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

Niederlassung Böblingen:
Otto-Lilienthal-Straße 36
71034 Böblingen
Tel: 07031 7145660

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

IT-Ticker 01/2022

Der IT-Ticker 01/2022 informiert Sie über folgende Themen:

Die neuen EVB-IT Cloud stehen seit dem 02.03.2022 zur Verfügung

Einführung

Das Bundesministerium des Innern und für Heimat (BMI) hat am 02.03.2022 die vertraglichen Grundlagen für die Vergabe von Cloud-Leistungen durch die öffentliche Verwaltung veröffentlicht. Grundlage hierfür war der Beschluss des IT-Planungsrates vom 11.02.2022 (Beschluss 2022/01). Der IT-Planungsrat nahm die EVB-IT Cloud zur Kenntnis und empfahl seinen Mitgliedern die Nutzung der EVB-IT Cloud.

Somit stehen erstmalig standardisierte Einkaufsbedingungen für Cloudleistungen zur Verfügung. Berücksichtigt sind u.a. Leistungsqualität, Daten- und IT-Sicherheit sowie Kontrollrechte bei der Nutzung von Cloudleistungen. Damit ist eine große Lücke geschlossen worden.

Die EVB-IT Cloud erweitern die zehn bestehenden EVB-IT für IT-Beschaffungen öffentlicher Auftraggeber. Die öffentliche Hand muss Vergaberecht anwenden. Das wirkt sich auf Einkauf und Vertragsgestaltung aus. Ab bestimmten Schwellenwerten ist das EU-Vergaberecht einschlägig (4. Teil des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) sowie Vergabeverordnung – VgV). Unterhalb der Schwellenwerte gelten über Haushaltsrecht ähnliche Vorschriften. In vielen Fällen stellen die im BGB (Bürgerliches Gesetzbuch) vorgesehenen Vertragstypen keine geeignete Grundlage für die Beschaffung von IT-Dienstleistungen und Lieferungen dar. Um den Bedarf an Verträgen bei Standardfällen in der IT-Beschaffung zu decken, sind die Ergänzenden Vertragsbedingungen (EVB-IT) entwickelt worden. Mit den EVB-IT Verträgen können einerseits oft nicht alle Besonderheiten des Einzelfalles abgedeckt werden. Andererseits sind viele Textbereiche im Einzelfall nicht einschlägig und sollten gelöscht werden, damit man die Übersicht behält. In der Praxis sind öffentlicher Auftraggeber und der Auftragnehmer daher gut beraten, genau zu prüfen ob und ggf. welche EVB-IT für die konkrete Leistung passend und angemessen sind. Auch wenn sich die Parteien gegen eine Nutzung der EVB-IT Verträge entscheiden, können diese in jedem Fall als „Check-Liste“ für einen individuellen Vertrag verwendet werden. EVB-IT eignen sich grundsätzlich gut für vergaberechtliche Verhandlungsverfahren.

Anwendungsbereich

Die EVB-IT Cloud sind für die Beschaffung von Cloudleistungen erarbeitet worden. Diese können bei der Beschaffung unterschiedlicher Lösungen wie Infrastructure as a Service (IaaS), Plattform as a Service (PaaS), Software as a Service (SaaS) und Managed Cloud Services (MCS) genutzt werden. Im Hinblick auf Fragen der IT-Sicherheit stellt Ziff. 1.2. der EVB-IT Cloud-AGB klar, dass der Auftragnehmer die Leistungen unter Einhaltung des bei Vertragsschluss geltenden Cloud Computing Compliance Criteria Catalogue (Kriterienkatalog C5) erbringt.

Die EVB-IT Cloud beinhalten zunächst ein Vertragsmuster (EVB-IT Cloudvertrag). Der Vertrag bindet die EVB-IT Cloud-AGB i.d.R. mit ein. Die EVB-IT Cloud enthalten die Basisregelungen für die Leistungserbringung und bilden den Kern der EVB-IT Cloud. Bei Bedarf können auch die weiteren EVB-IT Cloud Dokumente, wie der „Kriterienkatalog für Cloudleistungen“ sowie die „Anlage auftragnehmerseitiger AGB“ mit einbezogen werden, vgl. Ziff. 1.2.1 des Vertragsmusters.

Der „Kriterienkatalog für Cloudleistungen“ bietet die Möglichkeit, differenzierte Vorgaben für die konkreten Cloudleistungen zu machen und von den Regelungen in den EVB-IT Cloud-AGB abzuweichen oder über diese hinauszugehen. Zudem bietet der Kriterienkatalog die Möglichkeit, in Bezug auf konkrete Leistungs- und Regelungsbereiche, auf weitere auftraggeberseitige Anlagen sowie gezielt auf einzelne Regelungen in auftragnehmerseitigen AGB zu verweisen.

Die sonstigen EVB-IT Verträge verfügen nicht über Anlagen wie der „Anlage auftragnehmerseitige AGB“. Die „Anlage auftragnehmerseitige AGB“ - bestehend aus Anhang I und II - soll eine Öffnung der EVB-IT Cloud für auftragnehmerseitige AGB ermöglichen. Aufgrund des hohen Standardisierungsgrades von Cloudleistungen kann es je nach Leistungsgenstand erforderlich sein, diese AGB von Cloudanbietern partiell einzubeziehen. Anhang I ermöglicht dabei eine nachrangige Einbeziehung der Gesamtheit der auftragnehmerseitigen AGB. Anhang I kann als Alternative zu Ziff. 1.2.4 des EVB-IT Cloudvertrages genutzt werden der ebenfalls die Möglichkeit vorsieht, auftragnehmerseitige AGB einzubeziehen. Anhang II sieht daneben eine auf einzelne Klauseln bezogene vorrangige Einbeziehung auftragnehmerseitiger AGB vor. Der EVB-IT Cloudvertrag sieht eine solche Möglichkeit selbst nicht vor. Somit kann eine vorrangige Einbeziehung nur anhand der „Anlage auftragnehmerseitige AGB“ erfolgen.

Die Hinweise zur Nutzung unterstützen bei der Anwendung und beim Ausfüllen der EVB-IT Cloud.

Evaluierung der EVB-IT Cloud nach 18 Monaten

Die EVB-IT Cloud sollen 18 Monate nach der Veröffentlichung einer erneuten Prüfung unterzogen werden und ggf. angepasst werden. Erfahrungen und Anregungen können dabei an DGI5@bmi.bund.de übermittelt werden.
Zusammenfassung

Auftraggeber sollten die EVB-IT vor der Ausschreibung prüfen, ob die EVB-IT als Grundlage bei IT-Ausschreibungen geeignet sind. Falls die EVB-IT als geeignet erscheinen, sollten nicht benötigte Textteile vom Auftraggeber gelöscht werden, damit die Textmenge reduziert wird. Alternativ kann es durchaus sinnvoll sein einen individuellen, passgenauen Vertrag für die Ausschreibung zu erstellen. Etwas Vorbereitung zahlt sich gerade im Streitfall aus. Wichtig sind auch suffiziente Anpassungsklauseln bei Leistungs- und Kostenänderungen.

Bieter/Auftragnehmer sollten sich auf die EVB-IT einstellen und dabei genau prüfen, ob Vorgaben sinnvoll gemacht worden sind. Unklarheiten müssen per Bieterfragen frühzeitig adressiert werden. Dabei sollte man der Vergabestelle schon konkrete Antwortvorschläge machen und eine „goldene Brücke“ bauen. Unsinnige bzw. rechtswidrige Vorgaben müssen (freundlich) gerügt werden, sonst kann man sich später nicht mehr auf diese Punkte berufen.

Dr. Karin Deichmann | René M. Kieselmann | Dr. Mathias Pajunk

Datenpannen in Folge von Hacking-Angriffen

Cyberangriffe auf IT-Systeme stellen eine immer größer werdende Herausforderung im Datenschutzrecht dar. In regelmäßigen Abständen wird in einer Vielzahl relevanter Medien über groß angelegte Hackerangriffe auf Unternehmen berichtet. So waren bereits bekannte Unternehmen und Programme - bspw. Windows 10 - Ziel von Cyberangriffen. Aber auch in Zeiten steigender digitaler Wandlung - verstärkt durch die Covid-19 Pandemie - sowie politischer Spannungen sollten sich Verantwortliche umso mehr mit der Thematik auseinandersetzen. Der folgende Beitrag soll daher eine kurze Einführung in die in der DS-GVO vorgesehenen Melde- und Benachrichtigungspflichten liefern und dabei auf einige Besonderheiten bei Angriffen auf die unternehmensinterne IT-Infrastruktur eingehen. Trotz des Umstands, dass der Europäische Datenschutzausschuss (EDSA) erst kürzlich

seine „Guidelines 01/2021 on Examples regarding Personal Date Breach Notification“ aktualisiert hat, zeigt die datenschutzrechtliche Praxis, dass auch weiterhin Unklarheiten bei der Auslegung der maßgeblichen Vorschriften auftreten können.

Meldepflicht gegenüber der Aufsichtsbehörde gemäß Art. 33 DS-GVO

Art. 33 Abs. 1 DS-GVO statuiert zunächst die Pflicht für Verantwortliche, im Falle einer sogenannten Verletzung des Schutzes personenbezogener Daten, diese unverzüglich und möglichst binnen 72 Stunden bei der zuständigen Aufsichtsbehörde zu melden. Wann von einer entsprechenden Verletzung des Schutzes personenbezogener Daten auszugehen ist, wird in Art. 4 Nr. 12 DS-GVO konkretisiert. Hiernach muss eine Verletzung der Sicherheit - ob unbeabsichtigt oder unrechtmäßig - zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führen. Dies darf allerdings nicht dahingehend missverstanden werden, dass jedwede Datenschutzverletzung meldepflichtig ist. Auf die Frage, ob eine Datenverarbeitung bspw. rechtmäßig - also unter Beachtung einer datenschutzrechtlichen Rechtsgrundlage - erfolgte, kommt es nicht maßgeblich an. Es liegt auf der Hand, dass bereits an dieser Stelle einige Abgrenzungsprobleme auftauchen können.

