Ausgabe 2026

reichert reichert
steuern . recht . consulting

mitdenken

Datenschutz | Compliance | Künstliche Intelligenz



„Die digitale Zukunft braucht rechtliche Klarheit.“



Liebe Leserinnen und Leser,

mit dem vorliegenden Kanzleimagazin freuen wir uns, Ihnen bereits unser zweites Magazin zu Fokusthemen im Bereich Compliance, Datenschutzrecht und Künstlicher Intelligenz vorlegen zu können.
Wir geben Ihnen in unseren Beiträgen Impulse zur (Neu-)Bewertung Ihrer Compliance-Strategien, einen Überblick über neue Entwicklungen bei datengetriebenen Vorgängen auch mit übergreifenden Rechtsthemen und zeigen neue Perspektiven, wie Sie Ihr Unternehmen in das Digitale Zeitalter transformieren.
Die rasanten Fortschritte der Informationstechnologien und insbesondere der Einsatz immer leistungsfähigerer KI-Systeme eröffnen vielfältige Chancen und erlauben uns ein Umdenken aus klassischen Denkmustern, aber geben auch neue Fragestellungen.
Haben Sie schon die gesetzlich erforderliche KI-Richtlinie für Ihr Unternehmen erstellt? Wie weit sind Sie bei der Umsetzung der NIS2-Richtlinie, sofern Sie davon betroffen sind? Die erforderlichen Schritte bei den neuen EU-Richtlinien im Produktrecht oder den Datenschutzrechten – Haben Sie an alles gedacht?
Die digitale Transformation wird nicht allein durch technologische Innovationen geprägt, sondern zunehmend auch durch europäische Regulierungen, die neue Anforderungen schaffen und den Rahmen für unternehmerisches Handeln verändern.
Wir wissen, Vieles im Zeitalter der Neuen Digitalen Welt bedarf vieler Schritte – unser Fokus liegt genau darin: Unternehmen entsprechend ihrer Bedürfnisse passgenau zu beraten und auch Lösungen zu präsentieren. Auch bei der Umsetzung stehen wir als starke Kanzlei mit viel Expertise und einem vielfältigen Team genau da bereit, wo Ihr Unternehmen individuellen Bedarf hat.

Ob Gesellschafts- und Umwandlungsrecht, Arbeitsrecht oder Unternehmensnachfolge, Erbrecht oder Unternehmenskauf wie auch die Beratung für Unternehmen mit grenzüberschreitenden Interessen oder die nationale Steuerberatung für Ihr Unternehmen: wir denken agil und handeln auch so für Sie. Gefragt sind Lösungen, die rechtliche Sicherheit schaffen, sich in der Praxis bewähren und unternehmerische Handlungsspielräume erhalten und eröffnen.

Das Team von reichert & reichert verbindet hohe rechtliche Expertise mit einem ausgeprägten Verständnis für technologische Entwicklungen und betriebliche Zusammenhänge. Unser Anspruch ist es, Sie dabei zu unterstützen, Chancen frühzeitig zu erkennen, Risiken einzuordnen und gemeinsam tragfähige Wege für den verantwortungsvollen Umgang mit digitalen Technologien, Daten und Künstlicher Intelligenz zu gestalten.

In diesem Sinne wünschen wir Ihnen viel Spaß beim Lesen unseres Kanzleimagazins und freuen uns auf Ihre Fragen und den Austausch mit Ihnen.

Herzlichst Ihre Geschäftsführung:
Dr. Hansjörg Reichert, Jasmin Meßmer-Hadjiani, Isabell Sauter

INHALT

04 Compliance und Datenschutz

06 Das Ende der Ära „Cookie-Banner“

08 Datenschutz im Arbeitsrecht – ein Spannungsbogen

10 Die Aufsichtsbehörde klopft an Ihrer Tür? Ruhe bewahren und richtig handeln!

12 Litigation- und Krisen-PR – Strategische Rechtskommunikation in einer unternehmerischen Krise

14 Der Cyber Resilience Act (CRA) – Für Produkte mit digitalen Elementen

16 KI im Unternehmen

18 NIS2: Cybersecurity ist Chefsache – und die Lieferkette sitzt mit im Boot

20 Datenschutzbeauftragte sind keine Gegner, sondern Unterstützer!

21 Ein EU-Vertreter im Datenschutz – wann Ihr Unternehmen einen benötigt

22 Der Data-Act

23 Datenschutz und KI – Ein Widerspruch?

Hinweis: Alle Artikel dienen der ersten Orientierung und ersetzen keine individuelle Rechtsberatung

HERAUSGEBER

reichert & reichert
steuerberater & rechtsanwaltskanzlei
Max-Porzig-Straße 1 – 78224 Singen
+49 (0) 7731 9587-0
Reichenaustraße 19a – 78467 Konstanz
+49 (0) 7531 81987-0
kanzlei@reichert-reichert.de

Redaktion
Matthias Herkert, Sonali Mhalas-Bartels, Eileen Binder, Deniza Vehapi
Layout
Kieweg und Freiermuth GmbH – www.kuf.com
Fotografie
www.anij.de
stock.adobe.com

Hier das Magazin digital lesen!

erschienen im Oktober 2026
1. Auflage im Oktober 2026

Compliance und Datenschutz in Unternehmen – Mehr als „nice-to-have“ oder lästige Pflicht

WARUM IST COMPLIANCE SO WICHTIG UND HILFT IHREM UNTERNEHMEN?

Daten in jeder Form sind zum wichtigsten Handelsgut der Wirtschaft geworden – **Kundendaten, Produktdaten, Bewerberdaten, Bewegungsdaten, Zahlungsinformationen.** In einer zunehmend digitalisierten Wirtschaft verarbeiten Unternehmen täglich große Mengen personenbezogener und sensibler, teils sogar geheimer Daten. Gleichzeitig steigen regulatorische Anforderungen, gesellschaftliche Erwartungen und technologische Risiken. Ein einziger rechtlich belastbarer Vorfall kann hier reichen, um ein Unternehmen nachhaltig zu beschädigen.
Der Begriff „Compliance“ bedeutet zunächst nichts anderes als Regelkonformität. Es ist allerdings weitaus mehr: Es geht darum, Gesetze zu kennen und einzuhalten, interne Standards zu setzen und umzusetzen und Risiken frühzeitig zu erkennen. Dazu gehören neben Datenschutzvorschriften auch Regelungen aus dem Arbeitsrecht, Kartellrecht, Steuerrecht oder der Korruptionsprävention. Wer heute ein Unternehmen führt, bewegt sich zwischen Gesetzen, digitalen Prozessen und öffentlichen Blicken.

Compliance und Datenschutz sind daher nicht bloß juristische Bereiche. Sie bedeuten unternehmerische Verantwortung und sind zunehmend ein Wettbewerbsfaktor. Unternehmen, die gesetzliche Vorgaben einhalten und Datenschutz ernst nehmen, schützen nicht nur sich selbst vor Sanktionen, sondern stärken auch das Vertrauen von Kunden, Geschäftspartnern, Bewerbern und Mitarbeitenden.
Ein funktionierendes Compliance-System schafft klare Verantwortlichkeiten, transparente Prozesse und nachvollziehbare Kontrollmechanismen.

DIGITALISIERUNG ALS HERAUSFORDERUNG UND CHANCE

Künstliche Intelligenz, Cloud-Dienste, Homeoffice – moderne Arbeitsformen bieten enorme Steigerung der Produktivität, erhöhen jedoch Gefahr von Compliance-Verstößen. Bei der Nutzung einer KI-Software zur Bewerberauswahl zum Beispiel muss VOR der Nutzung geprüft werden, welche Daten verarbeitet werden, ob Diskriminierungsrisiken bestehen und wo die Server stehen. Datenschutz darf hier nicht, wie oft erlebt, nachträglich „hinzugefügt“ werden, das Prinzip „Privacy by Design“ verlangt, ihn von Anfang an mitzudenken.

DATENSCHUTZ ALS BESONDERER TEIL VON COMPLIANCE-STRUKTUREN MIT HOHEN BUSSGELDERN

Fast jedes Unternehmen verarbeitet personenbezogene Daten. Unternehmen müssen nachweisen können, dass sie diese Daten rechtmäßig, zweckgebunden und sicher verarbeiten. Dieses „Rechenschaftsprinzip“ macht Datenschutz zu einer ausdrücklichen Managementaufgabe.
Ein Beispiel: Ein Unternehmen speichert Kundendaten für Marketingzwecke. Ein Mitarbeiter exportiert versehentlich eine Kundendatenliste auf einen ungesicherten USB-Stick, der später verloren geht. Es entsteht eine Meldepflicht an die Datenschutzbehörde, dazu drohen Bußgelder, Schadenersatzforderungen und ein erheblicher Imageverlust.
Wenn es hier im Unternehmen klare Berechtigungskonzepte, Verschlüsselungsrichtlinien und deren Umsetzung sowie regelmäßige Schulungen gibt, ist der Vorfall vermeidbar.

DIE GRÖSSTE SICHERHEITSLÜCKE IST AUCH HIER SELTEN DIE TECHNIK – SONDERN DER MENSCH.

Phishing-Mails, schwache Passwörter oder unachtsam versendete Anhänge sind typische Einfallstore für Datenpannen.
Compliant arbeiten heißt: Risiken systematisch erkennen und reduzieren, bevor sie real werden.

FOLGEN VON COMPLIANCE-VERSTÖSSEN

Verstöße können im Compliance-Bereich mit erheblichen Bußgeldern geahndet werden – bis zu 20 Millionen Euro oder vier Prozent des weltweiten Jahresumsatzes allein im Datenschutzrecht. Daneben drohen Reputationsschäden. Auch Schadensersatzansprüche betroffener Personen sowie strafrechtliche Konsequenzen für Verantwortliche sind möglich. Dass Daten im Darknet landen oder Unternehmen Opfer von Cyberattacken werden, ist auch oft dann ein Thema für die Presse und auch für das operative Geschäft. Gerade in Zeiten sozialer Medien verbreiten sich negative Nachrichten schnell und können langfristige Auswirkungen auf die Marktposition eines Unternehmens haben.



DIE LÖSUNG: IMPLEMENTIERUNG EINES WIRKSAMEN COMPLIANCE-MANAGEMENT-SYSTEMS (CMS)

Geschäftsführung und Vorstand sind gesetzlich verpflichtet, geeignete Maßnahmen zu treffen, um Rechtsverstöße zu verhindern. Ein Compliance-Management-System umfasst alle Maßnahmen, Strukturen und Prozesse zur Sicherstellung regelkonformen Verhaltens.

