Betreiber vornahm (u. a. Unternehmen im besonderen öffentlichen Interesse bestehend aus den Gruppen Rüstung, Wertschöpfung und Gefahrstoffe) und gleichzeitig auch zusätzliche Pflichten für KRITIS-Betreiber definiert (bspw. die Errichtung von Systemen zur Angriffserkennung).

Das ist der allseits bekannte Status quo der Cyber Security in Europa – bis Ende 2022. Die Umsetzung der NIS-Richtlinie in den einzelnen Mitgliedsstaaten erwies sich in der Rückschau insgesamt als schwierig und teilweise nicht zielführend. Dies führte dazu, dass sich die EU-Kommission veranlasst sah, Ende 2020 eine Überarbeitung der NIS-Richtlinie im Entwurf vorzunehmen, um durch auf die fortschreitende Digitalisierung und die damit in Zusammenhang stehende wachsende Bedrohungslage für kritische Infrastrukturen sowie die Zunahme von Cyberangriffen zu reagieren. Die vorgeschlagene Ausweitung des Geltungsbereichs der NIS 2.0, die mehr Einrichtungen und Sektoren dazu verpflichtet, Maßnahmen zur Absicherung zu ergreifen, würde dazu beitragen, das Niveau der Cybersicherheit in Europa langfristig zu erhöhen. Am 10.11.2022 hat das EU-Parlament dem Entwurf der NIS 2.0 Richtlinie zugestimmt (T9-0383/2022), am 27.12.2022 wurde diese im EU-Amtsblatt veröffentlicht. Sie ist am 16.01.2023 in Kraft getreten.

Hintergrund der RCE

Bereits 2008 wurde die sog. „European Critical Infrastructures (ECI) Direktive" bzw. die "Richtlinie 2008/114/EG des Rates vom

08.12.2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern" erlassen.
Gemäß der Richtlinie ist eine kritische Infrastruktur eine „Anlage, ein System oder ein Teil davon, die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind und deren Störung oder Zerstörung erhebliche Auswirkungen auf einen Mitgliedstaat hätte, da diese Funktionen nicht aufrechterhalten werden könnten" (Artikel 2, Richtlinie 2008/114/EG). Es wurden somit bereits vor beinahe 15 Jahren entsprechende Anforderungen an KRITIS Einrichtungen gestellt.

Ebenso wie NIS, bedurfte allerdings auch diese Richtlinie ein Update bzw. eine Anpassung an aktuelle Gegebenheiten. Dies führte dazu, dass Ende 2022 die RCE gemeinsam mit NIS 2.0 verabschiedet und Anfang Januar 2023 in Kraft getreten ist.

NIS 2.0 – wesentliche Änderungen

Die NIS 2.0 differenziert – anders als dies bisher aus dem KRITIS-Umfeld bekannt ist – zukünftig nach zwei Gruppen von Betreibern (sog. Entities), welche in achtzehn verschiedenen Sektoren Dienstleistungen erbringen und nach der Größe reguliert werden. „Essential Entities" sind Betreiber aus elf wesentlichen Sektoren, „Important Entities" sind Betreiber aus sieben wichtigen Sektoren. Die jeweiligen Unterschiede zwischen den beiden Gruppen beziehen sich im Wesentlichen auf den Umfang der staatlichen Aufsicht sowie der Sanktionsmöglichkeiten.

In NIS 2.0 wird definiert, dass bestimmte Betreiber und Branchen künftig unabhängig der Größe als Essential Entity geführt werden – dazu gehören:

- Digitale Infrastruktur: Anbieter elektronischer Kommunikation, Trust Service Provider, TLD Registries und Domain Registrare,
- Öffentliche Verwaltung: Zentralregierung und kritische Regionalregierungen
- Sonderfälle, die Mitgliedsstaaten als Essential festlegen – bspw. Betreiber, deren Ausfall einen „signifikanten Effekt" auf öffentliche Sicherheit oder Gesundheit hätten.

