Geschäftsstelle Dresden:
Königsbrücker Landstraße 40
01109 Dresden
Tel: 0351 8881251

Niederlassung Böblingen:
Otto-Lilienthal-Straße 36
71034 Böblingen

mail@sodalitas-gmbh.de
www.sodalitas-gmbh.de
Fax: 0351 8881252

IT-Ticker 01/2023

Der IT-Ticker 01/2023 informiert Sie über folgende Themen:

Künstliche Intelligenz

KI-Regulierung in Europa: Rechtliche Herausforderungen und Perspektiven

Während in den USA die Regulierung von KI-Applikationen entweder bereits vorhanden ist oder kurz vor der Einführung steht, scheint in Europa der Weg vom ersten Entwurf des „AI Acts“ (KI-Verordnung) bis zum Inkrafttreten noch ein weiter Weg...

Laut der Federal Trade Commission (FTC), der nationalen Verbraucherschutzorganisation in den USA, ist die Regulierung von KI-Applikationen dort bereits Status Quo („Die Realität ist, dass KI (in den USA) reguliert ist“). Vor allem die Gesetze gegen unlautere und betrügerische Handelspraktiken sollen demnach auch für KI-Applikationen gelten und ermöglichen der FTC auch entsprechende Eingriffsbefugnisse gegenüber Unternehmen, die KI entwickeln, verkaufen oder nutzen. In ihrem Blog gibt die FTC auch bei der Bewerbung von KI-Applikationen die Marschrichtung mit Transparenz als einem der obersten Gebote und der Warnung vor Irreführung vor. Den Leitfaden, wie Nutzerdaten für das Trainieren von Algorithmen und KI-Applikationen einzusetzen sind, gibt es bereits seit 3 Jahren – auch hier ist Transparenz die Leitlinie.

Seit dem 21.04.2021 existiert auch in Europa ein Entwurf zur unionsweiten Regulierung von KI, denn „Europa soll das globale Zentrum für vertrauenswürdige künstliche Intelligenz (KI) werden“. Seither wird der Entwurf unter den verschiedenen Vorsitzen im Rat der EU diskutiert und verhandelt. Der Entwurf sieht in erster Linie ein Verbotsgesetz vor, das den Einsatz von gewissen KI-Applikationen entweder ganz verbietet oder den Einsatz an weitere u.U. weitreichendere Voraussetzungen und Sicherungsmaßnahmen knüpft. Nun soll es Ende April zur Abstimmung im Europäischen Parlament kommen, damit dessen Vertreterinnen und Vertreter im Mai mit einer finalen Position in den Trilog mit der Europäischen Kommission und dem Europäischen Rat treten können.

Außerdem scheint im Moment verstärkt diskutiert zu werden, wie sog. Large Language Models (LLM), auf denen beispielsweise Applikationen wie ChatGPT beruhen, im Rahmen der Verordnung einzuordnen sind und ob diese nicht grundsätzlich als Applikationen mit „hohem Risiko“ im Sinne des Entwurfs eingestuft werden sollten.

Zusammenfassend zur besseren Einordnung: Der momentane Entwurf verfolgt einen risikobasierten Ansatz und unterscheidet zwischen KI-Applikationen, die als (i) unannehmbares Risiko, (ii) hohes Risiko oder (iii) geringes oder minimales Risiko einzustufen sind.

KI-Applikationen (bzw. „KI-Systeme“ wie sie der Entwurf definiert) sind primär dann mit einem unannehmbaren Risiko verbunden und damit verboten, wenn der Einsatz gegen die Werte der Union verstößt, zum Beispiel durch die Verletzung von Grundrechten (z.B. bei Manipulation menschlichen Verhaltens oder Social Scoring).

Chatbots wurden in bisherigen Diskussionen zu dem Entwurf grundsätzlich eher als Applikationen mit geringem oder minimalem Risiko eingestuft, was als Rechtsfolge lediglich zu „minimalen" Transparenzpflichten führen würde. KI-Applikationen die dagegen mit hohem Risiko einzustufen wären, müssten grundsätzlich eine Reihe zusätzlicher Anforderungen erfüllen:

- So dürften diese gem. Art. 10 „Daten und Daten-Governance" des Entwurfs u.a. nur mit Daten trainiert werden, die eine gewisse, in dem Entwurf näher ausgeführte, Qualität aufweisen.
- Die Applikationen müssten außerdem derart konzipiert und entwickelt sein;
    - (i) dass diese u.a. automatisch die „Vorgänge und Ereignisse" aufzeichnen/protokollieren (Art. 12 „Aufzeichnungspflichten");
    - (ii) dass der Betrieb hinreichend transparent ist, damit der Nutzer die Ergebnisse angemessen interpretieren und verwenden kann (Art. 13 „Transparenz und Bereitstellung von Informationen für die Nutzer");
    - (iii) dass die Applikationen während der Dauer der Verwendung von natürlichen Personen wirksam beaufsichtigt werden können (Art. 14 „Menschliche Aufsicht") sowie;
    - (iv) dass sie im Hinblick auf ihre Zweckbestimmung ein angemessenes Maß an Genauigkeit, Robustheit und Cybersicherheit erreichen und in dieser Hinsicht während ihres gesamten Lebenszyklus beständig funktionieren (Art. 15 „Genauigkeit, Robustheit und Cybersicherheit").
- Art. 16 „Pflichten der Anbieter von Hochrisiko-KI-Systemen" legt außerdem den Anbietern solcher Applikationen weitreichende Pflichten auf – so muss beispielsweise ein Konformitätsbewertungsverfahren durchgeführt werden.

Auch ohne europäische Verordnung ist KI allerdings in der EU oder Deutschland im Moment nicht unreguliert. Selbstverständlich können bereits geltende Gesetze auch auf KI-Applikationen im jeweiligen Einzelfall Anwendung finden. Dies ist aktuell unter den Vorschriften der DSGVO bereits zu sehen: Nach dem Verbot von ChatGPT in Italien (wir berichteten) prüfen momentan auch die deutschen Datenschutzbehörden den Einsatz in Deutschland und das European Data Protection Board (EDPB) beschloss hierzu letzte Woche die Einrichtung einer Task Force zur Förderung der Zusammenarbeit und zum Austausch von Informationen über mögliche Durchsetzungsmaßnahmen der Datenschutzbehörden. Auch unter dem neuen Digital Service Act (DSA) ist es denkbar, dass bestimmte Vorschriften auf KI-Applikationen (je nach Funktionsweise auch für LLMs denkbar) Anwendung finden könnten – so beispielsweise beim Einsatz von KI-Applikationen im Rahmen von Online-Schnittstellen unter dem Verbot von „Dark Patterns" (Art. 25 „Gestaltung und Organisation der Online-Schnittstelle" DSA) oder hinsichtlich der Transparenzregeln für Empfehlungssysteme unter Einsatz von KI-Applikationen (Art. 27 „Transparenz der Empfehlungssysteme" DSA).

Im Ergebnis bleibt es bei dem Thema Regulierung von KI in Europa und Deutschland in den nächsten Wochen spannend – insbesondere mit der Ende April erwarteten Abstimmung des Europäischen Parlaments zum Entwurf der KI-Vorordnung. Ende April läuft außerdem die von der italienischen Datenschutzbehörde gesetzte Frist an den Europäischen Vertreter des Unternehmens OpenAI als Anbieter von ChatGPT ab. Bis dahin muss der Anbieter Maßnahmen präsentieren, mit denen den identifizierten Missständen Abhilfe geschaffen werden soll. Ansonsten steht bei unzureichender Erfüllung eine Strafe von bis zu 20 Millionen EUR oder 4% des weltweiten Konzernumsatzes im Raum.

Helena Kasper, Moritz Mehner

ChatGPT bessert beim Datenschutz nach und Fortschritte beim AI Act im EU Parlament

Die italienische Datenschutzbehörde Garante hat die Sperrung von OpenAI's ChatGPT in Italien wieder aufgehoben. Die Sperre war Ende März verhängt worden, nachdem Bedenken hinsichtlich der mangelnden Transparenz im Umgang mit Nutzerdaten sowie des unzureichenden Jugendschutzes aufgekommen waren (wir berichteten). Nach intensiven Verhandlungen mit dem Entwickler OpenAI wurde ChatGPT in Italien Ende letzter Woche „mit verbesserter Transparenz und verbesserten Rechten für europäische Benutzer" wieder freigeschaltet.

Eine der Bedingungen der italienischen Behörde, die erfüllt wurde, ist der selbstbestimmtere Umgang

mit den Daten, die in den Chatbot eingegeben werden. Seit kurzer Zeit besteht für alle User die Möglichkeit, in den Einstellungen der Speicherung von Chats in der Chathistorie und damit der Nutzung seiner Daten zu Trainingszwecken zu widersprechen. Für User in der EU wurde jetzt schon ein Formular bereitgestellt, das den Widerspruch auch ohne Löschung der Chats ermöglicht. Zudem wurde eine Altersprüfung für neue User in Italien vorgeschaltet. Die italienische Datenschutzbehörde begrüßte die Kooperationsbereitschaft von OpenAI, gab jedoch bekannt, die Prüfung vorerst noch nicht zu beenden.

Das Unternehmen reagiert auf wachsende datenschutzrechtliche Bedenken mit mehr Aufklärung und immer neuen Funktionen. So soll in den nächsten Monaten „ChatGPT Business" eingeführt werden, das ein anfängliches Opt-Out für die Nutzung von Daten zu Trainingszwecken ermöglicht. Diese Einstellung, die es bis jetzt nur für die OpenAI API gibt, soll zusätzliche Sicherheit für den Einsatz der KI in Unternehmen schaffen. Auch andere Anbieter nutzen die Gelegenheit, um datenschutzfreundlichere Gestaltungen des GPT-Sprachmodells auf den Markt zu bringen. So ermöglicht der Entwickler Private AI Usern mit seinem Tool PrivateGPT, automatisch personenbezogene Daten aus User Prompts herauszufiltern. Auch Microsoft arbeitet an einer Business-Version von ChatGPT, die auf eigenen Servern laufen soll, insbesondere für datenschutzsensible Branchen wie Banken oder Gesundheitswesen.

Die rasante Entwicklung von ChatGPT hat inzwischen Gesetzgeber und Regulierungsbehörden in ganz Europa auf den Plan gerufen. Insbesondere auf die KI-Verordnung (AI Act) der europäischen Kommission haben die jüngsten Entwicklungen großen Einfluss. Medienberichten zu Folge, haben sich die zuständigen Unterhändler des EU Parlaments Ende letzte Woche auf die finalen Punkte des Entwurfs zur KI-Verordnung für das weitere Verfahren geeinigt.

Die zuletzt schwer diskutierte Frage, ob generative KI (insbesondere KI-Systeme wie ChatGPT, Midjourney etc.) per se als sog. Hochrisiko-KI-Systeme eingestuft werden sollen (wir berichteten), wurde hierbei laut der Berichte zu Lasten einer solchen pauschalen Einordnung beantwortet. Grundsätzlich scheint die Mechanik der Einordnung als Hochrisiko-KI-System mit einer zusätzlichen „Stufe" etwas entschärft worden zu sein, so dass nun möglicherweise KI-Systeme, die als Teil der festgelegten Kategorien in Anhang 3 der Verordnung automatisch als Hochrisiko-KI-System eingestuft werden sollten, diese Einstufung nur bekommen, wenn das System zusätzlich dabei auch eine erhebliche Gefahr für die Gesundheit, die Sicherheit oder die Grundrechte darstellt.

Dennoch führte die Diskussion rund um die generativen KI-Systeme wohl zu einer „Last-minute" Ergänzung des Entwurfs. So wird berichtet, dass ein weiterer Artikel mit erhöhten Pflichten für die Entwickler solcher KI-Systeme gelten soll. Solche KI-Systeme sollen nach den von ihnen ausgehenden Risiken überprüft werden und ggf. entsprechende Gegenmaßnahmen ergriffen werden. Es sollen bestimmte Anforderungen an die Datenqualität sowie Cybersicherheit erfüllt werden. Außerdem sind die zum Training der Systeme verwendeten Daten zu dokumentieren. Über die ganz konkreten Anforderungen geht die Berichterstattung zum jetzigen Zeitpunkt teilweise noch auseinander.

Sofern dies tatsächlich so beschlossen wäre, hieße dies natürlich nicht, dass eine solche generative KI grundsätzlich nicht als Hochrisiko-KI-System im Sinne der Verordnung einzustufen wäre – es käme vielmehr auf den konkreten Einsatzbereich des jeweiligen Systems und der oben erwähnten Einordnung unter Anhang 3 im Einzelfall an. Am 11. Mai soll entsprechend der zuständige Ausschuss final abstimmen und es wird erwartet, dass über den finalen Text Mitte Juni im Plenum abgestimmt wird.