„COMPLIANCE IM UNTERNEHMEN“ – WIR BERATEN KOMPETENT, AGIL UND INTERDISZIPLINÄR

Unser Ziel ist es, durch unser interdisziplinäres Know-how in der Beratung für Unternehmen **Risiken zu erkennen, zu minimieren, rechtliche Konsequenzen zu vermeiden** und zusammen mit unseren Mandanten eine Unternehmenskultur mit gesetzlich erforderlicher Regelkonformität zu etablieren, ebenso Ihre **Geschäftsprozesse und -entscheidungen an geltendes Recht anzupassen und interne Richtlinien gemeinsam zu erstellen.**

Compliance und Datenschutz sind keine kurzfristigen Projekte, sondern kontinuierliche Prozesse. Sie erfordern Engagement, Ressourcen, hohe fachliche Kompetenz und eine klare strategische Ausrichtung. Richtig umgesetzt bieten sie jedoch weit mehr als bloßen Rechtsschutz: Sie stärken die Reputation, erhöhen die Rechtssicherheit und schaffen Vertrauen bei Kunden und Partnern.

In einer datengetriebenen Wirtschaft ist nachhaltige Compliance daher nicht nur Pflicht, sondern ein entscheidender Baustein zum langfristigen Erfolg. Gerade im B2B-Bereich ist ein gutes Compliance-System oft Voraussetzung für Kooperationen oder andere unternehmensrechtliche Prozesse.

UM WAS GEHT ES?

Compliance ist die Erkennung und Einhaltung von Gesetzen, Richtlinien und Standard um Risiken im Unternehmen beherrschen zu können.

WER SOLLTE DAS LESEN?

Inhaber, Geschäftsführer, Vorstände und Mitarbeitende von Rechtsabteilungen.

WARUM IST DAS WICHTIG?

Bei Nichtbeachtung drohen hohe Bußgelder, zum Teil strafrechtliche Konsequenzen und ehebliche Reputationsschäden.

Sonali Mhalas-Bartels,
Rechtsanwältin; IT-Recht, Compliance und Datenschutz

ERFÜLLT IHR UNTERNEHMEN SICHER ALLE COMPLIANCE-ANFORDERUNGEN?

PRÜFEN SIE SELBST! DIESE BESTANDTEILE EINES CMS SOLLTEN VORHANDEN SEIN – WENN NICHT, SPRECHEN SIE UNS DAZU AN:

- ✓ **Einrichtung und Dokumentation klarer Zuständigkeiten**
- ✓ **Implementierung eines internen Kontrollsystems**
- ✓ **Risikoanalyse und -bewertung für alle Datenbereiche**
- ✓ **Vertragsmanagement**
- ✓ **Verhaltenskodex (Code of Conduct), Interne Richtlinien**
- ✓ **Hinweisgebersysteme**
- ✓ **Regelmäßige Schulungen zB im Datenschutz oder zur KI-Richtlinie**
- ✓ **Dokumentations- und Kontrollmechanismen, IT-Sicherheit**

Das Ende der Ära „Cookie-Banner“

WIE DIENSTE ZUR EINWILLIGUNGSVERWALTUNG LEICHTIGKEIT BRINGEN SOLLEN

Webseiten, die Schaufenster der Moderne. Wenn nicht die Mehrheit davon zunächst von einem breiten Türsteher namens „Cookie-Banner“ verdeckt werden würde. Sind sie weggeklickt, ist die Lust auf bunten Schaufensterbummel bereits vergangen. Die Einwilligungsverwaltungsverordnung (EinwV) könnte dem Banner-Chaos ein Ende setzen.

Die EinwV ist bereits seit 1. April 2025 in Kraft getreten. Damit ist der Rechtsrahmen für ein zusätzliches Einwilligungsverfahren zu Consent Managern (Cookie-Bannern) geschaffen. Es ermöglicht die Anerkennung von neuen Diensten zur Einwilligungsverwaltung, auch PIMS (= Personal Information Management Service) genannt.

WAS IST DAS PROBLEM BEI DEN HERKÖMMLICHEN EINWILLIGUNGSVERFAHREN?

Das Problem liegt in der Ausgestaltung der Banner. Banner sind in den allermeisten Fällen nicht datenschutzkonform ausgestaltet. Sie sind verschachtelt, kompliziert geschrieben, mit viel Text bestückt und oft geht es nur darum, die Nutzer durch sogenanntes „Nudging“ zur Abgabe einer Einwilligung zu drängen. Dadurch vertrauen Nutzer der Datenverarbeitung auf Webseiten nicht mehr, Websitebetreiber können nie ganz sicher sein, ob die von ihnen genutzten Dienste tatsächlich rechtskonform sind, es entsteht der Eindruck, dass kaum jemand Datenschutz ernst nimmt. Letztlich leidet der Glauben in einen funktionierenden Rechtsstaat. Es bleibt ein ungutes Gefühl beim Aufenthalt im Internet.



DIE EINWILLIGUNGSVERWALTUNGSVERORDNUNG ALS LÖSUNG?

Der Gesetzgeber erhofft sich mit Hilfe der EinwV Banner im Netz deutlich zu reduzieren. Ein sinnvolles Ziel. Durch die EinwV sollen Dienste geschaffen werden können, die die Einwilligungen zentral einsammeln und verwalten. Einwilligungsentscheidungen der Nutzer werden in den alternativen Diensten gespeichert und beim nächsten Besuch an die Website weitergegeben. Dadurch erscheint kein Banner mehr.

GANZ SO EINFACH IST ES DOCH NICHT

Nun ist das Verfahren sehr jung und damit entsprechend kritikanfällig. So könnte das zusätzliche Einwilligungsverfahren – je nach Ausgestaltung - erst ab dem zweiten Ansurfen der Seite greifen. Webseiten werden nach diesem Modell weiterhin Consent Manager brauchen, da Einwilligungsverwaltungsdienste die vom Nutzer getroffenen Einwilligungen erst nach dem ersten Besuch speichern. Ab dem zweiten Besuch wird die getroffene Einstellung an die Website übermittelt.

Jedoch werden Consent Manager aus einem weiteren Grund nicht obsolet. Hierfür ist einer der größten Kritikpunkte verantwortlich: PIMS-Dienste sind für Websitebetreiber freiwillig. Sie können von Websitebetreibern ignoriert werden. Die EinwV sieht keine Konsequenzen bei Nichtbeachtung vor. Lediglich der Einsatz von Cookies und ähnlichen Technologien zu Tracking- oder Analysezwecken ohne informierte Einwilligung kann gemäß § 28 Abs. 2, Abs. 1 Nr. 13 TDDDG ein Bußgeld in Höhe von bis zu EUR 300.000 nach sich ziehen. Nach der DSGVO können noch höhere Geldbußen drohen, wenn ein zeitgleicher Verstoß gegen die DSGVO vorliegt. Solange jedoch weiterhin informierte Einwilligungen über ein Consent-Banner eingeholt werden, finden die Bußgelder in der beschriebenen Thematik keine Anwendung.

Rechtlich gesehen gelten über PIMS geregelte Einstellungen nur für Einwilligungen nach § 26 TDDDG, nicht für Einwilligungen nach DSGVO. Die EinwV ist ein Produkt des TDDDG. In der Theorie müsste beim zweiten Ansurfen einer Website trotzdem wieder das Consent-Banner erscheinen, da die Einwilligung nach DSGVO nicht gespeichert wurde. Praktisch dürfte dieser Kritikpunkt jedoch schnell technisch überwunden werden.

Hingegen ist zum aktuellen Zeitpunkt unklar, was passiert, wenn viele Anbieter von Einwilligungsverwaltungsdiensten gleichzeitig genutzt werden (Stichwort Schnittstellenvielfalt).

Schließlich muss positiv hervorgehoben werden, dass Nutzer unter optimalen Bedingungen einige Zeit von eingestellten PIMS profitieren. Websitebetreiber müssen die Ablehnung des Nutzers akzeptieren, wenn sie Einwilligungsverwaltungsdienste zulassen. Es darf nicht in kurzen Abständen durch das erneute Einblenden des Banners gefragt werden, ob sich die Meinung geändert hat. Dies darf frühstens nach einem Jahr geschehen.

GIBT ES BEREITS EINWILLIGUNGSVERWALTUNGSDIENSTE?

Die Anforderungen an Dienste sind in der EinwV sehr genau geregelt und sehr hoch. Ein Dienst, der sich den Anforderungen stellt, muss am Ende von dem Bundesbeauftragten für Datenschutz und Informationstechnik (BfDI) freigegeben werden. Aktuell gibt es schlicht kein hohes Interesse bei Anbietern solche Dienste herauszubringen. Zumal sie wirtschaftlich unabhängig als auch unabhängig von Unternehmen sein müssen, die ein solches Interesse haben können. Es besteht kein wirtschaftlicher Anreiz.

Seit November 2025 gibt es einen Anbieter. Seines Zeichens erster von vom BfDI in Deutschland und Europa anerkannter Einwilligungsverwaltungsdienst. Das Unternehmen hat kein wirtschaftliches Eigeninteresse an den Einwilligungen der Nutzer. Der Dienst entstand in Zusammenarbeit mit Universitäten.

Das Ende der Ära Cookie-Banner ist noch nicht eingeläutet. Ein erster Schritt in einen mit weniger Türstehern bespickten viralen Schaufensterbummel ist gemacht. Spannend bleibt die kurzfristige Entwicklung. Es wäre zu wünschen, dass mehr Anbieter nicht gewinnbringende Anreize für die Entwicklung von Diensten zur Einwilligungsverwaltung finden. Konkurrenz unter Anbietern erhöht vielleicht auch den Druck auf Webseitenbetreiber, Einwilligungsverwaltungsdienste zuzulassen. Für Diensteanbieter sind Einwilligungsverwaltungsdienste eine echte Chance, im Urwald der Consent-Banner eine zuverlässige und rechtssichere Einwilligungslösung anzubieten. Das Vertrauen in das Unternehmen wird gestärkt, ein echter Wettbewerbsvorteil auf dem Markt.