Sofern eine zuvor identifizierte Verletzung des Schutzes personenbezogener Daten „voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt“, entfällt die grundsätzlich vorgeschriebene Meldepflicht. Die insoweit nicht stets einfach zu handhabende Risikobewertung muss am jeweiligen Einzelfall erfolgen und kann nicht uneingeschränkt „vorbereitet“ werden. Zur Beurteilung der Frage, welche Faktoren hierbei zu berücksichtigen sind, haben jedoch verschiedene nationale Datenschutzaufsichtsbehörden Hilfestellungen veröffentlicht, um Verantwortlichen einen Anhaltspunkt zur Hand zu geben (vgl. bspw. der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit). Neben der Art und dem Umfang der betroffenen Daten können bspw. die zu erwartenden Konsequenzen - etwa ein Identitätsdiebstahl des Betroffenen - eine Rolle spielen. Auch macht es einen entscheidenden Unterschied, wie einfach und wahrscheinlich es ist, dass die betroffene Person anhand der jeweiligen Daten tatsächlich identifiziert werden kann.

Kommt eine nach den vorbezeichneten Kriterien durchzuführende Bewertung zu dem Ergebnis, dass voraussichtlich ein Risiko für die Rechte und Freiheiten natürlicher Personen anzunehmen ist, muss der Verantwortliche die in Art. 33 Abs. 1 DS-GVO normierte 72 Stunden Frist beachten. Maßgeblicher Beginn für den Fristlauf ist dabei derjenige Zeitpunkt, indem die Datenpanne dem Verantwortlichen „bekannt wurde“. Regelmäßig wird diese Voraussetzung dann vorliegen, sofern eine hinreichende Gewissheit darüber besteht, dass ein Sicherheitsvorfall aufgetreten ist. Wann wiederum eine solche Gewissheit anzunehmen ist, hängt von den Umständen des Einzelfalls ab. Hierbei spielt es jedoch keine Rolle, auf welchem Wege dem Verantwortlichen der entsprechende Sachverhalt bekannt wurde - bspw. durch externe Dritte. Bei der Beachtung der 72 Stunden Frist kann sich zudem die Frage stellen, ob bspw. Wochenendtage - in Anlehnung an die Regelungen des deutschen Prozessrechts - zu einer Fristverlängerung auf den nächsten Werktag führen. Auch wenn an einem Sonntag regelmäßig nicht mit einer unmittelbaren Reaktion einer Aufsichtsbehörde zu rechnen ist, sieht Art. 33 DS-GVO eine solche Fristverlängerung grundsätzlich nicht vor. Daher sollte bspw. im Falle des Fristablaufs an einem Feiertag zumindest eine kurze Ankündigung dergestalt erfolgen, dass am nächsten Werktag eine ausführliche Meldung entsprechend Art. 33 DS-GVO vorgesehen ist. Bieten Aufsichtsbehörden spezielle Formulare auf ihren Webseiten an, können diese ohne Weiteres auch an einem Feiertag verwendet werden. Keinesfalls sollte „abgewartet“ werden, bis eine Behörde tatsächlich erreichbar ist.

Weitere Probleme können auftreten, sofern externe Dritte - bspw. IT-Dienstleister - involviert sind. Erlangen solche Dienstleister Kenntnis über eine Datenpanne, melden dies jedoch erst nach einer gewissen Zeitspanne, so stellt sich die Frage, wann die 72 Stunden Frist für eine Meldung zu laufen beginnt. Da Art. 33 DS-GVO jedoch ausdrücklich auf die Kenntnisnahme beim Verantwortlichen verweist, ist nach unserem Dafürhalten nicht auf den jeweiligen Dienstleister abzustellen. Der Verantwortliche muss in der Lage sein, die ihm zur Verfügung gestellte Frist auszuschöpfen, um eine Meldung des relevanten Vorfalls gegenüber der Behörde zu ermöglichen.

Benachrichtigungspflicht gegenüber dem Betroffenen gemäß Art. 34 DS-GVO

Neben der Pflicht zur Meldung der Datenpanne gegenüber der Aufsichtsbehörde kann der Verantwortliche - je nach den Umständen des Einzelfalls - auch dazu verpflichtet sein, den

Betroffenen direkt über den Vorfall zu benachrichtigen. Dies setzt gemäß Art. 34 Abs. 1 DS-GVO allerdings voraus, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat. Während eine Meldepflicht gegenüber der Aufsichtsbehörde häufig der Fall sein wird, muss dies im Hinblick auf die Verpflichtung zur Benachrichtigung des Betroffenen intensiver überprüft werden. Auch bei der hierbei anzustellenden Risikobeurteilung, sind die bereits aufgeführten Kriterien maßgeblich zu berücksichtigen.

Anwendung dieser Grundsätze auf Cyberangriffe

Um die Schwierigkeiten bei der Rechtsanwendung im Einzelfall aufzuzeigen, soll das folgende Beispiel zur Veranschaulichung dienen.

Viele Unternehmen stellen sich insbesondere die Frage, inwiefern eine Verschlüsselung der Daten im Falle eines Cyberangriffs einen Einfluss auf das Risiko für die Betroffenen und somit auch auf eine etwaige Melde-, bzw. Benachrichtigungspflicht haben kann. So können Situationen denkbar sein, in denen ein Angreifer zwar Zugriff auf bestimmte - verschlüsselte - Datensätze erhält, den entsprechenden Schlüssel zum Entschlüsseln der Daten jedoch gerade nicht in Erfahrung bringt. Auch ist es denkbar, dass die betroffenen Daten vorübergehend nicht mehr verfügbar sind. Wie so häufig, wird es auch in diesen Konstellationen maßgeblich auf den Einzelfall ankommen. Zunächst kann festgehalten werden, dass eine Verschlüsselung keinen Automatismus dergestalt auslöst, wonach ein Risiko für die Betroffenen von vornherein auszuschließen ist. Der Verantwortliche sollte in einer solchen Konstellation stets überprüfen, welche Folgen für die betroffenen Personen denkbar sind - bspw. in Form von finanziellen oder gesellschaftlichen Nachteilen - und über welchen Zeitraum ein Zugriff des Angreifers auf die entsprechenden Daten bestand. Ist eine Wiederherstellung der Daten erst nach Ablauf der Meldefrist aus Art. 33 Abs. 1 DS-GVO möglich, kann auch dies nach Ansicht des EDSA in eine durchzuführende Risikobewertung einfließen. Sind von dem Cyberangriff sensible Daten gemäß Art. 9 Abs. 1 DS-GVO betroffen, so muss auch dieser Umstand maßgeblich berücksichtigt werden.

Zum Verständnis sei an dieser Stelle folgendes angemerkt: Auch sofern personenbezogene Daten verschlüsselt wurden, findet die DS-GVO uneingeschränkte Anwendung. Die „Schwelle“ zur Anonymisierung der Daten ist sehr hoch anzusetzen und wird im Falle einer „bloßen“ Verschlüsselung regelmäßig nicht den Anwendungsbereich der DS-GVO ausschließen. Andererseits kann eine nach dem Stand der Technik erfolgte Verschlüsselung Risiken für die Rechte und Freiheiten natürlicher Personen ausschließen, bzw. zumindest minimieren. Unternehmen ist daher angeraten, die interne IT-Infrastruktur entsprechend den in Art. 32 DS-GVO vorgesehenen technischen und organisatorischen Maßnahmen zu schützen, um denkbare Risiken im Falle einer Datenpanne möglichst gering zu halten.

Weitere Besonderheiten können auftreten, sofern zwar ein Cyberangriff identifiziert wurde, die entsprechende Schadsoftware jedoch unschädlich gemacht werden konnte. Insbesondere sofern keine Anhaltspunkte dafür bestehen, dass ein tatsächlicher Zugriff auf die unternehmensinternen Daten erfolgte, muss eine gründliche Risikobewertung durchgeführt werden. Auch in dieser - auf den ersten Schein - „ungefährlichen“ Konstellation gilt es zu beachten, dass keine allgemeingültigen Aussagen für eine Risikobeurteilung getroffen werden können. Häufig lassen sich die Folgen eines Cyberangriffs gerade nicht ohne Weiteres abschätzen. Verantwortliche müssen daher auch in dem vorbenannten Szenario alle Umstände des Einzelfalls in einer Gesamtwürdigung bewerten.

Praxis-Tipp:

Cyberangriffe sind nicht bloß „lästig“, sondern können im Ernstfall zu hohen Risiken für die betroffenen natürlichen Personen führen. Auch für Unternehmen steht einiges auf dem Spiel. Neben der eigenen Reputation sind stets aufsichtsrechtliche Maßnahmen - bis hin zu Bußgeldern - im Blick zu behalten. Wir raten daher dringend dazu, die unternehmensinterne IT-Infrastruktur auf den Prüfstand zu stellen und dem Thema IT-Sicherheit eine gesteigerte Bedeutung zuzusprechen. Wird tatsächlich eine Datenpanne identifiziert, sollte nicht lange gezögert werden; in Zweifelsfällen ist Rechtsrat einzuholen.

