Datenschutz International

Determann

3. Auflage 2026
ISBN 978-3-406-84861-2
C.H.BECK

das Alter der Nutzer festzustellen, zB durch Überprüfung von Ausweisdokumenten, Verifizierung durch zusätzliche Datenpunkte (zB Zahlungssysteme oder Kommunikation per E-Mail- oder Telefonnummern) oder Altersschätzung mithilfe biometrischer Scans und Datenbankabfragen. Durch die Einführung solcher Maßnahmen erheben Unternehmen zusätzliche sensible Datenkategorien, die in einigen Jurisdiktionen zusätzliche Verpflichtungen und Risiken nach Datenschutzgesetzen und Gesetzen zur Gewährleistung der freien, anonymen Meinungsäußerung und Internetnutzung nach sich ziehen.

- *Eltern die Kontrolle geben:* Viele Jurisdiktionen fördern oder verlangen die Bereitstellung von Kindersicherungen für Dienste, die sich an Kinder richten. Mit Tools (Programmen, Hilfsmitteln, Instrumenten) und technischen Funktionen können Eltern kontrollieren, auf welche Dienste und Inhalte ihre Kinder zugreifen, wann und wie lange Kinder auf Dienste zugreifen können und welche Daten von ihnen erhoben werden. Nach kalifornischem Recht müssen Unternehmen jedoch Kindern ein deutliches Signal geben, wenn sie überwacht oder verfolgt werden, wenn der Online-Dienst, das Produkt oder die Funktion es Eltern ermöglicht, auf die Aktivitäten oder Standorte ihrer Kinder zuzugreifen.
- *Durchführung von Jugendfolgenabschätzungen:* Unternehmen sollten individuelle Folgenabschätzungen durchführen, die auf ihre besonderen Umstände zugeschnitten sind, um Fakten darüber zu sammeln, welche Arten von personenbezogenen Daten sie über Minderjährige erheben, wie sie die Daten verwenden, gegenüber wem sie die Daten offenlegen und zu welchen Zwecken sie diese verwenden und offenlegen; Unternehmen sollten die geltenden gesetzlichen Anforderungen auf der Grundlage ihrer Interaktion mit Minderjährigen und der Erfahrungen dieser Minderjährigen mit ihren Diensten bewerten; Unternehmen sollten die Schäden ermitteln, denen Minderjährige durch ihre Dienste ausgesetzt sein können; und Unternehmen sollten einen Plan zur Umsetzung von Schutzmaßnahmen entwickeln, um Minderjährige vor diesen Schäden zu schützen. Wenn Rechtsanwälte die Bewertungen zum Zwecke der Rechtsberatung leiten, können Unternehmen Entwürfe und Mitteilungen im Zusammenhang mit Risikobewertungen möglicherweise durch das Anwaltsgeheimnis schützen.
- *„Datenschutz" als Standardeinstellung festlegen:* Wenn Unternehmen Optionen für Opt-In, Opt-Out (insbes. Widerspruch, Ablehnung, Abmeldung, Abwählbarkeit) und technische Einstellungen anbieten, sollten sie für Minderjährige *„Opt-Out"* und *„hohe Datenschutzeinstellungen"* als Standardeinstellung in Betracht ziehen. Unternehmen sollten besonders auf gesetzliche Beschränkungen hinsichtlich der Verwendung personenbezogener Daten von Minderjährigen für gezielte oder verhaltensbezogene Werbung, die Erstellung von Profilen zur Ableitung von Merkmalen über sie, die Verfolgung ihres genauen Standorts oder das Streamen ihrer Echtzeit-Videoaufnahmen oder verbalen Äußerungen achten. Durch technische Einstellungen können Unternehmen Minderjährige davon abhalten oder daran hindern, personenbezogene Daten anderen zugänglich zu machen, und unterschiedliche Erfahrungen mit unterschiedlichen Funktionen für verschiedene Altersgruppen gestalten, um minderjährigenspezifische Risiken wie Sucht, übermäßige Käufe, unerwünschte Kontakte und den Zugriff auf oder die Verbreitung von altersunangemessenen Inhalten zu mindern.
- *Verständliche Kommunikation:* Unternehmen sollten ihre Datenschutzerklärungen und rechtlichen Bestimmungen regelmäßig überprüfen und aktualisieren, um sicherzustellen, dass junge Menschen sie verstehen können, und sie sollten Datenschutzerklärungen zum jeweiligen Zeitpunkt bereitstellen, die genau erklären, was eine Funktion tut, wenn der Nutzer mit dieser Funktion interagiert. Rechtliche Bestimmungen, die junge Nutzer vor unangemessenen Situationen schützen sollen, sollten

klar formuliert sein, und Unternehmen sollten Mechanismen einrichten, um sicherzustellen, dass sie diese Bestimmungen gegenüber denjenigen durchsetzen, die gegen sie verstoßen.