Eileen Binder
Wirtschaftsjuristin, LL.B., Datenschutzbeauftragte

DATENSCHUTZKONFORMER UMGANG MIT COOKIES

- ✓ **Bestandsaufnahme unabhängig der EinwV: Welche Cookies und andere Technologien werden eingesetzt? Welche sind einwilligungspflichtig? Werden Drittanbieter eingesetzt (Maps, YouTube, Google Tag Manager)?**
- ✓ **Einwilligung nach TDDDG und DSGVO: Wird die Einwilligung im Consent-Banner richtig abgeholt (textlich, technisch und im Design)?**
- ✓ **Transparenz: Ist die DS-Information auf der Website aktuell und vollständig?**
- ✓ **PIMS (optional): Ist der Consent Manager-Anbieter mit dem PIMS-Dienst kompatibel? Ist der Consent-Manager so konfigurierbar, dass er nur Einwilligungen nach DSGVO abfragt und Einwilligungen nach TDDDG über PIMS laufen?**



Datenschutz im Arbeitsrecht – ein Spannungsbogen

UNTERNEHMEN MÜSSEN AUCH IM ARBEITSRECHT DEN DATENSCHUTZ IM BLICK HABEN – SONST WIRD ES TEUER!

Fehler beim Umgang mit personenbezogenen Daten können im Arbeitsrecht erhebliche Kosten verursachen. Vom Recruiting-Prozess über das Onboarding bis zur Kündigung oder Freistellung – überall lauern Fallstricke, wenn der Datenschutz nicht mitgedacht wird.

FEHLER BEIM DATENSCHUTZ HABEN EINFLUSS AUF ARBEITSRECHTLICHE PROZESSE UND SIND KOSTENINTENSIV

Wussten Sie, dass Mitarbeiterfotos auch firmenintern oft nur mit ausdrücklicher Zustimmung verwendet werden dürfen? Dass Krankmeldungen nicht unendlich gespeichert werden dürfen? Dass bei Kündigungen oft bei der Nichtbeachtung von Datenschutzvorschriften Fehler gemacht werden (fehlende Datenschutzinformation bei Wiedereingliederung-Maßnahmen als ein Beispiel)? Der Schaden kann immens sein und liegt dann auf der Unternehmensseite.

Das Zusammenspiel zwischen Arbeitsrecht und Datenschutz liegt natürlich auch auf Arbeitnehmerseite vor. Gegenüber Beschäftigten können Abmahnungen bei Verletzungen von Datenschutzregeln erfolgen, wenn geschäftliche Mails mit sensiblen Daten an private E-Mail-Adressen weitergeleitet werden. Ob es für eine Kündigung nach § 626 Abs. 1 BGB reicht, ist nicht immer gewährleistet, es bleibt eine Einzelfallentscheidung nach Interessensabwägung.

DIE RECHTSPRECHUNG IM ARBEITSRECHT GREIFT VERMEHRT FEHLER BEIM DATENSCHUTZ AUF

Die Entwicklung in der Rechtsprechung im Arbeitsrecht zeigt, dass oft die Missachtung von Regeln und Normen aus der DSGVO gerade bei Kündigungen zum Scheitern eines Prozesses und Zahlung von Schadenersatz führt. So scheiterte vor dem LAG Baden-Württemberg eine Kündigung u.a. auch wegen eines datenschutzbewehrten Aufklärungsfehlers, es ging um ein nicht allzu seltenes BEM-Verfahren (Betriebliches Eingliederungsmanagement).

NUTZUNG VON MITARBEITERDATEN – OFT EINE FALLE

Man darf als Unternehmen nicht einfach beliebig und wahllos Daten von Mitarbeitenden nutzen – diese Nutzung muss absolut zweckgebunden und mit einer Rechtsgrundlage versehen sein. In einem Fall hatte ein Unternehmen zur Testung einer Personalsoftware zu viele Daten eines Mitarbeiters an den testenden Mutterkonzern weitergeben, einer Betriebsvereinbarung zuwiderlaufend. Im Ergebnis hat der Arbeitgeber damit seine Übertragungsbefugnis von Daten des Mitarbeitenden überschritten und zu viele Daten an einen Dritten ohne Befugnis übermittelt. Der Mitarbeiter hat zu Recht einen Schadensersatz zugesprochen bekommen. EuGH-Urteil vom 19. Dezember 2024 (Az. C-65/23).

Damit man als Arbeitgeber nicht in die Falle der Nicht-Beachtung des Datenschutzes in seinen Prozessen läuft, ist ein gutes Compliance-Management nötig.

WIR HABEN ALS BERATUNGSUNTERNEHMEN DIE ERFAHRUNG IN BEIDEN RECHTSGEBIETEN:

Arbeitsrecht und Datenschutz – beides erforderliche Komponenten im korrekten Umgang im HR. Kontaktieren Sie uns, wenn Sie Unterstützung in der Umsetzung in Ihrem Unternehmen möchten. Als Unternehmen macht es Sie nach außen und innen stark, kompetent im Personalrecht zu sein.

Sprechen Sie uns an. Wir klären Fragen arbeitgeberseitig im Arbeitsrecht UND Datenschutz.

Sonali Mhalas-Bartels,
Rechtsanwältin; IT-Recht, Compliance und Datenschutz

ERFÜLLT IHR UNTERNEHMEN ALLE INFORMATIONSPFLICHTEN ZUM DATENSCHUTZ? HABEN SIE DAZU Z.B. EINE KLAUSEL BZW. ANLAGE IM RECRUITING-PROZESS UND IN DEN ARBEITSVERTRAG ZUM DATENSCHUTZ EINGEBAUT?

Allein im Arbeitsvertrag sollten u.a. folgende Informationen enthalten sein:

- ✓ **Welche Daten werden verarbeitet und zu welchem Zweck und wie lange werden Daten gespeichert?**
- ✓ **An wen werden die Informationen ggf. weitergeleitet?**
- ✓ **Kontaktdaten des Arbeitgebers**
- ✓ **Gibt es einen Datenschutzbeauftragten, wenn nötig? Wenn ja, wer ist es und wie kann ich ihn kontaktieren?**
- ✓ **Aufklärung über Widerrufsrecht zur Einwilligungserklärung**
- ✓ **Nach Einstellung Belehrung über die Rechte als Arbeitnehmer**

GRUNDFRAGEN ZU RECRUITING UND DATENSCHUTZ:

- **Wo und wie bewerben wir als Unternehmen Stellen? Kennen wir die Datenschutz-Problematiken z.B. bei HR-Tools?**
- **Gibt es digitale Schnittstellen, die wir nicht selbst kontrollieren?**
- **Brauchen wir bei der neunen Personalsoftware einen Auftragsverarbeitungsvertrag?**
- **Ist unsere Datenschutzerklärung im Recruiting wirklich überalleingebunden und aktuell?**

Die Aufsichtsbehörde klopft an Ihre Tür? Ruhe bewahren und richtig handeln!

EIN SCHREIBEN DER DATENSCHUTZAUFSICHTSBEHÖRDE FÜHLT SICH FÜR VIELE UNTERNEHMEN WIE EIN UNANGEKÜNDIGTER BESUCHER AN.

Kein Grund zur Panik! Die nachfolgenden Erläuterungen geben einen Einblick in die Handlungsoptionen und zeigen, welche Befugnisse dabei zur Verfügung stehen und wie man strukturiert und rechtssicher handelt, wenn man unangekündigt ein Schreiben der Aufsichtsbehörde bekommt.

Die Datenschutz-Grundverordnung stellte 2018 einheitlich sicher, dass in allen EU-Mitgliedsstaaten Aufsichtsbehörden bestehen müssen. Sie wird auf Grundlage ihrer datenschutzrechtlichen Kontroll- und Aufsichtsbefugnisse tätig, etwa nach Beschwerden betroffener Personen oder im Rahmen von Routineprüfungen, die einen Blick hinter die Kulissen wirft. Der Kontakt ist damit kein Ausnahmefall, sondern fester Bestandteil eines Systems, das die Einhaltung von Datenschutzvorgaben sicherstellen soll.

AUFSICHTSVERFAHREN

Sobald die Aufsichtsbehörde nach der Auswertung Ihrer Informationsanfrage zu dem Entschluss kommt, dass bei Ihrer Datenverarbeitung etwas nicht ganz rund läuft und den datenschutzrechtlichen Vorgaben widerspricht, kann die Aufsichtsbehörde eine Prüfung vornehmen, die nicht nur sehr komplex ist, sondern auch dazu führen kann, dass auf der Basis der Rechte des Art. 58 Abs. 1–3 DSGVO der Behörde, die Fortführung der Datenverarbeitung untersagt werden kann. Gerade deshalb sollte man schon frühzeitig Strategien entwickeln, um mögliche Konflikte zu vermeiden.

BUSSGELDVERFAHREN

Die Sorge vor Bußgeldern oder umfangreichen Prüfungen ist groß. Es ist wichtig, nicht nur strukturiert vorzugehen, sondern sich auch Kontrolle über die Situation zu verschaffen. Sobald Ihr Unternehmen einer Anordnung der Aufsichtsbehörde nicht nachkommt oder ein weiterer Datenschutzverstoß eintritt, droht Ihnen ein erhebliches Bußgeld nach Art. 83 Abs. 4 bis 6 DSGVO.

Die Aufsichtsbehörden können bei Verstößen gegen die DSGVO **Bußgelder von bis zu 20 Millionen Euro** verhängen, da sich die Bemessung des Betrages unter anderem an dem gesamten, weltweit erzielten Jahresumsatz eines Unternehmens orientieren kann. Bußgeldverfahren sind nicht nur finanziell belastend, sondern können auch den Ruf Ihres Unternehmens gefährden.

STRAFRECHTLICHE VERFOLGUNG

Verstöße gegen die DSGVO können neben Bußgeldern auch strafrechtlich verfolgt werden. Dabei sind insbesondere die, auf unrechtmäßige Datenverarbeitungen abzielenden, Strafvorschriften des § 42 BDSG und der §§ 202a, b und d StGB zu beachten. Wer sich unbefugt Zugang zu gesicherten Daten verschafft, die nicht für ihn bestimmt sind, macht sich strafbar. Anders als Bußgelder, drohen dem Verantwortlichen bei strafrechtlichen Verfahren hohe Konsequenzen, die bis hin zu Geld- oder sogar Freiheitsstrafe zielen.