Für Verantwortliche bietet es sich zudem an, sich im Rahmen der Vielzahl an Veröffentlichungen von Behörden zu informieren. So hat bspw. das Bayerische Landesamt für Datenschutzaufsicht in einem

Flyer zum Thema „Cybercrime“ verschiedene Informationen zusammengetragen, um einen Überblick zu der Thematik zu liefern und Unternehmen entsprechend zu sensibilisieren. Aber auch der Bayerische Landesbeauftragte für den Datenschutz hält zum Thema „Cyberabwehr“ eine eigenständige Informationsseite bereit. Schließlich hat auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) einen „Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle“ veröffentlicht und informiert in diesem Zusammenhang über unterschiedliche Angriffsszenarien sowie entsprechende Gegenmaßnahmen. Darüber hinaus bieten die Webseiten des BSI einen stets aktualisierten Überblick über den Stand der Abwehrtechnik, den Unternehmen im Rahmen der für sie angemessenen Möglichkeiten umsetzen sollten. Wer diese BSI Empfehlungen beachtet, dem wird man kaum vorwerfen können, seine Pflichten zur Herstellung von Datensicherheit aus Art. 32 DSGVO nicht erfüllt zu haben.

SKW Schwarz verfügt über eine eigenständige Taskforce zum Thema Datenpannen (insbesondere zu Problemstellungen von Cyberangriffen) und unterstützt Unternehmen im Ernstfall gerne bei einem datenschutzkonformen Umgang. Aufgrund der Aktualität des Themas wird SKW Schwarz zudem kurzfristig zu einem Webinar laden, um aktuelle Rechtsfragen zu Cyberangriffen mit Interessenten zu besprechen. Schließlich ist uns als Empfehlung an die Unternehmen noch einmal der Hinweis auf die Umsetzungsmöglichkeiten und -probleme bei der Inanspruchnahme eines Versicherungsschutzes gegen Cyberbedrohungen wichtig (vgl. auch der Beitrag: „Hauptsache cyberversichert!“) Ob und wie der Schutz einer Cyberversicherung geeignet sein kann, die Folgen eines Cyberangriffs für die Unternehmen abzufedern, setzt in vielen Fälle voraus sich - bereits vor Abschluss eines entsprechenden Vertrages - mit den spezifischen Problemen dieser Versicherung auseinanderzusetzen.

Dr. Oliver Hornung, Marius Drabiniok, Dr. Matthias Orthwein

EU-Kommission veröffentlicht Entwurf des EU Data Act

Am 23. Februar 2022 hat die EU-Kommission den Verordnungsentwurf für harmonisierte Vorschriften für einen fairen Zugang zu Daten und deren Nutzung veröffentlicht („Data Act“; COM(2022), 68). Vorab wurde bereits eine Fassung geleakt.

Der Data Act ist ein weiterer Baustein der EU-Kommission zur Umsetzung der europäischen Datenstrategie vom Februar 2020. Als Verordnung wäre der Data Act ein unmittelbar anwendbares europäisches Gesetz, vergleichbar zur EU-Datenschutz-Grundverordnung („DSGVO“).

Zielsetzung des Data Acts

Mit dem Data Act sollen gesetzliche, wirtschaftliche und technische Hemmnisse für die Data Economy möglichst beseitigt werden. Der Zugang zu und die Weitergabe von Daten, die bei der Nutzung bestimmter Produkte und Dienstleistungen generiert werden, soll jeweils vereinfacht werden.

Der Data Act soll Produkthersteller dazu verpflichten, netzwerkfähige Produkte möglichst „daten-transparent“ zu gestalten. Nutzer eines solchen Produkts sollen einfachen Zugang zu bei der Nutzung des Produkts erhobenen oder generierten Daten haben. Der Datenbegriff ist dabei weit gefasst und nicht etwa beschränkt auf personenbezogene Daten.

Der Data Act schafft allerdings keine Rechtsgrundlage für die Datenverarbeitung durch den Data Holder („Dateninhaber“). Der Vorschlag setzt bei der tatsächlichen Kontrolle des Dateninhabers über die entsprechenden Daten an (vgl. Erwägungsgrund „EG“ Nr. 5 Data Act). Daher ist ein Dateninhaber verpflichtet, neben den Anforderungen des Data Acts insbesondere auch datenschutzrechtliche Anforderungen zu beachten. Diese können sich vornehmlich aus der DSGVO und dem deutschen Telekommunikation-Telemedien-Datenschutz-Gesetz („TTDSG“) ergeben.

Sachlicher Anwendungsbereich des Data Acts

Der sachliche Anwendungsbereich des Data Acts bezieht sich auf physische Produkte, die durch entsprechende Komponenten Daten über ihre Leistung, Verwendung oder Umgebung sammeln oder erzeugen und die solche Daten über einen öffentlich zugänglichen elektronischen

Kommunikationsdienst übermitteln können. EG Nr. 14 Data Act bezeichnet dies als „Internet of Things“ („IoT“). Solche IoT-Produkte können vernetzte Fahrzeuge, Haushaltsgeräte und andere Konsumgüter ebenso sein, wie medizinische Geräte und landwirtschaftlich oder industriell genutzte Maschinen.

Entsprechende (Roh-)Daten sollten zugänglich sein, weil sie die Digitalisierung von Nutzeraktivitäten und Ereignissen darstellen. Daraus abgeleitete Daten sollen aber nicht vom Anwendungsbereich des Data Acts umfasst sein (EG Nr. 14 Data Act).

Im Gegensatz zu IoT-Produkten sollen Produkte, die in erster Linie dazu bestimmt sind, Content anzuzeigen oder abzuspielen, oder zur Aufzeichnung und Übertragung von Content dienen, nicht vom Data Act umfasst sein. Zu diesen Produkten gehören z. B. PCs, Server, Tablets und Smartphones, Kameras und Webcams (EG Nr. 15 Data Act).

Überblick über die Kerninhalte des Data Acts

Verpflichtung zur Ermöglichung eines Datenzugangs, Art. 3 Data Act

Produkte und verbundene Dienste im Anwendungsbereich des Data Acts sollen so gestaltet sein, dass bei der Nutzung generierte Daten standardmäßig einfach, sicher und – nach Möglichkeit – dem Nutzer unmittelbar zugänglich sind.

Zudem sollen vor einem Vertragsschluss bestimmte Informationen über Art und Umfang der möglicherweise generierten Daten, den Dateninhaber, den Datenzugang sowie etwaige Datenempfänger zur Verfügung gestellt werden. Ist der potentielle Vertragspartner nicht der Dateninhaber, soll der potentielle Vertragspartner auch Informationen zur Verfügung stellen, wer der tatsächliche Dateninhaber ist.

Recht auf Datenzugang und Datennutzung, Art. 4 Data Act

Ist ein unmittelbarer Datenzugang nicht möglich, soll der Dateninhaber die entsprechenden Daten auf Anfrage ohne schuldhaftes Zögern und kostenlos zur Verfügung stellen, ggf. laufend in Echtzeit.

Art. 4 Data Act enthält auch gewisse Einschränkungen für einen Datenzugang und eine Datennutzung. Wenn ein Datensatz z. B. auch personenbezogene Daten („pbD“) umfasst, dürfen solche pbD nur zur Verfügung gestellt werden, wenn dafür eine Rechtsgrundlage nach Art. 6 bzw. Art. 9 DSGVO gegeben ist. Ein Dateninhaber darf generierte Daten ferner nicht dazu verwenden, um Erkenntnisse über die wirtschaftliche Lage, die Vermögenswerte und die Produktionsmethoden des Nutzers abzuleiten, wenn dies den Nutzer beeinträchtigen könnte.

Recht auf Data Sharing mit Dritten, Art. 5 Data Act

Ein Nutzer kann von einem Dateninhaber verlangen, Daten mit bestimmten Dritten zu „teilen“ („Data Sharing“), also z. B. einem solchen Dritten eine Datenkopie zur Verfügung zu stellen. Für pbD kann dies als Ergänzung zum Recht auf Datenübertragbarkeit nach Art. 20 Abs. 1 DSGVO interpretiert werden.

Verpflichtungen eines Dritten als Datenempfänger, Art. 6 Data Act

Ein Dritter als Datenempfänger darf ihm gemäß Art. 5 Data Act zur Verfügung gestellte Daten nur für Zwecke und unter den Bedingungen verarbeiten, die mit dem Nutzer vereinbart wurden. Ein Datenempfänger muss bei pbD die Betroffenenrechte und weitere DSGVO-Grundsätze beachten, z. B. zur Datenlöschung.

Zudem darf ein Datenempfänger einem Nutzer vertraglich nicht verbieten, entsprechende Daten auch weiteren Dritten zur Verfügung zu stellen. Er darf die Daten nicht nutzen, um Konkurrenzprodukte zu entwickeln und er darf grundsätzlich kein Profiling im datenschutzrechtlichen Sinn (Art. 4 Nr. 4 DSGVO) vornehmen, außer soweit dies für eine vom Nutzer gewünschten Dienstleistung notwendig ist.

Verpflichtungen für Dateninhaber für die Datenbereitstellung, Art. 8 ff. Data Act

Dateninhaber, die Daten nach dem Data Act zur Verfügung stellen, müssen bestimmte Verpflichtungen einhalten. Dazu zählt etwa, dass die Datenbereitstellung auf der Grundlage von fairen, angemessenen und nichtdiskriminierenden Bedingungen und in transparenter Weise erfolgt (Art. 8 Abs. 1 Data Act).

Verlangt der Dateninhaber für die Bereitstellung von Daten eine Vergütung vom Datenempfänger, muss diese angemessen sein (Art. 9 Abs. 1 Data Act).

