Newsletter IP/IT

Dezember 2024

Inhalt

Künstliche Intelligenz und IT-Sicherheit: NIS, DORA, KRITIS und DSGVO sind die Hot Topics für 2025

Künstliche Intelligenz wird für Unternehmen immer relevanter und der Gesetzgeber reagiert mit einer ganzen Reihe von Gesetzesänderungen, die in 2025 relevant werden. Denn sowohl der europäische als auch der deutsche Gesetzgeber haben kurze Umsetzungsfristen festgelegt, sodass bereits ab Februar 2025 die ersten Vorgaben und Pflichten der KI-Verordnung gelten. Angesichts der geopolitischen Lage und der oft grenzüberschreitenden Cybersicherheitsbedrohungen wurden zudem zwei neue Gesetze zur Stärkung der europäischen Cybersicherheit verabschiedet: die NIS-2-Richtlinie und der Digital Operational Resilience Act (DORA).

Die neuen Vorschriften zur IT-Sicherheit regeln den Betrieb kritischer Infrastrukturen und hierbei wurde der Anwendungsbereich der betroffenen Unternehmen stark ausweitet. Das Inkrafttreten des deutschen NIS-2-Umsetzungs- und Stärkungsgesetzes (NIS-2-UmsuCG) wird Anfang 2025 erwartet. Der DORA setzt einen einheitlichen europäischen Rechtsrahmen für das Management von Cybersicherheits- und IKT (Informations- und Kommunikationstechnologie)-Risiken auf den Finanzmärkten; die Umsetzungsfrist hierfür läuft im Januar 2025 ab. Im kommenden Jahr 2025 wird es daher weiterhin wichtig sein, diese Regulierung im Blick zu haben und die dort vorgesehenen Pflichten fristgemäß umzusetzen. Wir bieten daher auch in 2025 wieder die notwendigen Schulungen und Beratung an.

Executive Briefings: Pflicht-Schulungen zur KI-Kompetenz, zur Cybersicherheit (NIS/KRITIS-Compliance) sowie zu aktuellen DSGVO/IT-Sicherheitsanforderungen für die Geschäftsleitung und Beschäftigte mit konkreten To-Do-Listen und Zertifikat nach Art. 4 KI-VO

Mit Inkrafttreten der KI-Verordnung (Verordnung EU 2024/1689) werden Anbietern und Betreibern von KI-Systemen umfangreiche Pflichten auferlegt (siehe unseren letzten Newsletter). Ab Februar 2025 sind Unternehmen u.a. verpflichtet sicherzustellen, dass ihr Personal und alle Auftragsverarbeiter über ein ausreichendes Maß an KI-Kompetenz verfügen (Art. 4 KI-VO). Auch nach der NIS-2-Richtlinie (bzw. dem deutschen „NIS-2-UmsuCG “) und der BSI-KRITIS-Verordnung sind die Umsetzung technischer Schutzmaßnahmen und Cybersicherheits-Schulungen Pflicht und müssen nachgewiesen werden!

Für unsere Bestandsmandanten wird es wieder spezielle Fokus-Schulungen (sowohl in Präsenz am 13. Februar 2025 als auch nach Vereinbarung via MS-Teams) geben, um das erforderliche Wissen zielgruppengerecht (GF, Beschäftigte etc.) zu vermitteln. Unsere Intensiv-Workshops vermitteln die notwendigen Inhalte kompakt und praxisnah. Sie erhalten zudem konkrete To-Do-Listen, Best-Practice-Empfehlungen und einen Schulungsnachweis (Zertifizierung), welcher die erfolgreiche Teilnahme und die nach Art. 4 KI-VO bzw. NIS/BSI-KRITIS-Verordnung erforderliche Kompetenz bescheinigt. Zusätzlich ist der Workshop für die Rechtsabteilung auch als Nachweis im Rahmen der Fachanwaltsausbildung (IT-Recht) geeignet.

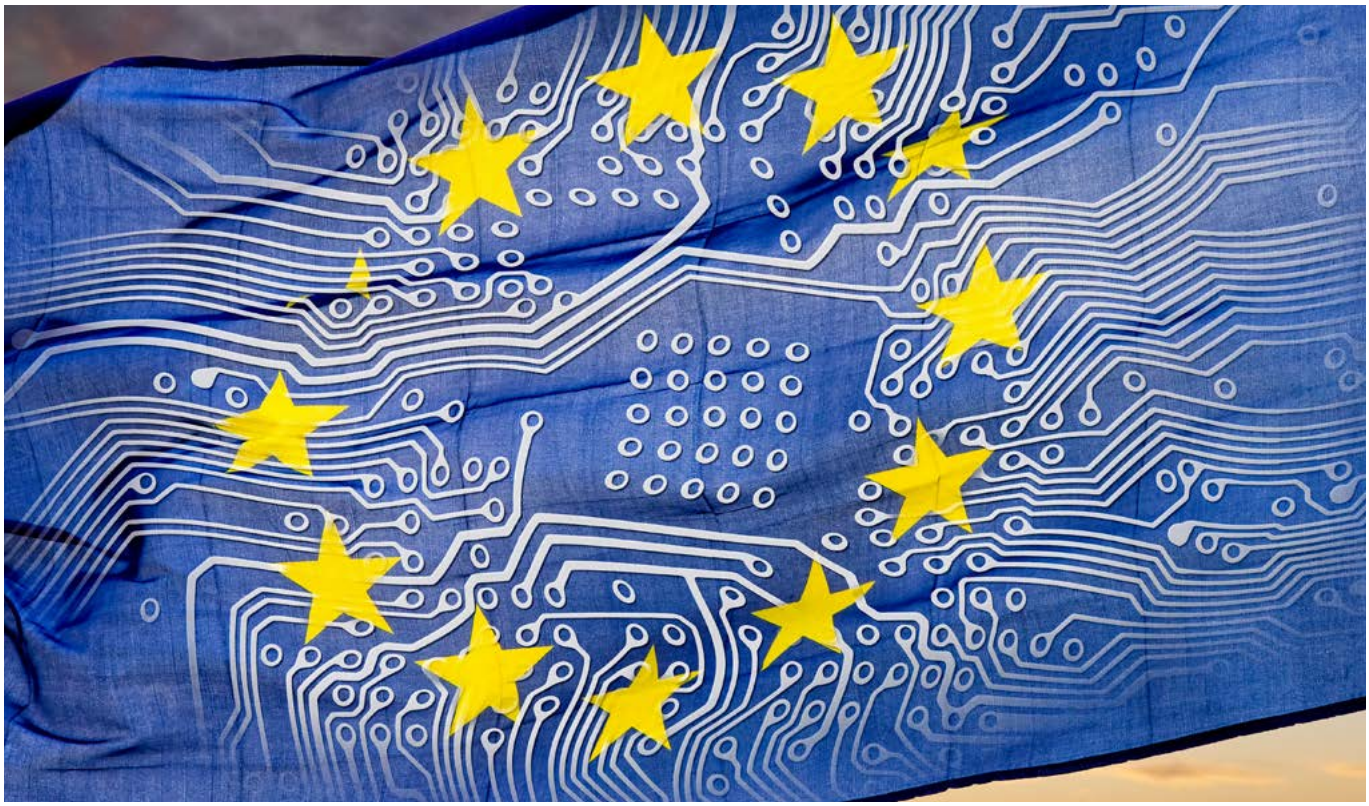
Das Angebot richtet sich mit einer Kompaktschulung an die Geschäftsleitung. Darauf aufbauend werden Intensiv-Schulungen für die Mitarbeiter aus den Bereichen HR, IT, Datenschutz und der Rechtsabteilung angeboten.