ZWEITER SCHRITT – RECHTSSICHER VORGEHEN

Nach der Risikoabwägung und der geeigneten Auswahl der Verteidigungsmöglichkeit unter Berücksichtigung von Verfahrensart und Verfahrensstand ist maßgeblich, gezielt auf die Aufsichtsbehörde zu reagieren. In Bußgeldverfahren besteht die Möglichkeit, den Bußgeldbescheid mittels Einspruchs anzugreifen. Es ist somit wichtig alle Schritte vollständig zu dokumentieren, um die Nachvollziehbarkeit zu gewährleisten und die Erfolgschancen zu erhöhen.
Fazit: Keine Panik bekommen - strukturiert und rechtssicher vorgehen. Schon dieser kurze Überblick reicht aus, um aufzuzeigen, dass es gegen Maßnahmen der Datenschutzaufsichtsbehörde mehr Handlungsoptionen gibt als man zunächst denkt. Daher ist es wichtig in einen Dialog zu treten, um Missverständnisse zu vermeiden, oder rechtliche Schritte zu prüfen, die die Verteidigung anbelangen. Treten Sie in diesen Fällen gerne jederzeit mit uns in Kontakt und profitieren Sie von unserer Erfahrung, wenn „die Aufsichtsbehörde an Ihre Tür klopft".

Deniza Vehapi
Werkstudentin BWL, Bereich Recht und Consulting in der Kanzlei

HANDLUNGSOPTIONEN

ERSTER SCHRITT – RUHE BEWAHREN

Zunächst ist zu differenzieren, ob es sich um einen informellen Erstkontakt, eine Auskunft oder bereits um eine formelle Anordnung handelt. Wer gegen eine Maßnahme der Aufsichtsbehörde vorgehen möchte, sollte zunächst den Ansprechpartner klären, um Missverständnisse zu vermeiden, da man sonst das Risiko widersprüchlicher Angaben erhöht. Neben dem frühzeitigen Dialog mit der Behörde ist zu beachten, dass sich das Aufsichtsverfahren bei einer Verteidigung jederzeit in ein Bußgeldverfahren weiter entwickeln kann, wenn man nicht strategisch vorgeht sowie die rechtlichen und wirtschaftlichen Folgen im Blick hat. Neben der strafrechtlichen Verfolgung, die nicht außer Acht gelassen werden sollte, ist die Zusammenarbeit mit der Aufsichtsbehörde maßgebend, um die Maßnahmen ordnungsgemäß umsetzen zu können. Durch die konkrete Abwägung der Risiken, kann man die Verteidigungsstrategie so gestalten, dass man den Maßnahmen zwar gerecht wird, gleichzeitig aber auch die Auswirkungen auf ein möglich anbahnendes Bußgeldverfahren minimiert. Nur durch eine strategische Planung lassen sich die rechtlichen und wirtschaftlichen Risiken frühzeitig steuern und kontrollieren.
Um eine umfassende Bewertung im Einzelfall beurteilen zu können, sollte in solchen Fällen immer auf fachliche Expertise im Datenschutzrecht zurückgegriffen werden.

SCHREIBEN VON DER AUFSICHTSBEHÖRDE ERHALTEN?

- ✓ **Frist prüfen**
- ✓ **Strukturiert und rechtssicher vorgehen**
- ✓ **Zuständigkeit klären**
- ✓ **Antwort fachlich abstimmen - datenschutzrechtliche Expertise einholen**
- ✓ **Fristgerecht auf die Aufsichtsbehörde reagieren**

Litigation- und Krisen-PR – Strategische Rechts-kommunikation in einer unternehmerischen Krise



KEIN KOMMENTAR? ODER IST ANGRIFF DIE BESTE UNTERNEHMENSVERTEIDIGUNG?

In einer zunehmend transparenten und digital vernetzten Welt entscheiden nicht nur Gerichte über den Ausgang rechtlicher Auseinandersetzungen, sondern auch Öffentlichkeit, Medien und Stakeholder. Unter Litigation-PR und Krisen-PR (PR = Public Relation) versteht man die Art von strategischer Öffentlichkeitsarbeit während oder nach einem Rechtsstreit, eines Gerichtsprozesses oder bei anderen juristischen Auseinandersetzungen von Unternehmen, um vor allem Reputationsschäden bei diesen zu vermeiden und doch compliant zu bleiben.

Vor der Digitalisierung waren es z.B. Finanzkrisen, Veruntreuung in den Vorstandsebene oder andere strafrechtlich relevante Themen, die in der Regel zu schlechter Presse führten. Heutzutage gesellen sich hierzu noch Themen wie Datenpannen oder Cyberattacken, die einem Unternehmen schaden, nicht nur in finanzieller Hinsicht, sondern eben auch in der Reputation. **Und um es noch schlimmer zu machen, werden diese ganzen Fehltritte auch noch in Social-Media in einer wesentlich höheren Frequenz einer wesentlich größeren Gruppe gezeigt.**

Eine unbedachte Äußerung zu einem laufenden Verfahren oder zu einem Prozess in einem Unternehmensverkauf, vielleicht durch einen Mitarbeiter gegenüber der Presse, kann immensen Schaden anrichten. Und auch noch ein Gerichtsverfahren als solches juristisch beeinträchtigen.

GESTEUERTE KOMMUNIKATION KANN IM RECHTSSTREIT DEESKALIEREN

Unternehmen tun sich oft schwer, juristische Auseinandersetzungen in angemessener Form nach außen zu kommunizieren. Oftmals auch, weil sie fürchten, sich hier noch angreifbarer zu machen oder juristisch vielleicht nicht sauber aufzutreten oder weil sie einfach grundsätzlich die Öffentlichkeit vermeiden.

Allerdings gibt es hier keinen Grundsatz, der heißen könnte: Keine PR ist gute PR. Sondern eher: Angriff durch PR ist auch eine Form der Verteidigung!

In der Öffentlichkeit kommen eine kooperative Haltung und eine Informationspolitik mit Strategie oft besser an. Was bei nicht mit guter PR begleiteten Verfahren dann im schlechtesten Fall ausbricht, ist der berühmte Shitstorm – und der schafft kein Vertrauen in ein Unternehmen!

In anderen, vor allem außereuropäischen, Ländern sind Studieninhalte zu Litigation-PR schon gängige Praxis – hierzulande sind Universitäten und Hochschulen noch nicht ganz so weit. Zwar bereitet man mit so genannten „Moot Courts“* Studierende schon auf verbale Auseinandersetzungen in Gerichtsverfahren vor, dies jedoch ist noch lange nicht dazu geeignet, öffentlichkeitswirksam Ruf und Ansehen von Unternehmen in einer echten Krisensituation in der Presse wieder herzustellen.

UMSETZUNG DURCH INTERDISZIPLINÄRE TEAMS

Wir, die auch als Unternehmensberatung arbeiten, wissen, dass es möglich ist, Unternehmen in einer Krise durch gute juristische Kommunikation beiseitezustehen, wenn nicht sogar Krisen abzuwenden.

Es braucht zur einer gelingenden Krisen-PR ein gut eingespieltes Team mit Juristen, Unternehmensberatern, Marketing-/PR-Beratern, und eventuell noch ein bis zwei anderen Player. In so einem agilen interdisziplinären Team, bei dem untereinander mit offenen Karten gespielt wird, kann eine gute Litigation-PR nach außen gelingen. Eine so erstellte Tatsachen-Berichterstattung wird dann juristisch fest und journalistisch nicht angreifbar sein.

STRUKTUR UND STRATEGIE

Mit Kenntnis der Prozesskommunikation, der Analyse der vorliegenden Prozesse im Rechtsstreit und dann der Erstellung von Maßnahmenkatalogen können ergebnisorientierte juristische Strategien erarbeitet werden.

In der Regel geht es nicht zwingend nur darum, ein Unternehmen in ein gutes Licht zu rücken, oder eine „Weste reinzuwaschen“, sondern Kommunikation zu den Beteiligten zu suchen und Erkenntnisse zu teilen, in angemessener Form. Und auch darum, empathisch aufzutreten



und vielleicht Stakeholdern besondere Erkenntnisse mitzuteilen, um auch berechtigte Anfragen zu beantworten.
Die Beteiligten auf Unternehmensseite müssen sich hierzu Regeln geben, wie in den einzelnen Schritten verfahren wird; Wer Wann Was berichtet.

VERSTÄNDNIS FÜR KULTURELLE UNTERSCHIEDE

In Zeiten der Globalisierung und der international agierenden Unternehmen ist es auch wichtig, Gepflogenheiten, Sitten und Gebräuche aus anderen Ländern zu kennen, wenn Unternehmenskrisen oder juristische Auseinandersetzungen in deren länderspezifischen Pressemedien stehen. Hier empfiehlt es sich auch, mit Unternehmensberatungen zusammen zu arbeiten, die sich in den anderen Kulturkreisen auskennen und hineindenken können. Was in einem Land noch als charmant gilt, kann in einem anderen eine Beleidigung sein.

GRENZEN DER LITIGATION-PR

Man muss in Rechtstreitigkeiten, die zudem noch in der Öffentlichkeit ausgefochten werden, immer vorsichtig sein, keine wettbewerbsrechtlichen Normen zu verletzen, ebenso natürlich ist immer die Wahrung des Persönlichkeitsrechts zu beachten. Auch strafrechtliche Konsequenzen können sich aus Falschbehauptungen ergeben, eine gründliche Recherche ist daher unabdingbar.

WO GEHT'S HIN?

Nicht alles, was aus anderen Ländern an Entwicklungen in Zusammenhang mit Presse und Recht kommt, ist immer zukunftsweisend. Die Litigation- und Krisen-PR ist jedoch heutzutage in Zeiten von Social-Media und einer Veränderung der Art und Weise der Meinungsäußerungen unsererseits eine wirkliche Unterstützung für Unternehmen, auch außerhalb von Gerichtsverfahren.

Sonali Mhalas-Bartels,
Rechtsanwältin; IT-Recht, Compliance und Datenschutz

TYPISCHE ANWENDUNGSFÄLLE FÜR LITIGATION-PR UND KRISEN-PR, ALS BEGLEITUNG ZUR RECHTSBERATUNG:

- ✓ **Compliance Verstöße**
- ✓ **Zivilrechtliche Verfahren bei Großunternehmen**
- ✓ **Wirtschaftsstrafverfahren**
- ✓ **Ermittlungen durch staatliche Behörden**
- ✓ **Whistleblower**

SCHÄDEN DURCH MANGELHAFTE KOMMUNIKATION BEI BEKANNTWERDEN VON REGELVERSTÖSSEN ODER MISSTÄNDEN:

- ✓ **Vertrauensverlust**
- ✓ **Reputationsschäden**
- ✓ **Wirtschaftliche Einbußen und Folgeschäden**
- ✓ **Kosten bei Verfahren vor Gerichten**

* moot court: simulierte Gerichtsverhandlungen, die in der juristischen Ausbildung stattfinden

Der Cyber Resilience Act (CRA) – Für Produkte mit digitalen Elementen

WEITERE PFLICHTEN IN DER CYBERSECURITY FÜR UNTERNEHMEN AB SEPTEMBER 2026

Der Cyber Resilience Act (CRA) der EU führt ab dem 11. September 2026 verbindliche Pflichten für Hersteller von Produkten mit digitalen Elementen ein. Risikobewertung, Konformitätserklärung und Meldepflichten bei Sicherheitsvorfällen sind einige Punkte daraus. Auch Importeure und Händler können von den Pflichten betroffen sein, sofern Sie im Sinne des CRA als Hersteller gelten oder eine andere Rolle dort innehaben.