Die Identifikation von Betreibern weicht dabei von der bisher bekannten deutschen Anlagenmethodik (zumeist gilt: versorgt eine Anlage mehr als 500.000 Personen mit einer kritischen Dienstleistung (kDL), dann ist diese KRITIS) ab. Künftig erfolgt die Identifikation nicht mehr durch Schwellenwerte, sondern wird unternehmensgrößenbezogen durch die NIS Direktive vorgegeben.

Es obliegt also künftig nicht mehr den jeweiligen Mitgliedsstaaten, die Größenklassen selbst festzulegen. Inwieweit allerdings bei nationaler Umsetzung der Richtlinie bei der Definition der Unternehmen, die schlussendlich in den Anwendungsbereich der NIS 2.0 national fallen, andere Erleichterung durch die Berücksichtigung der Verhältnismäßigkeit, des höherwertigen Risikomanagements und eindeutiger Kritikalitätskriterien Einfluss finden, bleibt abzuwarten. Die Größenordnung der NIS stellt sich derzeit wie folgt dar:

- Mittlere Unternehmen: 50 bis 250 Beschäftigte, 10 bis 50 Mio. Euro Umsatz, bis zu 43 Mio. Euro Bilanzsumme,
- Große Unternehmen: mehr als 250 Beschäftigte, mehr als 50 Mio. Euro Umsatz, mehr als 43 Mio. Euro Bilanzsumme.

Gleichzeitig wird auch definiert, welche Unternehmen nicht betroffen sind:

- Kleinst-Unternehmen: weniger als 9 Beschäftigte und weniger als 2 Mio. Euro Umsatz/Bilanzsumme,
- Klein-Unternehmen: weniger als 50 Beschäftigte und weniger als 10 Mio. Euro Umsatz/Bilanzsumme.

Dies führt insb. dazu, dass nicht mehr nur ausschließlich Betreiber wesentlicher/kritischer Dienste betroffen sind, sondern die Anzahl deutlich steigen wird. Bisher waren vor allem größere Unternehmen betroffen, die sich mit der KRITIS-Verordnung und den Anforderungen auseinandersetzen mussten – nun gilt dies mehr für die breite Masse an Unternehmen in Europa und damit auch in Deutschland.

Hinweis: Es ist teilweise bei den jeweiligen Branchenverbänden zu lesen, dass man von einer Verzehnfachung der jetzigen KRITIS relevanten Unternehmen ausgehen kann.

NIS 2.0 legt ebenfalls Maßnahmen zur Optimierung der Cyber-Security fest – dazu gehören:

- Die Richtlinie gibt erstmals Mindestanforderungen für Essential und Important Entities an Cyber-Security vor (Art. 20),
- Definition von 14 Cyber Security Maßnahmenbereichen, welche Betreiber in der EU umsetzen müssen, u. a. Supply Chain/Lieferkettenmanagement, Business Continuity, Authentification Management, Kryptographie (Art. 21),
- Betreiber müssen die nationale Sicherheitsbehörde (in Deutschland das Bundesamt für Sicherheit in der Informationstechnik (BSI)) über signifikante Störungen, Vorfälle und Cyber Threats der jeweiligen kDL informieren,
- Kritische Betreiber von digitalen Diensten und Infrastrukturen müssen sich bei der ENISA registrieren (Art. 25).

Des Weiteren werden in NIS 2.0 Anforderungen an die nationalen Aufsichtsbehörden festgelegt. Dazu gehört, dass jeder Mitgliedsstaat bis April 2025 Anbieter von Essential und Important Entities an die EU-Kommission melden muss (Art. 3). Ebenso müssen nationale Cyber-Sicherheitsstrategien (NCSS) definiert und umgesetzt werden (Art. 7). Zusätzlich sind in den jeweiligen Mitgliedsstaaten Behörden zu beauftragen und zu ermächtigen, u. a. eine zentrale Cyber-Security- und Aufsichtsbehörde (Art. 8) für das Krisen-Management von „large-scale Cyber Security Incidents und Krisen" (Art. 9) oder CSIRTs für das Incident Handling

(Art. 10). Sofern gegen die Anforderungen von NIS 2.0 verstoßen wird, wurden entsprechend die Sanktionen erhöht. Die Maximalstrafen belaufen sich auf 10 Mio. Euro oder 2 % des weltweiten Umsatzes bei Essential Entities sowie 7 Mio. Euro oder 1,4 % des weltweiten Umsatzes bei Important Entities.