Der Dateninhaber kann geeignete technische Schutzmaßnahmen implementieren, einschließlich sog. smart contracts, um einen unbefugten Datenzugriff zu verhindern und die Einhaltung der jeweiligen Anforderungen des Data Acts sowie entsprechender Vereinbarungen über die Datenbereitstellung zu gewährleisten. Diese technischen Schutzmaßnahmen dürfen allerdings nicht als Mittel eingesetzt werden, um etwaige Nutzerrechte nach dem Data Act zu beeinträchtigen (Art. 11 Abs. 1 Data Act).

„Unfaire" Vereinbarungen über Datenzugang und -nutzung, Art. 13 Data Act

Über das Prinzip eines möglichst einfachen und barrierefreien Datenzugangs hinaus sollen einseitige „unfaire" Vertragsklauseln über Datenzugang und -nutzung gegenüber Kleinstunternehmen sowie kleinen und mittleren Unternehmen ausgeschlossen werden.

Stets unwirksam sein sollen etwa vertragliche Ausschlüsse der Haftung für Vorsatz und grobe Fahrlässigkeit oder vollständige Gewährleistungsausschlüsse.

Daneben erklärt der Data Act bestimmte Regelungsinhalte als üblicherweise unwirksam. Dies betrifft beispielsweise unangemessene Gewährleistungsbeschränkungen oder Regelungen zu Datenzugang und Datennutzung, die legitime Interessen der anderen Vertragspartei erheblich beeinträchtigen.

Datenportabilität, Art. 23 ff. Data Act

Dateninhaber müssen nach Art. 23 ff. Data Act sicherstellen, dass Kunden zu einem anderen Dienstleister mit vergleichbaren Dienst wechseln und dabei u.a. entsprechende Daten portieren können. Während Art. 20 Abs. 1 DSGVO das Recht auf Datenübertragbarkeit für personenbezogene Daten regelt, die eine betroffene Person selbst zur Verfügung gestellt hat, umfassen die entsprechenden Anforderungen des Data Acts alle Daten im Anwendungsbereich des Data Acts.

Verhältnis zu datenschutzrechtlichen Regelungen

Dateninhaber und Datenempfänger im Sinne des Data Act müssen u. U. auch die DSGVO und das TTDSG beachten. Wenn nicht-personenbezogene und personenbezogene Daten untrennbar verbunden sind, sind die Anforderungen der DSGVO bei der Verarbeitung solcher Datensätze zu beachten (vgl. EG Nr. 30 Data Act; Art. 2 Abs. 2 VO (EU) 2018/1807 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union; „Datenverkehrs-VO")). Nationale Umsetzungen der ePrivacy-Richtlinie und eine etwaige EU-ePrivacy-Verordnung sind ebenfalls neben dem Data Act zu beachten (EG Nr. 32 Data Act).

Die Abgrenzung von nicht-pbD und pbD ist aufgrund der europäischen Rechtsprechung und der Reichweite der DSGVO-Definition von pbD (Art. 4 Nr. 1 DSGVO) in der Praxis eine gewisse Herausforderung.

Daher sollte ein Dateninhaber zunächst klären, ob er pbD von nicht-pbD trennen kann (vergleichbar zu der entsprechenden Fragestellung im Rahmen der Datenverkehrs-VO). Dabei wird es voraussichtlich darauf ankommen, ob z. B. Umweltsensordaten gesondert generiert werden, ohne Personenbezug. Zudem könnte es entscheidend sein, ob ein Dateninhaber pbD ausreichend anonymisieren kann.

Für die Praxis bedeutet dies, dass neben den Anforderungen an eine Anonymisierung im Datenschutzrecht, z. B. auf der Grundlage einer Einwilligung oder eines überwiegenden berechtigten Interesses, auch die Anforderungen des Data Acts an den Umgang mit nicht-personenbezogenen

Daten beachtet werden müssen. Auf (vollständig) anonymisierte Daten ist die DSGVO nicht anwendbar, der der Data Act allerdings schon. Nur zur Vollständigkeit sei hier erwähnt, dass auch § 25 TTDSG für nicht-personenbezogene Daten gilt. Danach sind die Speicherung von Daten in der Endeinrichtung eines Endnutzers und der Zugriff auf bereits in der Endeinrichtung gespeicherte Daten grundsätzlich nur zulässig, wenn der Endnutzer auf der Grundlage von klaren und umfassenden Informationen eingewilligt hat.

Ausblick

Durch den Data Act wird kein absolutes Recht an Daten geschaffen (nicht-juristisch formuliert: Es wird kein „Dateneigentum“ geschaffen). Es werden der Zugang und die Nutzbarkeit von Daten im Zusammenhang mit bestimmten Produkten geregelt.

Der Data Act ist damit ein weiterer Beitrag zur Data Economy, welcher in der Praxis durchaus bedeutsam werden könnte. Er deutet einen Paradigmenwechsel bei Datenzugang und -nutzung an.

Dr. Daniel Meßmer | Dr. Stefan Peintinger | Martin Schweinoch

Hauptsache cyberversichert!

In Zeiten stark zunehmender Angriffe auf die Unternehmens IT aus dem Internet lautet die Empfehlung vieler Experten an die Unternehmen rechtzeitig für einen ausreichenden Versicherungsschutz gegen Cyberbedrohungen zu sorgen.

Deren Umsetzung ist jedoch gar nicht so einfach, da der Risikohunger der Versicherungen, d. h. die Bereitschaft neue Kunden in den Versicherungsschutz aufzunehmen, zuletzt erheblich gesunken ist. Die Kombination aus einigen Jahren, in denen die Versicherungen ihre Policen quasi ohne jegliche vorgeschaltete Risikoanalyse verkauft haben, mit einer drastisch gestiegenen Anzahl von Angriffen und Bedrohungsszenarien führt dazu, dass die Versicherungsbranche Alarm schlägt und sich im Segment der Cyberversicherungen existenzgefährdenden Risiken ausgesetzt sieht.

Wie reagieren die Versicherungen auf aktuelle Cyberwar- und staatlich gesponserte Hackingattacken?

Die Versicherungsindustrie reagiert auf diese Situation mit neuen Musterklauseln, die den Umfang der versicherten Risiken erheblich einschränken sollen.

Ende 2021 hat Lloyds of London vier neue Musterklauseln vorgestellt, die den Versicherern zur Aufnahme in ihre Cyberversicherungspolicen empfohlen werden, um insbesondere Schäden aus Cyberwar-Aktivitäten aus dem Haftungsrisiko auszuschließen (LMA21-042-PD (lmalloyds.com). Viele der bis dahin verwendeten „Kriegsklauseln“ stammten noch aus der Zeit vor dem Zweiten Weltkrieg und waren insbesondere auf kriegerische Situationen unter Einsatz physischer Gewalt ausgerichtet.

In den USA hat der New Jersey Superior Court gerade erst im Dezember 2021 festgestellt, dass die bis dahin üblichen Kriegsausnahmen nicht auf digitale Angriffe anwendbar sein sollen (Cyber Risks and Business Interruption Insurance - Merck and International Indemnity v ACE (et al.) - The 36 Group). Das Beispiel Ukraine zeigt jedoch aktuell, dass in unserer heutigen Cyberwirklichkeit Angreifer einen ganzen Staatsapparat zumindest digital lahmlegen können, ohne dass ein einziger Soldat fremdes Staatsgebiet betreten muss. Microsoft hat bei den dort zum Einsatz kommenden Viren festgestellt, dass diese zwar wie klassische Ransomware die angegriffenen Festplatten verschlüsseln, ihnen aber der Mechanismus zum Freikaufen durch Lösegeld gänzlich fehlt, was wiederum für Sabotage- und gegen kommerzielle Angriffe spricht (Malware attacks targeting Ukraine government - Microsoft On the Issues).

Das Argument der Versicherungsbranche für einen Haftungsausschluss im Fall kriegerischer oder staatlicher Aggressionen besteht darin, dass solche Kumulativschäden, bei denen sich einzelne Schadensereignisse durch ihre Häufung zu enormen Summen aufaddieren können, für die private Versicherungswirtschaft nicht tragbar sind (vgl. Risiko durch Cyberangriffe: »Schäden, die ein privater Versicherer nicht tragen kann« - DER SPIEGEL).

Was beinhalten die neuen Musterklauseln für Cyberversicherungen?

Die vier neuen Musterklauseln für Cyberversicherungen sind dafür gedacht, die modernen Cyberwar-Aktivitäten in den Haftungsausschluss für kriegerische Aktivitäten zu integrieren.

Die vier Musterklauseln unterscheiden sich abgestuft in der Strenge, mit der sie den Haftungsausschluss des Versicherers formulieren. Allen Klauseln gemeinsam ist die Annahme, dass nicht nur kriegerische Aktivitäten, sondern jeder staatlich geförderte oder geschützte Angriff auf IT-Infrastrukturen als sogenannte Cyberoperation dazu führen, dass die Haftung der Versicherung ausgeschlossen ist.

Abgesehen von den Fällen wie zurzeit in der Ukraine, in denen der angegriffene Staat offiziell bestätigt das Ziel fremder staatlicher Cyberoperations geworden zu sein, soll es nach den Musterklauseln den Versicherern zustehen festzustellen, dass objektive Anhaltspunkte für einen staatlichen Angriff bestehen. Die Versicherungen sollen sogar das Recht erhalten, so lange die Schadensersatzzahlungen auszusetzen, solange der angeblich angegriffene Staat den Angriffsakt zwar noch nicht als kriegerischen Akt bezeichnet hat, die Versicherung aber objektive Anhaltspunkte für einen staatlichen Hintergrund des Angriffs hat. Je nach Strenge der Klausel muss der entsprechende Angriff auch nicht auf die kritische Infrastruktur im Zielland abzielen, um dennoch als kriegerische Cyberoperations dafür zu sorgen, dass die Versicherung nicht zahlen muss.

