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 04/2020

Der IT-Ticker 04/2020 informiert Sie über folgende Themen:

Videokonferenzen und Datenschutz – was ist zu beachten?

Die Covid19-Pandemie und damit einhergehende Kontaktbeschränkungen haben die Bedeutung von Videokonferenzen in verschiedenen Kontexten immens erhöht. Nicht nur Unternehmen nutzen Videokonferenzen zur internen und kundenseitigen Abstimmung, auch für die Aufrechterhaltung des Schulbetriebs oder im öffentlichen Bereich stellen sie mittlerweile ein unverzichtbares Kommunikations-Tool dar. Gerade weil Videokonferenzen in diesen Zeiten so wichtig sind, ist sich auch mit den hiermit einhergehenden Risiken auseinanderzusetzen.

So werden je nach genutztem Funktionsumfang im Rahmen von Videokonferenzen umfangreich personenbezogene Daten generiert und verarbeitet. Die Datenschutzkonferenz (Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bunds und der Länder, „DSK“) hat aus diesem Grund am 23.10.2020 eine hilfreiche Orientierungshilfe veröffentlicht. Wir stellen hier die wesentlichen Inhalte dar und erläutern diese. In Ergänzung hierzu findet sich auf der Webseite des Landesbeauftragten für Datenschutz und Informationsfreiheit NRW eine zusammenfassende Checkliste sämtlicher Anforderungen.

Datenverarbeitung durch Videokonferenzen

Im Rahmen von Videokonferenzen werden eine Vielzahl unterschiedlicher personenbezogener Daten verarbeitet. Der Umfang erschöpft sich dabei nicht nur in den eigentlichen Inhaltsdaten wie übertragenen Ton- und Bilddaten der teilnehmenden Personen sowie der Umgebung wie die jeweilige Wohnung, der Arbeitsplatz oder sonstige Aufenthaltsorts. Je nach Funktionsumfang sind zusätzlich auch Chatnachrichten oder die Übertragung des eigenen Bildschirms möglich. Weiterhin ist es ebenso denkbar, dass aus diesen Informationen auch weitere Schlüsse gezogen werden wie die Art der Kommunikation, berufliche Kontakte, Arbeitszeiten sowie die Arbeitsleistung.
Anwendbarkeit der Datenschutz-Grundverordnung

Eine häufige Fehlvorstellung im Zusammenhang mit der Datenverarbeitung durch Videokonferenzen betrifft die Frage der Anwendbarkeit der Datenschutz-Grundverordnung („DS-GVO“). Der Umstand, dass eine Vielzahl der marktbeherrschenden Videokonferenzsysteme außerhalb Europas gehostet werden, führt nicht zur Unanwendbarkeit der DS-GVO. Vielmehr wurde mit Art. 3 Abs. 2 DS-GVO das sogenannte Marktortprinzip etabliert, welches die Anwendbarkeit der DS-GVO auch für außerhalb der EU niedergelassene Anbieter regelt.
Auftragsverarbeitung?

Die Inanspruchnahme von Videokonferenz-Diensten kann den Abschluss eines Vertrages zur Auftragsverarbeitung nach Art. 28 DS-GVO erforderlich machen. Grundsätzlich sind entsprechende

Verträge abzuschließen, wenn personenbezogene Daten im Auftrag eines Verantwortlichen durch einen Dritten verarbeitet werden. So verhält es sich auch häufig in diesem Zusammenhang. Die DSK stellt klar, dass die Unternehmen, die entsprechende Videokonferenzdienste nutzen, für die Datenverarbeitung verantwortlich sind, da sie maßgeblich die diesbezüglichen Zwecke bestimmen. Sofern eine Konferenzplattform nicht ausnahmsweise selbst betrieben wird, werden häufig die Dienste Dritter in Anspruch genommen.

Da die Datenverarbeitung des Dienstleisters hier eng an die auftragsbezogenen Weisungen des Unternehmens gekoppelt ist, liegt nach Ansicht der DSK in der Regel auch eine Auftragsverarbeitung vor. Das Datenschutzrecht fordert in diesem Zusammenhang den Abschluss eines Vertrages zur Auftragsverarbeitung, der die Inhalte des Art. 28 Abs. 3 DS-GVO umfassen muss.

Gemeinsame Verantwortlichkeit?

Die DSK hebt hervor, dass unter Umständen auch eine sogenannte gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO vorliegen könnte, wenn der Betreiber der Videokonferenzplattform die Daten auch zu eigenen Zwecken nutzt. Eine ähnliche Wertung hat die DSK auch im Zusammenhang mit Google Analytics mit der Begründung vorgenommen, dass bei einer zusätzlichen Verarbeitung der Daten zu eigenen (Werbe-)Zwecken die Datenverarbeitung nicht mehr nur im Auftrag erfolge. Die einzelnen Aspekte der Datenverarbeitung durch Google Analytics können dann auch nicht isoliert betrachtet und bewertet werden, da sie einen „einheitlichen Lebenssachverhalt“ betreffen würden. Die Konsequenz einer solchen Betrachtungsweise ist, dass das Unternehmen und der Dienstleister einen Vertrag nach Art. 26 DS-GVO zur gemeinsamen Verantwortlichkeit abzuschließen hätte. Ob dieses jedoch tatsächlich der Fall ist, muss immer anhand des Einzelfalles geprüft werden.

Zulässigkeit der Datenverarbeitung

Jede Verarbeitung personenbezogener Daten ist durch eine Rechtsgrundlage zu rechtfertigen. Die DSK stellt in diesem Zusammenhang fest, dass die Zulässigkeit der Datenverarbeitung bei Videokonferenzplattformen in der Regel gegeben ist, die einschlägige Rechtsgrundlage jedoch wiederum am Einzelfall zu identifizieren ist. Je nach Kontext der Verarbeitungssituation kann diese in Art. 6 Abs. 1 lit. a, b, e, f DS-GVO oder in Beschäftigungsverhältnissen auch in § 26 Abs. 1 BDSG zu sehen sein.

Von einer Einwilligung ist jedoch gerade im beruflichen oder im schulischen Kontext abzuraten. Die Nutzung von Videokonferenzen in diesen Verarbeitungssituationen liegt wegen fehlender Freiwilligkeit gerade nicht in der alleinigen Entscheidungsbefugnis der betroffenen Personen, sondern ist in der Regel verpflichtender und erforderlicher Bestandteil zur Erfüllung der Arbeitspflichten oder Schulpflicht.

Eine Weiterverarbeitung zu anderen Zwecken durch den Anbieter oder Dritte erfordert eine neue Rechtsgrundlage, die zudem an den engen Voraussetzungen der Zweckbindung nach Art. 5 Abs. 1 lit. b, Art. 6 Abs. 4 DS-GVO zu messen ist.

Übermittlung in Drittländer?