- *Minimierung der Datenerhebung und -speicherung:* Unternehmen könnten beschließen, weniger Daten von Minderjährigen als von Erwachsenen und nur die Mindestmenge an personenbezogenen Daten zu erheben, die erforderlich ist, um jungen Nutzern die Kernfunktionalität ihrer Dienste bereitzustellen. Dies kann bedeuten:
  - bei der Kontoerstellung nur die notwendigen Informationen abzufragen. Beispielsweise benötigt eine Spiel-App möglicherweise nur einen Benutzernamen und ein Passwort und nicht den vollständigen Namen, die Adresse oder Angaben zur Schule.
  - Standortdaten vom Gerät eines Minderjährigen weder zu erheben noch zu speichern, es sei denn, dies ist für den Dienst unbedingt erforderlich. Beispielsweise benötigen Anbieter von Online-Karten oder Mitfahrdiensten Standortinformationen, eine Bildungs-App hingegen nicht.
  - die Verwendung von Cookies oder anderen Tracking-Technologien zu beschränken.
  - die Datenspeicherung regelmäßig zu überprüfen und unnötige Daten regelmäßig zu löschen.
  - De-Identifikations- und Aggregationstechniken auf die personenbezogenen Daten von Minderjährigen anzuwenden, bevor diese für Nebenzwecke wie Forschung und Produktentwicklung verwendet werden.

L. Lauschen – Fernmeldegeheimnis und Abhören

52 Abhören, Mithören, Anrufaufzeichnung, E-Mail-Filterung und ähnliche Formen der Überwachung von (Live-)Kommunikation sind besonders schwere Eingriffe in die Privatsphäre und Kommunikationsfreiheit. Daher verbieten viele Jurisdiktionen das Abhören, Aufzeichnen und Überwachen von Anrufen und anderen Kommunikationsformen, sofern nicht alle Beteiligten einwilligen. Traditionell verboten Gesetze zunächst die Überwachung von analogen Telefongesprächen und Briefen. Teilweise wurde angezweifelt, ob E-Mail-Korrespondenz von den Telekommunikationsüberwachungsgesetzen erfasst ist, da E-Mails iRd Übermittlungsprozesses gespeichert werden und somit in gewisser Weise eher der Aufzeichnung von Sprachnachrichten ähneln als einem analogen Telefongespräch. Viele Länder haben die gesetzliche Definition jedoch geändert, um alle verschiedenen Formen der elektronischen Kommunikation zu erfassen, einschließlich Sofortnachrichten, Online-Chats, Textnachrichten (SMS), E-Mail und Website-Zugriffe (einschließlich über Cookies und ähnliche Technologien).

Unternehmen überwachen die Kommunikation aus verschiedenen Gründen, unter anderem zur Qualitätskontrolle (Aufzeichnung von Verkaufsgesprächen), zum Netzwerkschutz (Spam- und Virusfilter), zur Sicherung ihrer Grundstücke und Gebäude (Videoüberwachung), Werbung (mit Cookies und Pixeln zur Analyse von Interessen) und Überwachung des Mitarbeiterverhaltens (Aufzeichnung der Tastenbetätigung, Speicherung von Screenshots, E-Mail- und Webfilter). Unternehmen können relativ leicht die Einwilligung ihrer Mitarbeiter hierzu einholen. In einigen Jurisdiktionen (vor allem in Europa) müssen sie sich um die Gültigkeit der Einwilligung der Mitarbeiter kümmern, in anderen Jurisdiktionen gibt es jedoch weniger Hindernisse. Die Einholung der Einwilligung von Dritten ist jedoch viel schwieriger. Bei eingehenden Anrufen können Unternehmen Ansagen abspielen, die die

Anrufer darüber informieren, dass *„Anrufe zur Qualitätskontrolle aufgezeichnet und überwacht werden"*. Bei ausgehenden Anrufen jedoch würden viele der Angerufenen wahrscheinlich gleich wieder auflegen, wenn sie als erstes mit einer solchen Ansage begrüßt werden würden. Daher können Unternehmen entweder ganz auf die Aufzeichnung ausgehender Anrufe verzichten oder die Aufzeichnung erst nach Einholung der Einwilligung während des Anrufs zu einem geeigneten Zeitpunkt aktivieren. Auf Websites können Unternehmen *„Einwilligungsbanner"* platzieren, die Besucher über die Platzierung von Cookies und die Nachverfolgung des Website-Zugriffs durch Dritte informieren, müssen jedoch gemäß dem California Consumer Privacy Act (CCPA) innerhalb von 12 Monaten nach Erhalt eines Opt-Out-Antrags davon absehen, Kalifornier um ihre Einwilligung zu bitten.