Helena Kasper, Moritz Mehner

Datenschutz

EuGH: Nicht jeder Datenschutzverstoß rechtfertigt immateriellen Schadensersatz – Rechtsunsicherheit bleibt dennoch

Immer häufiger fordern Betroffene, die Opfer von Datenschutzverstößen geworden sind, von den Verantwortlichen Entschädigungszahlungen, selbst wenn es sich um eher leichte Datenschutzverstöße (sogenannte „Bagatellverstöße") handelt. Möglich macht das eine mitunter

ausufernde Auslegung einiger Gerichte von Art. 82 DSGVO, nach dessen Wortlaut „jede Person, der wegen eines Verstoßes ein (…) immaterieller Schaden entstanden ist, Anspruch auf Schadensersatz hat“. Mehrere Gerichte, hierunter das Bundesarbeitsgericht, vertreten die Auffassung, dass bereits der bloße Datenschutzverstoß selbst eine Geldentschädigungspflicht auslöse. Eine Beeinträchtigung von einigem Gewicht, wie sie etwa im Persönlichkeits- und Presserecht gängige Praxis und Voraussetzung für Entschädigungszahlungen ist, sei nicht erforderlich.

Der EuGH hat sich einer derart extensiven Auslegung nun mit Urteil vom 04.05.2023 [CURIA - Dokumente (europa.eu)] nicht angeschlossen. Allerdings hat er festgestellt, dass für die Annahme eines immateriellen Schadens eine bestimmte Erheblichkeitsschwelle nicht überschritten sein müsse.

Die Kernaussagen des Gerichts:

1. Nicht jeder Datenschutzverstoß begründet automatisch eine Verpflichtung zur Zahlung einer Geldentschädigung.
2. Art. 82 DSGVO hat keinen Strafcharakter und begründet somit auch keinen Anspruch auf Strafschadensersatz.
3. Die betroffene Person muss nachweisen, dass der Datenschutzverstoß tatsächlich zu einem immateriellen Schaden geführt hat.
4. Es ist jedoch nicht erforderlich, dass ein nachgewiesener immaterieller Schaden eine bestimmte Erheblichkeitsschwelle überschreitet. Die „Kriterien für die Ermittlung des Umfangs des Schadensersatzes“ sind von den mitgliedstaatlichen Gerichten selbst zu bestimmen, solange diese Kriterien nicht die Ausübung der durch die DSGVO gewährleisteten Rechte verhindern.

Die Entscheidung bringt Unternehmen leider nicht den von Vielen erhofften Mehrwert an Rechtssicherheit. Begrüßenswert ist, dass nicht jeder Bagatellverstoß und jedes „bloße Ärgernis“ per se zur Schadensersatzpflicht führt. Unwägbar bleiben aber die konkreten Kriterien, nach denen Gerichte künftig das Vorliegen eines immateriellen Schadens beurteilen. Zwar dürften sich Gerichte nicht mehr – wie bislang teilweise der Fall – ausdrücklich an der hohen Erheblichkeitsschwelle aus dem allgemeinen Persönlichkeitsrecht orientieren. Positiv aus Unternehmenssicht ist aber, dass der Betroffene zumindest einen Schaden tatsächlich erlitten haben und nachweisen muss. „Trittbrettfahrern“, die aus Datenschutzvorfällen z.B. durch Cyberattacken, zusätzlich Profit schlagen wollen ohne einen tatsächlichen Schaden belegen zu können, kann mit Hilfe dieser aktuellen EuGH Rechtsprechung wirksam entgegengetreten werden.

Fazit

Obwohl der EuGH nunmehr gewisse Mindest-Hürden für Entschädigungsansprüche definiert, müssen sich Unternehmen nach wie vor darauf einstellen, nicht nur bei schwerwiegenden Datenschutzverletzungen mit Entschädigungsforderungen konfrontiert zu werden. Es wird spannend zu beobachten, für welche Arten von Datenschutzverletzungen die deutschen Gerichte künftig Entschädigungssummen in welcher Höhe anerkennen und auf welche Kriterien sie hierbei schwerpunktmäßig abstellen. Bis zu einer Entscheidung durch die höchsten Instanzgerichte (BGH, BAG) dürfte abermals ein Vakuum an Rechtsunsicherheit bestehen bleiben. Unverändert bleibt es dabei, dass es für Unternehmen im schlimmsten Fall zu einem Nebeneinander von Bußgeldern der Aufsichtsbehörden und direkten Schadensersatzklagen der Betroffenen kommen kann. Umso mehr ist anzuraten, Datenschutzvorfälle jeder Art professionell und mit einer entsprechend hohen Sorgfalt zu behandeln.

Fabian Bauer, Dr. Oliver Hornung, Dr. Matthias Orthwein

Aktualisierte Leitlinien des EDSA zur Meldung von Datenschutzverletzungen: Was Unternehmen jetzt dringend beachten müssen

Wir berichteten bereits im November 2022 von den neuen Leitlinien für die Meldung von Datenschutzverletzungen des Europäischen Datenschutzausschusses (EDSA) (siehe hierzu unseren Webseitenbeitrag). Nachdem nunmehr das öffentliche Konsultationsverfahren durchgeführt wurde, hat der EDSA am 4. April 2023 seine aktualisierten Leitlinien zur Meldung von Datenschutzverletzungen

veröffentlicht. Was die aktualisierten Leitlinien für Unternehmen konkret bedeuten und was Unternehmen ab sofort zwingend berücksichtigen sollten, erfahren Sie hier.

Hintergrund

Unternehmen, welche nicht in der EU niedergelassen sind, aber nach Art. 3 DS-GVO dennoch in den Anwendungsbereich der DS-GVO fallen, mussten bisher etwaige Datenschutzverletzungen in dem Mitgliedsstaat melden, in dem der Vertreter des verantwortlichen Unternehmens in der EU seine Niederlassung hatte („One-Stop-Shop"-Prinzip).

Neue Regelung

In seinen neuen Leitlinien hat der EDSA nunmehr klargestellt, dass die bloße Anwesenheit eines Vertreters in der EU nicht das „One-Stop-Shop"-Prinzip auslöst. Vielmehr müssen daher betroffene Unternehmen ab sofort Datenschutzverletzungen, die Personen in mehreren Mitgliedsstaaten betreffen, bei sämtlichen Aufsichtsbehörden der jeweiligen Mitgliedsstaaten melden.

Handlungsempfehlungen für Unternehmen

Da Datenschutzverletzungen unverzüglich und möglichst binnen 72 Stunden nach Bekanntgabe der Verletzung gemeldet werden müssen, kann dies Unternehmen vor große Herausforderungen stellen. Die neuen Leitlinien erhöhen diesen Druck zusätzlich, da die Meldung von Datenschutzverletzungen an sämtliche zuständigen Aufsichtsbehörden der jeweiligen Mitgliedsstaaten erfolgen muss und dies zu einem enormen Aufwand führen kann. Um die datenschutzrechtlichen Vorgaben im Unternehmen erfüllen zu können ist es umso wichtiger, rechtzeitig entsprechende Richtlinien und Prozesse im Unternehmen zu implementieren, welche eine einheitliche und geregelte Vorgehensweise für Datenschutzverletzungen festhalten und den Anforderungen der europäischen Aufsichtsbehörden entsprechen.

Eine organisierte Notfallplanung und ein praxisgerechtes Data Breach Management bilden das Fundament für die wirksame Prävention von Unternehmen, um aufsichtsbehördliche Maßnahmen, Bußgelder sowie ggf. Schadensersatzansprüche Betroffener vorzubeugen. Die sorgfältige Umsetzung der Melde- und Benachrichtigungspflichten ist in datenschutzrechtlicher Hinsicht von sehr hoher Relevanz. Verstöße können unter anderem zu Bußgeldern für Unternehmen führen. Vor diesem Hintergrund sollten Unternehmen dringend ihre internen Prozesse und Richtlinien in Bezug auf den Umgang von Datenschutzvorfällen überprüfen und diese einer sorgfältigen Revision unterziehen, um eine ordnungsgenmäße und fristgemäße Meldung von Datenschutzverletzungen zu gewährleisten.

Dr. Oliver Hornung, Marwah Kamal

EuGH zum Auskunftsanspruch: Pflicht zur Nennung aller Empfänger von Daten?

Datenschutzrechtliche Auskunftsansprüche sind längst Unternehmensalltag geworden und bedeuten für die betroffenen Unternehmen häufig einen großen Aufwand. Es stellt sich die Frage, ob dieser Aufwand nach einer im Januar ergangenen EuGH Entscheidung noch größer wird.

Nach Artikel 15 DSGVO hat eine betroffene Person das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob personenbezogene Daten von ihr verarbeitet werden. Wenn dies der Fall ist, hat sie zudem den Anspruch auch weitere Einzelheiten wie u.A. die Verarbeitungszwecke oder Kategorien der personenbezogenen Daten zu erfahren. Umstritten ist allerdings schon länger, ob dieser Anspruch auch die Pflicht der Unternehmen umfasst, der betroffenen Person die Identität sämtlicher Empfänger der jeweiligen Daten zu nennen.

In Artikel 15 Abs. 1 lit. c DSGVO ist diesbezüglich eine Wahlentscheidung vorgesehen. Hier steht, dass „Empfänger oder Kategorien von Empfängern" mitzuteilen sind. Unklar war bisher, ob das Wahlrecht hierbei der betroffenen Person oder dem verantwortlichen Unternehmen zukommen soll.

Entscheidung des EuGH
Mit Urteil vom 12. Januar 2023 hat der EuGH (Rs. C-154/21) nun entschieden, dass der betroffenen

Person das entsprechende Wahlrecht zusteht, ob sie alle Empfänger oder lediglich die Empfängerkategorien benannt bekommen möchte. Eine Pflicht der Nennung der konkreten Identität der Empfänger besteht somit grundsätzlich, wenn die Person dies gegenüber dem Unternehmen verlangt. Laut EuGH gilt dieses Recht allerdings nicht uneingeschränkt. Es gilt nicht, wenn es dem Verantwortlichen unmöglich ist, die einzelnen Empfänger konkret zu benennen oder wenn es sich um offenkundig unbegründete oder exzessive Anträge der Betroffenen handelt.

Um die Auswirkungen dieser Entscheidung auf die Praxis der Unternehmen bewerten zu können, muss man sich die konkreten Umstände dieser EuGH Entscheidung genauer ansehen. Die Entscheidung betraf konkret einen Streit über einen Auskunftsanspruch einer betroffenen Person gegen die österreichische Post. Ursprünglich hatte die österreichische Post gegenüber der betroffenen Person lediglich angegeben, sie verwende Daten, soweit das rechtlich zulässig sei, im Rahmen ihrer Tätigkeit als Herausgeberin von Telefonbüchern und biete diese personenbezogenen Daten Geschäftskunden für Marketingzwecke an. Im Übrigen verwies sie für detailliertere Informationen und weitere Datenverarbeitungszwecke auf eine Website. Im Laufe des Rechtsstreits teilte die österreichische Post der betroffenen Person dann mit, dass die personenbezogenen Daten zu Marketingzwecken verarbeitet und an Kunden weitergegeben worden seien, zu denen werbetreibende Unternehmen im Versandhandel und stationären Handel, IT-Unternehmen, Adressverlage und Vereine wie Spendenorganisationen, Nichtregierungsorganisationen (NGOs) oder politische Parteien gehört hätten.

Seine juristische Argumentation stützt der EuGH vor allem darauf, dass den betroffenen Personen durch Ausübung ihrer Auskunftsrechte auch eine Überprüfung ermöglicht werden muss, ob die Daten in zulässiger Weise verarbeitet werden. Zudem müsse es den betroffenen Personen auch möglich gemacht werden, auch die anderen Rechte (Löschung, Einschränkung, Widerspruchsrecht) ausüben zu können und mögliche Rechtsbehelfe einzulegen.

Auswirkung der Entscheidung auf die Praxis
Gerade der Blick auf die hier im konkreten Streitfall betroffenen Empfängerkategorien (werbetreibende Unternehmen und Kunden zu Marketingzwecken) zeigt, dass es sich hierbei um eine Datenweitergabe an eigene Verantwortliche handelt, welche die Daten dann für eigene Zwecke (nämlich Marketingzwecke) verwendet haben. In solchen Fällen besteht nach der Entscheidung des EuGH immer dann eine Pflicht zur Nennung aller einzelnen Empfänger, wenn diese dem Verantwortlichen bekannt sind.

Nicht ausdrücklich behandelt hat der EuGH die Frage, ob sich der Auskunftsanspruch auch auf alle Auftragsverarbeiter und deren Subunternehmer erstreckt. Gerade bei komplexen Datenverarbeitungen wie SaaS- und Clouddiensten können sehr viele Subunternehmer auch für kleinste Nebentätigkeiten eingesetzt werden, die im Zweifel nach der Definition der DSGVO „Empfänger“ von Daten sind. Im Unterschied zu den eigenen Verantwortlichen dürfen Auftragsverarbeiter Daten nicht für eigene Zwecke verarbeiten, sondern nehmen die Verarbeitung der Daten immer nur im Auftrag des Verantwortlichen vor. Die Rechte der betroffenen Person wie zum Beispiel auf Auskunft, Löschung oder Berichtigung richten sich jeweils ausschließlich gegen den oder die Verantwortlichen, nicht gegen einzelne Auftragsverarbeiter. Die betroffene Person kann also alle ihre Rechte nach der DSGVO wirksam ausüben, wenn sie die Verantwortlichen kennt. Die Kenntnis aller einzelnen Auftragsverarbeiter und aller weiteren Unterauftragsverarbeiter ist jedoch für die Durchsetzung der Rechte der betroffenen Person gerade nicht erforderlich. Es lässt sich somit nach unserer Ansicht weiter argumentieren, dass das Wahlrecht der betroffenen Person nur für verantwortliche Empfänger greift und bei Auftragsverarbeitern weiterhin die Nennung von Empfängerkategorien ausreichend ist.