Eine zusätzliche datenschutzrechtliche Rechtfertigung ist erforderlich, wenn die Daten in Drittländer, also in Länder außerhalb der EU oder des Europäischen Wirtschaftsraums übermittelt werden. Dann sind auch die besonderen Bedingungen der Art. 44 ff. DS-GVO einzuhalten. Wichtig ist in diesem Zusammenhang, dass mit dem Urteil C-311/18 (Schrems II) der Beschluss der EU-Kommission zum sogenannten EU-U.S. Privacy Shield für ungültig erklärt wurde, was wiederum für sämtliche in den US gehosteten Konferenzsysteme von Bedeutung sein kann. Alternativ ließe sich der Datentransfer auch durch die Standarddatenschutzklauseln der EU-Kommission rechtfertigen, die der Verantwortliche mit dem Anbieter abzuschließen hätte. Allerdings sind nach dem Meinungsbild des Europäischen Datenschutzausschusses vom 10. November 2020 auch diese Klauseln durch zusätzliche Garantien, die der Datenempfänger im Drittland abzugeben hat, anzupassen. Unsere Einschätzung zur Stellungnahme des Europäischen Datenschutzausschusses vom 10. November 2020 finden Sie hier.

Die Europäische Kommission hat am 12. November 2020 einen Vorschlag für neue Standarddatenschutzklauseln veröffentlicht. Sollte dieser Entwurf angenommen werden, sind

bestehende Standarddatenschutzklauseln innerhalb eines Jahres zu überarbeiten und auf den dann neuen Stand zu bringen. Unsere diesbezügliche Einschätzung find Sie hier.

Gesundheitsdaten

Eine besondere Situation liegt vor, wenn im Rahmen von Videokonferenzen sogenannte besondere Kategorien personenbezogener Daten nach Art. 9 DS-GVO wie etwa Religions- oder Gesundheitsdaten verarbeitet werden. Dieses sei bereits dann der Fall, wenn in einer Videokonferenz Themen mit entsprechenden Bezügen bestehen, etwa im Religionsunterricht oder Theologiestudium. Da die Zulässigkeitsvoraussetzungen der Datenverarbeitung nach Art. 9 DS-GVO sehr viel enger formuliert sind als in Art. 6 Abs. 1 DS-GVO, kann sich insbesondere für Gesundheits- und Religionsdaten eher das Erfordernis einer expliziten Einwilligung nach Art. 9 Abs. 2 lit. a DS-GVO ergeben. Problematisch ist allerdings auch in diesem Zusammenhang die Freiwilligkeit der Einwilligung, die jedoch von der DSK für solche Fälle nicht weiter thematisiert wird.

Technische und organisatorische Maßnahmen

Ein weiteres wichtiges Thema betrifft die Sicherheit der Datenverarbeitung nach Art. 32 DS-GVO durch Implementierung technischer und organisatorischer Maßnahmen. Als wesentliche Maßnahmen identifiziert die DSK für Videokonferenzen eine wirksame Verschlüsselung, Authentifizierungsmechanismen, Softwareaktualisierungen sowie die Zuweisung von Rollen innerhalb der Videokonferenzsysteme.

Erforderlich sei nach der DSK zuvorderst die Implementierung einer Verschlüsselung nach dem Stand der Technik, die sich an den diesbezüglichen Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) orientieren sollte. Die DS-GVO schreibt dabei keine konkrete technische Lösung oder Schutzstandard fest. Vielmehr ist die Wirksamkeit der technischen Lösung nach dem risikobasierten Ansatz zu bestimmen. Je sensitiver die verarbeiteten Daten sind, desto wirksamere Verschlüsselungsmethoden sind zu wählen. Zu beachten ist, dass bei einzelnen Videokonferenz-Anbietern die Verschlüsselung nicht voreingestellt ist, sondern explizit durch den Nutzer einzustellen ist.

Weiterhin sollen nach der DSK nur berechtigte Personen auf die Videokonferenzen und die hierbei verarbeiteten Daten zugreifen können. Auch in diesem Zusammenhang hängt die Mindeststärke der Authentisierung von der Schwere der Risiken für die betroffenen Personen ab, die sich bei Bruch der Vertraulichkeit oder Integrität ergeben können. Wert gelegt werden sollte durch den Verantwortlichen dabei auf eine konsistente Verwaltung der Nutzungsberechtigungen. Die DSK schlägt in diesem Zusammenhang die Abstufung nach Admins, moderierende Personen, präsentierende Personen sowie einfache Teilnehmer und die Festlegung korrespondierender Berechtigungen vor.

Heimliches Mitschneiden

Unbedingt ist das heimliche Mitschneiden von Videokonferenzen zu unterlassen, da dieses eine Straftat darstellt, worüber sämtliche Nutzer wiederum belehrt werden sollten. Soweit möglich, sollte nach der DSK die Möglichkeit der Aufzeichnung durch bloß teilnehmende Personen technisch unterbunden werden. Die ausnahmsweise Aufzeichnung dürfe nur durch besonders privilegierte Nutzer wie Moderatoren durchgeführt werden. Unbedingt erforderlich sei auch ein expliziter Hinweis an alle anwesenden Teilnehmer über den Umstand der Aufzeichnung.

Informationspflichten

Als datenschutzrechtliche Grundpflicht kann die Gewährleistung von Transparenz durch die Erfüllung von Informationspflichten nach Art. 13, 14 DS-GVO gesehen werden. Die DSK weist darauf hin, dass alle Teilnehmer Zugang zu diesen Informationen haben müssen. Hierzu zählen insbesondere Informationen über die Zwecke und die Rechtsgrundlage der Datenverarbeitung, Art der verarbeiteten personenbezogenen Daten, Anbieter des Videokonferenzdienstes sowie Speicherfristen und geplante Übermittlungen in sogenannte Drittländer. Hierbei sollten zu komplexe Formulierungen und technische oder juristische Fachbegriffe vermieden werden.

Weitere datenschutzrechtliche Pflichten

Weitere datenschutzrechtliche Erfordernisse sind die Aktualisierung des Verarbeitungsverzeichnisses nach Art. 30 DS-GVO, die Erfüllung von Meldepflichten nach Art. 33, 34 DS-GVO sowie die Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO, sofern diese erforderlich ist.

Fazit und Ausblick

Die Orientierungshilfe der DSK stellt einen guten Überblick über die relevanten datenschutzrechtlichen Pflichten bei der Nutzung von Videokonferenzsystemen dar. Da entsprechende Anbieter sich überwiegend in den USA befinden, sollten insbesondere die Vorgaben zum Drittlandtransfer geprüft werden. Da sich die pandemisch bedingten (technischen) Veränderungen für Beschäftigte und Unternehmen voraussichtlich längerfristig nicht ändern werden, sollte die Erfüllung der datenschutzrechtlichen Vorgaben als notwendige Investition für Zukunft verstanden werden.

Dr. Oliver Hornung, Frankfurt am Main
o.hornung@skwschwarz.de
Dr. Hendrik Skistims, Frankfurt am Main
h.skistims@skwschwarz.de

Vorschlag der EU Kommission zu neuen Standarddatenschutzklauseln – Post Schrems II

Am 12. November 2020 hat die Europäische Kommission einen Vorschlag für neue Standarddatenschutzklauseln (auch Standardvertragsklauseln genannt; im Folgenden: „SCC-Entwurf“) veröffentlicht. Diese Veröffentlichung erfolgte damit kurz nach der Veröffentlichung der Empfehlungen des Europäischen Datenschutzausschusses („EDSA“) für Drittlandtransfers (Sie finden unsere erste Einschätzung dazu hier) sowie der EDSA-Veröffentlichung „European Essential Guarantees“.

Ziel der Veröffentlichung ist die Durchführung eines kurzen Konsultationsverfahrens. Am Ende sollen neue SCC veröffentlicht werden. Diese möglichen neuen SCC, verbunden mit Empfehlungen für Drittlandtransfers, auch unter Berücksichtigung der Schrems II-Entscheidung, könnten mehr Rechtssicherheit für die Anwender bieten (Sie finden unseren Beitrag zu der Schrems II-Entscheidung hier).