Noch viel komplizierter ist es, die Einwilligung von externen Parteien einzuholen, die über E-Mail, Sofortnachrichten oder SMS kommunizieren. Die meisten Unternehmen verlassen sich diesbezüglich auf allgemeine Informationen, die automatisch in ausgehende Nachrichten eingefügt werden. Diese Informationen kommen jedoch technisch gesehen zu spät, da die Nachricht gefiltert wird, bevor der Empfänger die Information über die Aufzeichnung erhält. In der Praxis scheinen sich die meisten Menschen und Aufsichtsbehörden nicht um solche technischen Filter zu kümmern, und die Technologien sind so weit verbreitet, dass das Risiko für ein einzelnes Unternehmen relativ gering erscheint. Dennoch haben Anwaltskanzleien der Kläger in den USA in großem Umfang Ansprüche nach den Telekommunikationsüberwachungsgesetzen geltend gemacht, und viele Unternehmen einigen sich auf Vergleichszahlungen in Höhe des Belästigungswerts.

M. Mitarbeiter

Arbeitgeber erheben Daten von Bewerbern, Mitarbeitern und ehemaligen Mitarbeitern in verschiedenen Systemen und für unterschiedliche Zwecke. In diesem Zusammenhang müssen Arbeitgeber nicht nur datenschutzrechtliche, sondern auch arbeitsrechtliche Vorschriften befolgen, welche in den einzelnen Ländern – auch innerhalb der EU – sehr unterschiedlich gestaltet sind. **53**

Einstellung. Arbeitgeber sollten sorgfältig eine Liste mit Fragen erstellen, die sie Bewerbern stellen dürfen, und solchen, die sie nicht stellen dürfen (zB auf Bewerbungsinternetseiten oder in einem Bewerbungsgespräch), um zu vermeiden, dass sie Informationen erheben, die sie gemäß den Antidiskriminierungsgesetzen nicht berücksichtigen dürfen. In einigen Jurisdiktionen müssen Lebensläufe für einen bestimmten Zeitraum aufbewahrt werden, während es in anderen Jurisdiktionen üblich oder sogar gesetzlich vorgeschrieben ist, die Bewerbungsunterlagen an nicht eingestellte Bewerber zurückzusenden. Nach der DS-GVO und anderen Gesetzen, die automatisierte Entscheidungen einschränken, müssen Arbeitgeber möglicherweise den Einsatz künstlicher Intelligenz für die Überprüfung von Lebensläufen einschränken, da sie keine freiwillige Einwilligung der Bewerber einholen können (aufgrund eines wahrgenommenen Ungleichgewichts der Verhandlungsmacht und damit einer vermuteten Nötigung). Nach Ansicht des EuGH kann bereits die vorbereitende Bewertung eine automatisierte Entscheidungsfindung darstellen, die die Einwilligung der betroffenen Person erfordert. Arbeitgebern sollte es gestattet sein, deterministische Filtertools einzusetzen (zB die Ablehnung von Bewerbungen, die nicht den gesetzlich zulässigen binären Bedingungen entsprechen, wie erforderliche Berufsabschlüsse, Führerscheine oder eine Mindestanzahl von Jahren Berufserfahrung), wenn ein Mensch die Entscheidung trifft, solche Bedingungen zu verlangen. Außerdem könnten Arbeitgeber ein zusätzliches Überprüfungsverfahren einrichten, um Kandidaten durch künstliche Intelligenzsysteme in die engere Wahl zu nehmen, sofern Menschen parallel dazu dieselben Lebensläufe überprüfen und die endgültige Entscheidung nach Überprüfung der aus dem automatisierten und dem menschlichen Überprüfungsprozess resultierenden Auswahllisten treffen. Gemäß einer Ver- **54**

ordnung in New York City müssen Arbeitgeber automatisierte Entscheidungstools für die Einstellung jährlich auf das Risiko illegaler Voreingenommenheit überprüfen.

55 *Hintergrundüberprüfung.* Anbieter von Hintergrundüberprüfungen und die Verwendung von Hintergrundüberprüfungen im Beschäftigungskontext unterliegen in den USA strengen Vorschriften, die im Fair Credit Reporting Act und in zahlreichen staatlichen Gesetzen geregelt sind. Einige US-Bundesstaaten beschränken die Abfrage von Kredit- und Fahrtenverläufen, selbst wenn der Mitarbeiter seine Einwilligung gegeben hat. Gemäß der DS-GVO darf die Verarbeitung personenbezogener Daten im Zusammenhang mit strafrechtlichen Verurteilungen und Straftaten nur unter der Kontrolle einer Behörde oder wenn die Verarbeitung gesetzlich zulässig ist, erfolgen, und ein umfassendes Register strafrechtlicher Verurteilungen darf nur unter der Kontrolle einer Behörde geführt werden. Aufgrund dieser gesetzlichen Beschränkungen und auch aufgrund der Nichtverfügbarkeit oder Unzuverlässigkeit relevanter Daten halten Arbeitgeber Hintergrundüberprüfungen in vielen Ländern für praktisch sinnlos oder sogar illegal. Arbeitgebern wird dringend empfohlen, sich sorgfältig mit Anbietern von Hintergrundüberprüfungen über die Quellen und die Rechtmäßigkeit ihrer Berichte zu beraten.