Executive Briefing: 2-stündige Kompakt-Schulung (einschl. Nachweis)
Intensiv-Schulungen: ca. 4 Stunden parallele, fachlich fokussierte Workshops für Mitarbeiter der Abteilungen HR, IT, Datenschutz und Recht

Die Schulungen sind kostenpflichtig und stehen derzeit nur den Bestandsmandanten von Luther offen. Bei Interesse wenden Sie sich bitte an Ihre/n Ansprechpartner bei Luther oder Rath/Kuss/Bauer.

Der Cyber Resilience Act

Der am 10. Dezember 2024 in Kraft getretene Cyber Resilience Act (CRA) legt verbindliche Anforderungen an die Cybersicherheit vernetzter Geräte fest. Der CRA soll dazu beitragen, Verbraucher und Unternehmen besser vor Cyberangriffen zu schützen.



I. Hintergrund des CRA

Durch die fortschreitende Digitalisierung sind immer mehr Geräte und Produkte miteinander vernetzt, angefangen von Smart-Home-Anwendungen über die Luftfahrtechnik bis hin zu medizinischen Geräten. Allerdings führt diese zunehmende Vernetzung auch zu einer erhöhten Anfälligkeit gegenüber Cyberangriffen. Schwachstellen in vernetzten Produkten können gravierende Folgen haben, darunter Datenverluste und sogar Sicherheitslücken, die die Privatsphäre und körperliche Unversehrtheit gefährden können. Von diesem Problem sind Haushaltsgeräte, Software, Cloud-Programme und Unterhaltungstechnik betroffen.

Bisher gab es in der EU keine einheitliche Regelung, die sicherstellt, dass vernetzte Produkte über einen ausreichenden Schutz vor Cyberbedrohungen verfügen. Mit dem CRA sollen vor allem Voraussetzungen für die Entwicklung sicherer Produkte mit digitalen Elementen geschaffen werden. So sollen die Hersteller die Sicherheit von Produkten mit digitalen Elementen bereits während der Konzeptions- und Entwicklungsphase und sodann während des gesamten Lebenszyklus verbessern.

II. Wesentliche Regelungsinhalte

1. Adressaten

Der CRA richtet sich an unterschiedliche Wirtschaftsakteure (Art. 3 Nr. 12 CRA), insbesondere an Hersteller, Einführer, Händler oder andere natürliche oder juristische Personen, die im Zusammenhang mit der Herstellung oder Bereitstellung von Produkten mit digitalen Elementen gemäß CRA bestimmten Verpflichtungen unterliegen.

2. Betroffene Produkte

Der CRA gilt für alle Produkte *mit digitalen Elementen, deren bestimmungsgemäße oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physi-*

sche Datenverbindung mit einem Gerät oder Netz einschließt (vgl. Art. 2 Abs. 1 CRA).

Dies sind Software oder Hardware und die zu dieser Software oder Hardware zugehörige Lösung zur entfernt stattfindenden Datenverarbeitung, ohne die das Produkt nicht funktionieren würde (Art. 3 Nr. 1 CRA). Nicht anwendbar ist der CRA u. a. auf Medizinprodukte nach der Medizinprodukteverordnung (Verordnung (EU) 2017/745), auf In-vitro-Diagnostika nach der Verordnung EU 2017/746 sowie auf Produkte nach der „General Safety Regulation“ für Kraftfahrzeuge (Verordnung (EU) 2019/2144).

3. Pflichtenkatalog

Im Rahmen des CRA werden neue Anforderungen an Produkte mit digitalen Elementen eingeführt. Ein zentrales Element ist die Verpflichtung, dass alle diese Produkte gegen Cyberbedrohungen abgesichert sein müssen. Um dem Grundsatz “Security by Design” zu entsprechen, müssen Hersteller bereits im Erstellungsprozess passende Maßnahmen ergreifen, um Cyberangriffe abzuwehren. Dazu gehören unter anderem, dass Produkte ohne bekannte Sicherheitslücken auf den Markt gebracht werden, mit sicheren Standardkonfigurationen ausgeliefert werden und die Möglichkeit bieten, in diesen Zustand zurückgesetzt zu werden. Sicherheitslücken müssen durch Updates behoben werden können. Die Produkte müssen durch Authentifizierungssysteme und andere Kontrollmechanismen vor unbefugtem Zugriff geschützt sein und unbefugten Zugriff melden. Weitere Pflichten betreffen die Vertraulichkeit, Integrität und Verfügbarkeit von Daten, einschließlich personenbezogener Daten. Dies ist durch Maßnahmen wie Verschlüsselung und Datenminimierung zu gewährleisten, und die Nutzer müssen die Möglichkeit haben, alle Daten und Einstellungen sicher zu löschen. Die Konformität der Produkte mit digitalen Elementen muss von den Herstellern gewährleistet werden (Art. 13 Abs. 1 CRA).