Aufbau des SCC-Entwurfs

Der SCC-Entwurf ist modular aufgebaut. Dies bedeutet, es soll eine SCC-Fassung geben, welche die folgenden vier Szenarien durch Textmodule abdeckt:

1. Modul 1: Übermittlung zwischen zwei (oder mehr) Verantwortlichen („Controller-Controller“).

2. Modul 2: Übermittlung von einem Verantwortlichem zu einem (oder mehr) Auftragsverarbeitern („Controller-Processor“).

3. Modul 3: Übermittlung von einem Auftragsverarbeiter zu einem (oder mehr) Auftragsverarbeitern („Processor-Processor“).

4. Modul 4: Übermittlung von Auftragsverarbeiter zu einem (oder mehr) Verantwortlichen („Processor-Controller“).

Ausgewählte Inhalte des SCC-Entwurfs im Rahmen der Schrems II-Entscheidung

Einige Anforderungen, die insbesondere aufgrund der Schrems II-Entscheidung in den Diskussionsfokus gerückt sind, spiegeln sich bereits in diesem SCC-Entwurf wieder. Dazu gehören ein verstärkter Fokus auf Transparenzanforderungen und ein ausdifferenzierterer Umgang mit verschiedenen landesrechtlichen Vorgaben.

Beispielsweise wird der Datenimporteur in einer Controller-Controller-Situation verpflichtet, bestimmte Informationen den jeweils Betroffenen zur Verfügung zu stellen, entweder direkt oder indirekt über den Datenexporteur. Dazu gehören insbesondere die Informationen über die Identität des Datenimporteurs und über alle relevanten Datenverarbeitungen, auch über eigene relevante Datenverarbeitungen des Datenimporteurs als Verantwortlicher.

Der SCC-Entwurf enthält im Grundsatz Klauseln mit Schutzwirkung für Dritte. Dies bedeutet, dass sich Betroffene direkt auf diese Klauseln stützen können, um Ansprüche gegen den Datenexporteur und/oder den Datenimporteur geltend zu machen (vgl. Section I, Clause 2).

Der SCC-Entwurf enthält die eindeutige Verpflichtung, dass bei einer weiteren Datenübermittlung des Datenimporteurs an einen Dritten (sog. „onward transfer“) entweder dieser Dritte ebenfalls die entsprechenden SCC-Verpflichtungen mitübernehmen muss oder ein andere Rechtfertigung nach der DSGVO für eine solche Datenübermittlung gegeben sein muss (vgl. Section II, Modul 1 Clause 1.7, Modul 2 Clause 1.8 und Modul 3 Clause 1.8).

Eine Klausel, die auf alle oben genannten Standardszenarien anwendbar ist, befasst sich mit dem nationalen Recht des Datenimporteurs. Dabei sichern die Parteien, also Datenexporteur und –importeur zu, dass sie davon ausgehen, dass lokales Recht den Datenimporteur nicht in der Wahrnehmung seiner entsprechenden Pflichten hindert (Section II, Clause 2). Zudem erarbeiten sie eine Datenübermittlungs-Folgenabschätzung und stellen sie auf Anforderung der zuständigen Datenschutzaufsichtsbehörde zur Verfügung (Section II, Clause 2 lit d)).

Eine weitere Klausel verpflichtet den Datenimporteur unverzüglich zumindest den Datenexporteur – und wenn möglich die jeweils Betroffenen – zu informieren, wenn eine hoheitliche Stelle Zugriff auf personenbezogenen Daten fordert. Der Datenimporteur soll zudem verpflichtet sein, gegen eine solche Anordnung vorzugehen, wenn es Anhaltspunkte für die Rechtswidrigkeit einer solchen Anordnung gibt (Section II, Clause 3).

Zudem wird dem Datenexporteur ein außerordentliches Kündigungsrecht eingeräumt, wenn der Datenimporteur sich nicht an eine SCC-Verpflichtung hält (vgl. Section III, Clause 1).

Der Anhang für die technischen und/oder organisatorischen Maßnahmen enthält Platzhalter mit Anregungen, welche Maßnahmenarten beispielsweise geregelt werden könnten.

Ausblick

Ein Kritikpunkt, der bereits in dem Konsultationsverfahren aufgekommen ist, ist die Tatsache, dass dieser SCC-Entwurf letztlich nicht einen geheimen Datenzugriff durch staatliche Stellen abwenden kann. Ein zentrales Problem der Schrems II-Entscheidung wird daher nicht durch diesen SCC-Entwurf gelöst.

Im Übrigen enthält der SCC-Entwurf gute Ansätze, um den Rechtsanwendern ein Update für ein sehr wichtiges Tool zur internationalen Datenübermittlung an die Hand zu geben. Nachdem der SCC-Entwurf selbst keine technischen und/oder organisatorischen Schutzmaßnahmen enthält, sind die Empfehlungen des EDSA für Drittlandtransfers parallel heranzuziehen. Zudem werden DSGVO-ähnliche Anforderungen auf den Datenimporteur eindeutig ausgeweitet.

Sollte dieser SCC-Entwurf angenommen werden, sind bestehende (alte) SCC innerhalb eines Jahres zu überarbeiten und auf den dann neuen Stand zu bringen (vgl. Art. 6 Abs. 3 des Entwurfs für die Implementierungsentscheidung).

Allerdings ist unklar, ob dieser SCC-Entwurf letztlich verabschiedet wird. Die europäischen Datenschutzbehörden haben bereits abweichende Auffassungen geäußert.

Hannah Mugler, Berlin, h.mugler@skwschwarz.de
Dr. Elisabeth von Finckenstein, München, E.vonFinckenstein@skwschwarz.de
Nikolaus Bertermann, Berlin, n.bertermann@skwschwarz.de
Dr. Stefan Peintinger, München, s.peintinger@skwschwarz.de

Verstöße gegen die DS-GVO doch nicht so schlimm? – Bußgelder reduzieren sich drastisch

Anstelle der angekündigten Rekord-Bußgelder verhängte die ICO deutliche geringere Strafen gegen British Airways und Marriott. Das Landgericht Bonn reduziert das gegen 1&1 verhängte Bußgeld drastisch. Was ist passiert?

ICO verhängt deutlich geringere Bußgelder gegen British Airways und Marriott

Im Juli 2019 kündigte die britische Datenschutzbehörde ICO das bislang in Europa höchste Bußgeld in Höhe von € 200 Mio. gegen British Airways und € 110 Mio. gegen die Hotelkette Marriott an (SKW Schwarz berichtete). Nunmehr wurden diese Bußgelder jedoch in erheblichen Umfang reduziert - € 22 Mio. bzw. € 20,3 Mio.

Nach den Vorgaben der DS-GVO können die nationalen Datenschutzaufsichtsbehörden Bußgelder von bis zu € 20 Mio. oder 4 % des gesamten weltweit erzielten Jahresumsatzes des vorausgegangenen Geschäftsjahres aussprechen je nach dem welcher Betrag der höhere ist. Bei der Bemessung der Höhe des Bußgeldes spielt auch die finanzielle Situation des Unternehmens unter Umständen eine gewichtige Rolle. Durch die sogenannte Regulatory Action Policy ist die Datenschutzbehörde ICO verpflichtet, bei der Höhe der festzulegenden Bußgelder auch die ökonomischen Folgen für das Unternehmen zu berücksichtigen, insbesondere zu bedenken, ob sich das Unternehmen, das einen Datenschutzverstoß begangen hat, das Bußgeld der Höhe überhaupt leisten kann.