Praxistipp

Erhält ein Unternehmen Auskunftsersuchen, sollte zunächst geprüft werden, in welchem Umfang konkret die Auskunft verlangt wird. Nur wenn ausdrücklich verlangt wird, dass alle Empfänger zu benennen sind, hat die betroffene Person ihr Wahlrecht (nach Verständnis des EuGH) ausgeübt.

Unternehmen sollten generell prüfen, ob ihre aktuelle Dokumentation ausreichend auf Auskunftsersuchen vorbereitet ist. Jedenfalls wenn Daten an Dritte, die Daten in eigener Verantwortung verarbeiten, übermittelt werden, müssen Unternehmen die einzelnen Empfänger

benennen können. Auch die konkret eingesetzten Auftragsverarbeiter sollten für Unternehmen leicht abrufbar sein. Dabei können die Angaben entweder unmittelbar im Verarbeitungsverzeichnis oder in separaten Listen geführt werden. In jedem Fall sollte die Dokumentation stets aktuell gehalten und regelmäßig überprüft werden. Empfehlenswert ist es zudem zu prüfen, ob von allen eingesetzten Auftragsverarbeitern Angaben zu deren Subunternehmern vorhanden sind. Auch hier sollte eine Routine zur Dokumentation festgelegt werden.

Nikolaus Bertermann, Hannah Mugler

Paukenschlag durch EuGH: Keine Generalklauseln im Beschäftigtendatenschutz

Per Urteil vom 30. März 2023 (Az. C-34/21) hat sich der Europäische Gerichtshof (EuGH) nunmehr zu der Frage positioniert, inwieweit dem nationalen Gesetzgeber (k)ein Spielraum bei der Ausgestaltung von Klauseln im Beschäftigtendatenschutz zusteht. Hintergrund der Entscheidung war eine Vorlage über eine Regelung im hessischen Beschäftigtendatenschutz, welche nahezu wortidentisch zur Regelung des § 26 Abs. 1 S. 1 des Bundesdatenschutzgesetzes (BDSG) ausgestaltet ist. Die Kernaussage des EuGH lässt sich dahingehend zusammenfassen, dass im Beschäftigungskontext erlassene nationale Generalklauseln unanwendbar sind, da diese im Widerspruch zu der Öffnungsklausel des Art. 88 DS-GVO stehen.

Der nachfolgende Beitrag soll den rechtlichen Hintergrund der Entscheidung sowie die daraus resultierenden praktischen Implikationen aufzeigen.

Hintergrund der Entscheidung

Die DS-GVO bezweckt – vgl. insoweit auch deren Erwägungsgrund 3 – ein möglichst harmonisiertes europäisches Datenschutzrecht. Dies bedeutet, dass es dem nationalen Gesetzgeber nicht ohne Weiteres möglich ist, eigenständige Normen zum Datenschutz zu schaffen. Soweit die DS-VO also einen bestimmten Sachverhalt bereits eindeutig adressiert, sind in diesem Kontext geschaffene nationale Regelungen grundsätzlich unanwendbar (sog. Anwendungsvorrang). Gleichsam muss das sog. Normwiederholungsverbot beachtet werden, welches es dem nationalen Gesetzgeber grundsätzlich verbietet, europäische Regelungen lediglich wortidentisch zu wiederholen.

Eine Ausnahme hiervon bilden jedoch sog. Öffnungsklauseln. Durch diesen Mechanismus ist es dem nationalen Gesetzgeber – im jeweils hierfür vorgesehenen Umfang – möglich, eigenständige Regelungen zu einer Materie zu erlassen, welche eigentlich ein bereits in sich abgeschlossenes Regelwerk darstellt. Der Mechanismus wurde insbesondere im Zusammenhang mit dem Beschäftigtendatenschutz in die DS-GVO übernommen, da insoweit einige Unterschiede in den jeweiligen Mitgliedsstaaten vorherrschen.

Die bereits angesprochene Öffnungsklausel des Art. 88 Abs. 1 DS-GVO ermöglicht es dem nationalen Gesetzgeber daher „spezifischere Regelungen“ im Beschäftigtendatenschutz zu erlassen. Dies wird in Art. 88 Abs. 2 DS-GVO dahingehend konkretisiert, als diese Regelungen gewissen Mindestanforderungen entsprechen müssen, etwa indem geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen sowie der Grundrechte der betroffenen Person vorgesehen werden. Zudem müssen die entsprechenden Regelungen „spezifischer“ sein, was insbesondere eine reine Wiederholung der Vorgaben der DS-GVO verbietet.

Der deutsche Gesetzgeber hat die vorgenannte Öffnungsklausel insoweit genutzt, als er die bereits vor Inkrafttreten der DS-GVO vorgesehene Vorschrift im alten Bundesdatenschutzgesetz nahezu wortidentisch in die Regelung des § 26 Abs. 1 S. 1 BDSG neu überführt hat. Hiernach dürfen personenbezogene Daten von Beschäftigten verarbeitet werden, sofern dies für die Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses erforderlich ist. Wortgleiche Regelungen sind ebenfalls teilweise in den Landesdatenschutzgesetzen der einzelnen Bundesländer enthalten.

Die Frage, die sich der EuGH nunmehr – im konkreten Fall auf den hessischen Beschäftigtendatenschutz bezogen – stellen musste, war, welche konkreten Anforderungen durch die Regelung des Art. 88 DS-GVO aufgestellt werden. Gleichsam sollte der EuGH darüber befinden, wie

im Falle des Fehlens dieser Anforderungen weiter zu verfahren ist.

Der EuGH hat nunmehr mit eindeutigen Worten klargestellt, dass Generalklauseln im Beschäftigtendatenschutz unanwendbar sind, da diese keine spezifischeren Regelungen im Sinne des Art. 88 Abs. 1 DS-GVO darstellen. Die Regelung des § 26 Abs. 1 S. 1 BDSG – sowie vergleichbare Regelungen in den Landesdatenschutzgesetzen – sind daher künftig nicht mehr geeignet, die Verarbeitung personenbezogener Daten im Beschäftigungskontext abzubilden. Weder heben sich diese Regelungen in gesonderter Weise von der allgemeinen Regelung des Art. 6 Abs. 1 lit. b) DS-GVO ab, noch werden die besonderen Anforderungen des Art. 88 Abs. 2 DS-GVO entsprechend umgesetzt.

Welche Auswirkungen hat die Entscheidung auf die Praxis?

Für Unternehmen und Arbeitgeber bedeutet dies, dass künftig – soweit es um die „klassischen" Verarbeitungsprozesse im Beschäftigungsverhältnis geht – auf die Regelungen der DS-GVO zurückgegriffen werden muss. So ist eine Verarbeitung personenbezogener Daten auch weiterhin zulässig, soweit diese gemäß Art. 6 Abs. 1 lit. b) DS-GVO zur Erfüllung eines Vertrags – etwa dem Arbeitsvertrag – erforderlich ist. Soweit die Erforderlichkeit im Einzelfall jedoch nicht als gegebenen angesehen werden kann, muss – sofern keine Einwilligung der Beschäftigten eingeholt wird – mitunter auf die Interessenabwägungsklausel des Art. 6 Abs. 1 lit. f) DS-GVO zurückgegriffen werden. Während sich hierbei in der Überzahl der praktisch bedeutsamen Fälle wohl keine größeren Neuerungen auftun, müssen jedoch insbesondere die Arbeitsgerichte einen Teil ihres Einflusses auf den Beschäftigtendatenschutz aufgeben. Während zuvor in arbeitsrechtlichen Streitigkeiten lediglich die Norm des § 26 Abs. 1 S. 1 BDSG ausgelegt werden musste, handelt es sich nunmehr um die Auslegung und Anwendung unmittelbar europarechtlicher Regelungen, was ggf. zu einer Vorlage beim EuGH führen kann, bzw. muss. Insgesamt ist daher davon auszugehen, dass eine stärkere Vereinheitlichung des Beschäftigtendatenschutzes erfolgen wird.

Angemerkt sei an dieser Stelle jedoch ausdrücklich, dass derzeit unklar ist, wie sich die o.g. Entscheidung des EuGH auf die weiteren Absätze in § 26 BDSG auswirkt. Während die Regelung des § 26 Abs. 1 S. 2 BDSG – aufgrund deren Kontext im Zusammenhang mit der Aufdeckung von Straftaten – ggf. als noch spezifisch genug angesehen werden kann, wird insbesondere auch die Regelung des § 26 Abs. 3 BDSG eine wesentliche Rolle in der Diskussion spielen. Die vorstehende Regelung lässt die Verarbeitung besonderer Kategorien personenbezogener Daten im Beschäftigungsverhältnis zu und kann wohl (auch) auf die Öffnungsklausel des Art. 9 Abs. 2 lit. b) DS-GVO gestützt werden. Auch werden in § 26 Abs. 3 S. 2 i.V.m. § 22 Abs. 2 BDSG spezifische Maßnahmen für eben diesen Verarbeitungskontext aufgestellt. Weiterhin möglich bleibt ebenfalls das Einholen einer datenschutzrechtlichen Einwilligung sowie die in § 26 Abs. 4 BDSG vorgesehene Möglichkeit zur Schaffung beschäftigungsspezifischer Regelungen in einer Betriebsvereinbarung.

Die Entscheidung des EuGH rüttelt den deutschen Beschäftigtendatenschutz dennoch zumindest einmal gründlich durch. Dies ist auch insoweit nichts neues, als die Datenschutzkonferenz (DSK) bereits mit Entschließung vom 29. April 2022 angeführt hat, dass § 26 BDSG „nicht hinreichend praktikabel, normenklar und sachgerecht" sei.

Praxishinweis

Die vorstehenden Ausführungen sind in weiten Teilen natürlich dogmatischer Natur, da diese auf eine Vielzahl der Verarbeitungsvorgänge keine praktisch spürbaren Auswirkungen entfalten. Soweit eine Datenverarbeitung zu Zwecken der Durchführung des Beschäftigungsverhältnisses nicht hinweg gedacht werden kann, wird diese auch weiterhin zulässig bleiben. Dennoch sollten Unternehmen die Entscheidung des EuGH ernst nehmen, da sich diese an vermeintlich unwichtigen Stellschrauben dennoch bemerkbar machen wird.

Praktisch bedeutsam sind insoweit insbesondere Datenschutzhinweise gemäß Art. 13 DS-GVO, welche sowohl im Beschäftigungsverhältnis als auch im Bewerberprozess den betroffenen Personen zur Verfügung gestellt werden müssen. Diese sollten zumindest mittelfristig dahingehend angepasst werden, als primär die in der DS-GVO vorgesehenen Rechtsgrundlagen anzugeben sind. Ob daneben weiterhin (auch) die Vorschrift des § 26 BDSG – etwa zu Klarstellungszwecken – angeführt wird, ist wohl eine Geschmacksfrage. Obgleich die Entscheidung des EuGH nicht ausdrücklich die

Anwendbarkeit des § 26 BDSG adressiert, können die dort getroffenen Ausführungen nur schwerlich ignoriert werden. Ratsam ist es daher, zumindest primär die einschlägigen Vorschriften der DS-GVO zu benennen, insbesondere um auch etwaige „Fehler“ beim Auffinden der nunmehr einschlägigen Rechtsgrundlage möglichst frühzeitig zu umgehen.

Bis der deutsche Gesetzgeber auf das Urteil des EuGH reagiert hat, müssen Unternehmen nunmehr eine Umstellung der einschlägigen Rechtsgrundlagen zur DS-GVO vornehmen. Für konzernweit tätige Unternehmen kann dies ggf. sogar mit einer Erleichterung einhergehen, da weniger nationale Besonderheiten beachtet werden müssen.

Marius Drabiniok, Dr. Oliver Hornung

Doppelt hält besser: Dürfen Betroffene bei Datenschutzverstößen mehrere Rechtsbehelfe gleichzeitig einlegen?

Bei Datenschutzverstößen steht es Betroffenen grundsätzlich frei, zwischen unterschiedlichen Rechtsbehelfen auszusuchen. Wie verhält es sich aber, wenn Betroffene nicht nur einen, sondern mehrere Rechtsbehelfe parallel eingelegen möchten? Kann sich das Verwaltungsgericht bspw. mit demselben Sachverhalt befassen, der gleichzeitig auch vor dem Zivilgericht behandelt wird? Dies hat der Europäische Gerichtshof in seinem Urteil vom 12. Januar 2023 (C-132/21) grundsätzlich bejaht.

Was war geschehen?

2019 nahm die betroffene Person an der Hauptversammlung des Verantwortlichen teil und richtete in diesem Zusammenhang mehrere Fragen an die Mitglieder des Verwaltungsrats sowie an weitere Teilnehmer. Im Nachhinein forderte die betroffene Person den Verantwortlichen auf, ihm die während der Versammlung aufgezeichneten Tonaufnahmen zu übermitteln. Dieser Aufforderung kam der Verantwortliche nur bedingt nach. Der betroffenen Person wurden Tonbänder ausgehändigt, welche nur seine Redebeiträge enthielten, aber nicht die Antworten auf die gestellten Fragen. Dabei berief sich der Verantwortlich darauf, dass es sich bei den Antworten um Daten Dritter gehandelt hätte, welche zu schützen seien.