WER IST BETROFFEN?

Die Meldepflichten des CRA treffen Hersteller von Produkten mit digitalen Elementen im Sinne der Verordnung. Dazu zählen Unternehmen, die Produkte unter eigener Marke vertreiben (Own-Brand-Labeling) oder wesentliche Änderungen an bestehenden Produkten vornehmen. Die Pflichten gelten ab dem 11. September 2026 für alle relevanten Produkte – auch für solche, die bereits vor dem vollständigen Anwendbarkeitsdatum am 11. Dezember 2027 in Verkehr gebracht wurden.

GELTUNGSBEREICH UND BETROFFENE PRODUKTE

Die CRA-Meldepflicht gilt für alle Produkte, die auf dem EU-Markt bereitgestellt werden. Und zwar unabhängig vom Sitz des Herstellers.

Dazu zählen:

- **Softwareprodukte, u.a. Desktop- und mobile Apps, Cloud-Management-Tools**
- **Vernetzte Hardware wie Smartphones, Smart-Home-Geräte, industrielle Steuerungssysteme**
- **B2B-Software und kommerzielle Open-Source-Produkte**

WAS IST MELDEPFLICHTIG?

Der CRA unterscheidet zwei Kategorien meldepflichtiger Ereignisse:

- **Aktiv ausgenutzte Schwachstellen:** Sicherheitslücken, für die belastbare Hinweise vorliegen, dass sie von Angreifern ohne Zustimmung des Systembetreibers ausgenutzt werden.
- **Schwerwiegende Sicherheitsvorfälle:** Vorfälle, die die Fähigkeit des Produkts beeinträchtigen oder beeinträchtigen können, sensible oder wichtige Daten bzw. Funktionen zu schützen, oder die zur Einführung oder Ausführung von Schadcode geführt haben oder führen können.

DAS DREISTUFIGE MELDESCHEMA

Der CRA verlangt ein gestuftes Meldeverfahren mit kurzen Fristen:

Die Fristen beginnen mit der **Kenntniserlangung** – also sobald das Unternehmen eine hinreichend sichere Einschätzung hat, dass ein meldepflichtiges Ereignis eingetreten ist. Das einfache Abwarten auf eine vollständige technische Analyse ist nicht zulässig.

EREIGNIS	FRÜHWARNUNG	DETAILMELDUNG	ABSCHLUSSBERICHT
Aktiv ausgenutzte Schwachstelle	innerhalb 24 Stunden nach Kenntniserlangung	innerhalb 72 Stunden nach Kenntniserlangung	spätestens 14 Tage nach Verfügbarkeit einer Korrektur- oder Minderungsmaßnahme
Schwerwiegender Sicherheitsvorfall	innerhalb 24 Stunden nach Kenntniserlangung	innerhalb 72 Stunden nach Kenntniserlangung	innerhalb eines Monats nach der 72-Stunden-Meldung

MELDEWEG UND EMPFÄNGER

Meldungen erfolgen einmalig über die ENISA Single Reporting Platform (SRP). Die Meldung wird an das für den Hauptsitz zuständige nationale Computer Security Incident Response Team, kurz CSIRT gerichtet (in Deutschland: BSI) und gleichzeitig an ENISA übermittelt. Das empfangende CSIRT leitet die Information an alle anderen betroffenen CSIRTs weiter.

Zusätzlich zur Behördenmeldung müssen Hersteller die **betroffenen Nutzer** – und soweit angemessen alle Nutzer – über die Schwachstelle oder den Vorfall informieren und konkrete Gegenmaßnahmen benennen.

NACHWEIS DER CRA-KONFORMITÄT VOR PRODUKTEINFÜHRUNG

Unternehmen müssen vor dem Inverkehrbringen eines Produkte im Sinne des CRA eine Konformitätserklärung erstellen, die die Erfüllung der CRA-Anforderungen bestätigt. Hier liegt die volle Verantwortung beim Hersteller, eine falsche Erklärung verursacht erhebliche Bußgeldrisiken.



WAS UNTERNEHMEN JETZT BEACHTEN SOLLTEN:

✓ **Herstellerrolle klären:**
Dokumentieren Sie für jedes Produkt, ob Sie als Hersteller im CRA-Sinne gelten

✓ **Produktinventar erstellen:**
Identifizieren und Listen der relevanten Produkte und Komponenten

✓ **Risikokategorie bewerten und zuordnen:**
3-Klassen von Risikostufen

✓ **Incident-Response-Prozesse anpassen:**
Stellen Sie sicher, dass Schwachstellen und Vorfälle schnell erkannt, bewertet und eskaliert werden können.

✓ **Kenntniserlangung definieren:**
Legen Sie intern fest, wann ein Ereignis als „bekannt" gilt (erste belastbare Information im Sicherheitsteam).

✓ **Meldeprozess einüben:**
Testen Sie das dreistufige Meldeschema (24h/72h/Abschluss) im Rahmen von Übungen.

✓ **ENISA SRP registrieren:**
Bereiten Sie die Registrierung auf der Single Reporting Platform vor.

✓ **Nutzerinformation vorbereiten:**
Entwickeln Sie Vorlagen für die risikobasierte Information betroffener Kunden.

✓ **Drittanbieter-Komponenten prüfen:**
Klären Sie, wie Schwachstellen in eingebundenen Komponenten bewertet und gegebenenfalls gemeldet werden.

RECHTLICHE UNTERSTÜTZUNG IN ANSPRUCH NEHMEN

Die CRA-Meldepflichten sind komplex und mit erheblichen Haftungsrisiken verbunden. Fehlerhafte oder verspätete Meldungen können zu regulatorischen Sanktionen führen. Für Unternehmen empfiehlt sich daher, frühzeitig rechtliche Beratung durch auf Cybersecurity- und Produkthaftungsrecht spezialisierte Rechtsanwälte hinzuzuziehen.

Diese können bei der Einordnung der Herstellerrolle, der Bewertung meldepflichtiger Ereignisse, der Gestaltung interner Prozesse und der Vorbereitung von Meldungen unterstützen.
Wir unterstützen Sie hier in der Erfüllung Ihrer Compliance Anforderungen – sprechen Sie uns gerne an!

Sonali Mhalas-Bartels,
Rechtsanwältin; IT-Recht, Compliance und Datenschutz

DER CYBER RESILIENCE ACT IST FÜR IHR UNTERNEHMEN WICHTIG, WENN:

✓ **Sie Hersteller, Lieferant oder Händler von Produkten mit Digitalen Elementen sind**
✓ **Sie diese im EU-Wirtschaftsraum anbieten**

KI im Unternehmen

WARUM EINE KI-RICHTLINIE FÜR IHR UNTERNEHMEN JETZT UNVERZICHTBAR IST

Schnell etwas recherchieren, Zeit, Kosten und Ressourcen sparen - das alles klingt verlockend mit der Möglichkeit der Unterstützung durch KI. Aber was ist mit dem Risiko? Datenverlust, Verletzung von Unternehmensregeln, Verstoß gegen Gesetze?

Künstliche Intelligenz (KI) ist bei den meisten Unternehmen längst im Arbeitsalltag angekommen – doch wer KI in betrieblichen Prozessen und Abläufen einsetzt, muss klare Spielregeln schaffen. Künstliche Intelligenz verändert die Arbeitswelt mit hoher Geschwindigkeit. Mitarbeitende nutzen generative KI inzwischen ganz selbstverständlich für Recherchen, Textentwürfe, Übersetzungen, Programmieraufgaben und für Präsentationen.

Die Vorteile liegen auf der Hand: KI kann Prozesse beschleunigen, Kosten senken und Mitarbeitende bei zahlreichen Aufgaben unterstützen. Gleichzeitig entstehen neue rechtliche Risiken. Um den Einsatz von KI-Systemen im Unternehmen zu ermöglichen, gleichzeitig aber Risiken weitmöglichst in den Griff zu bekommen sind daher klare Spielregeln und Vorgaben erforderlich.

DER AI ACT ERHÖHT DEN HANDLUNGSDRUCK UND FORDERT KOMPETENZ

Mit der europäischen KI-Verordnung (EU) 2024/1689 – dem sogenannten AI Act – existiert erstmals ein umfassender europäischer Rechtsrahmen für die Entwicklung und Vermarktung, insbesondere aber auch den Einsatz künstlicher Intelligenz. Die Verordnung zielt darauf, vertrauenswürdige, menschenzentrierte KI zu fördern und gleichzeitig ein hohes Schutzniveau bei deren Verwendung zu gewährleisten. Hierzu verfolgt sie einen risikobasierten Ansatz: Je höher das Risiko eines KI-Systems für Menschen und ihre Rechte ist, desto umfangreicher sind die rechtlichen Anforderungen bei dessen Verwendung.

Bestimmte Regelungen gelten bereits seit dem 2. Februar 2025. Dazu gehören unter anderem die Verbote bestimmter KI-Praktiken sowie Vorgaben zur sogenannten KI-Kompetenz der Mitarbeitenden. Unternehmen müssen sicherstellen, dass Personen, die mit KI-Systemen arbeiten, über ausreichende Kenntnisse und Fähigkeiten verfügen, um diese Systeme sachkundig und verantwortungsvoll einzusetzen.

Weitere Anforderungen der KI-Verordnung wie Kennzeichnungs- und Transparenzpflichten müssen stufenweise umgesetzt werden und stellen neue Compliance-Anforderungen an die betroffenen Unternehmen.

Um die gesetzlichen Forderungen jetzt und auch zukünftig zu erfüllen und dabei den Umfang und den Einsatz von KI-Systemen wie gesetzlich gefordert zu beherrschen, sollten Unternehmen jetzt handeln.

Eine KI-Richtlinie kann hier die erforderlichen Prozesse und Verantwortlichkeiten etablieren und den notwendigen verbindlichen Rahmen schaffen.

WAS STEHT IN EINER KI-RICHTLINIE?

Eine KI-Richtlinie regelt insbesondere, ob und unter welchen Voraussetzungen Beschäftigte personenbezogene Daten, Kundendaten, Geschäftsgeheimnisse und sonstige vertrauliche Informationen in das KI-System eingeben dürfen.