Nachweislich gehören British Airways und die Hotelkette Marriott zu den von der Corona-Pandemie stark betroffenen Unternehmen. Demzufolge berücksichtigte die Datenschutzbehörde ICO unter anderem die ökonomischen Folgen der Covid 19-Pandemie und reduzierte die Bußgelder gegen die beiden Konzerne erheblich. Auch der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg hat in seinem Bußgeldverfahren gegen die AOK Baden-Württemberg die gegenwärtigen Herausforderungen der AOK in Folge der aktuellen Corona-Pandemie in besonderem Maß berücksichtigt.

Neben der aktuellen Corona-Pandemie führten weitere Faktoren dazu, dass die Datenschutzbehörde ICO die hohen Millionenbußgelder gegen die Fluggesellschaft British Airways und die Hotelkette Marriott abmilderte. Die Behörde hob die Kooperationsbereitschaft beider Unternehmen hervor und betonte die erheblichen Anstrengungen beider Unternehmen die Maßnahmen zur Datensicherheit und IT-Sicherheit aufzurüsten.

Landgericht Bonn reduziert Bußgeld gegen 1&1 um 90 %

Anders lag der Fall bei dem Bußgeld, welches gegen die die 1&1 Telecom GmbH verhängt worden ist. Der Bundesbeauftragte für Datenschutz und Informationsfreiheit (BfDI) verhängte am 9. Dezember 2019 ein Bußgeld in Höhe von € 9,5 Mio. gegen den Telekommunikationsdienstleister wegen eines Verstoßes gegen Art. 32 DS-GVO, weil das Authentifizierungsverfahren für telefonische Auskünfte nicht dem Stand der Technik entspräche.

Die 1&1 Telecom GmbH klagte gegen den Bußgeldbescheid und begründete die Kläger damit, dass das Bußgeld unverhältnismäßig sei und die Bemessung gegen das Grundgesetz verstoßen würde. Das Landgericht Bonn bestätigte mit seinem Urteil vom 11. November 2020 zwar einen Verstoß gegen Art. 32 DS-GVO. Das Bußgeld wurde jedoch drastisch auf € 900.000,00 reduziert.

In der Sache sah das Landgericht Bonn nur einen leichten, nicht vorsätzlichen Verstoß gegen Art. 32 DS-GVO in einem Einzelfall für den ein Bußgeld in Millionenhöhe nicht angemessen sei. In das Urteil flossen zahlreiche mildernde Umstände ein. So seien keine besonderen Kategorien personenbezogener Daten betroffen und eine massenhafte Herausgabe von Daten sei nicht zu befürchten gewesen. Das Verschulden des Telekommunikationsdienstleisters sei gering anzusehen. Im Hinblick auf die über Jahre geübte Authentifizierungspraxis, die bis zu dem Bußgeldbescheid nicht beanstandet worden sei, habe es dort an dem notwendigen Problembewusstsein gefehlt. Demzufolge reduzierte das Landgericht Bonn die Höhe des Bußgeldes drastisch.

Eine weitere Kernfrage des Verfahrens – können Bußgelder überhaupt unabhängig von den Bestimmungen der §§ 30, 130 OWiG gegen Unternehmen verhängt werden – bejahte das Landgericht

Bonn. Dem Urteil liegt damit die Geltung des Europäischen Unternehmensbegriffs zugrunde - die Verhängung eines Bußgelds gegen ein Unternehmen würde nicht davon abhängen, dass der konkrete Verstoß einer Leitungsperson des Unternehmens festgestellt werde. Das nach Auffassung des Landgerichts Bonn anwendbare Europäische Recht stelle – anders als das Deutsche Ordnungswidrigkeitenrecht – kein entsprechendes Erfordernis auf.

Welche Folgen haben die drei aufgezeigten Reduzierungen für die Praxis?

Obwohl in den vorliegend benannten Fällen die Bußgelder drastisch reduziert worden sind, sollten Unternehmen sich jetzt nicht zurücklegen. Es muss bei Verstößen gegen die DS-GVO auch zukünfitg mit hohen Bußgeldern gerechnet werden. Verantwortliche können jedoch darauf bauen, dass aktuelle wirtschaftliche Entwicklungen sowie Verschuldensfragen bei der Bemessung des Bußgeldes zu berücksichtigen sind.

Die drei Verfahren gegen die Fluggesellschaft British Airways, die Hotelkette Marriott und den Telekommunikationsdienstleister 1&1 zeigen deutlich auf, dass Mängel bei der Datensicherheit einen der häufigsten Gründe darstellen, bei denen Datenschutzaufsichtsbehörden Bußgeldverfahren einleiten. Unternehmen sollten daher ihre Konzepte zur Datensicherheit regelmäßig überprüfen und bei Bedarf nachbessern. Eine regelmäßige Überprüfung der technischen und organisatorischen Schutzmaßnahmen nach Art. 32 DS-GVO kann zudem dazu beitragen, das Risiko zu minimieren, dass die zuständige Datenschutzaufsichtsbehörde einen Verstoß gegen Vorschriften der DS-GVO feststellt und widrigenfalls ein Bußgeld verhängt.

Weiterhin zeigt sich, dass Unternehmen gut beraten sind gegen verhängte/angekündigte Bußgelder vorzugehen. Das Beispiel des Telekommunikationsdienstleisters 1&1 zeigt, dass das Bußgeldkonzept der Datenschutzkonferenz vom 14. Oktober 2019 (SKW Schwarz berichtete) auf dem Prüfstand steht. Das Landgericht Bonn kritisierte, dass ein rein umsatzorientiertes Bußgeldkonzept wesentliche Bemessungspunkte außer Acht lässt. Demzufolge erklärte auch der Bundesdatenschutzbeauftragte Kelber in der Verhandlung, dass das Bußgeldkonzept der Datenschutzkonferenz überarbeitet werde.

Die Taskforce Datenschutz-Litigation von SKW Schwarz unterstützt Unternehmen bei allen Fragen rund um angedrohte oder verhängte Bußgelder sowohl bei außergerichtlichen Verhandlungen als auch bei der Vertretung vor staatlichen Gerichten bis hin zum EuGH. Zudem ist die Taskforce spezialisiert auf die Abwehr materieller und immaterieller Schadensersatzklagen sowie Abwehr von Einmeldeklagen von Verbrauchern gegen Inkassounternehmen und Auskunfteien.

Dr. Oliver Hornung, Frankfurt am Main
o.hornung@skwschwarz.de
Franziska Ladiges, Frankfurt am Main
f.ladiges@skwschwarz.de

Empfehlungen des EDSA für Drittlandstransfers veröffentlicht

Der Europäische Datenschutzausschuss (EDSA) hat am 10.11.2020 Empfehlungen für die Gestaltung von Datentransfers in so genannte Drittländer außerhalb der EU und des EWR veröffentlicht. Der EuGH hatte am 16.07.2020 entschieden, dass die Übermittlung personenbezogener Daten auf Grundlage des EU-US Privacy Shield unzulässig und bei der Nutzung von EU Standardvertragsklauseln eine eigene Wirksamkeitsprüfung durch die Verwender notwendig ist. In der Entscheidung hat der EuGH zudem klargestellt, dass Datentransfers in die USA allein auf Grundlage von EU Standardvertragsklauseln nicht mehr möglich sind. Dies stellt Unternehmen und Organisationen vor ganz erhebliche Probleme.