56 *Personalakten.* Viele Länder regeln, was Eingang in die Personalakte finden darf und muss (minimaler und maximaler Inhalt), und berechtigen die Mitarbeiter dazu, auf die Informationen zuzugreifen und die Berichtigung und Löschung falscher oder veralteter Informationen zu verlangen. Des Weiteren dürfen Informationen bezüglich Straftaten und verhängten Strafen entweder überhaupt nicht aufgenommen werden oder müssen jedenfalls nach gewisser Zeit wieder gelöscht werden. Arbeitgeber sind sowohl nach dem Arbeitsvertrag als auch nach verschiedenen Steuer-, Sozialversicherungs- und Arbeitsgesetzen gesetzlich dazu verpflichtet, personenbezogene Daten zu erheben und zu verarbeiten. Wenn Arbeitgeber jedoch Daten über den gesetzlich vorgeschriebenen Rahmen hinaus verarbeiten möchten, müssen Datenschutzvorschriften beachtet werden, insbes. hinsichtlich globaler Personalinformationssysteme (HRIS) innerhalb multinationaler Konzerne, Hinweisgeber-Meldestellen, Mitarbeiterüberwachung und internen Ermittlungen.

57 *Einwilligung des Mitarbeiters.* Arbeitgeber sollten es sich reiflich überlegen, bevor sie Mitarbeiter um Einwilligungen ersuchen. Durch die Einholung der Einwilligung wecken Arbeitgeber gewisse Erwartungen oder schaffen eventuell vertragliche Ansprüche dahingehend, dass künftige Änderungen auch der Einwilligung des Mitarbeiters bedürfen. In den meisten EWR-Mitgliedstaaten wird die Einwilligung der Mitarbeiter als erzwungen und daher als ungültig angesehen, es sei denn, die Einwilligung bezieht sich auf tatsächlich freiwillige Programme, zB auf Mitarbeiterbeteiligungsprogramme einer US-Muttergesellschaft, Angaben von Essenswünschen bei einer Fluggesellschaft iRd Vorbereitung von Geschäftsreisen oder auf Angaben zur Beziehung zu einem Notfallkontakt. Außerdem bitten seit der COVID-19-Pandemie viele Mitarbeiter ihre Arbeitgeber um die Erlaubnis, vorübergehend in anderen Ländern arbeiten zu dürfen. In diesem Fall sollten Arbeitgeber in der Lage sein, die freiwillige Einwilligung der Mitarbeiter zur fortgesetzten Datenverarbeitung und Computerüberwachung in Übereinstimmung mit den Gesetzen und Richtlinien des Landes einzuholen, in dem der Arbeitgeber seinen Sitz hat. Selbst wenn die Einwilligung nicht als erzwungen vermutet wird, ist zu bedenken, dass der Mitarbeiter berechtigt sein kann, die Einwilligung zu verweigern oder zu widerrufen. Das kann den Arbeitgeber in eine schwierige Situation bringen, wenn es um Programme geht, die die Beteiligung aller Mitarbeiter voraussetzen. Deshalb holen die meisten Arbeitgeber Einwilligungen nur dort ein, wo dies vorgeschrieben und leicht möglich ist, oder wenn es um Programme geht, die Mitarbeiter wirklich freiwillig annehmen oder ablehnen können.

58 *Globales HRIS.* Personalinformationssysteme (*„human resource information systems", „HRIS"*), auch als globale *„Mitarbeiterdatenbanken" („global employee databases")* bezeichnet, werden häufig von multinationalen Unternehmen zu Planungszwecken in Bezug auf den Personalbedarf und die berufliche Weiterentwicklung sowie zur Unterstützung der grenzüberschreitenden Zusammenarbeit eingesetzt. Im Interesse der Wirtschaftlichkeit, der Da-

tenintegrität und -sicherheit verwenden multinationale Konzerne häufig globale Mitarbeiterdatenbanken statt lokaler Systeme in jedem einzelnen Land. Die Einführung von HRIS geht einher mit einer beträchtlichen Erhebung von Daten, der Übermittlung personenbezogener Daten an andere juristische Personen innerhalb des Konzerns und der grenzüberschreitenden Übermittlung personenbezogener Daten in andere Länder. Arbeitgeber in einem multinationalen Konzern, die zu einem HRIS beitragen, müssen die drei bereits in → § 6 dieses Handbuchs erörterten Hürden nehmen:

Hürde 1. Die juristische Person, die als Arbeitgeber auftritt, muss die Erhebung von Daten iRd HRIS rechtfertigen. Eine juristische Person, die als Arbeitgeber auftritt, kann diese Hürde idR relativ leicht überwinden, da der Arbeitgeber die meisten der erforderlichen Datenkategorien bereits aus Gründen der Verwaltung des Arbeitsverhältnisses erheben kann oder muss (zB Lohnabrechnungen, Steuerabzug, Sozialleistungen und Bewertungen). Wenn sich die Muttergesellschaft in einem anderen Land befindet, ist es möglich, dass sie die Angabe von Datenfeldern verlangt, die in anderen Ländern rechtlich nicht erhoben werden dürfen. Beispielsweise erheben US-Unternehmen routinemäßig Daten zur ethnischen Zugehörigkeit, und deutsche Unternehmen müssen iRd Lohn- und Gehaltsabrechnung Kirchensteuern einbehalten, aber Daten zu Rasse und Religion dürfen in anderen Ländern idR nicht erhoben werden. Deshalb müssen Unternehmen vor der Befüllung des HRIS prüfen, welche Datenkategorien in den einzelnen Jurisdiktionen rechtmäßig erhoben werden dürfen.

Hürde 2. Der Arbeitgeber muss die Weitergabe von Daten an andere Unternehmen des Konzerns, die ebenfalls Zugriff auf das HRIS haben können, rechtfertigen. In manchen Ländern kann der Arbeitgeber ohne Schwierigkeiten die Einwilligung der Mitarbeiter für diese Art der Datenübermittlung einholen. Jedoch wird in den meisten EWR-Mitgliedstaaten eine Einwilligung des Mitarbeiters als erzwungen und daher als ungültig angesehen. Viele multinationale Arbeitgeber schrecken deshalb davor zurück, die Einwilligung der Mitarbeiter einzuholen, wo dies nicht möglich oder nicht zwingend erforderlich ist. Stattdessen versuchen sie, die Datenübermittlung mit organisatorischen Notwendigkeiten oder aufgrund einer Ausnahmeregelung wegen berechtigten Interesses zu rechtfertigen. Beispielsweise halten multinationale Unternehmen den internationalen Datenaustausch aufgrund einer Reihe von Überlegungen für notwendig:

- Alle Unternehmen des Konzerns brauchen zumindest Basisinformationen von ihren Mitarbeitern im Hinblick auf Namen, Berufsbezeichnung, Qualifikation und Kontaktdetails, um globale Zusammenarbeit, Kommunikation und Teamarbeit innerhalb des globalen Konzerns zu ermöglichen.
- Die Muttergesellschaft des Konzerns und, je nach Bedarf, Vorgesetzte in anderen verbundenen Unternehmen benötigen Leistungs- und Gehaltsinformationen für die weltweite Personalplanung und -verwaltung, einschließlich, aber nicht beschränkt auf die Sicherstellung einer angemessenen Personalausstattung und die Bewertung der Eignung von Mitarbeitern für eine bestimmte Stelle, Beförderungen, Entsendungen, Buchhaltung und die gegenseitige Abrechnung von Gehaltskosten zwischen den Unternehmen im Konzern.
- Wenn und soweit die Muttergesellschaft Leistungen oder Vorteile direkt für Mitarbeiter von Tochtergesellschaften erbringt (zB Mitarbeiterbeteiligungsprogramme), benötigt die Muttergesellschaft zusätzliche Informationen, um die jeweiligen Vorhaben und Programme anzubieten und verwalten zu können.
- Die Muttergesellschaft ist für die Einhaltung der gesetzlichen Vorschriften durch ihre Tochtergesellschaften verantwortlich und hat demnach auch ein berechtigtes Interesse daran, wie zB die Einhaltung von internationalen Embargos, Anti-Korruptionsgesetzen, Zollbestimmungen und kartellrechtlichen Vorschriften.

Die Unternehmen müssen sehr sorgfältig prüfen, welche Datenkategorien sie für diese Zwecke in rechtmäßiger Weise heranziehen dürfen – wahrscheinlich sind dies nicht alle, die

der Arbeitgeber erheben kann oder muss. Soweit bestimmte Datenkategorien von anderen Unternehmen des Konzerns nicht benötigt werden, kann es dennoch möglich sein, diese Daten in einem globalen HRIS zu speichern, das von einem Unternehmen gehostet wird, das als Datenverarbeitungsdienstleister für die anderen Unternehmen fungiert, solange nur das Arbeitgeberunternehmen für seine eigenen Zwecke auf bestimmte Datenfelder zugreifen kann.