Die betroffene Person beschwerte sich bei der Datenschutzaufsicht, welche die Beschwerde jedoch zurückwies, so dass Klage beim Verwaltungsgericht eingereicht wurde. Gleichzeitig klagte die betroffene Person jedoch auch vor den Zivilgerichten, so dass zwei Gerichte über den gleichen Sachverhalt zu entscheiden hatten.

Während die Klage noch beim Verwaltungsgericht anhängig war, gab das Zivilgericht der Klage statt und stellte fest, dass der Verantwortliche das Recht der betroffenen Person auf Auskunft über seine personenbezogenen Daten verletzt habe. Dieses Urteil wurde rechtskräftig.

Da sich allerdings das Verwaltungsgericht nun mit dem gleichen Sachverhalt und derselben Problematik befassen musste, legte es dem Europäischen Gerichtshof die Frage vor, ob es im Rahmen seiner Urteilsfindung an das rechtskräftige Urteil des Zivilgerichts gebunden sei, welches sich auf denselben Sachverhalt beziehe und die gleichen Rechtsfragen zu klären sind. Da eine parallele Einlegung von Rechtsbehelfen durchaus zu einander widersprechenden Entscheidungen führen könne, sollte in diesem Zusammenhang insbesondere geklärt werden, ob einer der Rechtsbehelfe gegenüber dem anderen Vorrang habe.

Wie hat der Europäische Gerichtshof entschieden?

Der Europäische Gerichtshof stellte fest, dass grundsätzlich eine parallele Einlegung von Rechtsbehelfen nach Art. 77 – 79 DSGVO zulässig sei. Die DSGVO stelle betroffenen Personen verschiedene Rechtsbehelfe zur Verfügung, wobei jeder dieser Rechtsbehelfe "unbeschadet" der anderen eingelegt werden könne. Eine vorrangige oder ausschließliche Zuständigkeit könne aus der DSGVO nicht entnommen werden – unabhängig von der Frage, ob es sich um eine Entscheidung einer Behörde oder eines Gerichts handele. Primäres Ziel der DSGVO in Anlehnung an Erwägungsgrund 10 sei ausschließlich, betroffenen Personen ein hohes Datenschutzniveau zu garantieren. Die parallele Einlegung mehrerer Rechtsbehelfe würde dieses Ziel garantieren und die Betroffenenrechte stärken.

Die konkrete Umsetzung eines hohen Datenschutzniveaus obliege nach Ansicht des Europäischen Gerichtshofs vor diesem Hintergrund den einzelnen Mitgliedstaaten.

Was bedeutet diese Entscheidung konkret für die Mitgliedsstaaten?

Die Mitgliedsstaaten sind nun im Rahmen ihrer Verfahrensautonomie in der Pflicht, entsprechende Verfahrensvorschriften zu erlassen und dafür zu sorgen, dass ein Zusammenspiel der Rechtsbehelfe geregelt wird, „um die Wirksamkeit des Schutzes der durch diese Verordnung garantierten Rechte, die gleichmäßige und einheitliche Anwendung ihrer Bestimmungen sowie das in Art. 47 der Charta der Grundrechte niedergelegte Recht auf einen wirksamen Rechtsbehelf bei einem Gericht zu gewährleisten."

Gleichfalls gilt es im Sinne der einheitlichen Auslegung der DSGVO widersprüchliche Entscheidungen zu vermeiden. Dies dürfte vor allem über Rechtsmittel erreicht werden.

Fazit

Das Urteil des Europäischen Gerichtshofs zeigt einmal mehr, welch überragende Bedeutung dem Schutz personenbezogener Daten zukommt. Unternehmen sollten daher stets aufmerksam darauf achten, sämtliche Datenverarbeitungen in Ihrem Betrieb gründlich zu überprüfen und die hierfür erforderlichen Schutzvorkehrungen zu treffen, um die Sicherheit und den Schutz dieser Daten zu garantieren.

Marwah Kamal, Franziska Ladiges

Einsatz von Wearables bei der Arbeit: Wie sicher sind die Daten von Beschäftigten?

Ob Smartwatches, Datenbrillen, Handschuhe mit Sensoren und Scannern oder Fitnesstracker für betriebliche Gesundheitsprogramme: Wearables gewinnen mit fortschreitender Digitalisierung immer mehr an Popularität und bieten Arbeitgebern eine hervorragende Möglichkeit, ihre betrieblichen Arbeitsprozesse zu optimieren und diesen technologischen Fortschritt in ihrem Betrieb effektiv einzusetzen. So können Wearables den betrieblichen Arbeitsprozess erheblich erleichtern und insbesondere Gesundheitsgefahren der Beschäftigten minimieren. Wie so oft, haben jedoch technologische Entwicklungen auch ihre Schattenseiten: Wearables generieren eine Menge an personenbezogenen Daten, weshalb an die Erhebung und Verarbeitung dieser Daten erhöhte Anforderungen zu stellen sind. Wie sicher sind eigentlich diese Daten wirklich und wie können Beschäftigte vor einer Leistungskontrolle des Arbeitgebers geschützt werden? Diese und weitere Fragen sollen nachfolgend näher beleuchtet werden:

1. Was sind Wearables?

Wearables sind mobile Kleincomputer, welche von Beschäftigten direkt am Körper bzw. am Kopf getragen werden. Sie fallen in der Regel kaum auf und erfassen mittels Sensoren Werte der Beschäftigten. Ein grundlegender Unterschied zwischen den herkömmlichen mobilen Computersystemen (wie z.B. Smartphones) und Wearables liegt beim Zweck: Bei Wearables ist nicht die Nutzung des Computersystems als solches die Haupttätigkeit, sondern vielmehr die Tätigkeit der jeweiligen Person, welche von dem am Körper getragenen Computersystem unterstützt wird.

2. Wo werden Wearables im Betrieb eingesetzt?

Der Einsatz von Wearables im Betrieb kann aus unterschiedlichen Gründen erfolgen: So können beispielsweise Beschäftigte zum Zwecke der betrieblichen Gesundheitsvorsorge mit Smartwatches oder Fitnessarmbändern ausgestattet werden, um auf diese Weise sowohl im beruflichen als auch im privaten Umfeld auf ihre Gesundheit zu achten. Vorteil für Arbeitgeber ist sicherlich, auf diese Weise Arbeitsausfälle durch Erkrankungen zu reduzieren und für eine stabile Arbeitsleistung ihrer Beschäftigten zu sorgen. Sehr beliebt ist auch der Einsatz von Wearables in der Logistik Branche. Im Rahmen von sog. „Pick-by-Voice-Systemen" erhalten die Beschäftigten ein Headset, auf welches sie die Lageranweisungen von der Software per Sprachausgabe erhalten. Auf diese Weise werden Handscanner und unzählige Papierlisten nicht mehr benötigt und Störungen im Arbeitsablauf

vermieden. Darüber hinaus erweist sich auch der Einsatz von Wearables zu Ausbildungszwecken als äußerst nützlich und wird von Unternehmen vermehrt eingesetzt.

3. Welche datenschutzrechtlichen Bedenken gibt es hierbei?

Die Möglichkeit zum Sammeln und Auswerten von Daten scheint mit dem Einsatz von Wearables schier endlos zu sein: Von personenbezogenen Daten bis hin zu sensiblen Gesundheitsdaten ist theoretisch vieles technisch umsetzbar. Aus diesem Grund müssen die Daten der Beschäftigten vor Zugriffen Dritter geschützt werden. Insbesondere ist aber auch aus arbeitsrechtlicher Perspektive sicherzustellen, dass keine Leistungskontrolle der Beschäftigten erfolgt. Es besteht nämlich die Möglichkeit, dass bspw. Smartwatches seitens der Arbeitgeber dazu genutzt werden, Bewegungsprofile systematisch aufzuzeichnen und die Leistungen der Beschäftigten zu überwachen. Der Beschäftigtendatenschutz spielt in diesem Kontext somit eine entscheidende Rolle (vgl. auch hierzu unser Webseitenbeitrag zum Thema „Einsatz von Videoüberwachungsanlagen unter datenschutzrechtlichen Gesichtspunkten“).

4. Auf welche Rechtsgrundlage kann der Einsatz von Wearables gestützt werden?

   a) § 26 Abs. 1 BDSG Vertragserfüllung im Beschäftigtendatenschutz
   § 26 Abs.1 BDSG sieht einerseits vor, dass die Verarbeitung von Beschäftigtendaten im Rahmen der Nutzung von Wearables erforderlich und im Übrigen verhältnismäßig sein müssen. Ob Wearables tatsächlich zur Durchführung des Beschäftigungsverhältnisses erforderlich sind, muss je nach Einzelfall beurteilt werden und kann sich unter Umständen als äußerst schwierig erweisen. Das VG Hannover hat jedenfalls im Februar 2023 entschieden, dass das Logistikzentrum Amazon in Winsen die Arbeitsgeschwindigkeit seiner Beschäftigten mithilfe von Handscannern überwachen darf (Az. 10 A 6199/20) und damit die Erforderlichkeit bejaht. Nach Auffassung des Gerichts überwiege nämlich das Interesse Amazons, die Abläufe im Logistikzentrum zu optimieren und die Leistung seiner Beschäftigten zu überwachen. Ob dieses Urteil in zweiter Instanz vor dem Oberverwaltungsgericht Lüneburg doch noch gekippt wird, bleibt abzuwarten. Fest steht jedenfalls, dass sich das Datenschutzrecht dem technologischen Fortschritt nicht gänzlich verschließt, aber gleichwohl klare Grenzen setzt. Die Unternehmen müssen jedenfalls vor dem Einsatz von Wearables dafür Sorge tragen, dass durch geeignete Vorkehrungen, wie z.B. durch die Regelung von Zugriffsrechten, die Umsetzung von technischen und organisatorischen Maßnahmen sowie die Achtung des Grundsatzes der Datenminimierung, die Rechte ihrer Beschäftigten hinreichend berücksichtigt werden.

   b) Einwilligung
   Sofern die Erforderlichkeit der Datenverarbeitung verneint wird, kommt als weitere Rechtsgrundlage eine datenschutzrechtliche Einwilligung nach § 26 Abs. 2 BDSG in Betracht. Eine solche Einwilligung ist jedoch nur wirksam, wenn sie freiwillig abgegeben wird. Problematisch hierbei in der Regel, dass aufgrund der wirtschaftlichen Abhängigkeit von Arbeitnehmern gegenüber ihren Arbeitgebern eine Freiwilligkeit oft nicht angenommen werden kann, weil Arbeitnehmer oftmals aus Sorge um ihren Arbeitsplatz der Maßnahme des Arbeitgebers zustimmen (vgl. hierzu DSK Kurzpapier Nummer 14)

   Insofern sind Einwilligungen im Beschäftigungsverhältnis häufig mit Risiken und gewissen Unsicherheiten verbunden.

   c) Betriebsvereinbarung
   Zumindest ist für Unternehmen, welche einen Betriebsrat haben, sicherste Rechtsgrundlage die Betriebsvereinbarung gem. Art. Art. 88 Abs.1 DS-GVO i.V.m. § 26 Abs. 4 BDSG. § 87 Abs. 1 Nr.6 BetrVG verpflichtet nämlich diese Unternehmen, vor Einführung technischer Einrichtungen den Betriebsrat stets einzubinden. Die Betriebsvereinbarung muss in diesem Zusammenhang insbesondere die Einhaltung der Grundsätze aus Art. 5 Abs.1 DS-GVO sicherstellen. Grundlegende Bedeutung kommt hierbei insbesondere dem Grundsatz der Zweckbindung aus Art. 5 Abs.1 lit. b) DS-GVO zu, wonach die Zwecke, für die die Beschäftigtendaten erhoben, verarbeitet oder genutzt werden, eindeutig und detailliert beschrieben werden müssen. Die Beschäftigten müssen klar erkennen können, zu welchem Zweck ihre Daten verarbeitet werden (Transparenzgebot). Darüber hinaus sind auch Regelungen zur Datenminimierung festzuhalten und die hierfür erforderlichen Maßnahmen zu

dokumentieren. Zudem ist auch der Grundsatz der Speicherbegrenzung zu beachten und klare Löschfristen zu vereinbaren. Nicht zuletzt sind auch Ausführungen zu den technischen und organisatorischen Maßnahmen aufzunehmen, um so sicherzustellen, dass die erhobenen Daten hinreichend geschützt werden.