Dabei kann die Nutzung eines KI-Dienstes immer auch eine Verarbeitung personenbezogener Daten darstellen und damit datenschutzrechtliche Anforderungen auslösen. Aber auch Geschäftsgeheimnisse können gefährdet sein, wenn sensible Informationen an ein externes KI-System übermittelt werden.

Bei der Verwendung der mit Hilfe künstlicher Intelligenz erzeugten Ergebnisse ist zu beachten, dass KI überzeugend formulieren, aber falsche Ergebnisse liefern kann. Deshalb muss für alle identifizierten Anwendungsfälle verbindlich festgelegt werden, welche Inhalte vor ihrer Verwendung durch einen Menschen überprüft werden müssen.

Besondere Vorsicht ist geboten, wenn KI im Beschäftigungskontext wie etwa zur Vorauswahl von Bewerbungen, zur Bewertung von Beschäftigten oder zur Unterstützung personalbezogener Entscheidungen eingesetzt wird.

BESONDERS SENSIBEL – KI IM PERSONALBEREICH

Besondere Vorsicht ist geboten, wenn KI im Beschäftigungskontext wie etwa zur Vorauswahl von Bewerbungen, zur Bewertung von Beschäftigten oder zur Unterstützung personalbezogener Entscheidungen eingesetzt wird. Der AI Act ordnet unter anderem bestimmte KI-Systeme im Personalmanagement als Hochrisiko-KI-Systeme ein und stellt hierfür besondere Anforderungen auf.

Daneben sind auch arbeitsrechtliche Rahmenbedingungen zu beachten. Wird eine technische Einrichtung eingesetzt, die geeignet ist, das Verhalten oder die Leistung von Beschäftigten zu überwachen, kann beispielsweise ein Mitbestimmungsrecht des Betriebsrats bestehen.

DIE EINFÜHRUNG EINES KI-SYSTEMS IST EINE TEAMAUFGABE

Für die Einführung eines KI-Dienstes muss daher immer neben technischem Know-How auch der Datenschutz, die Personalabteilung, die Rechtsabteilung oder externes anwaltliches Know-How und gegebenenfalls der Betriebsrat einbezogen werden.

Die Entwicklung einer KI-Strategie erfolgt in drei Schritten:

BESTANDSAUFNAHME

Zuerst ist feststellen, welche KI-Anwendungen bereits tatsächlich genutzt werden – offiziell und inoffiziell. Gerade bei frei verfügbaren Anwendungen besteht die Gefahr, dass KI-Dienste längst eingesetzt werden, ohne dass die Unternehmensleitung und die Verantwortlichen Stellen hiervon Kenntnis haben.

RISIKOBEWERTUNG

Im nächsten Schritt sind die Systeme nach ihrem jeweiligen Risiko zu bewerten. Abhängig von den KI-Diensten und den identifizierten Anwendungsfällen sind insbesondere datenschutzrechtliche Vorgaben, arbeitsrechtliche Schranken, urheberrechtliche und haftungsrechtliche Risiken, Themen der Cybersicherheit und Informationssicherheit sowie gegebenenfalls Mitbestimmungsrechte zu prüfen. Auch aus Verträgen mit Kunden und den jeweiligen KI-Dienstanbietern ergeben sich regelmäßig Themen, die in die Risikobeurteilung mit einfließen müssen.

VERBINDLICHE VORGABEN

Abschließend sind die hierüber abzuleitenden Ergebnisse zu verbindlichen Vorgaben, Freigabe- und Prüfprozessen, zulässigen KI-Anwendungen und Schulungen in einer KI-Richtlinie festzuschreiben und umzusetzen.
Das diese Vorgaben, einmal erstellt, nicht dauerhaft bestehen können, ergibt sich bereits aus der Natur künstlicher Intelligenzsysteme. Eine kontinuierliche Überprüfung und Weiterentwicklung, jeweils entlang dieses KI-Strategieprozesses, gewährleistet abschließend, dass die so erstellte KI-Richtlinie immer aktuell bleibt und die betriebliche Realität abbildet.

KI-RICHTLINIE ALS BESTANDTEIL MODERNER COMPLIANCE

Eine KI-Richtlinie ist damit mehr als eine interne Arbeitsanweisung. Sie ist ein wesentlicher Baustein der unternehmerischen Compliance.
Da die KI-Richtlinie dabei in den meisten Fällen viele, oft sogar fast alle Bereiche eines Unternehmens berührt, müssen bei ihrer Erstellung entsprechend zahlreiche rechtliche Einflüsse und Anforderungen berücksichtigt werden. Im Gegenzug werden die Vorgaben der KI-Richtlinie auf viele weitere Regelungen im Unternehmen einwirken und machen hierüber eine umfassende rechtliche Betrachtung notwendig.

Matthias Henkert,
Diplom-Kaufmann, Master of Laws (ll.m.),
Data Protection Risk Manager



UM WAS GEHT ES?

✓ **Eine KI-Richtlinie ist für jedes Unternehmen erforderlich, um den Einsatz von Künstlicher Intelligenz rechtssicher, transparent und einheitlich zu steuern und bestehende rechtliche sowie unternehmerische Risiken zu begrenzen. Sie schafft klare Vorgaben und Verantwortlichkeiten für Mitarbeitende und bildet damit eine wesentliche Grundlage für ein wirksames Compliance-System.**

WER SOLLTE DAS LESEN?

✓ **Inhaber und Geschäftsführer, Führungskräfte, Mitarbeitende von Rechtsabteilungen, aus dem Qualitätsmanagement und der Informationssicherheit.**

WARUM IST ES WICHTIG?

✓ **Bei Nichtbeachtung drohen Bußgelder, zum Teil strafrechtliche Konsequenzen und persönliche Haftungen.**

WANN WIRD DAS RELEVANT?

✓ **Umsetzung bereits erforderlich, keine Übergangsfristen.**

WIE KOMPLEX IST DAS?

✓ **Laufender Prozess, mittlere Komplexität, jedoch fundiertes juristisches und technisches Wissen erforderlich.**

WO BEKOMME ICH HILFE?

✓ **Das Expertenteam unserer Kanzlei unterstützt Sie gerne.**

NIS2: Cybersecurity ist Chefsache – und die Liefer-kette sitzt mit im Boot

WAS SIE JETZT MIT UND FÜR IHR UNTERNEHMEN TUN MÜSSEN

NIS2 ist kein weiteres IT-Projekt, das man nach dem Motto „Das macht unsere IT schon" delegieren kann. Mit dem deutschen NIS2-Umsetzungsgesetz gelten seit dem 6. Dezember 2025 für zahlreiche Unternehmen verbindliche Pflichten zu Cybersicherheit, Vorfallsmeldungen, Registrierung und Geschäftsführungsverantwortung.
Und doch haben die meisten Unternehmen noch nur ein paar unangenehme Gedanken daran verschwendet.

DER ERSTE SCHRITT: BETROFFENHEIT PRÜFEN

Die größte praktische Herausforderung liegt häufig nicht in der Umsetzung einzelner Sicherheitsmaßnahmen, sondern bereits in der Frage: Ist unser Unternehmen überhaupt betroffen?
Das Gesetz erfasst insbesondere Unternehmen aus bestimmten Sektoren, etwa Energie, Verkehr, Gesundheit, Wasser, digitale Infrastruktur, IT-Dienstleistungen, öffentliche Verwaltung, Lebensmittel, produzierendem Gewerbe und bestimmten weiteren Bereichen. Entscheidend sind neben dem Tätigkeitsbereich insbesondere Unternehmensgröße und konkrete Funktion innerhalb der Liefer- oder Leistungskette.
Typischerweise gelten Unternehmen ab 50 Beschäftigten (Achtung! Man ist durch Teilzeitkräfte, Aushilfen etc. oft schnell darüber) und über einem bestimmten Jahresumsatz oder einer Bilanzsumme als „wichtige Einrichtungen", sofern sie einem erfassten Sektor zuzuordnen sind. Für „besonders wichtige Einrichtungen" gelten teilweise höhere Anforderungen bzw. besondere gesetzliche Tatbestände. Atmen Sie aber nicht auf, wenn Sie bis hierher nicht betroffen sind!

Zu untersuchen sind insbesondere:

- **Welche Produkte und Dienstleistungen bietet das Unternehmen tatsächlich an?**
- **Gehören diese zu einem gesetzlich erfassten Sektor?**
- **Welche Gesellschaften und Betriebsstätten sind einzubeziehen?**
- **Sind Schwellenwerte bei verbundenen Unternehmen zu berücksichtigen?**
- **Liegt eine besondere gesetzliche Einstufung unabhängig von der Unternehmensgröße vor?**
- **Ist das Unternehmen möglicherweise als Anbieter digitaler Dienste oder digitaler Infrastruktur erfasst?**

Die Betroffenheit muss das Unternehmen grundsätzlich eigenständig prüfen und dokumentieren. Wer zu Unrecht von einer Nichtbetroffenheit ausgeht, riskiert, Registrierung, Sicherheitsmaßnahmen und Meldungen zu versäumen.

DIE WICHTIGSTEN PFLICHTEN

Betroffene Unternehmen müssen dann ein angemessenes Risikomanagement für die Netz- und Informationssysteme einrichten.
Die Maßnahmen müssen zur Risikolage, Größe und Struktur des Unternehmens passen. „Wir haben eine Firewall" ist daher ebenso wenig ein vollständiges Sicherheitskonzept wie „Unser Dienstleister kümmert sich darum". Das Unternehmen bleibt für seine gesetzliche Organisation und Kontrolle verantwortlich.
Hinzu kommt die Pflicht zur Registrierung beim BSI. Bereits betroffene Einrichtungen mussten sich grundsätzlich innerhalb von drei Monaten nach Inkrafttreten des Gesetzes registrieren; bei später eintretender Betroffenheit läuft die Frist ab diesem Zeitpunkt.

SICHERHEITSVORFÄLLE: 24 STUNDEN SIND SCHNELL

Erhebliche Sicherheitsvorfälle müssen dem BSI grundsätzlich unverzüglich gemeldet werden. In der Praxis gilt ein gestuftes Verfahren: eine erste Frühwarnung innerhalb von 24 Stunden, eine ausführlichere Meldung innerhalb von 72 Stunden und ein Abschlussbericht innerhalb eines Monats.
Die Frist beginnt nicht erst, wenn die IT-Abteilung sämtliche Ursachen gefunden, alle Server forensisch untersucht und einen 40-seitigen Bericht geschrieben hat. Entscheidend ist, wann das Unternehmen von einem erheblichen Vorfall Kenntnis erlangt.
Deshalb braucht es klare interne Eskalationswege: Wer bewertet einen Verdacht? Wer informiert die Geschäftsleitung? Wer entscheidet über die Meldung? Wer koordiniert IT, Datenschutz, Kommunikation und gegebenenfalls Strafverfolgungsbehörden?