Hürde 3. Um Beschränkungen für grenzüberschreitende Datenübermittlungen zu überwinden, müssen Unternehmen bestimmte Datenschutzmaßnahmen ergreifen und implementieren, um die Gesetze in Europa und einer Reihe anderer Rechtsordnungen einzuhalten (→ § 6). Manche Rechtsordnungen beschränken internationale Datentransfers nicht besonders oder erlauben Datenübermittlungen auf der Basis einer Einwilligung des Mitarbeiters. Datenschutzbehörden in Europa gehen jedoch davon aus, dass die Einwilligung der Mitarbeiter erzwungen und ungültig ist, und verlangen von den Arbeitgebern, EU-Standardvertragsklauseln abzuschließen und andere Maßnahmen zu ergreifen und zu implementieren, um ein angemessenes Datenschutzniveau sicherzustellen.

59 *Überwachungstechnologien.* Arbeitgeber sind dazu verpflichtet, in angemessenem Aufwand sicherzustellen, dass ihre Mitarbeiter geltende Gesetze einhalten, ihre beruflichen Pflichten erfüllen sowie die Interessen, das geistige Eigentum sowie die Daten des Unternehmens zu schützen. Außerdem müssen Arbeitgeber ihre Mitarbeiter vor Belästigung, feindseligen Arbeitsumgebungen und Sicherheitsbedrohungen schützen. Daher setzen viele Unternehmen Technologien ein, um die Netzwerksicherheit zu schützen und um Diebstahl von geistigem Eigentum des Unternehmens, exzessive private Computernutzung und illegales oder unangemessenes Mitarbeiterverhalten zu aufzudecken und zu verhindern. Solche Technologien können auch dazu verwendet werden, um gesetzliche, behördliche oder branchenbezogene Anforderungen zu erfüllen, zB Börsenvorschriften, die die Aufbewahrung der Korrespondenz mit der Öffentlichkeit vorschreiben, und Datensicherheitsanforderungen, die sich aus Datenschutzgesetzen ergeben. In der EU müssen Arbeitgeber objektive, zuverlässige und zugängliche Systeme einrichten, um die tägliche Arbeitszeit jedes Mitarbeiters zu messen.

60 Netzwerksicherheitstools nach dem Stand der Technik bieten die Möglichkeit, verschiedene Aspekte der Nutzung von Firmencomputern, Smartphones, Netzwerken und Systemen durch einzelne Personen zu überwachen. Solche Tools können die Adressen besuchter Websites sowie den tatsächlichen Inhalt gesendeter und empfangener Daten protokollieren, einschließlich der vom Benutzer an Websites übermittelten Formulardaten und Inhalte, wie E-Mails oder Chatprotokolle zwischen Mitarbeitern und Dritten. Einige Arbeitgeber setzen auch Sicherheitskameras (in Büroräumen oder Laptops) ein, verfolgen Tastenanschläge und überwachen den Standort ihrer Mitarbeiter mit Peilsendern (auch RFID Tags genannt, *„radio-frequency identification"*) in Fahrzeugen und Geräten.

Derartige Überwachungstechnologien können sehr effektiv und daher erforderlich sein, um die Einhaltung von Datenschutz- und Sicherheitsgesetzen zu unterstützen. Allerdings können solche Technologien auch stark in die Privatsphäre von Mitarbeitern und Personen außerhalb des Unternehmens, mit denen Mitarbeiter kommunizieren, eingreifen. Daher müssen Unternehmen eine Reihe von Einschränkungen und Beschränkungen hinsichtlich der Verwendung von Überwachungstechnologien beachten.

61 In den meisten EWR-Mitgliedstaaten ist die systematische Überwachung von Mitarbeitern durch Technologien weitgehend unzulässig. Es darf nur in Fällen von berechtigtem Einzelverdacht ermittelt werden. In Bezug auf Mitarbeiter in Kalifornien müssen Arbeitgeber spezifische *„Erhebungshinweise" („at collection notices")* ausgeben und die Anforderungen zur Datenminimierung gemäß dem California Consumer Privacy Act (CCPA) einhalten, der seit Ablauf der Übergangsfristen im Jahr 2023 auch im Beschäftigungskontext gilt. Ansonsten beschränken die meisten Datenschutzgesetze in den USA die Überwachung nur auf Fälle, in denen die Überwachten eine angemessene Erwartung an den Datenschutz bzw. die Privatsphäre haben *(„reasonable privacy expectations"),* dh eine tatsächliche Erwartung an Daten-