Vor diesem Hintergrund ist es zu begrüßen, dass nun auf europäischer Ebene erste belastbare Positionierungen erfolgt sind, auch wenn diese auf den ersten Blick nicht geeignet sind, die zahlreichen Probleme der Praxis zu lösen. Der EDSA folgt der harten Linie des EuGH und unternimmt keinen Versuch, Stellschrauben der DS-GVO für pragmatische Lösungen zu nutzen. Die Vorstellungen des EuGH und des EDSA zum Schutz personenbezogener Daten weichen so grundlegend von den Vorstellungen vieler anderer Länder außerhalb der EU ab, dass eine dauerhafte Lösung nur politisch und gesetzgeberisch erreicht werden kann. Leidtragende dieses globalen Konflikts sind derzeit in der Praxis allein die Unternehmen in der EU.

Der EDSA betont ausdrücklich die Verantwortung jedes Datenexporteuers, Übermittlungen in Drittländer genau zu prüfen und ein Schutzniveau für die personenbezogenen Daten sicherzustellen, welches dem der EU vergleichbar ist. Er formuliert dafür ein sechs stufiges Verfahren, welches nachfolgend mit der jeweiligen Bedeutung für die Praxis grob skizziert wird:

Stufe 1: Dokumentation aller Übermittlungen personenbezogener Daten in Drittländer

Der EDSA macht deutlich, dass der Dokumentation der Übermittlungen in Drittländern eine große Relevanz zukommt. Allerdings weist der EDSA ausdrücklich darauf hin, dass nach seiner Auffassung schon jede Zugriffsmöglichkeit aus einem Drittland (z.B. für Wartung und Support) einen Drittlandstransfer darstellt. Außerdem weist der EDSA darauf hin, dass auch Weiterübermittlungen z.B. an Subunternehmer in einem (anderen) Drittland zu berücksichtigen sind. Sämtliche Datentransfers in Drittländer sollten regelmäßig bereits im Verzeichnis der Verarbeitungstätigkeiten dokumentiert sein.

Stufe 2 und 3: Auswahl eines Transferinstruments sowie Prüfung der Wirksamkeit

Hinsichtlich der Wirksamkeit des gewählten Transferinstruments stellt der EDSA nochmals klar, dass sich Datenexporteure auf Angemessenheitsbeschlüsse der EU-Kommission nach Art. 45 DS-GVO oder der Datenschutzrichtlinie (95/46/EG) ohne weitere Prüfung berufen können, sofern die entsprechenden Beschlüsse nicht vom EuGH oder von der Kommission aufgehoben wurden (wie z.B. der für das EU-US Privacy Shield durch den EuGH). Für alle Garantien nach Art. 46 DS-GVO verlangt der EDSA eine individuelle Überprüfung der Wirksamkeit. Hinsichtlich der Ausnahmetatbestände des Art. 49 DS-GVO weist der EDSA darauf hin, dass diese nach seiner Auffassung in ihrem Anwendungsbereich eng auszulegen sind (siehe dazu auch Guidelines 2/2018).

Bei der Prüfung der Wirksamkeit von Garantien nach Art. 46 DS-GVO erwartet der EDSA eine Einzelfallprüfung des konkreten Datentransfers unter Berücksichtigung aller Verarbeitungsschritte und aller betroffenen Drittländer. Er betont ausdrücklich, dass auch sämtliche Subunternehmer einzubeziehen sind. Dabei soll die Einzelfallprüfung dokumentieren, ob die getroffenen Maßnahmen die Essenziellen Europäischen Garantien erfüllen, zu denen der EDSA ebenfalls am 10.11.2020 Empfehlungen veröffentlicht hat.

Stufe 4: Auswahl und verbindliche Vereinbarung zusätzlicher Schutzmaßnahmen

Kommt die Prüfung zu dem Ergebnis, dass die vereinbarten Garantien nach Art. 46 DS-GVO kein angemessenes Schutzniveau für die personenbezogenen Daten sicherstellen, müssen zusätzliche Schutzmaßnahmen geprüft werden. Diese Stufe wird somit in der Praxis die größte Relevanz haben. Diese zusätzlichen Maßnahmen können grundsätzlich vertraglicher, technischer oder organisatorischer Art sein, wobei der EDSA klarstellt, dass allein vertragliche und organisatorische Maßnahmen in der Regel keinen wirksamen Schutz gegen behördliche Zugriffe schaffen können. Sofern Maßnahmen gefunden und vereinbart werden, die ein angemessenes Schutzniveau für die Daten im Drittland schaffen, ist die Übermittlung grundsätzlich möglich.

Sehr hilfreich ist die umfangreiche Darstellung von Beispielen ergänzender Maßnahmen im Annex 2. Sie ermöglicht eine gute Orientierung, obwohl viele Beispiele lebensfremd und wenig praxistauglich erscheinen. Erfreulich ist jedoch, dass der EDSA die Pseudonymisierung von Daten ausdrücklich als mögliche Maßnahme beschreibt, sofern der Datenimporteur (und entsprechend auch die ausländische Behörde) keine Möglichkeit hat, die Daten auf einzelne Personen zurück zu führen.

Stufe 5: Formale Bestätigung der Prozessschritte (soweit erforderlich)

Es kann jedoch notwendig sein, die gefundenen zusätzlichen Maßnahmen mit der zuständigen Aufsichtsbehörde abzustimmen. Höchst erfreulich ist die ausdrückliche Klarstellung des EDSA, dass zusätzliche Vereinbarungen zu EU Standardvertragsklauseln keiner Zustimmung oder Freigabe der zuständigen Aufsichtsbehörde bedürfen, solange die Formulierungen der EU Standardvertragsklauseln nicht verändert sondern nur ergänzt werden und die zusätzlichen Regelungen den EU Standardvertragsklauseln nicht widersprechen. Jede Veränderung der Formulierungen der EU Standardvertragsklauseln bedarf jedoch der Zustimmung der Aufsichtsbehörde. Der EDSA stellt ferner klar, dass die Schrems-II-Entscheidung auch für verbindliche

interne Datenschutzvorschriften („Binding Corporate Rules“) gilt und stellt in Aussicht, dass dazu noch eine gesonderte Veröffentlichung des EDSA erfolgen wird.

Stufe 6: Regelmäßige Überprüfung der getroffenen Maßnahmen

Zuletzt stellt der EDSA klar, dass alle getroffenen Maßnahmen einer regelmäßigen Überprüfung bedürfen. Dabei verlangt der EDSA ausdrücklich, dass Maßnahmen getroffen werden müssen, die eine kurzfristige Beendigung der Datenübermittlung ermöglichen, wenn der Datenimporteur gegen die vereinbarten Regeln verstößt.

Erstes Fazit zu den Empfehlungen des EDSA

Die vom EDSA beschriebenen Stufen sind nachvollziehbar dargestellt und entsprechen im Wesentlichen den bisher schon diskutierten Maßnahmen. Die geforderte eingehende Prüfung des lokalen Rechts in den Empfängerländern dürfte insbesondere für kleine und mittelständische Unternehmen praktisch nicht leistbar sein und selbst große Unternehmen vor kaum lösbare Herausforderungen stellen. Möglicherweise wird es ratsam sein, das angemessene Schutzniveau im Drittland vorsorglich zu verneinen und eher nach technischen Schutzmaßnahmen zu suchen, die – wo dies möglich ist – einen Datenzugriff ausländischer Behörden wirksam verhindern.