Wie sind die Musterklauselvarianten in der Praxis zu bewerten?

Bei den eher kundenfreundlich ausgestalteten Musterklauselvarianten wird es allerdings in der Praxis vermutlich dem Versicherer schwerfallen, die dort formulierten Ausschlusskriterien zu erreichen, nach denen entweder eine staatliche Beteiligung oder erhebliche Auswirkungen auf die kritische Infrastruktur im Zielland bewiesen sein müssen. Selbst bei den größten bekannt gewordenen Angriffen der letzten Jahre wie z.B. „Solarwinds“ oder „wannacry“ wären diese Kriterien vermutlich nicht erfüllt gewesen.

Was kann aus der Haftung der Cyberversicherungen ausgeschlossen werden?

Nicht nur der Haftungsausschluss für staatliche oder kriegerische Cyberaktivitäten macht es den Unternehmen schwer eine beruhigende Versicherungsabsicherung zu erhalten, sondern auch der Umstand, dass immer mehr Versicherungen dazu übergehen, den Ersatz gezahlter Lösegeldforderungen aus dem Versicherungsschutz auszuschließen (z.B Axa und Generali France, vgl. www.inside-it.ch/kriminelle-verkaufen-kundenlisten-von-cyberversicherungen). Auch wenn alle Experten den Unternehmen von der Zahlung von Lösegeldsummen abraten, um sich nicht weiter erpressbar zu machen und gewichtige Stimmen in der Literatur sogar von einer strafbaren Unterstützung krimineller Aktivitäten durch Zahlung von Lösegeld ausgehen, wollen sich viele Unternehmen diese Option dennoch offenhalten, ohne auf einen entsprechenden Versicherungsschutz verzichten zu wollen.

Aber auch die zum Teil erheblichen Schäden, wenn das angegriffene Unternehmen mit seiner notwendigen Zulieferung zurLieferkette seines Kunden ausfällt, werden zum Teil aus der Haftung der Cyberversicherung ausgeschlossen; insbesondere wenn die Attacke offensichtlich einem bestimmten Staat oder staatlicher Institution galt, andere Staaten und Softwareanwender aber quasi kollateral mitbetroffen sind. Ohnehin schließen viele Versicherungen in ihren Policen die sogenannten Wiederherstellungskosten, die nicht nur der bloßen Abwehr des Angriffs gelten wie z.B. säubern und wieder einspielen von Backups Daten, aus dem Umfang ihrer Ersatzpflicht aus.

Worauf sollten Unternehmen beim Abschluss einer Cyberversicherung achten?

Gut beratene Unternehmen achten beim Abschluss einer Cyberversicherung nicht nur darauf, möglichst wenige der oben genannten Ausschlussklauseln zu akzeptieren, sondern versuchen durch aktive Maßnahmen zur Risikosenkung die Bereitschaft der Versicherer zu erhöhen, ihnen überhaupt eine Cyberversicherung und noch dazu zu attraktiven Konditionen anzubieten.

Zum Teil machen die Versicherungen auch die Beantwortung umfangreicher Fragenkataloge zur Feststellung des jeweils vorhandenen Risikopotenzials zur Bedingung für einen

Versicherungsvertragsabschluss. Diese Fragebögen sind derart umfangreich und auf die Verhinderung jedweden erkennbaren Risikos ausgerichtet, dass insbesondere mittelständische Unternehmen bei deren Beantwortung ohne externe technische und juristischen Sachverstand an ihre Grenzen geraten. Die von den Versicherungen zum Teil verlangten technischen Zertifizierungen wie z.B. ISO 27001 sind zwar geeignet den aktuellen Stand der Sicherheitstechnik bei den Unternehmen zu bestätigen, sind aber ebenfalls nur mit erheblichem finanziellen und zeitlichen Ressourcenaufwand erreichbar.

Unser Praxis Tipp

Unternehmen, die trotz sinkender Abschlussbereitschaft der Versicherungen einen Cyberversicherungsschutz anstreben, sollten daher unbedingt ihre Hausaufgaben im Bereich der Daten- und IT-Sicherheit machen und ihre Infrastruktur bereits im Vorfeld des Versicherungsvertragsabschlusses auf den aktuellen Stand der Technik bringen.

Mit weiteren dokumentierten präventiven Maßnahmen zum verbesserten Krisenmanagement wie z.B. dem Aufstellen eines Krisenhandbuchs oder der regelmäßigen Durchführung von Notfallübungen, lassen sich zudem Versicherungsprämien oft deutlich reduzieren.

Kommt es zu einem Versicherungsvertragsabschluss ist es aus Sicht des Unternehmens wichtig, auf faire Klauseln in den Policen zur Absicherung von Schäden in der Lieferkette oder Ersatz der Wiederherstellungskosten sowie vollen Ersatz der Wiederherstellungskosten und von Lösegeldzahlungen zu achten und gegebenenfalls Haftungsausschlüsse in den Versicherungsbedingungen zu vermeiden.

Dr. Matthias Orthwein

Datenschutzrecht in der Jahreswende - und was Unternehmen 2022 noch beschäftigt

Das Jahr 2021 neigt sich einem Ende zu. Während in Wirtschaft und Industrie allmählich die wohlverdiente Pause zwischen den Jahren ansteht, bleibt eine Vielzahl rechtlicher Themen höchst aktuell und sollte spätestens zu Beginn des Jahres 2022 - soweit dies nicht bereits geschehen ist - ernsthaft angegangen werden. Der digitale Umbruch ist in vollen Zügen und stellt Unternehmen mehr und mehr vor große Herausforderungen. Um diese These zu belegen, ist bereits der bloße Verweis auf die „neuen“ EU-Standardvertragsklauseln ausreichend.

Neben dem stetigen Wandel in der datenschutzrechtlichen Praxis rücken jedoch mehr und mehr auch weitere Themen in den Fokus. So sei an dieser Stelle bspw. auf die Neuerungen des digitalen Kaufrechts sowie das Lieferkettensorgfaltspflichtengesetz hingewiesen. Auch der Koalitionsvertrag von SPD, FDP und den Grünen lässt an einigen Stellen erkennen, dass verschiedene aktuelle Themen auf der Agenda der neuen Regierung stehen. Um vor lauter digitalen Bäumen noch den Wald zu sehen, möchten wir zur Jahreswende einen kurzen Überblick über aktuelle Themen liefern, welche im Jahre 2022 für Unternehmen (noch immer) von großer Bedeutung sein werden.

Immer wieder der Drittlandtransfer

Dass im Bereich des Datenschutzrechts niemals Stillstand herrscht, ist mittlerweile bekannt. So war das vergangene Jahr noch immer stark von der „Schrems-II“ Entscheidung des Europäischen Gerichtshofs geprägt. Die Implementierung der neuen EU-Standardvertragsklauseln (SCC) sowie die Durchführung eines Transfer Impact Assessments (TIA) gehören mittlerweile zum Alltag datenschutzrechtlicher Fragestellungen. Über die Verabschiedung der neuen SCC haben wir in unserem Beitrag vom 08. Juni 2021 („EU-Kommission verabschiedet neue Standarddatenschutzklauseln für internationalen Datentransfer“) bereits umfassend berichtet.

Während neue Drittlandtransfers bereits seit dem 28. September 2021 auf Grundlage der neuen SCC erfolgen müssen, haben Unternehmen noch bis zum 27. Dezember 2022 Zeit, ihre alten Drittlandtransfers entsprechend anzupassen. Neben der Frage, welches Modul im Hinblick auf den jeweiligen Drittlandtransfer zur Anwendung kommt, muss insbesondere sorgfältig überprüft werden, ob zusätzliche Maßnahmen erforderlich sind, um ein angemessenes Datenschutzniveau zu

gewährleisten. Die Vertragsparteien müssen gemäß Klausel 14 lit. a) der SCC versichern, dass sie keine Zweifel daran haben, dass der Datenimporteur durch geltende Rechtsvorschriften und Gepflogenheiten im Drittland an der Erfüllung der sich aus den SCC ergebenden Pflichten gehindert wird. Dies betrifft aktuell vornehmlich Datentransfers in die USA. Wir haben aus diesem Anlass bereits in unserem Beitrag vom 23. Juni 2021 („Empfehlungen des EDSA für Drittlandtransfers aktualisiert") auf das vom Europäischen Datenschutzausschuss (EDSA) aktualisierte sogenannte „6-Stufenmodell" hingewiesen.

Ebenfalls haben wir in unserem Beitrag vom 01. Oktober 2021 („Standardisierung und Automatisierung eines Transfer Impact Assessment im Zusammenhang mit den neuen EU-Standardvertragsklauseln") unsere standardisierte Lösung bei der Durchführung des TIA aufgezeigt. Dies bleibt auch im Jahr 2022 von höchster Relevanz, da - wie bereits aufgezeigt - die alten Drittlandtransfers entsprechend angepasst und ggf. um weitere Maßnahmen erweitert werden müssen.