Darüber hinaus müssen Hersteller von Produkten mit digitalen Elementen gewährleisten, dass Schwachstellen und Komponenten der Produkte identifiziert und dokumentiert werden, Schwachstellen unverzüglich behoben werden, idealerweise durch Sicherheitsupdates, die getrennt von Funktionsupdates bereitgestellt werden sollten. Die Sicherheit der Produkte muss regelmäßig getestet und überprüft werden und Informationen über behobene Schwachstellen veröffentlicht werden (Art. 6 CRA i. V. m. Anhang I Teil II zum CRA).

Zum Nachweis der Erfüllung der vorstehenden Pflichten müssen Hersteller ein Konformitätsbewertungsverfahren durchführen (Art. 13 Abs. 12 i. V. m. Art. 32 CRA). Darüber hinaus müssen Hersteller die Cybersicherheitsrisiken ihrer Produkte mit digitalen Elementen bewerten und dokumentieren (Art. 13 Abs. 2, 3 CRA).

III. Fazit und Ausblick

Der CRA hat Auswirkungen sowohl auf Unternehmen als auch auf Verbraucher. Unternehmen müssen sich auf einen erheblichen Mehraufwand bei der Produktentwicklung und -wartung einstellen. Verbraucher hingegen profitieren von den neuen Vorschriften, da vernetzte Produkte besser geschützt werden. Verbindliche Sicherheitsanforderungen an vernetzte Produkte reduzieren das Risiko von Cyberangriffen erheblich und schaffen die Grundlage für ein hohes Schutzniveau in der vernetzten Welt.

Das Gesetz wurde am 21. November 2024 offiziell im Amtsblatt der Europäischen Union veröffentlicht und trat am 10. Dezember 2024 in Kraft. Damit hat der Countdown für die Umsetzung der Cybersicherheitsvorschriften begonnen. Es gibt eine Übergangsfrist von 3 Jahren, in der alle Vorgaben umgesetzt sein müssen. Einige Regeln haben jedoch eine verkürzte Umsetzungsfrist von 21 Monaten.

Text- und Data-Mining im Spannungsfeld des Urheberrechts: Das Urteil des Landgericht Hamburg (Az.: 310 O 227/23) vom 27. September 2024

Künstliche Intelligenz (KI) ist auf eine Vielzahl von Quellen zur Generierung von Informationen angewiesen. Das Training einer KI erfolgt auf Basis von Datensätzen, die durch Text- und Data-Mining gewonnen wurden – aber wie sind diese Datensätze urheberrechtlich geschützt? Das Landgericht Hamburg hat mit Urteil vom 27. September 2024 erstinstanzlich über die gesetzlichen Schranken aus § 44b UrhG bzw. § 60 UrhG und damit über in der Rechtswissenschaft umstrittene Fälle entschieden.

Hintergrund

Im Zeitalter von Big Data und KI ist Text- und Data-Mining (TDM) zu einem wichtigen Werkzeug für Forschung, Entwicklung und Innovation geworden. Doch was bedeutet dies konkret? Werden Metadaten aus verschiedenen Quellen wie Bildern, Texten oder Tönen gesammelt und so extrahiert, dass sie von Computern gelesen und von Software ausgewertet werden können, spricht man von TDM. Gesetzlich wird TDM definiert als „die automatisierte Analyse von einzelnen oder mehreren digitalen oder digitalisierten Werken, um daraus Informationen insbesondere über Muster, Trends und Korrelationen zu gewinnen“. Obwohl dieses Verfahren nicht neu ist, war das TDM bis zum Urteil des Landgerichts Hamburg noch nie Gegenstand einer deutschen Gerichtsentscheidung.

Zum Sachverhalt in Kürze

Ein Fotograf klagte gegen den gemeinnützigen Verein LAION, der eine Reihe von Datensätzen öffentlich zugänglich macht. Diese Datensätze können zum Training generativer KI verwendet werden. Der Fall betraf einen Bild-Text-Datensatz aus dem Jahr 2021, der eine Art Tabelle mit Hyperlinks zu im Internet verfügbaren Bildern und zugehörigen Textinformationen enthielt. Zu diesem Zweck extrahierte der Beklagte URLs zu öffentlich zugänglichen Bildern und lud die Bilder - darunter auch ein Bild des Klägers - von den jeweiligen Speicherorten herunter. Bereits das Herunterladen stellt eine urheberrechtlich relevante Vervielfältigung dar. Der Fotograf hatte sein Bild auf eine Stockphoto-Internetseite hochgeladen, die die Nutzung der Bilder für generative KI ausdrücklich untersagte. Der

Fall betraf also nicht das KI-Training als solches, sondern die vorgelagerte Frage, ob das Urheberrecht es LAION erlaubt, die Datei in seinen Datensatz aufzunehmen, d. h. sie herunterzuladen, um sie mit der Bildbeschreibung abzugleichen.

Überblick über die TDM-Schrankenregelung im Urheberrecht

Das Urheberrecht erlaubt bestimmte Nutzungen geschützter Werke oder Daten ohne Zustimmung des Urhebers. Für Text- und Datamining (TDM) sieht die Urheberrechtsrichtlinie von 2019 eine Privilegierung des TDM insbesondere für Forschungszwecke vor. Die Richtlinie wurde durch die hier einschlägigen §§ 44b und 60d UrhG in nationales Recht umgesetzt.

In § 44b UrhG wird die Vervielfältigung von rechtmäßig zugänglichen Werken zum Zwecke des TDM für zulässig erklärt. Rechtmäßig zugänglich sind beispielsweise Werke, die bereits im Internet frei zugänglich sind. § 44b UrhG begründet daher keinen Anspruch auf Zugang zu Werken zum Zwecke des TDM. Die Nutzungsbefugnis wird eingeschränkt, wenn die Rechteinhaber einen Vorbehalt gegenüber der Nutzung ihrer Schutzgegenstände erklären (sog. Opt-Out-Option). Dieser Nutzungsvorbehalt muss bei online zugänglichen Werken maschinenlesbar sein; letztere Voraussetzung wurde im Urteil ausführlich diskutiert. § 44b UrhG enthält keine Einschränkung des Personenkreises, so dass sich jedermann auf die Schrankenwirkung berufen kann. Daraus ergibt sich ein gesteigertes Interesse der Privatwirtschaft.