schutz/auf Privatsphäre, die die Gerichte unter den gegebenen Umständen für angemessen halten. Arbeitgeber können die tatsächliche Erwartung ihrer Mitarbeiter auf Privatsphäre durch auffällige, detaillierte und weit gefasste Informationen zerstören. Für Arbeitgeber kann es schwieriger sein, die tatsächlichen Erwartungen und Rechte auf Privatsphäre derjenigen zu zerstören, mit denen ihre Mitarbeiter kommunizieren (Kunden, Lieferanten, persönliche Kontakte), aber Arbeitgeber können Informationen zu ausgehenden E-Mails, Websites, Verträgen und Callcenter-Skripten hinzufügen. Außerdem können Arbeitgeber ihre Mitarbeiter vertraglich verpflichten, ihre Kontakte zu benachrichtigen. Es ist wichtig, dass Arbeitgeber die Informationen auf dem neuesten Stand der tatsächlich eingesetzten Technologien halten, da Gerichte andernfalls feststellen könnten, dass Mitarbeiter angemessene Erwartungen an die Privatsphäre entwickelt haben, und daher eine eingreifende Überwachung verbieten könnten. Darüber hinaus sollten Arbeitgeber die gesetzlichen Anforderungen des jeweiligen Bundesstaates in Bezug auf besonders eingreifende Formen der Überwachung sorgfältig prüfen, wie zB Kameras in Umkleideräumen (die bspw. in Kalifornien ausdrücklich verboten sind), Standortverfolgung über RFID-Tags und ähnliche Ortungstechnologien (ebenfalls in Kalifornien verboten, wobei eine Ausnahmeregelung für bestimmte Formen der Fahrzeugortung besteht) sowie das Abhören von Live-Kommunikation (was in einer Reihe von US-Bundesstaaten die Einwilligung aller Beteiligten erfordert), wie zB einfache Telefonanrufe, Textnachrichten, Sofortnachrichten, Webzugriff und E-Mail-Korrespondenz. Selbst das Filtern von E-Mails zum Schutz vor Spam und Viren könnte eine Überwachung darstellen, kann jedoch unter gesetzlichen Ausnahmeregelungen oder wenn einzelne Mitarbeiter das Filtern für ihre eigenen Konten aktivieren und kontrollieren, gerechtfertigt sein. Die vorgesehenen Empfänger können nach den meisten Gesetzen idR nach eigenem Ermessen Nachrichten filtern oder löschen, obwohl für die Aufzeichnung von Sprachkommunikation ohne die Einwilligung aller Beteiligten Einschränkungen gelten.

62 In Europa und einigen Ländern außerhalb Europas sind Mitarbeiter und andere betroffene Personen vor Überwachung und anderen Eingriffen in ihre Privatsphäre geschützt, unabhängig davon, ob eine angemessene Erwartung an den Datenschutz/auf Privatsphäre besteht. Die meisten Arbeitsgesetze außerhalb der USA verlangen von Arbeitgebern, dass sie mit ihren Mitarbeitern eine ausdrückliche Vereinbarung über Änderungen der Arbeitsbedingungen, einschließlich der Einführung von Überwachungstechnologien, treffen. Nicht zustimmende Mitarbeiter können in einigen Rechtsordnungen sanktioniert oder entlassen werden, in Europa jedoch idR nicht. Darüber hinaus wird in den meisten europäischen Ländern davon ausgegangen, dass die Einwilligung der Mitarbeiter erzwungen und unwirksam ist. Unternehmen in Europa können die Durchsuchung von E-Mails in Fällen des begründeten Verdachts hinsichtlich eines Fehlverhaltens rechtfertigen. Die Anwendung von Überwachungstechnologien ohne Vorliegen eines konkreten Verdachts ist jedoch nur schwer zu rechtfertigen. Der Einsatz von Überwachungstechnologien erfordert ggf. eine Vereinbarung mit dem Betriebsrat, falls vorhanden, und ggf. eine vorherige Genehmigung der Datenschutzbehörde, des Arbeitsgerichts und anderer Behörden. Deshalb wenden viele Unternehmen systematische Überwachungstechnologien nicht auf ihre europäischen Mitarbeiter an, außer im Fall des begründeten Verdachts, der sich auf weitere Umstände stützt (zB explizite Beschwerden).

63 Bei einem global verwalteten System kann es Schwierigkeiten bereiten, die Überwachung für bestimmte Länder oder Regionen zu deaktivieren. Einige Unternehmen versuchen, vertragliche Ansätze zu nutzen und ihre technischen Mitarbeiter zu verpflichten, bestimmte Überwachungsfunktionen für europäische Mitarbeiter nicht zu aktivieren oder aktiv zu nutzen. Theoretisch könnten Arbeitgeber auch einige Einschränkungen umgehen, indem sie ihren Mitarbeitern die Nutzung von Unternehmensgeräten und Kommunikationsnetzen für persönliche oder private Zwecke kategorisch untersagen, da der Zugriff auf rein geschäftliche Informationen idR weitaus weniger reguliert ist. Die meisten Arbeitgeber halten solche Verbote jedoch für nicht praktikabel, und eine selektiv durchgesetzte Richtlinie idS würde von den Gerichten wahrscheinlich ignoriert werden (zB, wenn ein Arbeit-

geber ein Richtlinienverbot festlegt, in der Praxis jedoch die private Nutzung durch Mitarbeiter toleriert).