Verantwortlich heißt verantwortlich - Die Entscheidung „Cookiebot"

Für Aufsehen im Zusammenhang mit Drittlandtransfers hat jüngst ein Beschluss des VG Wiesbaden vom 01. Dezember 2021 gesorgt. Im einstweiligen Rechtsschutz wurde einem Antrag stattgegeben, welcher es der Hochschule RheinMain untersagt, den Dienst „Cookiebot" - als sogenannte Consent Management Plattform - auf der eigenen Webseite einzusetzen, um verschiedene Einwilligungen der Nutzer einzuholen. Die hierbei erhobenen Daten der Nutzer (u.a. die ungekürzte IP-Adresse) unterliegen dabei dem Zugriff eines Anbieters eines sogenannten Content Delivery Network (CDN) Tools mit Sitz in den USA. Neben der - insoweit bereits bekannten - Aussage, dass es sich bei IP-Adressen regelmäßig um personenbezogene Daten handelt, rückt vor allem eine weitere Aussage der 6. Kammer des VG Wiesbaden in den Fokus: Verantwortlich heißt verantwortlich. Trotz des Umstands, dass im vorliegenden Fall nicht die Hochschule RheinMain den Zugriff auf personenbezogene Daten durch den US-amerikanischen Dienstleister ermöglicht, entscheidet diese nach Ansicht des VG Wiesbaden durch den Einsatz von „Cookiebot" zumindest mittelbar über die Mittel und Zwecke der Datenübermittlung. Nach Ansicht des VG Wiesbaden handelt es sich vorliegend - insbesondere wegen der Regelungen des sogenannten Cloud-Acts - um einen Datentransfer in die USA ohne angemessenes Datenschutzniveau. Insbesondere seien solche Instrumente nicht implementiert worden, die dazu führen können, dass ein angemessenes Datenschutzniveau schlussendlich doch bejaht werden kann. Letzteres betrifft vornehmlich die neuen SCC, welche nicht zwischen dem Webseitenbetreiber und dem Anbieter von „Cookiebot" abgeschlossen wurden.

Auch wenn die vorbezeichnete Entscheidung massive Auswirkungen auf eine Vielzahl von datenschutzrechtlich Verantwortlichen entfalten kann, möchten wir die aktuell aufkommende Panik etwas dämpfen. Nach unserer Einschätzung sollten zunächst die weiteren Verfahrensschritte abgewartet werden. Da es sich vorliegend „nur" um eine Entscheidung im einstweiligen Rechtsschutz handelt, bleibt zu beobachten, wie sich der weitere Verfahrensgang entwickelt. Obgleich man dem VG Wiesbaden in einigen Punkten datenschutzrechtliche Ungenauigkeiten vorwerfen möchte - dies betrifft insbesondere den rechtlichen Umgang mit den SCC -, ist es Unternehmen anzuraten, zumindest mittelfristig nochmals ihre Auftragsverarbeitungsketten sowie Drittlandtransfers nachzuvollziehen. Werden personenbezogene Daten in die USA übermittelt, sollte geprüft werden, ob weiterer Handlungsbedarf besteht. Kommt eine - von dem Verantwortlichen durchzuführende - TIA Prüfung zu dem Ergebnis, dass weitere Maßnahmen zur Gewährleistung eines angemessenen Datenschutzniveaus ergriffen werden müssen, sollte auf dasjenige Glied in der Datenverarbeitungskette Einfluss genommen werden (bspw. durch konkrete Verpflichtungen in einem Auftragsverarbeitungsvertrag), welches den Drittlandtransfer unmittelbar veranlasst. Ist eine solche Einflussnahme dagegen nicht möglich, muss die verantwortliche Stelle - nimmt man die Entscheidung des VG Wiesbaden ernst - die vertraglichen Beziehungen zu dem Datenexporteur abbrechen.

Cookies und das TTDSG

Auch ohne einen Bezug zu einem Drittlandtransfer, ist der Einsatz von sogenannten Cookies von zentraler Bedeutung für eine Vielzahl von Unternehmen. Wie wir bereits in unserem Beitrag vom 06. Oktober 2021 („Gesetzliche Regelung für den Einsatz von Cookies") angekündigt haben, ist zum 01. Dezember 2021 nun das Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) in Kraft getreten. Da wir in dem verlinkten Beitrag

bereits die wesentlichen Neuerungen aufgezeigt haben, möchten wir nun einen Blick auf ein weiteres zentrales Problem bei der Gesetzesanwendung richten: Unter welchen Voraussetzungen ist ein Cookie „unbedingt erforderlich“ im Sinne des § 25 Abs. 2 TTDSG? Dies ist deshalb von besonderer Bedeutung, da in einem solchen Fall ausnahmsweise keine Einwilligung des Nutzers einer sogenannten Endeinrichtung erforderlich ist.

Nochmal zur Erinnerung: Das TTDSG trennt - wie auch die e-Privacy-Richtlinie - zwischen verschiedenen Arten von Cookies. Einerseits sind Cookies denkbar, ohne die eine Bereitstellung der angebotenen Leistung nicht möglich ist. Andererseits greifen insbesondere App- und Webseitenbetreiber gerne auf solche Cookies zurück, die ausschließlich dem Betreiber selbst einen Vorteil verschaffen (bspw. um Reichweitenmessungen durchzuführen). Folgt man der Ansicht einiger deutscher Datenschutzaufsichtsbehörden, muss das Kriterium der unbedingten Erforderlichkeit sehr restriktiv verstanden werden. Nach einer Stellungnahme des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit vom 30. November 2021 ist bspw. nur eine technische Notwendigkeit ausreichend, „nicht jedoch [eine] wirtschaftliche Notwendigkeit“. Als „unbedingt erforderlich“ wird man u.a. Cookies zur Speicherung der Cookie-Einstellungen, zur Erinnerung der Artikel im Warenkorb, zur (technischen) Ermöglichung von Videostreams, zur Personalisierung von Diensten sowie Cookies, die Sicherheitszwecken des Betreibers dienen, ansehen dürfen. Geht es dagegen um Cookies die der Werbung, Nachverfolgung oder Geolokalisierung dienen, muss der Anbieter zwingend eine Einwilligung vom jeweiligen Nutzer der Endeinrichtung einholen. Wie sich § 25 Abs. 1 S. 2 TTDSG entnehmen lässt, müssen Einwilligungen dabei den Maßstäben der DS-GVO entsprechen und insbesondere freiwillig und ohne das Vorliegen bereits vorangekreuzter Kästchen erfolgen. Abschließend sollten Betreiber von Endeinrichtungen unbedingt das „Zusammenspiel“ von TTDSG und DS-GVO beachten: Werden nach dem Einsatz eines Cookies personenbezogene Daten verarbeitet, muss dies mit den Anforderungen der DS-GVO im Einklang stehen. Dies erfordert insbesondere das Vorliegen einer datenschutzrechtlichen Rechtsgrundlage - regelmäßig auf Grundlage von Art. 6 DS-GVO.

Auch wenn das TTDSG wegen dem geplanten Erlass einer e-Privacy-Verordnung durch den Europäischen Gesetzgeber voraussichtlich nur einen begrenzten Zeitraum für den Einsatz von Cookies und vergleichbarer Tools herangezogen wird, sollten Unternehmen die Ausgestaltung ihrer Cookie-Banner nochmals gründlich überprüfen. Es liegt auf der Hand, dass das Inkrafttreten des TTDSG erneute Überprüfungen durch Aufsichtsbehörden provozieren wird.

Kaufrecht 4.0

Auch wenn wir liebend gerne weiter über das Datenschutzrecht als eines unserer Kernkompetenzen berichten würden, gibt es weitere spannende Neuerungen, die Unternehmen künftig beachten müssen. Wie wir bereits in unserem Beitrag vom 04. Oktober 2021 („Kaufrecht 4.0“) berichtet haben, treten zum 01. Januar 2022 einige weitreichende Neuerungen des Bürgerlichen Gesetzbuches (BGB) in Kraft. Neben Anpassungen des Kaufrechts findet sich künftig in den §§ 327 ff. BGB n.F. ein gänzlich neuer Vertragstypus über die Bereitstellung digitaler Inhalte oder digitaler Dienstleistungen. Auch wenn viele der Neuerungen primär den B2C-Bereich adressieren, sollten die Änderungen in ihrer Gesamtheit nicht unterschätzt werden.

Zum einen ist die Überarbeitung des Mängelrechts in § 434 BGB n.F. ohne Einschränkungen auch im B2B-Bereich von Relevanz. Während ein Mangel einer Kaufsache bisher dann vorgelegen hat, wenn sich diese bspw. entweder zur vertraglich vereinbarten oder zur gewöhnlichen Verwendung nicht eignet, müssen künftig sogenannte subjektive und objektive Voraussetzungen kumulativ vorliegen, um den Verkäufer vor Gewährleistungsansprüchen zu bewahren. Für den Verkäufer heißt dies in der Konsequenz, dass er seine Vertragsmuster entsprechend anpassen muss, ohne jedoch die Grenzen des rechtlich zulässigen zu überschreiten. Tritt der Verkäufer dabei (auch) im B2C-Bereich auf, gelten strenge Maßstäbe.

Auf der anderen Seite werden wir in unserer anwaltlichen Praxis regelmäßig damit konfrontiert, dass sich Unternehmen häufig nicht darüber bewusst sind, welche Regelungen im B2C-Bereich gelten. Ist ein Unternehmen jedoch nicht für den Fall der Fälle vorbereitet, wird es die Vielzahl zu beachtender Voraussetzungen und Informationspflichten kaum erfüllen können. Dies gilt umso mehr, da gemäß § 312 Abs. 1a BGB n.F. künftig bereits das Bereitstellen personenbezogener Daten zu einem Widerrufsrecht des Verbrauchers führen kann. Man denke in diesem Zusammenhang nur an die

pandemie-bedingte Vielzahl von Webinaren oder vergleichbaren Angeboten, in denen bspw. die Werbetrommel für das eigene Unternehmen gerührt wurde. Versteckt sich unter den Teilnehmern ein Verbraucher im Sinne des § 13 BGB und werden die bereitgestellten personenbezogenen Daten nicht ausschließlich verwendet, um das jeweilige Angebot (technisch) zu ermöglichen, kann dies ein Widerrufsrecht des Verbrauchers zur Folge haben.