In engem Zusammenhang mit § 44b UrhG steht § 60d UrhG, der TDM für Zwecke der wissenschaftlichen Forschung zulässt. Voraussetzung ist, dass die Einrichtung keine kommerziellen Zwecke verfolgt, Gewinne reinvestiert oder im Rahmen eines staatlich anerkannten Auftrags im öffentlichen Interesse tätig ist. In diesem Zusammenhang sind auch Public-Private-Partnerships zulässig, sofern das private Unternehmen keinen bestimmenden Einfluss auf die Forschungseinrichtung hat. Erlaubt ist die Vervielfältigung, also das Herunterladen und Digitalisieren von Werken. Eine Opt-Out-Option ist hier nicht gegeben, weshalb das TDM zu Forschungswecken privilegiert wird.

Das Wichtigste aus dem Urteil

Das Landgericht Hamburg entschied zugunsten des Beklagten und traf Aussagen zu den für das TDM relevanten Schranken aus § 44b UrhG und § 60 UrhG.

Zunächst stellte das Gericht in einem obiter dictum fest, dass § 44b UrhG bereits auf die Datensätze anwendbar sei, die erst in einem weiteren Schritt ggf. für das KI-Training verwendet werden könnten. Die Hauptfrage war, ob der Vorbehalt auf der Stockphotos-Website, dass die Bilder nicht für „automated programs“ verwendet werden dürfen, einen relevanten Nutzungsvorbehalt darstelle, der die Verwendung ihrer Bilder für TDM rechtlich ausschließt. Der Nutzungsvorbehalt muss nach § 44b Abs. 3 UrhG maschinenlesbar sein. Dabei ist umstritten, ob Maschinenlesbarkeit im engeren Sinne bedeutet, dass er tatsächlich von einer Maschine gelesen werden kann (z. B. mit Hilfe von robot.txt) oder ob auch ein Text in natürlicher Sprache (wie im vorliegenden Fall) ausreicht. In der Tendenz bejaht letzteres das Gericht, mit dem Hinweis, dass moderne KI-Systeme in der Lage seien, auch Texte in einfacher Sprache zu lesen und zu interpretieren.

Jedenfalls sei im vorliegenden Fall die Nutzung des Bildes nach § 60 UrhG zulässig, da es sich bei der Beklagten LAION um ein wissenschaftliches Forschungsnetzwerk handelt. Das Gericht begründete dies mit dem von LAION verfolgten Ziel des wissenschaftlichen Erkenntnisgewinns und der Tatsache, dass der Datensatz unentgeltlich zur Verfügung gestellt wurde. Da § 60 UrhG keine Opt-Out-Option vorsieht, konnte sich der Fotograf nicht auf den Nutzungsvorbehalt berufen. Der Gesetzgeber entschied sich mit der Regelung für Forschung und Innovation und in gewissen Rahmen gegen Urheberrechte.

Fazit und Ausblick

Die Maschinenlesbarkeit des Nutzungsvorbehalts bleibt ein großes Problem in der Praxis: Sollten weitere Gerichte dem Landgericht Hamburg folgen, könnte dies bedeuten, dass der Vorbehalt in jeder Sprache, solange sie von irgendeinem Menschen verstanden werden kann, einen relevanten Nutzungsvorbehalt nach § 40b UrhG darstellt. Dies wäre eine erhebliche Verunsicherung für Unternehmen, die Datensätze erstellen, insbesondere vor dem Hintergrund, dass mit robot.txt eine einfache Alternative für maschinenlesbare Opt-Out-Optionen zur Verfügung steht. Der Kläger hat beim Oberlandesgericht Hamburg gegen die Entscheidung Berufung eingelegt (Az.: 5 U 104/24), sodass abzuwarten bleibt, wie die aufgeworfenen Fragen in der nächsten Instanz beantwortet werden. Jedoch wird eine umfassende Rechtssicherheit durch das Verfahren aufgrund des spezifischen Klagezuschnitts nicht zu erwarten sein. Damit bleibt die Frage eines angemessenen Ausgleichs zwischen Rechteinhabern und Large-Language-Modell (LLM)-Entwicklern zwischen Werkschutz und Innovation weiterhin ungeklärt. Aufgrund der Do-

kumentationsanforderungen an die für das KI-Training verwendeten Inhalte gemäß Art. 53 Abs. 1 lit. d der KI-Verordnung, ist davon auszugehen, dass es in Zukunft vermehrt zu Rechtsstreitigkeiten über die für das LLM-Training verwendeten Inhalte kommen wird.

Auch international bleibt das Zusammenspiel von KI und Urheberrecht interessant: Auf europäischer Ebene wurde erst im Juli die KI-Verordnung ((EU) 2024/1689) verabschiedet, die sich ebenfalls mit den Risiken von KI für das Urheberrecht befasst. Die KI-Verordnung bestätigt, dass auch das Erstellen von Trainingsdatensätzen für KI unter die Urheberrechtrichtlinie fällt. Auf der Ebene der Rechtsprechung reiht sich das Urteil in eine Reihe ähnlicher Fälle im Ausland ein, wie die Klage von Getty Images gegen Stability AI in England oder die Klage von drei Künstlerinnen gegen Stability AI, Midjourney und DeviantArt in den USA.

Update zum Bewerberdatenschutz bei automatisierten Entscheidungsfindungen im Recruiting Prozess

Vor dem Hintergrund der Digitalisierung und des zunehmenden Einsatzes Künstlicher Intelligenz (KI) im Bewerbungsprozess ist der Schutz personenbezogener Daten wichtiger denn je. Aus diesem Grund hat der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) im Juni 2024 in einem Positionspapier aktuelle Entwicklungen und Herausforderungen im Beschäftigtendatenschutz beleuchtet.