Leider geht der EDSA gar nicht auf die Datenverarbeitung in multinationalen Unternehmen ein, in denen regelmäßig auch personenbezogene Daten aus der EU in Drittländern eingesehen und verarbeitet werden müssen. Nach den Beispielen des EDSA ist die Übermittlung von personenbezogenen Daten an Konzerngesellschaften in einem Drittland praktisch unmöglich. Ob es tatsächlich die Intention der DS-GVO ist, multinationale Unternehmen mit Beteiligung von europäischen Unternehmen faktisch zu verbieten, darf bezweifelt werden.

Auch das für die Praxis höchst relevante Problem temporärer Wartungszugriffe aus einem Drittland spricht der EDSA ausdrücklich nicht an, obwohl hier eine Hilfestellung für die betroffenen Unternehmen besonders wichtig gewesen wäre.

Die Empfehlungen des EDSA wurden ausdrücklich zur öffentlichen Kommentierung veröffentlicht. Es steht daher zu erwarten, dass umfangreiche Anmerkungen auch aus der Praxis beim EDSA eingehen werden. Möglicherweise wird dies zu weiteren praxisnahen Beispielen führen. Fundamentale Änderungen sind aber durch die Berücksichtigung der öffentlichen Kommentierung wohl nicht mehr zu erwarten.

Praxistipp

Der EDSA stellt klar, dass er die EuGH-Entscheidung sehr ernst nimmt und die nationalen Aufsichtsbehörden dazu anhält, die Übermittlungen in Drittländer zu prüfen. Viele nationale Aufsichtsbehörden haben bereits angekündigt, das Thema zu einem Prüfungsschwerpunkt zu machen. Verantwortlichen ist daher dringend anzuraten, das Thema entsprechend zu beachten, Datenübermittlungen in Drittländer dokumentiert zu prüfen, anzupassen oder sogar vorübergehend auszusetzen. Die aktuelle Rechtslage muss als ausgesprochen herausfordernd eingestuft werden.

Nikolaus Bertermann, Berlin, n.bertermann@skwschwarz.de
Hannah Mugler, Berlin, h.mugler@skwschwarz.de
Dr. Stefan Peintinger, München, s.peintinger@skwschwarz.de
Dr. Elisabeth von Finckenstein, München, E.vonFinckenstein@skwschwarz.de

Novelle des Jugendschutzgesetzes: Online-Plattformen im Fokus

Um die Reform des Jugendschutzrechts in Deutschland war es einige Zeit ruhig - vielleicht aufgrund der heftigen Kritik aus der Praxis. Am 14. Oktober hat die Regierung nun aber den Reformprozess eingeleitet. Dieser konzentriert sich deutlich auf die Regulierung von Online-Plattformen und etabliert neue Pflichten, die insbesondere Games- und Video-Plattformen treffen werden. Mit dem Reformgesetz soll ein breiter internationaler Anwendungsbereich, „Vorsorgemaßnahmen“ sowie neue Kennzeichnungspflichten eingeführt werden.

Die Bundesregierung hat am 14. Oktober den formellen Reformprozess für das Jugendschutzgesetz in Deutschland eingeleitet. Ziel soll es sein, dass das Gesetz im ersten oder zweiten Quartal 2021 in Kraft treten kann. Zum Hintergrund: In Deutschland gibt es derzeit einen Jugendmedienschutz-Staatsvertrag, der vor allem Jugendschutzstandards für Rundfunk und Telemedien festlegt. Daneben gibt es das Jugendschutzgesetz, ein Bundesgesetz, das unter anderem den Jugendschutz für Trägermedien und die Alterskennzeichnung abdeckt („Offline-Schutz"). Neben kritischen materiell-rechtlichen Aspekten von denen einige nachfolgend dargestellt werden, zielt das Reformgesetz auch darauf ab, die erwähnte „Zweiteilung" der Regel zu brechen. Es soll zudem auf neuen Interaktions- und Kommunikationsrisiken durch Online-Chats, User-Generated-Content sowie Cyber-Mobbing reagiert werden. Einige Änderungen sind auf die Richtlinie EU/2018/1808 über audiovisuelle Mediendienste zurückzuführen.

Weiter Anwendungsbereich

Zum einen weitet das Reformgesetz den Geltungsbereich des Bundesgesetzes auf Online-Dienste aus; Rundfunk ist nach wie vor nicht erfasst. Zum anderen wird eine Anwendung auf Dienste außerhalb der EU beabsichtigt und die Gesetzesbegründung enthält obendrein einige mehrdeutige Hinweise auf Ausnahmen vom Herkunftslandprinzip im Bereich des E-Commerce in der EU. Neben der Tatsache, dass letzteres z.B. praktische Schwierigkeiten bei der Durchsetzung der Regeln außerhalb Deutschlands aufwerfen würde, wird dieser Aspekt sicherlich auch während des nun beginnenden Gesetzgebungsprozesses kontrovers diskutiert.

„Vorsorgemaßnahmen" für Online-Plattformen

Das Reformgesetz führt die Verpflichtung für Online-Plattformen ein angemessene Vorsorgemaßnahmen einzurichten. Solche Vorsorgemaßnahmen können z.B. ein Beschwerde- bzw. „Notice-and-Take-Down"-Verfahren, Benachrichtigungsfunktionen für nutzergenerierte Inhalte, Bewertungssysteme für Nutzer (z.B. zur Bewertung der Inhalte mit „ab 18 Jahren"), technische Mittel zur Altersverifizierung oder leicht auffindbare Hinweise für Beratungs-, Hilfs- und Meldeeinrichtungen sein. Die Verpflichtung wird wahrscheinlich nur für Host-Provider die fremden Inhalte speichern gelten.

Kennzeichnungspflichten für Online-Plattformen

Neben der Einführung von „illustrativen Symbolen" sieht das Gesetz auch eine neue Kennzeichnungspflicht für Film- und Spiele-Plattformen vor, d.h. die Anbieter müssen die Inhalte jetzt auch selbst kennzeichnen. Gegenwärtig besteht lediglich die Pflicht bereits bestehenden Kennzeichnungen anzuzeigen. Die Pflicht soll wohl nur für Online-Plattformen gelten die eigene Inhalte anbieten, also beispielsweise Video-on-Demand-Plattformen oder auch Online-Stores für Games und Apps.

Zustellungsbevollmächtigter in Deutschland

Die Reform führt weiterhin die Verpflichtung zur Bestellung eines inländischen Zustellungs-bevollmächtigen ein. Eine ähnliche Regelung ist bereits aus dem Netzwerkdurchsetzungsgesetz bekannt.

Ausblick und nächste Schritte

Das Gesetz soll im ersten oder zweiten Quartal 2021 in Kraft treten. Branchenverbände haben das Gesetz aber auch bereits kritisiert. Es ist daher insgesamt noch nicht klar, ob es ohne Änderungen in Kraft treten wird - es muss nun erstmal den Gesetzgebungsprozess durchlaufen. Wir werden Sie gerne über die Entwicklung des Gesetzgebungsprozess informieren. Bitte kontaktieren Sie uns auch gerne, wenn wir Ihnen bei einer Einschätzung bezüglich einer möglichen Anwendung der neuen Pflichten auf Ihre Dienste helfen können.