Überschneidungen zur RCE-Directive

Im Vergleich zu NIS 2.0 werden die Betreiber in der RCE-Directive durch die jeweiligen Behörden identifiziert und registriert. Die Identifikation erfolgt auf Basis einer Risiko-Analyse (u. a. das Unternehmen erbringt Essential Services in einem der Sektoren, das Unternehmen hat den Geschäftsbetrieb und die kDL auf dem Territorium von mind. einem EU-Mitgliedsstaat) sowie dem sog. disruptiven Effekt, wenn Betreiber im Land ausfielen.

Spricht NIS 2.0 von Essential und Important Entities, sieht RCE sog. Critical Entities, welche Essential Services erbringen. Diese Entities sind mit denen aus der NIS 2.0 fast identisch, wesentliche Ausnahme: in NIS 2.0 ist der Sektor Ernährung ein Important Sektor, in RCE hingegen Essential.

Analog NIS 2.0 für Cyber-Security fordert RCE-Maßnahmen zur Resilienz der kDL und schreibt auch Mindestmaßnahmen vor. Dazu gehören u. a. Maßnahmen in den Bereichen Vorsorge, Physische Sicherheit, Wiederherstellung (Business Continuity Management) sowie Awareness, die in einem zentralen Resilienz-Plan festgehalten werden müssen. Darüber hinaus müssen Betreiber sechs Monate nach Identifikation eine Risikoanalyse vornehmen und ihre Ausfallrisiken identifizieren und bewerten. Dabei sind auch Abhängigkeiten u. a. zu anderen Betreibern, Sektoren und kDL zu berücksichtigen. Die Risikoanalyse muss mind. alle vier Jahre aktualisiert werden. Wie im NIS sind auch hier Meldewege bei Störungen und Vorfällen gegenüber nationalen Behörden definiert.

Auch in RCE werden Anforderungen an die nationalen Aufsichtsbehörden gestellt. Dazu gehört auch hier die Ermächtigung und Beauftragung von Behörden insb. für eine zentrale Aufsichtsbehörde für die Resilienz, welche mit jener bei NIS 2.0 eng zusammenarbeiten soll (in Deutschland soll dies das „Bundesamt für Bevölkerungsschutz und Katastrophenhilfe“ (BBK) werden). Darüber hinaus sollen Mitgliedstaaten zur Identifikation und Registrierung der kritischen Betreiber drei Jahre nach Inkrafttreten und mindestens alle vier Jahre eine Analyse von Ausfallrisiken der kritischen Dienstleistungen und Sektoren anfertigen.

In Art. 17 und 18 RCE ist zudem definiert, dass gemäß RCE spezielle Betreiber mit besonderer europäischer Relevanz, die kritische Betreiber sind und mindestens sechs oder mehr Mitgliedsstaaten mit Essential Services verfügen, in der EU identifiziert, gemeldet und besonders überwacht werden sollen.