Hintergrund

In dem vorliegenden Positionspapier befasst sich der HmbBfDI u. a. mit den aktuellen Entwicklungen im Bereich des Beschäftigtendatenschutzes, insbesondere mit dem Urteil des Europäischen Gerichtshofs vom 30. März 2023 (SCHUFA-Urteil, Az. C-34/21) sowie mit dem Entwurf für ein eigenes Gesetz zum Beschäftigtendatenschutz. Dem war das Urteil des EuGH (Az. C-34/21) vorausgegangen, mit dem das Gericht Zweifel an der unionsrechtlichen Rechtmäßigkeit der im Beschäftigtendatenschutz relevanten Norm des § 26 Abs. 1 Satz 1 BDSG aufwarf.

Wesentliche Inhalte

Das Papier definiert häufig genutzte Begriffe im Bewerbungsverfahren (wie beispielsweise Recruiting, Open-Sourcing, Talent-Management oder KI), um unterschiedliche Interpretationen einzelner Unternehmen bei der rechtlichen Bewertung der einzelnen Verarbeitungsvorgänge zu vermeiden. Zudem wird ein Überblick über die typischen Phasen im Bewerbungsprozess und die in diesen Phasen regelmäßig stattfindenden Verarbeitungsaktivitäten gegeben. Schließlich werden in dem Positionspapier verschiedene Anwendungsfälle von KI im Zusammenhang mit dem Beschäftigtendatenschutz behandelt.

Die Phasen im Bewerbungsverfahren

Um den Überblick über die verschiedenen Datenverarbeitungen zu erleichtern, unterscheidet der HmbBfDI verschiedene Phasen eines Recruiting-Prozesses. Die Rechtmäßigkeit der Datenverarbeitung, insbesondere die Einhaltung der datenschutzrechtlichen Grundsätze und das Vorliegen einer Rechtsgrundlage, muss in jedem einzelnen Schritt gesondert betrachtet und geprüft werden.

- Phase 1: Erstkontakt vor der Bewerbung
  Ein solcher Erstkontakt ist möglich aufgrund von Active oder Open Sourcing, beispielsweise durch eine Kaltakquise, aufgrund von der Bewerber:innensuche über Stellenaufschreibungen oder auch aufgrund von der Erstellung von Leads.

- Phase 2: Bewerbungsverfahren
  Die zweite Phase umfasst die Verarbeitung von Daten durch ein Assessment Center, durch Bewerbungsinterviews oder ganz allgemein die Verarbeitung durch den oder die Personaler:in.

- Phase 3: Anstellungsverhältnis
  Die Anstellungsphase kann alle Verarbeitungen von personenbezogenen Daten umfassen, die zu einer Einstellung und Beschäftigung dazugehören, beispielsweise das Erstellen einer Personalakte.

- Phase 4: Beendigung
  Die Beendigung des Anstellungsverhältnisses wird als eigene Phase aufgeführt. Dies erscheint sinnvoll, denn sie bringt eine Vielzahl von datenschutzrechtlichen Fragen wie die Löschung bzw. notwendige weitere Speicherung von Daten mit sich.

Nutzung von KI im Bewerbungsprozess

Der HmbBfDI macht auch Ausführungen zum Einsatz von KI-Systemen im Rahmen von Recruiting-Prozessen, wie z. B. das automatische Auslesen von Bewerbungen (CV Parsing). Dies soll grundsätzlich unter Beachtung des Grundsatzes der Datenrichtigkeit (Art. 5 Abs. 1 lit. d DSGVO) zulässig sein, soweit Daten lediglich ausgelesen und strukturiert in Bewerbungsmanagementsysteme übertragen werden. Für zusätzliche Datenanalysen im Anschluss sind die Vorgaben der DSGVO zur automatisierten Entscheidungsfindung (Art. 22 DSGVO) sowie die hierzu ergangene SCHUFA-Entscheidung des EuGH (Urteil, vom 30. März 2023, Az. C-34/21) zu beachten. Danach dürfen Entscheidungen mit Rechtswirkung nur von einem Menschen getroffen werden. Vorschläge einer KI, beispielsweise zur Auswahl eines Bewerbenden, müssen so ausgestaltet sein, dass nicht bloß eine formelle menschliche Beteiligung gegeben ist. Zudem wird der Einsatz von LLM-Chatbots für z. B. Stellenausschreibungen oder die Beantwortung von FAQs im Rahmen des Bewerbungsprozesses bewertet. Zum datenschutzkonformen Einsatz von LLM-Chatbots hatte der HmbBfDI bereits Ende des Jahres 2023 eine Checkliste veröffentlicht.

Fazit

Die im Positionspapier dargestellte Übersicht über die Phasen des Bewerbungsverfahrens und die damit verbundenen Verarbeitungsvorgänge kann den Unternehmen einen besseren Überblick über die in den eigenen Rekrutierungsprozessen stattfindenden Verarbeitungen geben. Das erleichtert es den verantwortlichen Unternehmen den Anforderungen zur Erstellung entsprechender Verarbeitungsverzeichnisse (Art. 30 Abs. 1 DSGVO) gerecht zu werden.

Daneben werden über die dargestellten Ausführungen hinaus weitere wichtige Begriffe (wie beispielsweise Assessment Center oder das Fragerecht) oder Prozesse im Zusammenhang mit KI (wie Predictive/People Analytics, Gender Bias oder Human Experience Management) benannt, die noch einer aufsichtsbehördlichen Einordnung bedürften.

Beschluss der Datenschutzkonferenz zur Übermittlung personenbezogener Daten im Rahmen eines Asset Deals

Ein Unternehmen wird oft durch die Übertragung von Anteilen als Share Deal oder von Wirtschaftsgütern als Asset-Deal verkauft. Der Share Deal ist datenschutzrechtlich weniger problematisch, da sich die verantwortliche Stelle nicht ändert. Im Falle eines Asset Deals ändert sich jedoch die verantwortliche Stelle. Die Datenschutzkonferenz (DSK) hat am 11. September 2024 ihre Leitlinien zur Unterstützung der Praxis bei der Umsetzung überarbeitet. Der folgende Beitrag stellt diese Leitlinien vor.