Auch muss das Nebeneinander der verschiedenen Vertragstypen zumindest überblicksartig durchdrungen werden. Während ein Vertrag über die Bereitstellung von Cloud-Diensten im B2C-Bereich künftig über die §§ 327 ff. BGB n.F. abzuwickeln ist, gilt dies nicht auch im B2B-Bereich. In letzterem Fall bleibt es voraussichtlich wie gewohnt bei der Anwendbarkeit mietrechtlicher Vorschriften. Auch bei der Frage, welches Gewährleistungsrecht anwendbar ist, finden sich einige Finten im Detail.

Auch wenn solche Unternehmen, die vornehmlich im B2B-Bereich auftreten, etwas „gelassener“ an das Thema herangehen können, ist ein grober Überblick über die neuen Regelungen unerlässlich.

Compliance als wachsende Herausforderung

Unter dem Oberbegriff Compliance erwarten Unternehmen künftig gleich zwei große Baustellen.

Wie wir in unserem Beitrag vom 02. Dezember 2021 („Aktueller Stand der Whistleblower-Richtlinie“) erst jüngst berichtet haben, hat Deutschland - zumindest nach jetzigem Stand - die Umsetzungsfrist zur Richtlinie (EU) 2019/1937 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (sog. Whistleblower-Richtlinie) „verschlafen“. Wir rechnen jedoch damit, dass ein Umsetzungsgesetz nicht lange auf sich warten lassen wird, sobald sich der Gesetzgeber auf eine finale Fassung geeinigt hat. Die Richtlinie sieht vor, dass Unternehmen mit einer Beschäftigtenzahl von mindestens 250 Mitarbeitern bis spätestens zum 17. Dezember 2021 ein Meldesystem für Compliance-Hinweise durch Whistleblower einrichten müssen. Unternehmen mit einer Beschäftigtenzahl von 50 bis 249 Mitarbeitern müssen die jeweiligen Vorgaben dagegen erst bis zum 17. Dezember 2023 umsetzen. Um von dem zu erwartenden Umsetzungsgesetz nicht „kalt erwischt“ zu werden, sollten Unternehmen tunlichst damit beginnen, ernsthaft an der Implementierung eines entsprechenden Meldesystems zu arbeiten. Mit „SKWhistle“ haben wir eine modulare Beratungslösung geschaffen, die Sie beim Aufbau, bei der Einrichtung sowie beim operativen Betrieb eines Hinweisgebersystems unterstützt. Die einzelnen Module können dabei wahlweise zu vereinbarten Festpreisen oder individuell nach dem jeweiligen Aufwand gebucht werden. Bei Bedarf beraten wir Sie auch gerne bei der Wahl einer technischen Lösung. Über weitere Einzelheiten in diesem Kontext haben wir in unserem Beitrag vom 11. Mai 2021 („SKWhistle: Hinweisgebersystem rechtssicher implementieren“) unterrichtet.

Als zweites großes Thema im Zusammenhang mit Compliance sollte das - unseres Erachtens weit unterschätzte - Lieferkettensorgfaltspflichtengesetz (LkSG) auf der Agenda von Unternehmen stehen. Vorbehaltlich einiger Sonderregelungen tritt das Gesetz in seiner endgültigen Fassung am 01. Januar 2023 in Kraft. Durch das Gesetz sollen Menschenrechte auch in arbeitsteilig funktionierenden Lieferketten besser gewahrt und deren Einhaltung effektiv durchgesetzt werden. So wird in § 2 Abs. 2 LkSG eine Vielzahl denkbarer „menschenrechtlicher Risiken“ aufgelistet, welche potenzielle Adressaten des Gesetzes künftig auch außerhalb der eigenen Arbeitsstrukturen beachten müssen. Exemplarisch zu nennen sind in diesem Zusammenhang insbesondere die Verbote von Kinder- und Zwangsarbeit, der Sklaverei, der Ungleichbehandlung in Beschäftigtenverhältnissen sowie die Beachtung der jeweils geltenden Pflichten des Arbeitsschutzes. Da neben weiteren zu beachtenden umweltbezogenen Risiken auch 11 dem Gesetz als Anlage beigefügte Übereinkommen zum Schutz der Menschenrechte Teil des Schutzkonzepts sind, kann der hierbei zu beachtende Sorgfaltsmaßstab als sehr weitreichend angesehen werden.

In § 1 LkSG werden die Adressaten des Gesetzes näher definiert. Primär betroffen sind hierbei Unternehmen -ungeachtet ihrer Rechtsform-, deren Hauptverwaltung, -niederlassung oder Sitz im Inland liegt, sofern darüber hinaus in der Regel mindestens 3.000 Arbeitnehmer im Inland beschäftigt werden. Ins Ausland entsandte Arbeitnehmer sind hierbei ebenfalls erfasst. Sofern ein Unternehmen lediglich eine Zweigniederlassung gemäß § 13d des Handelsgesetzbuches im Inland betreibt und in der Regel ebenso mindestens 3.000 Arbeitnehmer im Inland beschäftigt, ist es gleichwohl Adressat des Gesetzes. Ab dem 01. Januar 2024 muss zudem beachtet werden, dass die Schwellenwerte der beschäftigten Arbeitnehmer bei nur noch 1.000 liegen.

In den §§ 3 - 10 des Gesetzes werden die verschiedenen von den Adressaten zu beachtenden Sorgfaltspflichten näher dargestellt. Unterfällt ein Unternehmen dem Anwendungsbereich des Gesetzes, muss es künftig u.a. ein Risikomanagement, eine Risikoanalyse, Abhilfe- und Präventionsmaßnahmen sowie wiederum ein Beschwerdeverfahren unternehmensintern implementieren. Hier wird schnell klar: Das Thema Compliance wird aktuell sowohl auf europäischer als auch auf nationaler Ebene großgeschrieben.

Auch IT-Sicherheitsrisiken rücken in den Fokus

Unter dem höchst aktuellen Begriff der Java-Sicherheitslücke „Log4Shell" rückt auch das Thema IT-Sicherheit immer mehr in den Fokus. Die Java-Protokollierungsbibliothek „Log4j" ist Bestandteil einer Vielzahl kommerzieller Produkte. Da zudem auch Open-Source Produkte betroffen sein können, sind die Auswirkungen der kürzlich entdeckten Sicherheitslücke beachtlich. Zusammengefasst ermöglicht es die identifizierte Sicherheitslücke Angreifern über das Internet bestimmte Programmcodes auszuführen, um auf diese Weise weitere Angriffe auf ein System zu ermöglichen. Grund genug, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Sicherheitswarnung mit der „Warnstufe Rot" vergeben hat. Auf der Webseite des BSI wurde eine eigene Kategorie mit mehreren verlinkten Dokumenten veröffentlicht, in der weitere Informationen sowie Handlungsempfehlungen aufgezeigt werden. Auch das Bayerische Landesamt für Datenschutzaufsicht hat auf seiner Webseite eine Handreichung zur Erstanalyse veröffentlicht, um Verantwortlichen und deren betrieblichen Datenschutzbeauftragten gebotene Abhilfemaßnahmen an die Hand zu geben.

Die aktuellen Gegebenheiten zeigen erneut die nicht zu unterschätzende Bedeutung der in Art. 32 DS-GVO enthaltenen Vorgaben zur Sicherheit der Datenverarbeitung auf. Je nach konkreten Fall, kann die Identifizierung einer Sicherheitslücke auf eigenen Systemen zu einer meldepflichtigen Verletzung des Schutzes personenbezogener Daten im Sinne des Art. 33 DS-GVO führen. Auch wenn der Fokus regelmäßig auf das Vorliegen einer datenschutzrechtlichen Rechtsgrundlage gelegt wird, sollten Verantwortliche auch gerade der IT-Sicherheit ein angemessenes Gewicht beimessen.

Was ist noch neues geplant?

Dass die neue Ampel einiges zum Thema Digitalisierung in der Planung hat, haben wir bereits in unserem Beitrag vom 01. Dezember 2021 („Mehr Digitalisierung wagen – was plant die künftige Ampelkoalition?") aufgezeigt. Für Unternehmen heißt dies umso mehr, wachsam zu bleiben und die aktuellen Fokusthemen im Visier zu haben.

Auch wenn der vorliegende Beitrag den Eindruck vermitteln mag, dass man kaum Herr all dieser Themen werden kann, möchten wir Sie an dieser Stelle beruhigen. Es ist nachvollziehbar und auch nicht erforderlich, dass alle vorgenannten Themen gleichzeitig beherrscht und im eigenen Unternehmen berücksichtigt werden können. Dies erwartet auch niemand von Ihnen. Wir möchten Sie mit diesem kurzen Aufriss jedoch zum Ende des Jahres noch einmal sensibilisieren und auf die anstehenden Themen wappnen.