5. Wie können Beschäftigte geschützt werden?

Um zu gewährleisten, dass einerseits die Interessen des Arbeitgebers hinreichend berücksichtigt werden und andererseits keine Leistungskontrollen der Beschäftigten stattfinden, müssen für den Einsatz von technischen Einrichtungen zumindest folgende Maßnahmen ergriffen werden:

- Die Beschäftigten müssen im Rahmen von Datenschutzhinweisen auf die Datenverarbeitung hingewiesen und informiert werden, um auf diese Weise das Transparenzgebot der DS-GVO einzuhalten.
- Ein weiterer wichtiger Punkt ist die Klärung der rechtlichen Frage, ob die Durchführung einer Datenschutz-Folgenabschätzung für den Einsatz von Wearables nach Art. 35 DS-GVO erforderlich ist. Dies wird in der Regel beim Einsatz von neuen bzw. innovativen Technologien angenommen, weshalb in diesen Fällen regelmäßig eine entsprechende Risikobewertung vorgenommen werden muss (vgl. hierzu auch unseren Webseitenbeitrag zum Thema „How to Datenschutz-Folgenabschätzung“). In diesem Zusammenhang müssen unter anderem auch Ausführungen zu einem möglichen Drittlandtransfer gemacht werden, wobei im Falle einer Übermittlung der Beschäftigtendaten in ein Drittland noch weitere Maßnahmen, wie z.B. der Entwurf eines Transfer Impact Assessments, ausgearbeitet werden müssen. Im Falle von Wearables ist ein solcher Drittlandtransfer auch nicht unüblich, da eine Vielzahl dieser Geräte von Cloud Anbietern betrieben werden.
- Last but not least ist auch an die Aufnahme dieses Datenverarbeitungsprozesses in das Verarbeitungsverzeichnis zu denken, wobei hierzu unter anderem auch Ausführungen zur Rechtsgrundlage, den Empfängerkategorien sowie zu den betroffenen Datenkategorien gemacht werden müssen.

6. Fazit

Insgesamt kann festgehalten werden, dass der Einsatz von Wearables sowohl Unternehmern als auch Beschäftigten zu Gute kommt. Aus Sicht von Unternehmern tragen Wearables erheblich dazu bei, den Betriebsablauf zu optimieren und Kosten zu sparen. Gleichwohl profitieren Beschäftigte insbesondere im Hinblick auf die Förderung Ihrer Gesundheit. Aus datenschutzrechtlicher Sicht hingegen erfordern Wearables eine erhöhte Aufmerksamkeit und dürfen von Unternehmen nicht unterschätzt werden. Vor dem Einsatz von Wearables sollten sich Arbeitgeber daher intensiv damit beschäftigen, wie sie die Daten ihrer Beschäftigten ausreichend schützen und welche zwingend erforderlichen datenschutzrechtlichen Dokumente sie hierfür bereitstellen.

Dr. Oliver Hornung, Marwah Kamal

Sind Daten im EWR sicher? Die Datenschutzkonferenz positioniert sich erneut zum Thema Drittlandtransfer

Mit dem vorliegenden Beitrag möchten wir auf den aus unserer Sicht äußert praxisrelevanten Beschluss der Datenschutzkonferenz (DSK) vom 31. Januar 2023 näher eingehen. Die DSK hat sich erneut zum Thema Drittlandtransfer, bzw. genauer, zu (theoretischen) Zugriffsmöglichkeiten auf personenbezogene Daten im EWR aus Drittländern heraus, positioniert. Nach Bekanntwerden des Entwurfs für ein „EU US Data Privacy Framework“ – wir haben hierüber berichtet – kam zunächst eine gewisse Euphorie auf, da das Thema Drittlandtransfer nunmehr seit vielen Jahren eine Never-Ending-Story des Datenschutzrechts darstellt. Umso relevanter sind die nunmehr seitens der DSK aufgestellten Anforderungen, welche Unternehmen nochmals vor weitere Herausforderungen stellen. Was genau hat die DSK beschlossen?

Zunächst hat die DSK in dem angeführten Beschluss ausdrücklich festgehalten, dass die „reine Gefahr, dass – etwa über gesellschaftsrechtliche Weisungsrechte – die Drittlands-Muttergesellschaft eines EWR-Unternehmens dieses anweisen könnte, oder dass öffentliche Stellen von Drittländern

unmittelbar EWR-Unternehmen anweisen könnten, personenbezogene Daten in ein Drittland zu übermitteln“, nicht genügt, „um eine Übermittlung in ein Drittland i.S.d. Art. 44 ff. DS-GVO anzunehmen“. Obgleich dies bereits die bislang überwiegende Rechtsauffassung darstellte, ist die ausdrückliche Klarstellung der DSK zu begrüßen.

Gleichsam wird in dem vorgenannten Beschluss ausdrücklich festgehalten, dass eben diese Gefahren eines Drittlandtransfers dazu führen können, dass ein betroffener Auftragsverarbeiter nicht über die notwendige Zuverlässigkeit im Sinne des Art. 28 DS-GVO verfügt. Etwas anderes gelte nur dann, sofern der Auftragsverarbeiter – oder der Verantwortliche – technische und/oder organisatorische Maßnahmen ergreift, welche hinreichende Garantien dafür bieten, dass der Auftragsverarbeiter seinen vertraglichen Pflichten nachkommt.

Entsprechende Risiken bestehen also – so die Ausführungen der DSK – bereits dann, wenn im Drittland Normen oder Praktiken existieren, die – gemessen an den Vorgaben der DS-GVO – zu einer unrechtmäßigen Übermittlung personenbezogener Daten verpflichten können.

Um diese Risiken auszuräumen, muss der Verantwortliche letztlich eine umfangreiche (aus zehn Prüfpunkten bestehende) Bewertung und Dokumentation des Einzelfalls durchführen, um nachweisen zu können, dass hinreichende Garantien vorgesehen werden. Interessant ist hierbei, dass ausdrücklich auf die Empfehlungen 01/2020 des Europäischen Datenschutzausschusses Bezug genommen wird, welche sich eigentlich mit einem real stattfindenden Drittlandtransfer befassen.
Wie ist unsere Einschätzung?

Vorangestellt sei zunächst, dass im Hinblick auf jede Auftragsverarbeitung die Anforderungen des Art. 28 Abs. 1 DS-GVO zu erfüllen sind. In der Norm heißt es wörtlich:

„Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.“

So stellt es eine datenschutzrechtliche Selbstverständlichkeit dar, dass der ausgewählte Auftragsverarbeiter die jeweiligen vertraglichen Anforderungen einhalten (können) muss. Der Beschluss der DSK ist nach hiesigem Dafürhalten jedoch – trotz der Regelung des Art. 5 Abs. 2 DS-GVO – insgesamt als zu weitreichend zu bewerten. Im Einzelnen:

- Unseres Erachtens wird zunächst die Regelung des Art. 48 DS-GVO, welche die europäischen datenschutzrechtlichen Anforderungen an ein Herausgabeverlangen öffentlicher Stellen außerhalb des EWR aufzeigt, nicht hinreichend berücksichtigt. Vielmehr wird gewissermaßen zulasten der verantwortlichen Stelle gefordert, dass diese nachweisen muss, dass der ausgewählte Vertragspartner nicht bewusst gegen die Vorschriften der DS-GVO verstößt. Ebenfalls wird an keiner Stelle näher auf die Regelung des Art. 28 Abs. 10 DS-GVO eingegangen, welche gerade die unrechtmäßige Datenverarbeitung durch einen Auftragsverarbeiter adressiert.
- Die verantwortliche Stelle wird zudem dazu verpflichtet – obgleich gerade kein Drittlandtransfer stattfindet – eine Prüfung der Rechtslage im Drittland durchzuführen sowie das Risiko eines unrechtmäßigen Herausgabeverlangens zu bewerten. De facto handelt es sich hierbei um eine Art „Transfer-Impact-Assessment“, obgleich sich die Daten im EWR befinden, also gerade keine Datenübermittlung stattfindet.
- Die DSK stellt ausdrückliche Anforderung zum Ergreifen angemessener technischer und/oder organisatorischer Maßnahmen auf, ohne diese für den sehr speziellen Hintergrund der lediglich theoretischen Gefahr eines Drittlandtransfers näher zu konkretisieren. Es wäre wünschenswert gewesen, wenn die DSK konkrete Empfehlungen für Unternehmen im EWR ausgesprochen hätte.

Wie sollten Unternehmen nun reagieren?

Obgleich wir die Rechtsauffassung der DSK kritisch betrachten, müssen die nunmehr beschlossenen Anforderungen natürlich beachtet werden. Wir verstehen die großen Herausforderungen für kleine und mittelständige Unternehmen, um den Anforderungen der DS-GVO und der Aufsichtsbehörden gerecht zu werden.

Unseres Erachtens muss künftig für jeden Einzelfall geprüft werden, welcher Handlungsbedarf konkret besteht. Da die DS-GVO einem risikobasierten Ansatz folgt, müssen hierbei insbesondere die Art, die Zwecke sowie der Umfang der verarbeiteten Daten berücksichtigt werden.

Marius Drabiniok, Dr. Oliver Hornung, Franziska Ladiges

Dürfen Mitbewerber bei Datenschutzverstößen klagen?

Der Europäische Gerichtshof wird demnächst die lange umstrittene Frage entscheiden, ob Verstöße gegen die Datenschutzgrundverordnung (DSGVO) auch von Mitbewerbern auf Grundlage des Gesetzes gegen den unlauteren Wettbewerb (UWG) verfolgt werden können. Diese Frage hat der Bundesgerichtshof dem EuGH mit Beschluss vom 12.01.2023 – I ZR 223/19 im Rahmen eines Vorabentscheidungsverfahrens zur Klärung vorgelegt. Hintergrund sind zwei Rechtsstreitigkeiten zwischen Apothekern rund um den Vertrieb von apothekenpflichtigen Medikamenten über Amazon (vgl. BGH-Pressemeldung Nr. 6/2023). Die Kläger argumentieren u.a., dass im Rahmen des Bestellprozesses Gesundheitsdaten der Kunden ohne Einwilligung verarbeitet würden.

Christina Kufer, Dr. Stefan Peintinger

VfGH Österreich kippt datenschutzrechtliches Medienprivileg – Auch deutsches Medienprivileg in Gefahr?

Der österreichische Verfassungsgerichtshof (VfGH) hat das österreichische Medienprivileg in einem aktuellen Urteil für verfassungswidrig erklärt. Doch was bezweckt das Medienprivileg und was bedeutet die österreichische Entscheidung für die Rechtslage in Deutschland?

Das Medienprivileg als Ausgleich zwischen Pressefreiheit und Datenschutz

Insbesondere im Rahmen investigativer Recherchen sind Journalistinnen und Journalisten oftmals darauf angewiesen, (sensible) personenbezogene Daten zu erheben und zu verarbeiten. Bei uneingeschränkter Anwendbarkeit der DSGVO, die eine Verarbeitung personenbezogener Daten nur unter strengen Voraussetzungen – z. B. bei Vorliegen der Einwilligung des Betroffenen – erlaubt, könnten Betroffene eine kritische Berichterstattung daher oftmals unter dem Deckmantel des Datenschutzrechts unterbinden. Um dies zu verhindern, wurde das sog. Medienprivileg geschaffen. Es soll Pressefreiheit und Datenschutz zum Ausgleich bringen und gewährt daher bestimmte Ausnahmen vom Datenschutzrecht bei der Verarbeitung zu journalistischen Zwecken. In dem Zusammenhang erlaubt Art. 85 DSGVO den Mitgliedsstaaten, bestimmte Abweichungen oder Ausnahmen von den Regelungen der DSGVO vorsehen.

Die Entscheidung des österreichischen VfGH zum österreichischen Medienprivileg

Nach der angegriffenen Regelung des § 9 Abs. 1 des österreichischen Datenschutzgesetzes (DSG) gelten für Datenverarbeitungen zu journalistischen Zwecken durch bestimmte Medienakteure nur wenige datenschutzrechtliche Vorschriften. Die Anwendbarkeit des DSG ist dabei komplett ausgeschlossen. In Bezug auf die DSGVO finden neben den allgemeinen Bestimmungen zu Anwendungsbereich und Definitionen lediglich die Vorschriften zu Rechtsbehelfen, Haftung und Sanktionen Anwendung. Die wesentlichen materiell-rechtlichen Grundsätze des Datenschutzes hingegen, so wie u.a. der Grundsatz der Rechtmäßigkeit der Datenverarbeitung, die Gewährleistung von Betroffenenrechten, wie z. B. Informations- und Auskunftsrechten, sowie die Pflichten der Verantwortlichen und Auftragsdatenverarbeiter auf technischen Datenschutz sind nicht anwendbar. Im Ergebnis stellt dies eine fast vollständige Ausnahme von Datenverarbeitungen durch Medienunternehmen zu journalistischen Zwecken von Datenschutzgesetzen dar.

Nach Ansicht des VfGH ist das Medienprivileg im Datenschutz entsprechend Art. 85 Abs. 2 DSGVO nötig, da sonst ein nicht auflösbarer Konflikt journalistischer Arbeit mit dem Datenschutz besteht. Das Gericht betont jedoch, dass jeder (gesetzliche) Eingriff in das Grundrecht auf Datenschutz „notwendig“ sein muss und insoweit eine Abwägung zwischen Interessen der Betroffenen am Datenschutz und der Meinungs- und Informationsfreiheit der Medien stattzufinden hat. Art. 85 Abs. 2 DSGVO spricht hier

von „Abweichungen und Ausnahmen“, die die Mitgliedsstaaten im Sinne eines Medienprivilegs vorsehen können, wenn dies „erforderlich“ ist, um Pressefreiheit und Datenschutz in Einklang zu bringen. Der VfGH führt unter Verweis auf die Rechtsprechung des EuGH aus, dass Ausnahmen und Einschränkungen in Bezug auf den Datenschutz sich auf das absolut Notwendigste zu beschränken haben.