LIEFERKETTE: DAS SCHWÄCHSTE GLIED SITZT OFT AUSSERHALB

NIS2 nimmt die Lieferkette ausdrücklich in den Blick. Ein Unternehmen kann technisch gut geschützt sein und dennoch erheblich betroffen werden, wenn ein Cloud-Anbieter, Softwarelieferant, IT-Dienstleister oder sonstiger wichtiger Partner ausfällt oder kompromittiert wird.
Ein bloßer Vertragssatz wie „Der Dienstleister gewährleistet angemessene Sicherheit" reicht regelmäßig nicht aus. Unternehmen sollten ihre Lieferanten risikobasiert klassifizieren und für kritische Anbieter insbesondere Folgendes vorsehen:

- **Mindestanforderungen an Informationssicherheit**
- **Pflicht zur unverzüglichen Information über Sicherheitsvorfälle**
- **Unterstützung bei Untersuchungen und Beweissicherung**
- **Anforderungen an Subunternehmer und Unterauftragnehmer**
- **Regelungen zu Zugriffen, Datenstandorten und Notfallbetrieb**
- **Audit-, Nachweis- und Kontrollrechte**
- **Exit- und Ersatzszenarien bei Ausfall oder Vertragsbeendigung**

Der Lösungsansatz ist ein Lieferketten-Register mit Risikoklassen. Für jeden kritischen Dienstleister sollten Geschäftsbereich, Systemzugriffe, Abhängigkeiten, Ausfallfolgen, Sicherheitsnachweise, Meldewege und Notfalloptionen dokumentiert werden. Kritische Anbieter werden anschließend regelmäßig überprüft; weniger kritische Lieferanten erhalten ein vereinfachtes Prüfprogramm. So entsteht aus einer unüberschaubaren Lieferantenliste eine steuerbare Risikolandkarte.

GESCHÄFTSLEITUNG TRÄGT VERANTWORTUNG

Die Geschäftsleitung muss die erforderlichen Risikomanagementmaßnahmen billigen, ihre Umsetzung überwachen und sich mit den Sicherheitsrisiken auseinandersetzen. Dazu gehören ausreichende Ressourcen, klare Verantwortlichkeiten und regelmäßige Berichte an die Unternehmensleitung.

Verstöße können aufsichtsrechtliche Maßnahmen, Zwangsgelder und empfindliche Bußgelder auslösen. Zusätzlich drohen Betriebsunterbrechungen, Vertragsstörungen, Haftungsansprüche, Reputationsschäden und gegebenenfalls datenschutzrechtliche Folgen. Die Geschäftsleitung sollte Cybersicherheit daher nicht als rein technische Angelegenheit behandeln, sondern als Teil von Risikomanagement, Compliance und Unternehmensführung.

NIS2 verlangt keine perfekte IT-Welt. Gefordert ist aber ein nachvollziehbares, risikobasiertes und tatsächlich gelebtes Sicherheitsmanagement.

Gerade bei der Prüfung der Betroffenheit, der Gestaltung von Lieferantenverträgen und der Verzahnung von IT-, Datenschutz- und Haftungsfragen können Rechtsanwälte unterstützen.

Wir bei reichert + reichert helfen dabei, die gesetzliche Einordnung belastbar zu dokumentieren, Verantwortlichkeiten zu klären und Sicherheitsanforderungen rechtssicher in Prozesse und Verträge zu übersetzen.

Sonali Mhalas-Bartels,
Rechtsanwältin; IT-Recht, Compliance und Datenschutz

QUICK NIS2-CHECKLISTE

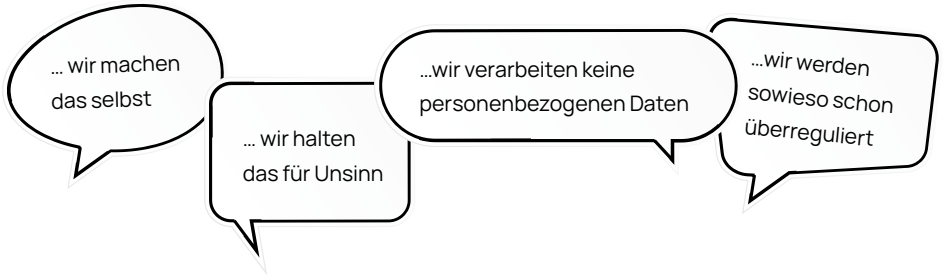
- ✓ **Betroffenheit anhand Tätigkeit, Sektor, Größe und Konzernstruktur prüfen.**
- ✓ **Prüfung mit Begründung, Quellen und Verantwortlichem dokumentieren.**
- ✓ **Falls betroffen: BSI-Registrierung und Fristen kontrollieren.**
- ✓ **IT-Risiken erfassen und angemessene Maßnahmen beschließen.**
- ✓ **Melde- und Eskalationsprozess für 24-/72-Stunden-Fristen festlegen.**
- ✓ **Kritische Lieferanten und Abhängigkeiten inventarisieren.**
- ✓ **Sicherheitsanforderungen in Verträgen und Nachweisen verankern.**
- ✓ **Geschäftsleitung regelmäßig informieren und Entscheidungen dokumentieren.**
- ✓ **Schulungen, Notfallübungen und Wirksamkeitskontrollen durchführen.**



Datenschutzbeauftragte sind keine Gegner, sondern Unterstützer!

WIR LÖSEN IHRE KONFLIKTE RUND UM DEN DATENSCHUTZ IN IHREM UNTERNEHMEN

Sie denken sicher oft, Ihr Unternehmen ist im Datenschutz gut aufgestellt, bzw. eine Datenschutzberatung oder gar ein Datenschutzbeauftragter ist überflüssig. Dann hier einmal die gängigste Aussagen dazu, die uns im Beratungsalltag begegnen: Unser Unternehmen braucht keine Datenschutzberatung …



Na, war etwas Passendes dabei?

DANN MAL ZU DEN FAKTEN:

Ein Datenschutzbeauftragter wird zwingend gemäß der DSGVO benötigt, wenn im Unternehmen die Verarbeitung von personenbezogenen Daten durch mindestens 20 Personen erfolgt oder wenn sensible Daten verarbeitet werden.

JETZT MÜSSTE MAN NATÜRLICH WISSEN, WAS PERSONEN BEZOGENE ODER SENSIBLE DATEN SIND.

- **Können Sie das aus dem Stehgreif rechtssicher beantworten?**
- **Kennen Sie alle Regulatorien und Dokumentationspflichten, die daraus entstehen?**
- **Auch in Bezug auf Social-Media, Webseite, HR-Compliance, Marketing und Vertrieb, KI?**

DER DSB ALS HILFE, COMPLIANT ZU SEIN

Weiterhin berät ein DSB die Unternehmensleitungen und schult Mitarbeitende im Datenschutz; überwacht die Einhaltung der Vorschriften intern und extern; ist Ansprechperson für Behörden; hilft bei Datenschutz-Folgeabschätzungen, und unterstützt bei Betroffenenanfragen und Datenpannen. Viele gesetzliche Aufgaben, die Unternehmen aus sich selbst heraus oft gar nicht leisten können.

Kennen Sie auch den Bußgeldkatalog, der die Versäumnisse, wie auch bei unsachgemäßer Behandlung von personenbezogenen Daten, bestraft? Falls Sie also Daten nicht korrekt löschen, oder Auskunftsanfragen Betroffener nicht nachkommen (können) oder eine meldepflichtige Datenpanne nicht melden?

KLEINE AUFLÖSUNG: DIE DSGVO SIEHT ZWEI STUFEN VOR

Schwere Verstöße gegen Grundsätze,
Betroffenenrechte oder Datenübermittlung; diese können mit bis zu 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes geahndet werden, je nachdem, welcher Wert höher ist.

Weniger gravierende Verstöße,
wie Unterlassung einiger Dokumentationspflichten, können mit bis zu 10 Millionen Euro oder 2 % des Umsatzes bestraft werden.

WAS AM ENDE WICHTIG IST:

Der Schutz von natürlichen Personen in ihrem Selbstbestimmungsrecht über ihre Daten und die Außenwirkung, die ein datenschutzkonformes Unternehmen zeigt.
Daher ist es unerlässlich in Unternehmen sorgsam und rechtskonform mit personenbezogenen Daten umzugehen – es könnte nämlich auch Ihre Daten betreffen!

Sprechen Sie uns an, wenn Sie zu den datenschutzrechtlichen Themen im Compliance-Kontext Beratung möchten – wir freuen uns auf den Austausch.

Sonali Mhalas-Bartels,
Rechtsanwältin; IT-Recht, Compliance und Datenschutz



Ein EU-Vertreter im Datenschutz – wann Ihr Unternehmen einen benötigt

IHR TEAM FÜR INTERNATIONALEN UND NATIONALEN DATENSCHUTZ

EIN EU-VERTRETER IM DATENSCHUTZ – WANN IHR UNTERNEHMEN EINEN BENÖTIGT

- ✓ **Betroffenheit anhand Tätigkeit, Sektor, Größe und Konzernstruktur prüfen.**
- ✓ **Prüfung mit Begründung, Quellen und Verantwortlichem dokumentieren.**
- ✓ **Falls betroffen: BSI-Registrierung und Fristen kontrollieren.**
- ✓ **IT-Risiken erfassen und angemessene Maßnahmen beschließen.**
- ✓ **Melde- und Eskalationsprozess für 24-/72-Stunden-Fristen festlegen.**

– dann hat sich diese Frage schon beantwortet.

SIE BENÖTIGEN EINEN EU-VERTRETER FÜR DEN DATENSCHUTZ!

Bei einem EU-Vertreter handelt es sich um eine in der Europäischen Union niedergelassene natürliche oder juristische Person, welche von einem Verantwortlichen oder Auftragsverarbeiter, jeweils ohne Niederlassung in der EU, bestellt wurde. Der EU-Vertreter vertritt den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die gem. Art. 27 DSGVO vorliegenden Pflichten.