Dr. Oliver Hornung

Digitale Service Act: Änderungsvorschläge beschlossen

Der federführende Ausschuss für Binnenmarkt und Verbraucherschutz des EU Parlaments hat Anpassungsvorschläge für den DSA beschlossen. Damit nimmt der DSA eine weitere Hürde. Über den Kompromissvorschlag soll nun bereits im Januar 2022 im Plenum abgestimmt werden.
Die inhaltlichen Vorschläge betreffen nachfolgende Punkte:

- „Erotik-Plattformen": Das Hochladen von Inhalten soll dort nur noch Nutzern erlaubt sein, die beim Betreiber eine E-Mail-Adresse und Mobilfunknummer hinterlegt haben.
- Die Notice-and-Action-Pflichten im Zusammenhang mit besonders schwerwiegenden Rechtsverstöße (wie z.B. strafbare radikale Hasskommentare, Darstellungen von Kindesmissbrauch und Urheberrechtsverletzungen) sollen verschärft werden.
- Behördenanordnungen gegen illegale Inhalte sollen auf das Hoheitsgebiet des anordnenden Mitgliedsstaats beschränkt werden.

- Bezüglich Werbetracking bzw. -targeting enthält der Kompromissvorschlag eine Forderungen nach mehr Transparenz, aber kein Verbot – so wie offenbar von andere politische Gruppierungen ins Feld geführt.
- Wie bereits von den Mitgliedsstaaten gefordert, enthält der Vorschlag eine Klausel gegen sog. "Dark Patterns".
- Der Vorschlag soll zudem den Plattformen ein Recht auf eine Ende-zu-Ende-Verschlüsselung zubilligen.

Dr. Christoph Krück | Johannes Schäufele

Verbandsklagen bei Verstößen gegen die DS-GVO?

Der Bundesgerichtshof (BGH) musste sich kürzlich mit der Frage befassen, ob bei Verstößen gegen die Datenschutz-Grundverordnung (DS-GVO) auch nationale Verbraucherverbände klagen dürfen. Da der BGH im Hinblick auf die Zulässigkeit einer entsprechenden Klage Zweifel hatte, legte er dem Europäischen Gerichtshof (EuGH) die Frage zur Entscheidung vor (C-319/20). Dass die Problematik nicht nur dogmatisch interessant ist, liegt auf der Hand. Eine entsprechende Klagebefugnis von Verbraucherverbänden kann enorme Auswirkungen auf die datenschutzrechtliche Praxis für Unternehmen entfalten. Man denke insoweit nur an Social-Media-Plattformen oder Webshops sowie vergleichbare Unternehmen, die regelmäßig personenbezogene Daten einer Vielzahl von betroffenen Personen verarbeiten. Da es sich bei den Nutzern entsprechender Plattformen/Webshops regelmäßig gerade um Verbraucher handelt, ist auch das Interesse von Verbraucherverbänden nachvollziehbar. Neu ist eine solche Praxis indes nicht. Im Hinblick auf die Datenschutzrichtlinie 95/46/EG hatte der BGH eine Klagebefugnis von Verbraucherverbänden bereits bejaht. Umso mehr wurden daher die Schlussanträge des Generalanwalts Jean Richard De La Tour mit Spannung erwartet.

Worum geht es in dem Fall?

Die Verbraucherzentrale Bundesverband e.V. (im Folgenden „Bundesverband“) wirft der Facebook Ireland Limited einen Verstoß gegen die Rechtsvorschriften über den Schutz personenbezogener Daten vor, welcher aus Sicht des Bundesverbands gleichzeitig eine unlautere Geschäftspraxis, einen Verstoß gegen ein Verbrauchergesetz sowie einen Verstoß gegen das Verbot der Verwendung unwirksamer Allgemeiner Geschäftsbedingungen darstellt. Auf der Internetplattform Facebook befindet sich ein „App-Zentrum“, in welchem Nutzer der Plattform u.a. kostenlose Spiele von Drittanbietern in Anspruch nehmen können. Bei Aufruf der verschiedenen Spiele erscheint unter dem Button „Sofort spielen“ eine Reihe von Informationen, in denen der Nutzer darauf hingewiesen wird, dass der Spielebetreiber im Falle der Inanspruchnahme seines Spiels eine Reihe personenbezogener Daten des Nutzers erhält. Im Falle des Spiels „Scrabble“ erfolgt zudem die Information, dass der Spielebetreiber im Namen des Nutzers Bilder, Texte und andere Informationen posten darf. Mit der Inanspruchnahme des Spiels stimmt der Nutzer den Allgemeinen Geschäftsbedingungen der Anwendung sowie deren Datenschutzhinweisen zu.

Der Bundesverband beanstandet insbesondere die Präsentation der unter dem Button „Sofort spielen“ gegebenen Hinweise im „App-Zentrum“ als unlauter und rügt zudem die Nichteinhaltung der gesetzlichen Anforderungen für die Einholung einer wirksamen datenschutzrechtlichen Einwilligung des Nutzers. Ferner sieht der Bundesverband in dem abschließenden Hinweis bei Aufruf des Spiels „Scrabble“ eine den Nutzer unangemessen benachteiligende Allgemeine Geschäftsbedingung. Der Bundesverband ist in Deutschland in die Liste qualifizierter Einrichtungen nach § 4 des Gesetzes über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen (UKlaG) eingetragen und gemäß § 3 Abs. 1 UKlaG berechtigt, bei Verstößen gegen sogenannte Verbraucherschutzgesetze auf Unterlassung, Widerruf und Beseitigung zu klagen.

Welche rechtliche Frage stellt sich?

Der BGH ersucht den EuGH nunmehr, da der Klage des Bundesverbands gerade kein Auftrag einer betroffenen Person zugrunde liegt, um eine Auslegung von Art. 80 Abs. 2 DS-GVO. In der Norm heißt es wörtlich:

„Die Mitgliedstaaten können vorsehen, dass jede der in Absatz 1 des vorliegenden Artikels genannten

Einrichtungen, Organisationen oder Vereinigungen unabhängig von einem Auftrag der betroffenen Person in diesem Mitgliedstaat das Recht hat, bei der gemäß Artikel 77 zuständigen Aufsichtsbehörde eine Beschwerde einzulegen und die in den Artikeln 78 und 79 aufgeführten Rechte in Anspruch zu nehmen, wenn ihres Erachtens die Rechte einer betroffenen Person gemäß dieser Verordnung infolge einer Verarbeitung verletzt worden sind."

In Art. 80 Abs. 1 DS-GVO findet sich demgegenüber eine Regelung, welche es bestimmten „Organisationen oder Vereinigungen ohne Gewinnerzielungsabsicht" ermöglicht, im Auftrag von betroffenen Personen, Verstöße gegen die DS-GVO geltend zu machen. Vorliegend begehrt der BGH insbesondere die Feststellung, ob es der Anwendbarkeit des Art. 80 Abs. 2 DS-GVO entgegensteht, dass die durch den Bundesverband gerügten Verstöße auch andere unionsrechtliche und nationalrechtliche Vorschriften, insbesondere auf dem Gebiet des Verbraucherschutzrechts sowie der Bekämpfung unlauterer Geschäftspraktiken, betreffen.

Was sagt der Generalanwalt?

Der Generalanwalt hat dem EuGH in seinen Schlussanträgen nunmehr den folgenden Vorschlag unterbreitet:

„Art. 80 Abs. 2 der Verordnung 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) ist dahin auszulegen, dass er einer nationalen Regelung nicht entgegensteht, die es Verbänden zur Wahrung von Verbraucherinteressen erlaubt, unter den Gesichtspunkten des Verbots der Vornahme unlauterer Geschäftspraktiken, des Verstoßes gegen ein Verbraucherschutzgesetz oder des Verbots der Verwendung unwirksamer Allgemeiner Geschäftsbedingungen gegen den mutmaßlichen Verletzer des Schutzes personenbezogener Daten Klage zu erheben, wenn die betreffende Verbandsklage auf die Wahrung von Rechten gerichtet ist, die den Personen, die von der beanstandeten Verarbeitung betroffen sind, unmittelbar aus dieser Verordnung erwachsen."

Nach Ansicht des Generalanwalts entspricht die Wahrung kollektiver Verbraucherinteressen gerade dem Zweck der DS-GVO, ein hohes Niveau für personenbezogene Daten zu schaffen. Hervorzuheben ist an dieser Stelle, dass - so der Generalanwalt - lediglich das Vorliegen einer Verarbeitung personenbezogener Daten unter Verstoß gegen die Bestimmungen der DS-GVO erforderlich ist, um den Anforderungen des Art. 80 Abs. 2 DS-GVO zu entsprechen. Eine entsprechende Klage müsse daher einzig auf die Verletzung solcher Rechte stützen, die einer natürlichen Person infolge einer Verarbeitung ihrer personenbezogenen Daten aus der DS-GVO erwachsen können.

Welche Entscheidung des EuGH ist zu erwarten?

Auch wenn die Schlussanträge des Generalanwalts grundsätzlich keine Bindung für die Entscheidung des EuGH entfalten, ist die Tendenz zu erkennen, dass der Gerichtshof der dort vertretenen Rechtsauffassung regelmäßig folgt. Wir erwarten daher, dass sich der EuGH ebenfalls dahingehend positionieren wird, die Klage des Bundesverbands als zulässig zu erachten. Für Unternehmen heißt dies umso mehr: Die Beachtung der Anforderungen der DS-GVO ist kein bloßer Formalismus, sondern kann im Falle eines Verstoßes zu beachtlichen Sanktionen und Rechtsfolgen führen. Ist das „Gegenüber" zudem ein Verbraucherverband, hat dies deutliche Auswirkungen auf das wirtschaftliche Ungleichgewicht, welches Betroffene regelmäßig von gerichtlichen Rechtsbehelfen absehen lässt.

Die endgültige Entscheidung des EuGH ist in einigen Monaten zu erwarten.

Dr. Oliver Hornung