NIS 2.0		RCE	KRITIS
Essential	▶ Energie ▶ Transport ▶ Bankwesen ▶ Finanzmärkte ▶ Gesundheit ▶ Trinkwasser ▶ Abwasser ▶ Digitale Infrastruktur ▶ Verwaltung von IKT-Diensten ▶ Öffentliche Verwaltung ▶ Weltraum	▶ Energie ▶ Transport ▶ Bankwesen ▶ Finanzmärkte ▶ Gesundheit ▶ Trinkwasser ▶ Abwasser ▶ Digitale Infrastruktur - ▶ Öffentliche Verwaltung ▶ Weltraum ▶ Ernährung	▶ Energie ▶ Transport und Verkehr ▶ Finanzwesen ▶ Gesundheit ▶ Wasser ▶ IT & IK - - - - ▶ z. T. Transport (nicht vollständig) ▶ Ernährung
Important	▶ Post und Kurierdienste ▶ Abfallbewirtschaftung ▶ Produktion, Herstellung und Handel mit chemischen Stoffen ▶ Produktion, Verarbeitung und Vertrieb von Lebensmitteln ▶ Verarbeitendes Gewerbe/ Herstellung von Waren ▶ Anbieter digitaler Dienste ▶ Forschung	- - - - - - -	▶ z. T. Transport (nicht vollständig) ▶ Entsorgung ▶ Unternehmen im besonderen öffentlichen Interesse – Gefahrstoffe ▶ Ernährung ▶ Unternehmen im besonderen öffentlichen Interesse – Wertschöpfung ▶ z. T. Telemedien (nicht vollständig) -

Gegenüberstellung Entities- NIS 2.0 vs. RCE vs. KRITIS

Eine Gegenüberstellung der Entitites zeigt, dass es einige Überschneidungen gibt, allerdings auch Differenzen in der Auslegung bestehen. Insb. hinsichtlich der Subsektoren gibt es noch einige Unterschiede, die mit der Umsetzung in nationales Recht konkretisiert werden müssen. Der Sektor „Ernährung" wird bei NIS 2.0 als Important Entity geführt, wohingegen bei RCE als Critical Entity.

Am Beispiel des Sektors Energie lässt sich der erweiterte Anwendungsbereich aufzeigen. Der Anwendungsbereich war bei KRITIS im Wesentlichen auf Unternehmen beschränkt, die Energie im Strom- und Gassektor erzeugen, liefern oder regulieren bzw. in der Kraftstoff- und Heizölversorgung bzw. Fernwärmeversorgung tätig waren. Durch NIS 2.0 wird allerdings auch die Lieferkette relevant – und damit bspw. auch Betreiber von Ladepunkten/Ladestellen.

RCE sieht zudem den ÖPNV als Subsektor im Bereich Transport als Critical an, wohingegen dies in NIS 2.0 nicht aufgenommen wurde.

Daran zeigt sich, dass künftig eher mehr als weniger Unternehmen betroffen sein werden.

Umsetzung in nationales Recht

Beide Direktiven müssen bis Oktober 2024 in deutsches Recht überführt werden. Diese Mindestanforderungen müssen allerdings noch verabschiedet werden.

Das IT-SiG 2.0 nahm einige Anpassungen, wie bspw. die Meldung von Cybersicherheitsvorfällen innerhalb eines definierten Zeitraums, die Aufnahme weiterer Sektoren sowie erhöhte Cyber-Security Anforderungen, aus der NIS 2.0 bereits auf. Allerdings sind bei Weitem nicht alle Anforderungen durch das IT-SiG 2.0 umgesetzt – bspw. spezifische festgelegte Maßnahmen im Bereich Lieferkettenmanagement, Cyber-Risikomanagement oder die Definition der Betroffenheit von großen und mittleren Unternehmen. Bei der Umsetzung in nationales Recht sind noch einige Vorgaben der NIS 2.0 zu berücksichtigen.

KRITIS-Dachgesetz

In aller Munde ist das sog. KRITIS-Dachgesetz, über das künftig neben wesentlichen Faktoren aus NIS 2.0 insb. die RCE umgesetzt werden soll. Dazu gehören u. a. einheitliche Mindestvorgaben, Krisen- und Risikomanagement sowie insb. das Meldewesen und die staatliche Steuerung kritischer Infrastrukturen. Schwerpunkt stellt neben der physischen Sicherheit insb. die Resilienz dar.