Datenschutzrechtliche Herausforderungen bei Asset Deals

Unter einem Asset Deal versteht man hierbei eine Form des Unternehmenskaufs, bei der Wirtschaftsgüter/Vermögenswerte eines Unternehmens im Rahmen der Singularsukzession auf die Erwerberin oder den Erwerber übertragen werden. Den Veräußerer trifft hierbei die datenschutzrechtliche Verantwortlichkeit bei der Übermittlung personenbezogener Daten an den Erwerber. Er hat insbesondere für ein angemessenes Schutzniveau im Sinne von Art. 32 DSGVO zu sorgen und eigene datenschutzrechtliche Pflichten zu erfüllen – z.B. Kundendaten bei Vorliegen der Voraussetzungen des Art. 17 DSGVO grundsätzlich zu löschen. Der Erwerber hat mit dem Erwerb grundsätzliche die Pflichten als Verantwortlicher zu erfüllen. Ihn treffen – außer in Fällen des Art. 14 Abs. 5 DSGVO – Informationspflichten nach Art. 13 und 14 DSGVO sowie die Hinweispflicht auf ein Widerspruchsrecht nach Art. 21 DSGVO.

Differenzierung zwischen den Stadien der Vertragsdurchführung

Die DSK stellt im Ausgangpunkt fest, dass hinsichtlich der Art der Daten und den verschiedenen Stadien der Vertragsdurchführung differenziert werden sollte.

Eine Übermittlung personenbezogener Daten im Rahmen von Vertragsverhandlungen vor Abschluss des Asset Deals (Due Diligence-Phase) ist grundsätzlich unzulässig, kann jedoch bei Vorliegen einer Einwilligung des Betroffenen oder eines berechtigten Interesses an der Verarbeitung erlaubt sein.

Hinsichtlich der Übermittlung von Kundendaten ist zwischen den Stadien des zwischen Veräußerer und Kunden bestehenden Vertrags zu differenzieren. In der Phase der Vertragsanbahnung sowie in laufenden vertraglichen Beziehungen mit dem Kunden kommt eine Rechtfertigung der Übermittlung von Kundendaten an den Erwerber weitestgehend durch Berufung auf die Erlaubnistatbestände des Art. 6 Abs. 1 DSGVO, insbesondere Art. 6 Abs. 1 lit. b, Art. 6 Abs. 1 lit. f. DSGVO in Betracht. Dies gilt grundsätzlich auch bezüglich Daten, die im Zusammenhang mit offenen Forderungen stehen und hinsichtlich relevanter personenbezogener Daten von Lieferantinnen und Lieferanten oder deren Beschäftigten.

Bei beendeter vertraglicher Beziehung zum Kunden kommt eine Übermittlung dieser Daten zur Erfüllung der gesetzlichen Aufbewahrungsfristen in Betracht. Hier ist zusätzlich gemäß Art. 28 Abs. 3 DSGVO der Abschluss eines Vertrags über eine Auftragsverarbeitung erforderlich. Auch hat der Erwerber die Daten von jenen der Kundinnen und Kunden mit einer laufenden vertraglichen Beziehung zu trennen („Zwei-Schrank-Lösung“), es sei denn, es liegt eine wirksame Einwilligung der Kunden und Kundinnen in die Verwendung dieser Daten vor.

Die Daten der Kunden und Kundinnen dürfen gemäß Art. 6 Abs. 1 lit. f DSGVO durch den Erwerber grundsätzlich in demselben Umfang für Werbezwecke verwendet werden, wie dies auch dem Veräußerer möglich gewesen wäre. Gegebenenfalls sind bei Werbemaßnahmen mittels elektronischer Post oder Telefon die Anforderungen des § 7 UWG zu berücksichtigen.

Spezielle Anforderungen an ausgewählte Kategorien von Daten

Eine Übermittlung von besonderen Kategorien von personenbezogenen Daten, wie z.B. Gesundheitsdaten, ist nur bei informierter und ausdrücklicher Einwilligung des Kunden nach Art. 9 Abs. 2 lit. a, Art. 7 DSGVO zulässig. Bankdaten können im Falle einer Vertragsanbahnung oder bei einer laufenden Vertragsbeziehung gemäß Art. 6 Abs. 1 lit. b DSGVO übermittelt werden. Ansonsten ist hierfür die ausdrückliche Einwilligung des jeweiligen Kunden erforderlich.

Schließlich führt die DSK bezüglich der Übermittlung von Beschäftigtendaten aus, dass dies im Falle eines (Teil-) Betriebsübergangs nach § 613a BGB entweder auf Art. 6 Abs. 1 lit. b DSGVO oder im Fall von besonderen Kategorien personenbezogener Daten auf § 26 Abs. 3 BDSG zu stützen ist, wobei hier zusätzlich die besonderen rechtlichen Anforderungen des Betriebsübergangs gemäß § 613a BGB beachtet werden müssen. Eine Übermittlung solcher Daten ist auch hier im Stadium von Vertragsverhandlungen zwischen Veräußerer und Erwerber grundsätzlich unzulässig.

Verkauf von Kundendatenbanken

Werden lediglich die Kundendaten als einziges „Asset“ übermittelt, so ist hierfür regelmäßig eine Einwilligung der Kunden und Kundinnen einzuholen. Beim Austausch von Kundendaten zwischen Unternehmen mit weniger als 50 Beschäftigten und einem Jahresumsatz von höchstens 10 Mio. Euro kann eine Übermittlung ausschließlich der Postadressen auch im Wege der Widerspruchslösung, ausnahmsweise bei Ausbleibens des Widerspruchs gemäß Art. 6 Abs. 1 lit. b DSGVO erfolgen.

Fazit

Um die Übermittlung von personenbezogenen Daten im Rahmen eines Asset Deals datenschutzkonform zu vollziehen, müssen sich Unternehmen zunächst darüber bewusst werden in welchem Stadium des Unternehmenskaufs sie personenbezogene Daten übermitteln wollen. Anschließend ist zu schauen, in welcher Phase der Vertragsdurchführung sich die betroffenen Kunden mit dem Veräußerer befinden und welche Art von Daten zu welchen Zweck übermittelt werden sollen.