Dr. Christoph Krück, München
c.krueck@skwschwarz.de

Einsatz von Datenbrillen (Smart Glasses) im Unternehmen

Die Auswirkungen der Corona-Pandemie haben zeitweise ganze Volkswirtschaften zum Erliegen gebracht und eine der schwersten wirtschaftlichen Krisen seit Jahrzehnten verursacht. Neben der Tourismusbranche hat es insbesondere auch das produzierende Gewerbe besonders hart getroffen. So ist etwa laut des Verbands der Automobilindustrie („VDA“) die Zahl der Kfz-Neuzulassungen in Deutschland im ersten Halbjahr 2020 um 35 Prozent auf 1,21 Millionen Einheiten eingebrochen. Für das gesamte Jahr rechnet der VDA mit einem Rückgang von rund 23 Prozentpunkten in Deutschland, wobei perspektivisch auch der europäische Markt mit einem Rückgang von 24 Prozentpunkten ähnlich stark schrumpfen wird. Nachdem der anfängliche Schock überwunden und erste Maßnahmen zur Abmilderung der unmittelbaren Auswirkungen ergriffen worden sind, heißt es nun, langfristig wirkende Maßnahmen zu implementieren, um ein Mindestmaß an Robustheit gegen weitere „Wellen“ oder völlig neue Pandemien zu erlangen.

Ein momentan zu beobachtender Trend ist der Einsatz von sogenannten „Datenbrillen“ oder „Smart Glasses“, welche routinemäßig insbesondere bereits in der Lagerlogistik und der Kommissionierung eingesetzt werden. Smart Glasses stellen eine noch relativ neuartige Mensch-Maschine-Schnittstelle dar, die mittels Videosensorik Umgebungsbedingungen erfasst und die Nutzer in Echtzeit via Internet anhand der gesammelten Informationen unterstützt. Aus Produktionsbetrieben heraus können etwa den Wartungsdienstleistern die Videodaten übermittelt und so direkte Kommunikationsmöglichkeiten mit dem Träger der Brille ermöglicht werden. Die Nutzer können so in Echtzeit bei einfachen Reparaturen oder Bedienungsschwierigkeiten unterstützt werden, wobei die Use Cases nahezu beliebig erweiterbar sind. Marktreif sind etwa die Vernetzung von Datenbrillen mit den unternehmenseigenen ERP- und CRM-Systemen, die IT-gestützte Abarbeitung von Checklisten oder die schnittstellenbasierte Anbindung von weiteren Maschinen oder Werkzeugen. Perspektivisch lassen sich auch Anwendungen Künstlicher Intelligenz („KI“) in das System einbinden, wodurch die KI den Nutzer automatisiert unterstützt, indem sie eigenständig Reparaturbedarf oder fehlerhafte Einstellungen von Anlagen erkennt. Mit Blick auf Covid-19 erlangt diese Technologie einen besonderen Nutzen: Sämtliche Arbeiten an oder Kontrollen von Produktionsmaschinen können vollständig per Remote durchgeführt werden und erfordern keine physische Präsenz von Dienstleistern. Auch rein betriebsinterne Vorgänge lassen sich so ohne physische Kontakte reorganisieren.

Rechtlichen Risiken – Was ist zu beachten?

Die Verwirklichung der vorgenannten Chancen geht auch mit rechtlichen Risiken einher, die es zu identifizieren und abzumildern gilt. Zwar besitzt der Arbeitgeber das Recht, die Angestellten zur Nutzung von modernen Arbeitswerkzeugen anzuweisen. Das diesbezügliche arbeitgeberseitige Ermessen reicht allerdings nur so weit, wie durch die Nutzung Rechte und rechtlich geschützte Interessen der betroffenen Belegschaft nicht verletzt werden. Hierzu gehören im Kontext IT-getriebener Datenverarbeitung insbesondere auch persönlichkeitsrechtliche und datenschutzrechtliche Belange, da die Nutzung von Smart Glasses in der Regel mit der Verarbeitung einer Vielzahl personenbezogener Beschäftigtendaten einhergeht. Das Bundesarbeitsgericht hat in einer Vielzahl von Entscheidungen die Schutzwürdigkeit der Beschäftigten vor einer unzulässigen Überwachung mittels unterschiedlicher Technologien immer wieder bestätigt.

Betriebsvereinbarungen und Verarbeitungsregeln

Elementar für einen datenschutzkonformen Einsatz sind die Heranziehung der richtigen Rechtsgrundlage sowie die Identifizierung der diesbezüglichen gesetzlichen Grenzen. Auch wenn gesetzliche Erlaubnistatbestände wie § 26 Abs. 1 BDSG (Datenverarbeitung im Beschäftigtenverhältnis) oder Art. 6 Abs. 1 lit. f) DSGVO (berechtigtes Interesse des Arbeitgebers) nicht per se ausgeschlossen sind, sollte aus Gründen der Rechtssicherheit der Abschluss einer Betriebsvereinbarung zur Legitimierung der Verarbeitungstätigkeiten mittels Smart Glasses in Betracht gezogen werden, wenn das für den Datenschutz verantwortliche Unternehmen über einen Betriebsrat verfügt.

Betriebsvereinbarungen können kraft gesetzlicher Anordnung eine wirksame datenschutzrechtliche Rechtsgrundlage darstellen, die gegenüber gesetzlichen Legitimierungen den Vorteil haben, dass hierdurch für das jeweilige Unternehmen passgenaue Regelungen entworfen werden können. Insbesondere darf der Einsatz entsprechender Technologien nicht dazu führen, dass die

Beschäftigten einer lückenlosen Leistungs- und Verhaltenskontrolle unterzogen werden. Existiert kein Betriebsrat, so sollten zumindest interne Verarbeitungsregeln (Richtlinie zum Einsatz von Datenbrillen) geschaffen werden, die rechtlich zwar unverbindlich sind, jedoch den Entscheidungsträgern im Unternehmen wertvolle Rechtssicherheit geben.

Einbindung eines IT-Dienstleisters

Wenn die Implementierung von Smart Glasses unter Einbindung eines IT-Dienstleisters geschieht ist mit diesem ein Vertrag zur Auftragsverarbeitung mit den Pflichtinhalten des Art. 28 Abs. 3 DSGVO abzuschließen. Herzstück des Vertrags zur Auftragsverarbeitung sind angemessene technische und organisatorische Maßnahmen nach Art. 24, 25 und 32 DSGVO.

Art. 25 Abs. 1 DSGVO und Art. 32 DSGVO verpflichten den Verantwortlichen mit dem Dienstleister technische und organisatorische Maßnahmen zu treffen, um die Grundsätze der DSGVO wirksam umzusetzen und die Rechte der betroffenen Personen zu schützen.