Dies sei bei der quasi vollständigen Ausnahme der medialen Datenverarbeitungen aus dem Datenschutz, ohne zusätzliche Anforderungen an ordnungsgemäße Datenverarbeitung oder -sicherung, nicht verfassungsgemäß umgesetzt. § 9 DSG halte den vom Gericht dargestellten Anforderungen als pauschaler und undifferenzierter Ausschluss aller wesentlichen Datenschutzbestimmungen für Medien nach Ansicht des VfGH nicht stand. Die Ausnahmen vom Datenschutz für die Meinungs- und Informationsfreiheit der Medien seien auf die Bestimmungen zu begrenzen, die mit den Besonderheiten der Ausübung journalistischer Tätigkeit nicht vereinbar sind. Die pauschale Ausnahme der einschlägigen journalistischen Tätigkeit von datenschutzrechtlichen Anforderungen sei keine der Abwägung zwischen Datenschutz und Meinungs- und Informationsfreiheit genügende Umsetzung des in Art. 85 Abs. 2 DSGVO angelegten Medienprivilegs.

Neben der Verpflichtung des österreichischen Gesetzgebers zu einer Neuregelung bis Mitte 2024 schlägt der VfGH vor, als Ausgleich zum Privileg den Medienschaffenden erhöhte Anforderungen an interne Organisation, Dokumentation und technische Sicherung aufzuerlegen.

Das deutsche Medienprivileg – ein gerechter Ausgleich?

In Deutschland ist das Pendant zum österreichischen Medienprivileg insbesondere in § 12 und § 23 des Medienstaatsvertrages (MStV) geregelt. Darüber hinaus enthalten die jeweiligen Landespressegesetze entsprechende Regelungen.

Die Regelungen des MStV verpflichten Journalistinnen und Journalisten zur Einhaltung des Datengeheimnisses, wonach personenbezogene Daten nicht zu anderen als journalistischen Zwecken verarbetiet werden dürfen. Ansonsten gilt insbesondere der Grundsatz der Vertraulichkeit und Integrität zur Gewährleistung der Datensicherheit. In diesem Zusammenhang müssen die Verantwortlichen geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten, z. B. vor unbefugter oder unrechtmäßiger Verarbeitung, treffen. Der Sicherheit der personenbezogenen Daten wird dabei eine große Bedeutung zugemessen. Die Geltendmachung von Schadensersatzansprüchen durch Betroffene sowie die mögliche Verhängung von Geldbußen (Art. 82, 83 DSGVO) werden auf Verletzung des Datengeheimnisses und der vorgenannten Grundsätze begrenzt.

Insoweit sind die deutsche Regelungen des MStV zum Medienprivileg wesentlich differenzierter als die bisherige österreichische Regelung. Das deutsche Medienprivileg statuiert u.a. Anforderungen an Datensicherheit und Datenintegrität. Zudem sieht es unter bestimmten Voraussetzungen einen besonderen Auskunftsanspruch vor.

Die Regelungen lassen erkennen, dass eine Abwägung zwischen Datenschutz und Meinungs- bzw. Informationsfreiheit stattgefunden hat. Angesichts der überragenden Bedeutung der Letzteren bedarf es erheblicher Einschränkungen im Datenschutz, diesem wird jedoch angesichts der hohen technischen Anforderungen und der Betonung des Datengeheimnisses Genüge getan. Denn mit diesen Anforderungen an die journalistische Tätigkeit wird sichergestellt, dass die Medien ihren verfassungsmäßigen Auftrag effektiv wahrnehmen können und der Bürger dennoch aufgrund von Zweckbindung (Datengeheimnis) und hohen Anforderungen an die Datensicherheit vor der Gefahr des Kontrollverlusts über seine Daten geschützt ist. Das „Grundrecht auf Datenschutz“ wird insoweit nicht ausgehebelt, sondern im Lichte der Meinungs- und Informationsfreiheit auf das notwendige Minimum im Sinne des Art. 85 Abs. 2 DSGVO beschränkt.

Zu einem vergleichbaren Ergebnis kam im Juli 2021 auch das Landgericht Dresden (3 O 1965/20). Wir haben diesen Rechtsstreit u.a. über Rechtsfolgen und Umfang des datenschutzrechtlichen Medienprivilegs geführt und unsere Mandantin, ein überregionales Medienportal, erfolgreich gegen einen zivilrechtlichen Anspruch auf Schmerzensgeld verteidigt. Das Gericht betonte die Verpflichtung und den weiten Spielraum der Mitgliedstaaten, zur bzw. bei Umsetzung der Vorgaben des Art. 85 Abs. 2 DSGVO zum Schutze der Meinungs- und Informationsfreiheit. Das Landgericht Dresden bestätigte,

dass das Medienprivileg Ergebnis einer rechtskonformen Abwägung im Sinne des Art. 85 Abs. 1 DSGVO darstellt.

Es ist daher davon auszugehen, dass die deutsche Regelung des Medienstaatsvertrags zum Medienprivileg verfassungskonform ist.

Korbinian Hauf, Johanna Ludwig, Dr. Stefan Peintinger

Kopie oder nicht – Generalanwalt gibt Stellungnahme ab (Art. 15 Abs. 3 DSGVO)

Bereits seit langem ist umstritten, wie der Anspruch auf Zurverfügungstellung einer Kopie der personenbezogenen Daten nach Art. 15 Abs. 3 S. 1 DSGVO zu verstehen ist. Vielfach wird versucht diesen Anspruch zu nutzen, um an Kopien von Dokumenten zu kommen, welche anderenfalls nur kostenpflichtig zur Verfügung gestellt werden, z.B. Kontoauszüge oder Patientenakten, aber auch in arbeitsrechtlichen Auseinandersetzungen wird immer wieder um die Herausgabe der Kopie der personenbezogenen Daten gerungen.

So ist es nicht weiter verwunderlich, dass die Frage vom Österreichischem Bundesverwaltungsgericht schlussendlich dem EuGH vorgelegt worden ist (Rechtssache C-487/21). Zu dieser Frage hat sich nunmehr der Generalanwalt Giovanni Pitruzzella in seinem Schlussantrag geäußert. Erfreulicherweise fällt diese Äußerung zugunsten der Verantwortlichen aus.

Hintergrund

Nach Art. 15 Abs. 1 DSGVO hat jede betroffene Person das Recht, von dem Verantwortlich eine Bestätigung darüber zu verlangen, ob sie betreffende Daten verarbeitet werden. Sofern dies der Fall ist, sind weitergehende Auskünfte in Bezug auf diese personenbezogenen Daten zu erteilen. So weit, so klar. Interessant wird es bei Art. 15 Abs. 3 S. 1 DSGVO, wonach der Verantwortliche eine kostenfreie Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung stellen muss. Auch deutsche Gerichte haben sich mit dieser Frage schon hinreichend beschäftigt (vgl. unseren Beitrag vom 21. Juli 2021). Dahinter steht der Streit, ob eine Kopie des gesamten Dokuments, in dem die personenbezogenen Daten enthalten sind, herauszugeben ist oder lediglich die personenbezogenen Daten selbst.

Diese Frage ist keineswegs rein theoretischer Natur, da die Herausgabe von Kopien der Dokumente zum einen erheblichen Aufwand bei dem Verantwortlichen verursacht. So wird vor allem in arbeitsrechtlichen Streitigkeiten vermehrt die Herausgabe der Kopien sämtlicher E-Mails der betroffenen Person gefordert, da diese ja deren personenbezogene Daten enthalten würde. Zum anderen ist die Herausgabe von Kopien von Dokumenten zum Teil gem. AGB oder Gesetze kostenpflichtig, z.B. Patientenakte. Betroffene Personen versuchen nun durch den Anspruch nach Art. 15 Abs. 3 S. 1 DSGVO kostenfrei an diese Kopien heranzukommen.

Stellungnahme des Generalanwalts

In seinen Schlussanträgen hat sich der Generalanwalt deutlich zu dieser Frage positioniert. Nachdem er zunächst die Begriffe „Kopie“, „personenbezogene Daten“ und „Verarbeitung“ ausgelegt hat, stellt er fest,

„dass die ‚Kopie der personenbezogenen Daten eine getreue Wiedergebe dieser Daten sein muss.“

Der Verantwortliche muss danach bei seiner Zusammenstellung der personenbezogenen Daten beachten, dass diese vollständig und richtig ist. Dabei sind nicht nur die erhobenen Daten zu berücksichtigen, sondern auch selbst generierte Daten, z.B. Bewertungen.

Im weiteren Verlauf führt der Generalanwalt jedoch deutlich weiter aus:

„Da sich diese Bestimmung jedoch ausschließlich auf Kopien der personenbezogenen Daten bezieht, kann sie zum einen kein Recht auf Zugang zu Informationen begründen, die nicht als solche eingestuft werden können und verleiht zum anderen nicht – zwangsläufig – ein Recht auf Erhalt von

Kopien von Dokumenten oder anderen Trägern, die personenbezogene Daten enthalten.“

Damit hat sich zumindest der Generalanwalt klar dahingehend positioniert, dass betroffene Person kein grundsätzliches Recht auf Herausgabe von Kopien von Dokumenten aus Art. 15 Abs. 3 S. 1 DSGVO haben. Der Generalanwalt betont jedoch auch, dass es Ausnahmen von diesem Grundsatz geben kann, wenn z.B. im Einzelfall die Herausgabe erforderlich ist, um die Verständlichkeit der herausgegebenen Daten herzustellen. Dann kann es auch erforderlich sind, vollständige Dokumente oder Auszüge aus einer Datenbank zu übermitteln.

In seinem Schlussantrag stellt der Generalanwalt ferner klar, dass nach seiner Ansicht Art. 15 Abs. 3 S.1 DSGVO kein eigenständiges Recht begründet, sondern lediglich das Recht aus Art. 15 Abs. 1 konkretisiert. Dies ist am Ende stimmig zu seiner Auffassung, dass grundsätzlich keine Kopien herauszugeben sind.

Praxishinweis

Die Schlussanträge des Generalanwalts bringen endlich Klarheit in eine seit Jahren diskutierte Frage und erhebliche Erleichterung für Verantwortliche. Es jedoch dennoch weiterhin darauf zu achten, dass personenbezogenen Daten vollständig herausgegeben werden. Dies kann insbesondere bei der Verarbeitung in verschiedenen Systemen noch immer zu einem erheblichen Aufwand führen. In diesem Zusammenhang sollte auch immer geprüft werden, ob die Herausgabe mit Blick auf § 34 Abs. 1 BDSG zum Teil verweigert werden kann.

Dennoch sollten Verantwortliche vor allem die Entscheidung des EuGHs in der Sache selbst abwarten bevor eventuell bestehende Prozesse umgestellt werden. Zwar folgt der EuGH mitunter dem Schlussantrag des Generalanwalts, sicher ist dies jedoch keinesfalls. Im vorliegenden Fall bleibt für die Verantwortlichen nur zu hoffen, dass der EuGH die Schlussanträge ebenfalls überzeugend findet. Bis dahin sollten Verantwortliche abwägen, welche Unterlagen sie den betroffenen Personen herausgeben.

Franziska Ladiges

Einsatz von Videoüberwachungsanlagen unter datenschutzrechtlichen Gesichtspunkten

Vertrauen ist gut, Kontrolle ist besser?

Videoüberwachung ist in Mode. Eine Vielzahl von Unternehmen setzt bei dem hauseigenen Sicherheitskonzept auf den Einsatz von mehr oder minder umfangreichen Videoüberwachungsanlagen. Der Grund hierfür ist plausibel und kann ohne Weiteres nachvollzogen werden: Während eine (erkennbare) Videoüberwachungsanlage bereits eine gewisse präventive „Abschreckung“ gewährleisten kann, können auch Straftaten oder sonstige Fehlverhalten schnell und einfach aufgedeckt werden. Aber ist dies datenschutzrechtlich unproblematisch?

Der folgende Beitrag soll einen ersten Überblick über typische datenschutzrechtliche Fallstricke bei dem Einsatz von Videoüberwachungsanlagen liefern. Dabei wird – da eine Vielzahl weiterer „Ausnahmefälle“ in Betracht kommt – zunächst der „typische“ Einsatz einer Videoüberwachungsanlage auf dem Betriebsgelände eines Unternehmens beleuchtet.

Bereits an dieser Stelle sei der Hinweis erlaubt, dass der Einsatz einer Videoüberwachungsanlage – zumindest nach unserer Erfahrung – im absoluten Fokus der Aufsichtsbehörden steht, da es hier immer wieder zu Beschwerden betroffener Personen kommt. Auch dies ist nachvollziehbar, da Videoaufzeichnungen – je nach deren Verwendung – zu sehr einschneidenden Folgen für die betroffenen Personen führen können.

Rahmenbedingungen

Unternehmen haben natürlich den nachvollziehbaren Wunsch, das eigene Betriebsgelände sowie ggf. Mitarbeiter und/oder Kunden im Wege einer Videoüberwachungsanlage zu schützen. Hierbei muss jedoch eine Vielzahl datenschutz- sowie arbeitsrechtlicher Aspekte beachtet werden.