Drastische Preiserhöhungen bei VMware und Maßnahmen zur Gegenwehr

Auf den Punkt.

Für Kunden von VMware-Software gibt es Möglichkeiten, sich gegen die drastischen Preiserhöhungen für die Softwarepflege zu wehren. Dies ist u. a. abhängig von der eigenen Vertragssituation. Die Verträge sollten gerade im Hinblick auf die Vergütungsregelungen sehr genau geprüft werden. Manchmal kann es vorteilhaft sein, eine Ausschreibung am Markt vorzunehmen oder auf eine Virtualisierungssoftware eines anderen Herstellers umzusteigen.

Hintergrund

VMware Inc./VMware International Unlimited Company (nachfolgend „VMware“) hat die Kosten für die Softwarepflege drastisch erhöht. VMware ist ein Anbieter von Software-Lösungen im Bereich Cloud Computing sowie der Virtualisierung von Rechenzentrumsinfrastrukturen. Das Marktumfeld für die Virtualisierung von Rechenzentrumsinfrastrukturen ist überschaubar. Daher haben zahlreiche Unternehmen in den letzten Jahren mit VMware Lizenzverträge geschlossen, teils mit VMware-Vertriebspartnern, teils ohne.

Preiserhöhung und mögliche Maßnahmen

Von den Kunden wird eine drastische Preiserhöhung für die Softwarepflege verlangt und gleichzeitig wird ein Wechsel in ein Mietmodell offeriert. In beiden Fällen wird der Kunde zukünftig erheblich höhere Kosten haben als bislang. Wenn der Kunde solche Preiserhöhungen nicht akzeptiert, droht VMware in vielen Fällen offen mit einer Sperrung von Downloads. Diese Drohung dürfte aber in den meisten Fällen nicht verfangen. Denn häufig wird die VMware Software nicht in einem von VMware kontrollierten Rechenzentrum genutzt, sondern in einem vom Kunden ausgewählten Rechenzentrum. Auf dieses hat VMware keinen Zugriff. Ebenso hat VMware in der Regel keine Möglichkeit, die für den Download zur Verfügung gestellten Lizenz-Keys zu sperren. Das könnte sich in Zukunft natürlich ändern. Im Mietmodell bestehen diese Schutzmechanismen allerdings nicht.

Vor weiteren Maßnahmen muss jeder Kunde natürlich seine eigene Vertragssituation prüfen. Das Ergebnis kann durchaus sein, dass eine Preiserhöhung von VMware nicht oder noch nicht verlangt werden kann. Sofern eine erhöhte Pflegegebühr bereits bezahlt worden ist, kann diese in unberechtigten Fällen regelmäßig zurückverlangt werden. Eine weitere Maßnahme könnte eine Kündigung des bisherigen Softwarepflegevertrages mit VMware sein und die Durchführung einer Ausschreibung mit einem Neuabschluss eines Softwarepflegevertrages mit einem VMware Vertriebspartner. Dadurch werden regelmäßig erhebliche Kosten eingespart. Letztlich kann man sich am Markt auch nach Alternativen umsehen und mit einem neuen IT-Dienstleister Verträge schließen.

Unser Kommentar / Empfehlung

Jeder Kunde muss zunächst ein genaues Bild von der eigenen Vertragssituation haben und im Anschluss eine Zieldefinition für die eigene IT-Infrastruktur unter Berücksichtigung von technischen und finanziellen Abhängigkeiten erarbeiten. Dies bildet die Entscheidungsgrundlage für das weitere Vorgehen.

Die Novelle der eIDAS-Verordnung: Neue Vorgaben für digitale Signaturen und EUDI-Wallets

Mit der Novelle der eIDAS-Verordnung möchte die Europäische Union neue Maßstäbe für sichere digitale Identitäten und Transaktionen sowie einen einheitlichen digitalen Binnenmarkts setzen. Das Ziel ist klar: Sicherere und effizientere digitale Prozesse, die grenzüberschreitend funktionieren und eine breite Akzeptanz finden. Doch welche Neuerungen bringt die Verordnung mit sich?

Die eIDAS-Verordnung

Zu den elektronischen Vertrauensdiensten zählen beispielsweise elektronische Signaturen, elektronische Siegel, Zeitstempel, elektronische Zustelldienste und Website-Authentifizierung. Die Verordnung aus 2016 diente der Ermöglichung sicherer grenzüberschreitender Transaktionen sowie der Anerkennung elektronischer Vertrauensdienste über Ländergrenzen hinweg.

Da sich die „alte“ eIDAS-Verordnung jedoch auf den öffentlichen Sektor fokussierte und keine Pflicht zur Entwicklung nationaler Verfahren zur Schaffung digitaler Identitäten sowie zur Interoperabilität vorsah, blieben die erhofften Erfolge hinter den Erwartungen zurück. Während einige Mitgliedstaaten mit dem Aufbau flächendeckender digitaler Lösungen zur Identifizierung und zur digitalen Abwicklung von Verwaltungsdienstleistungen begonnen haben und sich über eine große Akzeptanz dieser Lösungen freuen können, haben andere Mitgliedstaaten bislang wenig Initiative gezeigt.

Kernelemente der eIDAS-Novelle

Mit der Novelle wird der Rahmen der eIDAS-Verordnung nun erweitert, insbesondere durch die Einführung der EU Digital Identity Wallets (EUDI-Wallets). In Deutschland arbeitet derzeit das Bundesministerium des Inneren und Heimat an der Umsetzung der europäischen Vorgaben für die EUDI-Wallets. Bei den EUDI-Wallets handelt es sich um digitale Anwendungen, die es Bürgerinnen und Bürgern ermöglichen, zentrale Dokumente wie Personalausweise, Führerscheine und andere Nachweise sicher auf ihrem Smartphone zu speichern. Die EUDI-Wallets sollen für alle Bürgerinnen und Bürger kostenfrei nutzbar sein, ohne dass eine Nutzungspflicht vorgesehen ist.