Der EU-Datenschutzvertreter ist die externe Anlaufstelle für Aufsichtsbehörden und Betroffene und steht diesen zur Verfügung. Ausnahmen sind lediglich dann möglich, wenn die Verarbeitung nicht nur gelegentlich erfolgt und keine besonderen Kategorien nach Art. 9 DSGVO betroffen sind. Bei einem fehlenden EU-Vertreter drohen hohe Bußgelder von bis zu 10 Millionen Euro oder 2 Prozent des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres gem. Art. 83 Abs. 4 lit. a) DSGVO, je nachdem, welcher der Beträge höher ist.

Daher: Prüfen Sie nach der obigen Checkliste und kommen Sie auf uns zu, wenn Sie betroffen sind. Mit langjähriger Expertise im internationalen Datenschutz möchten wir mit Ihnen zusammenarbeiten und stehen mit einem kompetenten Team an Ihrer Seite!

Sonali Mhalas-Bartels,
Rechtsanwältin; IT-Recht, Compliance und Datenschutz

Der Data-Act

WAS ER FÜR DEN MITTELSTAND / DIE DIGITALWIRTSCHAFT BEDEUTET

CHANCEN UND RISIKEN FÜR DIE STRATEGISCHE NEUAUSRICHTUNG DER DATENFLÜSSE

Der Data Act ist ein EU-Gesetz, das die Nutzung und Weitergabe von Daten vernetzter Produkte und damit verbundenen Diensten regelt. Es ist als Teil des Digital Omnibus im europäischen Digitalpaket bereits am 12.09.2025 in Kraft getreten.

WARUM DER DATA ACT FÜR DEN MITTELSTAND RELEVANT IST

Der Data Act soll fairen Zugang zu Datenströmen in der gesamten wirtschaftlichen Wertschöpfungskette ermöglichen und dadurch den Wettbewerb und die Innovation innerhalb der EU antreiben. Unternehmen der Digitalwirtschaft und Verbraucher sollen hierdurch gestärkt werden. Durch den Data Act sollen Abhängigkeiten von großen (Cloud-) Plattformen reduziert und mehr Transparenz über Daten hergestellt werden.

WELCHE UNTERNEHMEN SIND BETROFFEN?

Unter den Data Act fallen Hersteller vernetzter Produkte wie Smart-Home-Geräte, Fahrzeuge, Smartwatches, Anbieter datenbasierter und verbundener Dienste wie Apps, mit denen sich ein vernetztes Produkt steuern lässt sowie Cloud- und IT-Dienstleister.
Primär unterfallen hierbei industriell und maschinell erzeugte Daten der Verordnung. Die Regeln für personenbezogene Daten richten sich weiterhin nach der DSGVO. Sie gilt innerhalb des Data Act weiter, z.B. dann, wenn Gesundheitsdaten über Fitness-Tracker gesammelt werden.

ZENTRALE PFLICHTEN FÜR MITTELSTÄNDISCHE UNTERNEHMEN

Betroffene Unternehmen sind verpflichtet einen uneingeschränkten Datenzugang für Kunden auf die erzeugten Daten bereitzustellen, sie dürfen diese Daten also nicht mehr für sich behalten. Auf Anforderung des betroffenen Verbrauchers müssen diese Daten an Dritte weitergegeben werden (Beispiel: Fahrzeugdaten, die beim Autohersteller gespeichert sind, werden an Werkstätten weitergegeben).
Organisatorisch müssen Unternehmen erweiterten Transparenz- und Informationspflichten über die Entstehung, den Zugriff und die Nutzung erzeugter Daten nachkommen, neue Vertragsklauseln über den Austausch von Daten unter Unternehmen müssen fair, angemessen und transparent gestaltet werden.

CHANCEN FÜR DEN MITTELSTAND

Durch den Zugang zu bisher abgeschotteten Daten lassen sich neue Geschäftsmodelle entwickeln, neue datenbasierte Services anbieten oder sich stärker in Richtung Reparatur-, Analyse- oder Optimierungsdienste ausbauen. Insbesondere Start-Ups sowie kleinere und mittlere Unternehmen könnten hiervon sehr stark profitieren.

RISIKEN UND HERAUSFORDERUNGEN

Das größte Risiko in der Umsetzung der Anforderungen des Data Acts liegt regelmäßig in der Preisgabe von Geschäftsgeheimnissen bei der Datenweitergabe. Während Daten- und Geschäftsgeheimnisse zwar auch durch den Data Act weiterhin geschützt sind, gilt es in der Umsetzung den technischen und organisatorischen Rahmen so zu gestalten, dass alle relevanten Anforderungen erfüllt sind, bestehende Verträge angepasst wurden und die Interessen des Unternehmens dennoch gewahrt bleiben.

Betroffene Unternehmen sind verpflichtet einen uneingeschränkten Datenzugang für Kunden auf die erzeugten Daten bereitzustellen, sie dürfen diese Daten also nicht mehr für sich behalten.

Insbesondere Cloud-Anbieter sehen sich weiteren Herausforderungen gegenüber, da sie technisch den Wechsel zu anderen Anbietern erleichtern, technische Hürden abbauen und sogenannte „Lock-In-Effekte“ reduzieren müssen. Daten aus vernetzten Produkten dürfen beim Hersteller nicht mehr in Datensilos „eingesperrt“ und damit Dritten gegenüber unzugänglich sein. Dies kann strategische Auswirkungen auf die IT-Architektur mit sich bringen und fordert eine vorausschauende und rechtsichere Gestaltung.

HANDLUNGSEMPFEHLUNGEN FÜR MITTELSTÄNDISCHE UNTERNEHMEN

Mit unserem Schulungs-Format „Einführung in den EU Data Act“ zeigen wir Ihnen, worauf Sie als Unternehmen achten müssen, welche Gefahren damit einhergehen und wie Sie rechtssicher agieren. Parallel unterstütz unser spezialisiertes Team sie dabei, die für Sie relevanten Anforderungen des Data Acts zu identifizieren, zu verstehen und rechtsicher in ihrem Unternehmen umzusetzen.

Eileen Binder
Wirtschaftsjuristin, LL.B., Datenschutzbeauftragte



Datenschutz und KI – Ein Widerspruch?

WIE KI-SYSTEME DATENSCHUTZRECHTSKONFORM EINGESETZT WERDEN KÖNNEN

Der Datenschutzbeauftragte ist heute oft ein juristisch und technisch wichtiger Partner bei der Planung und Einführung Künstlicher Intelligenz (KI).

WAS TECHNISCH PASSIERT

Generative KI-Systeme bestehen in aller Regel aus großen Sprachmodellen (Large Language Models, sog. „LLMs“). Diese Modelle werden mit sehr großen Datenmengen trainiert, um statistische Zusammenhänge zu erlernen. Im späteren Betrieb wird die Eingabe verarbeitet und unter Nutzung der Inputdaten hieraus eine Ausgabe konstruiert.
Während die Eingabe, der sogenannte „KI-Prompt“, und die Ausgabe für die Anwender „sichtbar“ sind, umfassen KI-Systeme auch zahlreiche weitere Komponenten. Protokollierungen, Speicherung von Dokumenten und Bildern und Verwendung für spätere Abfragen anderer Anwender. Bei sogenannten Retrieval-Augmented-Generation-Systemen (RAG) werden neben Trainingsdaten auch Informationen aus externen Datenbanken durchsucht, um präzisere Antworten zu generieren; relevante Daten werden dem Sprachmodell wieder zur Verfügung gestellt, um die Qualität der Antworten zu verbessern.
Technisch entstehen hierbei Verarbeitungsschritte, die datenschutzrechtlich bewertet werden müssen, da wir immer auch personenbezogene Daten in Texten, Bildern und Audios verwenden könnten.

WANN IST KI ALSO ERLAUBT?

Dass eine Verarbeitung technisch möglich oder für den Einsatz praktisch sinnvoll ist, bedeutet nicht, dass sie datenschutzrechtlich zulässig ist. Unternehmen müssen daher vor dem Einsatz von KI-Diensten Zwecke, Umfang und Erforderlichkeit bestimmen, um deren rechtliche Zulässigkeit beurteilen zu können.
Auch Daten die zulässig für einen ursprünglichen Zweck erhoben wurden, können nicht ohne Weiteres zur Verwendung oder gar zum Training in einem KI-Modell eingesetzt werden. Hier benötigt man eine Prüfung des Sachverhalts.

FAZIT

Wer KI im Unternehmen einsetzen möchte, kann nicht erst nach dem Roll-out den Datenschutz prüfen. Der Datenschutzbeauftragte muss „mit an den Tisch“ – und er muss technisch wie rechtlich „auf der Höhe der Zeit“ sein, denn: Technische Architektur, Datenflüsse und rechtliche Anforderungen, genauso wie das jeweilige Daten- und Lizenzmodell, Zugriffskonzepte, Verschlüsselung, Löschmechanismen und Protokollierungen müssen von Anfang an gemeinsam betrachtet werden.
Datenschutz und KI ist also kein Widerspruch, aber es geht nur zusammen gedacht.

Matthias Henkert,
Diplom-Kaufmann, Master of Laws (ll.m.),
Data Protection Risk Manager

Bild mit KI erstellt

reichert reichert
steuern . recht . consulting



reichert & reichert
Alles aus einer Hand.

Steuern, Recht und Unternehmensberatung. Kompetenzen, die ineinandergreifen.

Steuerberatung & Steuergestaltung

Wir entwickeln vorausschauende Steuerkonzepte, optimieren Unternehmensstrukturen und schaffen steuerliche Sicherheit bei wichtigen Entscheidungen.

Wirtschaftsrecht & Vertragsgestaltung

Von Gesellschaftsverträgen bis zu komplexen Unternehmensvereinbarungen. Wir gestalten rechtssichere Lösungen, die auch wirtschaftlich überzeugen.

Unternehmensnachfolge & M&A

Ob Unternehmensverkauf, Übernahme oder Nachfolgeregelung: Wir begleiten den gesamten Prozess mit rechtlicher, steuerlicher und wirtschaftlicher Expertise.

Unternehmensberatung & Strategie

Wir unterstützen bei strategischen Entscheidungen, Unternehmensbewertungen, Restrukturierungen und der wirtschaftlichen Weiterentwicklung Ihres Unternehmens.

Wirtschaftsprüfung & Compliance

Beratung und Unterstützung bei Compliance, Datenschutz und regulatorischen Anforderungen und über unsere Netzwerkpartner in der Wirtschaftsprüfung und prüfungsnahen Beratung.

Deutschland & Schweiz

Grenzüberschreitende Aktivitäten erfordern besondere Kompetenz. Wir beraten Sie in steuerlichen, rechtlichen und wirtschaftlichen Fragen.

Mehr über uns und was wir für Sie tun können unter www.reichert-reichert.de