64 Manche Unternehmen gehen einen Mittelweg und erteilen die Erlaubnis zur Privatnutzung von unternehmenseigenen Systemen und Netzwerken nur unter der Bedingung, dass Mitarbeiter eine ausdrückliche Einwilligung zur Überwachung erteilen. Mitarbeiter, die diese Einwilligung erteilen, dürfen die Systeme, vorbehaltlich der Überwachung, auch zu privaten Zwecken nutzen. Ebenso dürfen Mitarbeiter, die ihre eigenen Smartphones und andere Geräte bei der Arbeit oder für arbeitsbezogene Zwecke nutzen möchten, dies im Rahmen freiwilliger *„Bring your own device"*-Programme (BYOD) tun, sofern sie sich bereit erklären, ihre eigenen Geräte denselben Überwachungs- und Sicherheitsmaßnahmen zu unterwerfen, die der Arbeitgeber zum Schutz der firmeneigenen Systeme einsetzt. Das bedeutet zB, dass der Arbeitgeber aus der Ferne alle Daten (einschließlich privater Bilder) löschen darf, wenn das Gerät verloren oder gestohlen wird (sofern keine Containerlösung vorliegt, die selektive Löschung von Unternehmensdaten zulässt) und dass der Arbeitgeber das private Gerät iRv internen Ermittlungen untersuchen darf oder eine Aufbewahrungspflicht für Rechtsstreitigkeiten anwenden kann. Auch wenn Mitarbeiter ihre Einwilligung nicht erteilen, werden sie auf firmeneigenen Geräten dennoch der Überwachung unterworfen. Eine derartige Überwachung sollte keinen unverhältnismäßigen Eingriff in die Privatsphäre darstellen, da die firmeneigenen Geräte gerade nicht zu persönlichen Zwecken genutzt werden dürfen. Mit einer solchen Richtlinie würden Arbeitgeber offenbar das Bewusstsein der Mitarbeiter sicherstellen und einen angemessenen Kompromiss zwischen den Datenschutzinteressen der Mitarbeiter und den legitimen Datensicherheits- und Compliance-Interessen des Arbeitgebers finden. Es ist jedoch unklar, ob Gerichte und Behörden diesen Ansatz unter allen Umständen akzeptieren werden.

Wenn Unternehmen die gesetzlichen Anforderungen nicht einhalten, riskieren sie Verstöße gegen Arbeits-, Datenschutz-, Abhör- und andere Gesetze, von denen viele mit schweren strafrechtlichen Sanktionen geahndet werden. In einem viel beachteten Fall in Frankreich durchsuchte ein Arbeitgeber die E-Mails eines Mitarbeiters auf den Unternehmenssystemen und fand Beweise dafür, dass der Mitarbeiter während der Arbeitszeit mit den Ressourcen des Arbeitgebers ein illegales Konkurrenzunternehmen betrieb. Da die E-Mail-Durchsuchung jedoch als illegal eingestuft wurde, musste der Arbeitgeber den illoyalen Mitarbeiter wieder einstellen und Schadensersatz zahlen. Außerdem kann es vorkommen, dass Unternehmen über Beweise verfügen, aufgrund derer sie nach den Gesetzen einer Jurisdiktion handeln müssen, während es ihnen nach den Gesetzen anderer Jurisdiktionen untersagt ist, solche Informationen zu haben oder zu verwenden.

Handlungsempfehlungen!

65 Zusammenfassend sollten Arbeitgeber Folgendes beachten:

- Den Einsatz künstlicher Intelligenz und automatisierter Entscheidungsfindung im Einstellungsprozess einschränken.
- Die Rechtmäßigkeit und Zuverlässigkeit von Hintergrundüberprüfungen für jede Jurisdiktion überprüfen.
- Schulung von Personalverantwortlichen und Führungskräften zu den Anforderungen der Datenschutzgesetze, insbes. zu den möglichen Auswirkungen von Datenzugriffsanfragen durch Mitarbeiter, die Anspruch auf Kopien von Bewertungen und anderen vertraulichen Unterlagen mit personenbezogenen Daten über sie haben.
- Verfolgung, welche Technologien eingekauft und eingesetzt werden, die Daten über Mitarbeiter aufzeichnen, einschließlich Technologien, deren Hauptzweck die Überwachung ist (wie Sicherheitskameras, Tastenanschlagprotokollierung, Tools zum Schutz vor Datenverlust, Weblogs, Anrufaufzeichnung, automatische E-Mail-Speicherung und Ortungsgeräte), sowie Technologien, die andere Zwecke haben, aber auch Daten speichern, ohne dass die Mitarbeiter dies ausdrücklich und absichtlich