Die EUDI-Wallets bieten vielseitige Nutzungsmöglichkeiten, z. B. für:

- öffentliche Dienstleistungen;
- die Eröffnungen von Bankkonten;
- die Abgabe von Steuererklärungen;
- die grenzüberschreitende Bewerbung an einer Universität;
- Altersnachweise oder Hotelbuchungen.

Unternehmen in bestimmten Branchen wie Energie, Gesundheit und Telekommunikation werden verpflichtet, die EUDI-Wallets unter bestimmten Voraussetzungen zu akzeptieren, wenn eine starke Nutzerauthentifizierung für die Online-Identifizierung erforderlich ist. Dies soll die Verbreitung und Akzeptanz der EUDI-Wallets fördern und langfristig die digitale Souveränität Europas stärken.

Chancen und Herausforderungen

Die Novelle bietet zahlreiche Chancen. So ermöglicht sie unter anderem die Erleichterung einer Vielzahl von Prozessen im öffentlichen und privaten Bereich. Die EUDI-Wallets sollen vor allem Authentifizierungen und Identitätsnachweise sicherer machen und dabei zugleich vereinfachen. Ein Use Case ist beispielsweise die digitale Abwicklung des Abschlusses eines Darlehensvertrags, bei dem aus der EUDI-Wallet heraus alle wichtigen Unterlagen an die Bank übermittelt werden und der Vertrag schlussendlich digital signiert wird.

Ein weiterer Vorteil ist die mit der EUDI-Wallet verbundene Datensparsamkeit. Nutzerinnen und Nutzer sollen kontrollieren können, welche Daten sie abhängig vom konkreten Bedarf des Datenempfängers preisgeben. Ist es beispielsweise zwingend erforderlich, eine Altersverifikation durchzuführen, soll es möglich sein, nur die Tatsache eines bestimmten Mindestalters zu übermitteln, dabei aber auf die Übermittlung weiterer Daten wie das Geburtsdatum und die Adresse zu verzichten.

Zudem spielt Interoperabilität eine zentrale Rolle bei der Ausgestaltung der EUDI-Wallets. Unterschiedliche nationale Systeme sollen besser miteinander vernetzt werden, wodurch grenzüberschreitende Anwendungen nahtloser funktionieren und nationale EUDI-Wallets idealerweise im gesamten EWR-Raum einsetzbar sein sollen.

Trotz der mit der Novelle verbundenen Chancen, bestehen auch diverse Herausforderungen.

Im Hinblick auf die elementaren Themen Datenschutz und Sicherheit befürchten Kritiker, dass die EUDI-Wallets mit neuen Risiken für sensible Daten einhergehen. Ein Faktor könnte beispielsweise Phishing sein, welches insbesondere unbedarfte Nutzerinnen und Nutzer treffen könnte.

Darüber hinaus wird speziell für Deutschland das vergleichsweise langsame Voranschreiten der Digitalisierung als Hürde betrachtet. Hier ist derzeit fraglich, ob die Infrastruktur für den Einsatz der EUDI-Wallet überhaupt zur Verfügung steht und ob notwendige Synergien mit anderen Gesetzen vollumfänglich hergestellt werden.

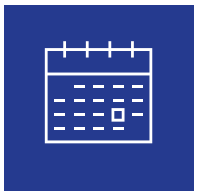
Zeitplan und Umsetzung

Bis Ende 2026 sollen die EUDI-Wallets in allen Mitgliedstaaten zur Verfügung stehen und ab 2027 allen Bürgerinnen und Bürgern zur Nutzung angeboten werden. In Deutschland findet aktuell ein Wettbewerb für die Entwicklung der deutschen EUDI-Wallet statt, dessen Schirmherrin die Bundesagentur für Sprunginnovationen ist. Dieser dient der Entwicklung eines „*Prototypen für eine vertrauenswürdige, nutzerfreundliche und universell einsetzbare European Digital Identity Wallet für Nutzer:innen in der Bundesrepublik Deutschland*“.

Fazit

Die Novelle der eIDAS-Verordnung ist ein ambitionierter Schritt in Richtung einer europäischen digitalen Identität. Sie könnte ein echter „Gamechanger“ für die Digitalisierung werden – vorausgesetzt, die rechtlichen und tatsächlichen Rahmenbedingungen werden im gesamten EWR und insbesondere in Deutschland geschaffen. Unternehmen, die frühzeitig auf die Neuerungen reagieren, haben die Chance, sich als Vorreiter in der digitalen Transformation zu positionieren. Gleichzeitig sollten sich Unternehmen und öffentliche Institutionen frühzeitig auf die neuen Anforderungen vorbereiten.

Veranstaltungen, Veröffentlichungen und Blog



Eine Übersicht mit unseren Veranstaltungen finden Sie hier.

Eine Liste unserer aktuellen Veröffentlichungen finden Sie hier.

Unseren Blog finden Sie hier.

Impressum

Verleger: Luther Rechtsanwaltsgesellschaft mbH
Anna-Schneider-Steig 22, 50678 Köln, Telefon +49 221 9937 0
Telefax +49 221 9937 110, contact@luther-lawfirm.com
V.i.S.d.P.: Dr. Michael Rath, Partner
Luther Rechtsanwaltsgesellschaft mbH
Anna-Schneider-Steig 22, 50678 Köln, Telefon +49 221 9937 25795
michael.rath@luther-lawfirm.com

Bildnachweise:
AdobeStock/stnazkul: Seite 1; AdobeStock/gopixa: Seite 4; AdobeStock/www.freund-foto.de: Seite 6; AdobeStock/denisismagilov: Seite 9; iStock/Kiattisak: Seite 11;AdobeStock/Joshua Montgomery: Seite 13; AdobeStock/Grecaud Paul: Seite 14

Luther.

Bangkok, Berlin, Brüssel, Delhi-Gurugram, Düsseldorf, Essen, Frankfurt a. M., Hamburg, Hannover, Ho-Chi-Minh-Stadt, Jakarta, Köln, Kuala Lumpur, Leipzig, London, Luxemburg, München, Shanghai, Singapur, Stuttgart, Yangon

Weitere Informationen finden Sie unter
www.luther-lawfirm.com
www.luther-services.com

unyer GLOBAL ADVISORS