Gemäß dem am 07.12.2022 veröffentlichten „Eckpunkte-Papier" für das KRITIS-Dachgesetz des Bundesministeriums des Innern und für Heimat (BMWI) heißt es: „Vor dem Hintergrund uneinheitlicher bzw. fehlender Regelungen für den physischen Schutz Kritischer Infrastrukturen und angesichts sektoren- sowie länderübergreifender Abhängigkeiten wird mit dem KRITIS-Dachgesetz zum ersten Mal das Gesamtsystem zum physischen Schutz Kritischer Infrastrukturen in Deutschland in den Blick genommen und im Rahmen der dem Bund zustehenden Zuständigkeiten gesetzlich geregelt. Das KRITIS-Dachgesetz ergänzt damit auch die bestehenden Regelungen zum Cyberschutz von Kritischen Infrastrukturen und trägt zu einem kohärenten und resilienten System bei […]. Das sektoren- und gefahrenübergreifende KRITIS-Dachgesetz ordnet ein und ergänzt sektorenspezifische gesetzliche und nicht-gesetzliche Regelungen. Auf Grundlage des KRITIS-Dachgesetzes sollen wertvolle Erkenntnisse zur Lage in den einzelnen KRITIS-Sektoren als Teil eines umfassenden Lagebildes gewonnen werden."

Gemäß dem Papier sind bereits folgende Sektoren als kritische Sektoren definiert:

- Energie
- Verkehr
- Bankwesen
- Finanzmärkte
- Gesundheit
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- Öffentliche Verwaltung
- Weltraum
- Lebensmittel
- (Kultur und Medien).

Es erfolgt eine klare Ausrichtung an der RCE. In Bezug auf die Ermittlung der Kritischen Infrastrukturen sollen sowohl quantitative als auch qualitative Kriterien (bspw. die Zahl der Nutzer oder die Bedeutung der Kritischen Infrastruktur) für die Aufrechterhaltung der kritischen Dienstleistung berücksichtigt werden.

Ausblick

Inwieweit eine Umsetzung sämtlicher Anforderungen durch das KRITIS-Dachgesetz erfolgt, bleibt abzuwarten – ziemlich sicher wird ein IT-SiG 3.0 veröffentlicht, da mit dem Dachgesetz im Wesentlichen die RCE umgesetzt wird. Interessant wird insb. die Schwellwert-Thematik und welche Auflagen (bspw. in Form von Audits und/oder regelmäßiger Meldungen) welchen Betreibern und in welcher Form auferlegt werden.

Auch wenn eine Umsetzung in nationales Recht noch aussteht, sollten Unternehmen so früh wie möglich prüfen, ob sie von NIS 2.0 oder RCE betroffen sind. Die vergangenen Monate und Jahre haben gezeigt, dass entsprechende Maßnahmen im (Cyber-) Security- und Resilienzbereich notwendig sind. Dies können sowohl organisatorische wie auch technische Maßnahmen sein. Beide Direktiven zeigen, dass Mindestanforderungen mit entsprechenden Auflagen in dem Umfeld an eine stetig steigen Anzahl an Unternehmen gestellt werden, da die Abhängigkeit im Lieferkettenzyklus ununterbrochen hoch ist. In jedem Fall stellen NIS 2.0 und RCE einen gravierenden und nachhaltig verändernden Einschnitt der europäischen Regulatorik dar.