In einem ersten Schritt sollte stets geprüft werden, zu welchen konkreten Zwecken die Videoüberwachungsanlage eingesetzt werden soll. Geht es bspw. (nur) um den Schutz des eigenen Betriebsgeländes oder sollen (zumindest auch) weitergehende Zwecke verfolgt werden? So müssen bspw. strenge arbeitsrechtliche Kriterien berücksichtigt werden, sofern Mitarbeiter – bei Vorliegen konkreter Verdachtsmomente – beim Begehen einer Straftat überführt werden sollen. Erst wenn der Anwendungsbereich der Videoüberwachungsanlage eindeutig definiert wurde, kann in eine konkrete datenschutzrechtliche Prüfung eingestiegen werden.

Grundsätzlich sollten Unternehmen – bevor eine Videoüberwachungsanlage implementiert wird – genauestens prüfen und festhalten, welcher Anlass für diese Maßnahme besteht. Kam es bspw. bereits zu Einbrüchen, Diebstählen oder sonstigen einschneidenden Fehlverhalten? Etwas „einfacher" ist die Begründung ggf. im Falle besonders sensibler Unternehmen, welche aufgrund hochwertiger Waren oder deren Einstufung als kritische Infrastruktur häufiger als Zielobjekte für Angriffe Dritter herhalten müssen. Jedenfalls muss der Grund der Videoüberwachung bekannt sein und entsprechend dokumentiert werden.

Umfang der Videoüberwachung

Beim Thema Videoüberwachung sollte zunächst der Grundsatz „Weniger ist Mehr" berücksichtigt werden. Nach den Anforderungen der Aufsichtsbehörden muss jede vorgesehene Videokamera einen messbaren Beitrag zu dem verfolgten Sicherheitskonzept leisten (können). Hierbei müssen also der Standort der Kameras, deren genaue Einsatzzeiten sowie die technischen Funktionalitäten der jeweiligen Kameras geprüft werden.

Während Audioaufnahmen zu deaktivieren sind, da diese bis hin zu strafrechtlichen Konsequenzen führen können, sollten auch weitergehende Funktionen, wie etwa manuelle oder automatische Zoom- und/oder Schwenkfunktionen, genauestens begründet werden. Hier sollte sich stets die Frage gestellt werden: Warum sind Kameras mit fest definierten Erfassungsbereichen nicht ausreichend, um den jeweils verfolgten Zweck zu erreichen?

Auch sollte besonders gründlich geprüft werden, aus welchen Gründen bspw. ein Live-Monitoring erfolgt. Sofern der Zweck verfolgt wird, Beweismittel für das Verfolgen von Straftaten bereithalten zu können, ist ein Live-Monitoring offensichtlich vollkommen ungeeignet. Geht es demgegenüber (bspw. im medizinischen Bereich) um die Bereitstellung einer schnellen Hilfe im Falle von Notfällen, kann diese Bewertung wieder anders ausfallen. Merken sollten Sie sich jedenfalls, dass der Einsatz eines Live-Monitorings grundsätzlich als schwererer Eingriff in das Persönlichkeitsrecht der Betroffenen angesehen wird, als die „bloße" Aufzeichnung.

Übrigens: Nach dem Meinungsbild der Aufsichtsbehörden müssen Videoaufzeichnungen – sofern keine Besonderheiten vorliegen – grundsätzlich nach 72 Stunden (bestenfalls durch automatisiertes Überschreiben) gelöscht werden.

Um der Nachweispflicht gemäß Art. 5 Abs. 2 DS-GVO nachkommen zu können, ist es daher unerlässlich, dass ein Lageplan erstellt wird, welcher sämtliche Kameras sowie deren konkrete Erfassungsbereiche festhält. Zudem ist es aus unserer Sicht ebenfalls sinnvoll, eine zusätzliche Auflistung sämtlicher (oder zumindest ausgewählter) Kameras zu erstellen, in welcher der konkrete Zweck der jeweiligen Kameras dokumentiert wird. Um keinerlei Angriffsfläche offen zu lassen, sollte die gesamte Anlage – da voraussichtlich ohnehin eine Datenschutz-Folgenabschätzung durchzuführen ist – mit einer umfassenden Systembeschreibung versehen werden, welche sämtliche technischen und organisatorischen Aspekte aufzeigt.

Nur sofern die vorgesehene Videoüberwachungsanlage in deren Gesamtheit betrachtet wird, kann bspw. geprüft werden, ob eine (unumkehrbare) Verpixelung solcher Aufnahmen erforderlich ist, welche „über das Betriebsgelände hinaus" angefertigt wurden.

Gebot der Transparenz

Dass eine verdeckte Videoüberwachung – sofern sie überhaupt zulässig ist – zu erheblichen datenschutzrechtlichen Risiken führen kann, sollte bekannt sein. Als ein wichtiger Bestandteil der Datenschutz-Compliance muss daher eine ordnungsgemäße Beschilderung auf dem eigenen

Betriebsgelände angesehen werden. Letzteres umso mehr, da dieser Umstand letztlich jeder Person offen erkennbar ist und daher – im wahrsten Sinne des Wortes – als „Aushängeschild“ der ergriffenen Maßnahmen anzusehen ist.

Im Falle einer Videoüberwachungsanlage wird regelmäßig ein 2-stufiges Vorgehen vorgeschlagen, welches zwischen einer vorläufigen und einer umfassenden Information differenziert. Während zunächst die „Eckdaten“ des Art. 13 DS-GVO für jede betroffene Person erkennbar sein müssen, kann für weitergehende Informationen (bspw. betreffend die Ausübung von Betroffenenrechten) etwa auf einen QR-Code zurückgegriffen werden. Wichtig ist jedoch in jedem Fall, dass betroffene Personen diese Informationen in Erfahrung bringen können, bevor diese einen von der Videoüberwachung erfassten Bereich betreten. Für das Bereithalten der umfassenden Informationen schlagen wir zudem regelmäßig vor, zumindest an einem „markanten“ Ort des Betriebsgeländes eine umfassende Beschilderung vorzusehen, um bspw. auch Personen, welche über kein Smartphone verfügen, eine Information zu ermöglichen.

Vorliegen einer Rechtsgrundlage

Weiter sollten sich Unternehmen die konkrete Frage stellen, auf welche Rechtsgrundlage die Videoüberwachung gestützt werden kann. Während in vielen Fällen die Interessenabwägungsklausel des Art. 6 Abs. 1 lit. f) DS-GVO herangezogen werden kann, sollte für Mitarbeiter regelmäßig der Abschluss einer Betriebsvereinbarung im Sinne des § 26 Abs. 4 BDSG als datenschutzrechtliche Rechtsgrundlage in Erwägung gezogen werden. Dies umso mehr, da § 87 Abs. 1 Nr. 6 BetrVG ohnehin die Einbindung des Betriebsrats voraussetzt.

Eine datenschutzrechtliche Einwilligung wird in diesen Fällen – losgelöst von ohnehin bestehenden Problemen im Beschäftigtendatenschutz – regelmäßig ungeeignet sein, da der Einsatz der Videoüberwachungsanlage gerade nicht vom Einverständnis der betroffenen Personen abhängig sein soll.

Schutz der Videoaufzeichnungen

Letztlich müssen – wie auch sonst – die Anforderungen des Art. 32 DS-GVO beachtet werden, welche die verantwortliche Stelle zum Ergreifen angemessener technischer und organisatorischer Maßnahmen verpflichtet. Hierbei muss insbesondere geprüft werden, wer, wann und in welchem Umfang eine Zugriffsmöglichkeit auf die Videoaufnahmen hat. Zudem muss sichergestellt sein, dass die Videoüberwachungsanlage in einer (technisch) sicheren Umgebung vorgesehen wird, welche eine dem aktuellen Stand der Technik entsprechende Verschlüsselung der Daten sowie der jeweiligen Kommunikationswege vorsieht. Werden Sicherheitsdienstleister oder sonstige (IT-)Dienstleister eingesetzt, muss zudem geprüft werden, ob ein Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO abzuschließen ist. Um die ganze Sache unnötig komplizierter zu machen, können auch Fragen des Drittlandtransfers im Sinne der Art. 44 ff. DS-GVO zu berücksichtigen sein, sofern zur Speicherung der Daten eine (internationale) Cloud genutzt wird.

Sie sehen recht schnell, dass der Einsatz von Videoüberwachungsanlagen gründlich geprüft und von „Profis“ zumindest gegengecheckt werden sollte.

Praxishinweis

SKW Schwarz berät eine Vielzahl von Unternehmen bei der Planung und dem Einsatz von Videoüberwachungsanlagen. Aufbauend auf unserer Erfahrung haben wir für nahezu jede denkbare Situation ein entsprechendes Muster-Dokument vorliegen. Dies umfasst insbesondere

- Betriebsvereinbarungen und/oder Richtlinien für den Einsatz von Videoüberwachung
- Datenschutzhinweise für Beschäftigte sowie Muster für eine Beschilderung
- Muster für eine Datenschutz-Folgenabschätzung, welche gerade auf den Einsatz einer Videoüberwachungsanlage ausgerichtet sind

Marius Drabiniok, Dr. Oliver Hornung, Alexander Möller, Michael Wahl

Digital Regulation

Der Digital Services Act – Revolution für Vermittlungsdienste?

Der Digital Services Act wird die rechtlichen Rahmenbedingungen für jede Art von Vermittlungsdienst im Internet nachhaltig verändern. Zwar bleiben die grundlegenden Haftungsregeln bestehen. Die vielen Sorgfalts- und Transparenzpflichten, die alle Bereiche des unternehmerischen Handelns betreffen und bereits bei der technischen Gestaltung der Dienste ansetzen, werden bei Anbietern jedoch zu einem spürbaren organisatorischen Mehraufwand führen. Auch die AGB der Dienste werden in vielen Fällen mit dem DSA in Einklang zu bringen sein. Es ist deshalb für alle betroffenen Unternehmen unumgänglich, sich frühzeitig mit den notwendigen Anpassungen im Detail auseinanderzusetzen.

Dr. Christoph Krück, Johannes Schäufele

Hinweisgeberschutzgesetz

Hinweisgeberschutz – neuer Anlauf zur Umsetzung der Richtlinie

Nachdem am 10. Februar 2023 der Gesetzesentwurf zum Hinweisgeberschutzgesetz an der Zustimmung des Bundesrats gescheitert war, musste dringend eine Alternativlösung her (siehe hierzu auch unseren Webseitenbeitrag).

Statt der von vielen Beobachtern erwarteten Anrufung des Vermittlungsausschusses, haben die Regierungsparteien einen anderen Weg gewählt. In Anbetracht des laufenden Vertragsverletzungsverfahrens vor dem Europäischen Gerichtshof ist es jedoch nicht weiter verwunderlich, dass die Regierung eine schnelle Lösung bevorzugt.

Um eine zeitnahe Umsetzung der Richtlinie zu gewährleisten, wurde der bestehende Gesetzesentwurf in zwei Entwürfe gesplittet – Entwurf eines Gesetzes für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden und Entwurf eines Gesetzes zur Ergänzung der Regelungen zum Hinweisgeberschutz. Die wesentlichen Regelungen des ursprünglichen Entwurfs sind nunmehr getrennt von den zustimmungspflichtigen Aspekten.

Die wichtigsten Regelungen im Überblick

Um die Zustimmungspflicht des Bundesrats für den neuen Entwurf zu vermeiden, wurden Beamte und Richter der Länder, Gemeinden, Landeskörperschaften und öffentliche Anstalten der Länder aus dem persönlichen Anwendungsbereich des Gesetzes herausgenommen. Damit berührt der Gesetzentwurf nicht mehr die Belange der Länder und eine Zustimmung des Bundesrats nach Art. 74 Abs. 2 GG ist nicht mehr erforderlich. Ob sich die Zustimmungspflicht dennoch aus z.B. Art. 84 Abs. 1 ergeben könnte, ist derzeit offen.

Inhaltlich gibt es keine wesentlichen Änderungen im Vergleich zum Gesetzesentwurf aus dem letzten Jahr. Insbesondere die Regelungen, an welchen die Zustimmung des Bundesrats gescheitert ist, finden sich weiterhin im nunmehr wohl nicht zustimmungspflichtigen Gesetzentwurf:

Unternehmen mit mehr als 249 Mitarbeitern müssen umgehend interne Meldekanäle einrichten, welche eine mündliche Meldung oder Meldung in Textform ermöglichen. Für Unternehmen ab 50 Mitarbeitern gilt diese Pflicht ab 17. Dezember 2023. Ab dem 1. Januar 2025 muss auch die Abgabe anonymer Meldungen und deren anschließende Bearbeitung unter Wahrung der Anonymität des Hinweisgebers möglich sein. Weiterhin ist im Gesetzesentwurf die Vermutung enthalten, dass anschließende Repressalien mit der Meldung im Zusammenhang stehen. Sofern ein Unternehmen keine internen Meldekanäle einrichtet, droht nicht nur die Nutzung von externen Meldekanälen, sondern auch die Verhängung eines Bußgeldes. Die Bußgeldpflicht tritt allerdings erst 6 Monate nach Verkündung des Gesetzes in Kraft. Schließlich sind weiterhin Verstöße gegen nationale Strafvorschriften und bestimmte Ordnungswidrigkeiten von dem Gesetz erfasst. Weiterhin ermöglicht der deutsche Gesetzgeber jedoch die Nutzung eines Meldekanals im Konzern und ignoriert damit die

Stellungnahmen der EU-Kommission (wir berichteten).