ANSPRECHPARTNER

PARTNER

Holger Klindtworth
Tel. +49 40 37097-220
E-Mail: holger.klindtworth@ebnerstolz.de

Mark Alexander Butzke
Wirtschaftsprüfer, Steuerberater, CISA, CRISC, ISO/IEC 27001 Senior LA
Tel. +49 89 549018-292
E-Mail: mark.butzke@ebnerstolz.de

Christian Wieder
CISA, CRISC
Tel. +49 211 30143213
E-Mail: christian.wieder@ebnerstolz.de

FACHGEBIETE

CLOUD COMPUTING / OUTSOURCING

Michael Burkhardt
CISA, CRISC, ISO/IEC 27001 LA
Tel. +49 89 549018-293
E-Mail: michael.burkhardt@ebnerstolz.de

COMPLIANCE MANAGEMENT / SECURITY

Sabine Riederer
Zert. Datenschutzbeauftragte (GDD), CDPSE, ISO 27001 LA
Tel. +49 89 549018-293
E-Mail: sabine.riederer@ebnerstolz.de

Christian Burth
ISO 27001 Lead Auditor, ISO 22301 Lead Auditor
Tel. +49 89 549018-153
E-Mail: christian.burth@ebnerstolz.de

IT-COMPLIANCE MANAGEMENT / TAX & ACCOUTING

Hanna Pentzek
CISA, Prüferin für Interne Revisionssysteme[DIIR], Certified Tax Compliance Officer (DIZR)
Tel. +49 211 91332-664
E-Mail: hanna.pentzek@ebnerstolz.de

Ralf Körber
Wirtschaftsprüfer, Steuerberater, CISA, CRISC
Tel. +49 711 2049-1378
E-Mail: ralf.koerber@ebnerstolz.de

REVISION

Claudia Stange-Gathmann
CISA, CIA, CISM, QA (DIIR), ISO/IEC 27001 LA
Tel. +49 40 37097-313
E-Mail: claudia.stange@ebnerstolz.de

IT IN DER JAHRESABSCHLUSSPRÜFUNG

John Hoffmann
CISA, CIA
Tel. +49 711 2049-1219
E-Mail: john.hoffmann@ebnerstolz.de

Philipp Mattes
CISA, ISO/IEC 27001 LA, DSB (TÜV)
Tel. +49 221 20643-177
E-Mail: philipp.mattes@ebnerstolz.de

Alexander Götze
CISA
Tel. +49 40 37097-311
E-Mail: matthias ruhe@ebnerstolz.de

ERP

Matthias Ruhe
CISA, CASA, ISO 27001 Lead Auditor
Tel. +49 40 37097-311
E-Mail: matthias.ruhe@ebnerstolz.de

FIN-IT

Sebastian Adam
CISA, ISO/IEC 27001 LI
Tel. +49 69 1539249-21
E-Mail: sebastian.adam@ebnerstolz.de

SOFTWAREENTWICKLUNG

David Koall
CISA
Tel. +49 341 2444356
E-Mail: david.koall@ebnerstolz.de

ESECURITY-CERT GMBH

Marc Alexander Luge
ISO ISO/IEC 27001 LA,
zus. Prüfverfahrenskompetenz für §8a (3) BISG, IT-Sicherheitskatalog §11 (1a und 1b) EnWG
Tel. +49 211 540148-02
E-Mail: marc.luge@esecurity-cert.com

IMPRESSUM

Herausgeber:
Ebner Stolz GmbH & Co. KG
www.ebnerstolz.de

Ludwig-Erhard-Straße 1, 20459 Hamburg
Tel. +49 40 37097-0

Holzmarkt 1, 50676 Köln
Tel. +49 221 20643-0

Kronenstraße 30, 70174 Stuttgart
Tel. +49 711 2049-0

Redaktion:
Marc Alexander Luge, Tel. +49 211 91332-663
Hanna Pentzek, Tel. +49 211 91332-664
Dr. Ulrike Höreth, Tel. +49 711 2049-1371
novus.it@ebnerstolz.de

Wir legen großen Wert auf Gleichbehandlung. Aus Gründen der besseren Lesbarkeit verzichten wir jedoch auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers. Im Sinne der Gleichbehandlung gelten entsprechende Begriffe grundsätzlich für alle Geschlechter. Die verkürzte Sprachform beinhaltet also keine Wertung, sondern hat lediglich redaktionelle Gründe.

Fotonachweis:
©www.gettyimages.com