Damit sind Kritikpunkte des Bundesrats nicht aufgegriffen worden. Insbesondere die vermutete Benachteiligung bei Repressalien nach einer Meldung und die Bußgeldvorschriften sind so in der EU-Richtlinie nicht vorgesehen und belasten deutsche Unternehmen damit mehr als andere europäische Unternehmen. Im Hinblick auf die Ermöglichung der anonymen Meldung müssen Unternehmen auf IT-basierte Systeme zurückgreifen, welche Kosten verursachen.

Wie geht es weiter?

Aktuell ist geplant, dass das Hinweisgeberschutzgesetz bereits am 30. März 2023 im Bundestag verabschiedet werden soll. Dies dürfte mit den Stimmen der Regierungsparteien auch gelingen. Rechnet man eine Woche für die Veröffentlichung des Gesetzes im Bundesgesetzblatt sowie einen Monat für den Termin des Inkrafttretens, so kann mit großer Wahrscheinlichkeit davon ausgegangen werden, dass das Hinweisgeberschutzgesetz bereits im Mai 2023 in Kraft treten wird.

Fazit

Unternehmen, welche noch über kein Hinweisgebersystem verfügen, sollten sich dringend mit dem neuen Entwurf des Hinweisgeberschutzgesetzes auseinandersetzen. Die Tatsache, dass das Gesetz mit großer Wahrscheinlichkeit bereits im Mai 2023 in Kraft treten wird, macht ein schnelles Handeln erforderlich. Auch Unternehmen ab 50 Mitarbeitern müssen ab 17. Dezember 2023 entsprechende Meldekanäle vorhalten. In diesem Zusammenhang sollten Unternehmen insbesondere auch berücksichtigen, dass die Implementierung des Hinweisgebersystems mit zahlreichen rechtlichen sowie technischen und organisatorischen Fragen verbunden sein kann.

Dr. Oliver Hornung, Franziska Ladiges, Alexander Möller

Bundesrat verweigert Zustimmung zum Hinweisgeberschutzgesetz

Am 16. Dezember 2022 hatte der Bundestag das lang erwartete Hinweisgeberschutzgesetz beschlossen (wir berichteten). Am heutigen Tage, 10. Februar 2023, sollte nun der Bundesrat dem Gesetz zustimmen. Trotz laufenden Vertragsverletzungsverfahren der EU-Kommission hat der Bundesrat seine Zustimmung zum Hinweisgeberschutzgesetz nicht erteilt. Damit ist das Gesetz vorerst gescheitert und kann nicht wie geplant im April 2023 in Kraft treten.

Warum keine Zustimmung?

Kritikpunkt war vor allem die hohe wirtschaftliche Belastung von kleinen und mittelständischen Unternehmen in wirtschaftlich schwierigen Zeiten. Die Vertreter aus Hessen und Bayern kritisierten u.a. den zu weiten sachlichen Anwendungsbereich des Gesetzes, welcher weit über die EU-Vorgaben hinausgehen würde. Ferner würde die geforderte Möglichkeit der anonymen Hinweisabgabe dazu führen, dass IT-basierte Lösungen eingeführt werden müssen, welche weitere Kosten in den Unternehmen zur Folge hätten. Auch die mögliche Geldbuße von bis zu 20.000 Euro bei Nichteinführung eines internen Meldekanals stieß auf Widerstand, da eine solche Konsequenz von der EU-Richtlinie nicht gefordert sei und es in diesem Fall externe Meldekanäle geben würde. Schließlich stieß auch die Vermutung, dass eine Repressalie gegen einen Hinweisgeber aufgrund dessen Hinweis erfolge, auf Unverständnis. Diese Beweislastverteilung würde zu Missbrauch führen, indem Mitarbeitern, denen eine Kündigung droht, das Hinweisgebersystem nutzen und sich damit in eine bessere Position bringen.

Ausblick

Insgesamt sind die Kritikpunkte im Sinne der Unternehmen gut nachzuvollziehen. Aufgrund der nichterteilten Zustimmung des Bundesrats haben die Unternehmen jedoch weiterhin keine richtige Orientierung, was bei der Einführung einer Hinweisgeberlösung zu beachten ist.

Es steht zu erwarten, dass der Bundestag nunmehr den Vermittlungsausschuss anrufen wird. Dort wird man versuchen einen inhaltlichen Kompromiss zu finden, um das Gesetz durch entsprechende

Änderungen zustimmungsfähig zu machen. Dieser Prozess wird jedoch weitere Zeit in Anspruch nehmen. Unternehmen sind dennoch gut beraten sich bereits jetzt nach Lösungen umzusehen und Angebote einzuholen.

Dr. Oliver Hornung, Franziska Ladiges, Alexander Möller

Branded Content

LG München I stuft § 25 TTDSG als Datenschutzvorschrift ein und eröffnet Verbrauchern Auswahlmöglichkeiten bei Cookie-Bannern im Rahmen des UKlaG

Das LG München I hat am 29. November 2022 ein Urteil hinsichtlich der Zulässigkeit der Speicherung von Cookies in Endgeräten von Webseitennutzern erlassen (Az. 33 O 14776/19). Geklagt hatte ein Verbraucherschutzverein gegen die Anbieterin und Betreiberin eines bekannten online Nachrichtenportals.

Das Urteil ist aus zwei Gründen für die Praxis sehr relevant. Zum einen hat das Gericht § 25 Telekommunikation-Telemedien-Datenschutz-Gesetz („TTDSG“) als Verbraucherschutzgesetz eingestuft. Zum anderen hat das Gericht zur praktischen Gestaltung von sog. Cookie-Bannern entschieden.

1. § 25 TTDSG als Verbraucherschutzgesetz

Das LG München I hat festgestellt, dass es sich bei § 25 TTDSG um ein Verbraucherschutzgesetz im Sinne des § 2 Abs. 2 S. 1 Nr. 11 UKlaG handelt. Es ist zwar allgemein umstritten, ob das Wettbewerbsrecht auf Datenschutzvorschriften nach der Datenschutz-Grundverordnung („DSGVO“) Anwendung finden kann, aber § 25 TTDSG steht gesetzessystematisch neben der DSGVO. Das TTDSG geht nicht auf die DSGVO zurück, sondern auf die ePrivacy-RL.

§ 25 TTDSG sei als Datenschutzvorschrift vom Anwendungsbereich des § 2 Abs. 2 S. 1 Nr. 11 UKlaG umfasst. Das TTDSG regelt u.a. den Schutz personenbezogener Daten. Ferner enthalte das TTDSG eine verbraucherschützende Komponente, da es zumindest auch um die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten von natürlichen Personen in ihrer Eigenschaft als Verbraucher durch Unternehmen als Teil des Marktes gehe.

Nach den Feststellungen des LG München I stellt es einen Verstoß gegen § 25 TTDSG dar, wenn der Betreiber einer Webseite veranlasst, dass Cookies auf dem Endgerät des Nutzers gespeichert und im Anschluss zum sog. „Tracking“ des Nutzers genutzt werden, ohne zuvor eine wirksame Einwilligung des Nutzers einzuholen. Die Einwilligung sei insbesondere nur dann wirksam, wenn sie freiwillig erteilt worden ist.

2. Gestaltung von Cookie-Bannern

Das LG München I hat zu der praktisch hochrelevanten Frage hinsichtlich der Gestaltung von Cookie-Bannern ausgeführt, dass eine Einwilligung dann nicht freiwillig sei, wenn es auf der ersten Ebene des Cookie-Banners nur zwei Optionen zur weiteren Webseitennutzung gebe:

Entweder eine umfassende Einwilligung erteilen oder über die Schaltfläche „Einstellungen“ auf eine zweite Ebene zu gelangen.

Von Freiwilligkeit könne nur dann die Rede sein, wenn ein Nutzer tatsächlich eine Wahlmöglichkeit habe, also auch ohne Nachteile auf die Erteilung der Einwilligung verzichten kann. Bereits der Umstand, dass ein Nutzer die Webseite der Beklagten nicht ohne weitere Interaktion mit der Consent Management Platform nutzen könne, spricht gegen eine freiwillige Entscheidung.

Aufgrund des Webseitenaufbaus der Beklagten war dies hier nicht der Fall. Ein Nutzer musste zunächst die Schaltfläche „Einstellungen“ betätigen, um eine gesonderte Auswahl bzgl. seiner Einwilligung treffen zu können. Selbst dieser verhältnismäßig geringe Aufwand sei nach dem LG München I bereits erheblich. Das Internet lebe von seiner Schnelligkeit und Nutzer seien daher

grundsätzlich weniger aufmerksam. Hinzu komme, dass die Schaltfläche „Akzeptieren“ auf der ersten Ebene des Cookie-Banners blau hervorgehoben war, was dem jeweiligen Nutzer signalisiere, dass das bloße Akzeptieren ohne Auswahlmöglichkeit den „schnelleren“ Weg zur eigentlichen Webseite darstelle.

Praktische Relevanz

Das Urteil des LG München I ist ohne Wenn und Aber ein Paukenschlag, der eine hohe praktische Relevanz hat.

Die Anforderungen an die rechtssichere Gestaltung von Cookie-Bannern sind hoch. Zudem könnte in der Zukunft § 25 TTDSG auch als Marktverhaltensregelung nach § 3a UWG eingestuft werden, wodurch ggf. auch Konkurrenten einen entsprechenden Wettbewerbsverstoß möglicherweise verfolgen könnten (vgl. hier den Vorlagebeschluss des BGH vom 12.01.2023, Az. I ZR 223/19, an den EuGH zum Verhältnis der DSGVO zum UWG).

Wahrscheinlich werden viele Webseitenanbieter ihre Cookie-Banner anpassen müssen. Nach dem LG München I genügt es nicht mehr, wenn auf der ersten Ebene des Cookie-Banners lediglich zwei Schaltflächen vorhanden sind: „Akzeptieren“ oder „Einstellungen“. Eine weitere Auswahl über die Schaltfläche „Einstellungen“, auf der (mindestens) zweiten Ebene des Cookie-Banners ist nach dem LG München I nicht zulässig.

Zum einen sollte es wohl auf der ersten Ebene weitere Auswahlmöglichkeiten geben, z. B. eine Schaltfläche mit dem Inhalt „Abbrechen“ oder „Weiter nur mit unbedingt erforderlichen Cookies“.

Zum anderen ist unklar, wie viel Auswahl auf der ersten Ebene des jeweiligen Cookie-Banners tatsächlich möglich sein muss. Bei strenger Auslegung des Urteils könnte sich die Frage stellen, ob alle nicht unbedingt erforderlichen Cookies auf der ersten Ebene des Cookie-Banners bei Webseiten zur Auswahl angezeigt werden müssten. Gerade bei einer Vielzahl solcher Cookies / Tracker / Identifiern dürfte dies ziemlich unübersichtlich werden, insbesondere auf kleineren Display (wie z. B. auf Smartphones).

Dr. Stefan Peintinger

Müssen Corporate Influencer ihre Posts als Werbung kennzeichnen?

Corporate Influencer sind nach wir vor DAS Trendthema im Influencer Marketing. Mehr und mehr Unternehmen erkennen den Vorteil des Einsatzes von Mitarbeitern, welche als Firmenbotschafter eingesetzt werden. Diese ergänzen die klassische Unternehmenskommunikation und helfen ihren Arbeitgebern durch ihre Persönlichkeit, die gewünschte Zielgruppe zu erreichen.

Wie steht es jedoch mit den Kennzeichnungspflichten von Posts von Corporate Influencern? Sind diese genauso wie bei klassischen Influencern mit WERBUNG oder ANZEIGE zu kennzeichnen?

Auch bei den Posts von Corporate Influencern handelt es sich regelmäßig um geschäftliche Handlungen. Bereits vor der UWG-Novelle stand fest: auch Corporate Influencer müssen deshalb ihre Posts entsprechend als Werbung kenntlich machen. Denn festzuhalten ist, dass die Corporate Influencer in der Absicht handeln das Unternehmen zu fördern und dafür durch ihr Gehalt auch eine Gegenleistung erhalten. So sollten auch die Unternehmen sicherstellen, dass ihre Mitarbeiter ihren Pflichten nachkommen, da sonst eine eigene Haftung droht.

Leider weiterhin unklar ist, wie die Kennzeichnung erfolgen muss. Während sich für klassische Influencer eine Kennzeichnung mit WERBUNG oder ANZEIGE in der Rechtsprechung durchgesetzt hat, ist dies für Corporate Influencer in Ermangelung eines Urteils noch völlig unklar. In der Praxis bilden sich daher unterschiedliche Formen der Kennzeichnung aus. Ob jedoch Bezeichnungen wie „Unternehmensbotschafter“, „Social Media Manager(in)“ oder Formulierungen wie „mein Arbeitgeber“ von den Gerichten als ausreichend erachtet werden, ist leider noch offen. Bis diese Unsicherheiten beseitigt werden, ist daher anzuraten, dem Transparenzgebot so gut es geht nachzukommen.

Margret Knitter