Grenzüberschreitender Datenverkehr

Ferner bestehen zusätzlich zu beachtende Vorgaben, wenn die Implementierung von Smart Glasses unter Einbindung eines IT-Dienstleisters geschieht, dessen Server sich in den USA oder einem sonstigen Drittland befinden. In diesem Fall sind die besonderen Regelungen zum grenzüberschreitenden Datenverkehr nach Art. 44 ff. DSGVO zu berücksichtigen, wobei auch das Urteil des EuGH zur Nichtigkeit des EU-US-Privacy Shields („Schrems II“) zu berücksichtigen ist, da hierin wichtige Anhaltspunkte zur Anpassung der Standarddatenschutzklauseln enthalten sind. Insbesondere in größeren Konzernen stellt die wirksame Einbindung der Standarddatenschutzklauseln eine komplexe Angelegenheit dar, bei der sich Rahmenvertragslösungen anbieten.

Weitere formelle Pflichten zum Datenschutz

Bei der Implementierung von Smart Glasses bestehen weitere formelle Pflichten wie die Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO, die Erfüllung von Informationspflichten Art. 13, 14 DSGVO sowie die Aufnahme des jeweiligen Smart Glasses Produkts in das Verarbeitungsverzeichnis nach Art. 30 Abs. 1 DSGVO.

Zusammenfassung

Die Implementierung von Smart Glasses ist wirtschaftlich sinnvoll und stellt insbesondere ein langfristig wirkendes Instrument dar, ein Stück mehr Robustheit gegen die wirtschaftlichen Folgen weiterer Pandemien zu erlangen. Der Einsatz entsprechender Technologien geht jedoch auch mit einigen datenschutzrechtlichen Pflichten einher. Insbesondere sind die höchstrichterlichen Vorgaben zum Beschäftigtendatenschutz zu berücksichtigen und weitere formelle Pflichten zu erfüllen.
Wir unterstützen Sie bei der Implementierung von Datenbrillen in Ihrem Unternehmen

SKW Schwarz Rechtsanwälte hat zum Einsatz von Datenbrillen in Unternehmen eine Task Force gegründet. Wir beraten Sie gerne im Hinblick auf datenschutzrechtliche und arbeitsrechtliche/arbeitschutzrechtliche Fragen sowie zu den relevanten IT-Sicherheitsthemen.

Nutzen Sie unser Bausteinkonzept: Die einzelnen Bausteine bieten wir wahlweise zu vereinbarten Festpreisen oder individuell nach Aufwand an. Kostentransparenz ist für uns in jedem Fall selbstverständlich.

<u>Basisbausteine</u>

- Sie erhalten von uns Checklisten zu allen rechtlichen Fragen, die vor dem Einsatz von Datenbrillen in Ihrem Unternehmen geprüft werden müssen.
- Wir führen praxisnahe Schulungen in Ihrem Unternehmen durch und stellen entsprechende Schulungsunterlagen und Service Cards zur Verfügung.

Datenschutz

- Sie erhalten eine konkrete Bewertung der marktüblichen Datenbrillen bezüglich allgemein gültiger Datenschutz- und Datensicherheitsanforderungen.
- Wir beantworten Ihnen alle relevanten Fragen:
    - Was ist die Rechtsgrundlage der Datenverarbeitung?
    - Welche Informationen dürfen zu welchen Zwecken genutzt werden?
    - Welche Mitbestimmungsrechte haben Beschäftigte?
    - Müssen personenbezogene Daten geschützt werden?
    - Für welchen Zweck dürfen sie genutzt werden und müssen die Beschäftigten einer Nutzung zustimmen?
- Wir erstellen direkt einsetzbare Datenschutzhinweisen für Beschäftigte in deutscher und englischer Sprache.

Arbeitsrecht/Arbeitssicherheit

- Wir erstellen individuell abgestimmte Betriebsvereinbarungen, Richtlinien und Arbeitsanweisungen unter Beachtung sämtlicher Gesichtspunkte zur Arbeitssicherheit.

IT-Sicherheit

- Wir begleiten Sie bei der Auswahl der Hard- und Software.
- Wir beraten Sie bei der Wahl des richtigen Modells (on premise oder Cloud-basiert).
- Wir beraten Sie beim Rollout und bei der Implementierung.

Dr. Oliver Hornung, Frankfurt am Main, o.hornung@skwschwarz.de
Dr. Hendrik Skistims, Frankfurt am Main, h.skistims@skwschwarz.de
Oliver Korte, Hamburg, o.korte@skwschwarz.de
Alexander Möller, Frankfurt am Main, a.moeller@skwschwarz.de
Julian Westpfahl, Frankfurt am Main, j.westpfahl@skwschwarz.de
Franziska Ladiges, Frankfurt am Main, f.ladiges@skwschwarz.de
Dr. Niels Witt, Hamburg, n.witt@skwschwarz.de

Kein Schadensersatz trotz Datenschutzverstoß

Im Urteil vom 18. September 2020 (Az.: 2-27 O 100/20) befasste sich das Landgericht Frankfurt am Main mit verschiedenen geltend gemachten Ansprüchen eines Verbrauchers gegen Mastercard. Im Rahmen eines Bonusprogramms für deutsche Kunden, welches durch einen Dienstleister gesteuert wurde, kam es zu einem Datenvorfall. Bei diesem Vorfall machten unbekannte Täter die im Rahmen des Bonusprogramms erhobenen Daten von ca. 90.000 Teilnehmern im Internet öffentlich zugänglich.

Beurteilung des Vorfalls durch das Landgericht Frankfurt am Main

Das Landgericht Frankfurt am Main wies in seinem Urteil sowohl Unterlassungsansprüche als auch Schadensersatzansprüche des Klägers ab. Hinsichtlich des geltend gemachten Unterlassungsanspruchs, sah das Landgericht die Wiederholungsgefahr trotz gegebener rechtswidriger Beeinträchtigung nicht gegeben. Insofern sei darauf abzustellen, dass der Eingriff durch eine einmalige Sondersituation entstanden sei, welche durch das kriminelle und unvorhersehbare Verhalten eines externen oder internen Dritten begründet wurde. Die Beklagte hatte nach Bekanntwerden umfangreiche Maßnahmen ergriffen, welche einen erneuten Verstoß in der Art ausschließen würden.

Auch die geltend gemachten Schadensersatzansprüche des Klägers wies das Landgericht Frankfurt am Main ab. Der Kläger sei als Anspruchsteller zunächst für den Verstoß gegen datenschutzrechtliche Vorschriften beweisbelastet. Darüber hinaus müsse ein etwaiger Verstoß gegen Pflichten aus der DSGVO für den Datenvorfall und den Schaden des Betroffenen kausal sein. Diese Kausalität ließ sich im vorliegenden Fall in Bezug auf die vom Kläger geltend gemachten Verstöße nicht feststellen. Schließlich sei zu berücksichtigen, dass nicht jede Datenschutzverletzung in Form einer nicht (vollständig) rechtskonformen Datenverarbeitung automatisch ein ersatzfähiger Schaden sei. Es müsse vielmehr aufgrund der Verletzung zu einer konkreten Verletzung von Persönlichkeitsrechten

der betroffenen Person gekommen sein. Ein Strafschadensersatz widerspricht der Systematik des deutschen Rechts. Insofern führt das Landgericht Frankfurt am Main die bereits durch andere Gerichte bestätigte Auffassung fort (vgl. Beitrag „Kein Schadensersatzanspruch nach der DSGVO bei individuell empfundenen Unannehmlichkeiten oder immateriellen Bagatellschäden“).

Was ist für Unternehmen hinsichtlich Schadensersatzansprüche im Datenschutzvorfall zu beachten?

Im Einzelnen führte das Landgericht Frankfurt am Main folgende für von Hackerangriffen betroffene Unternehmen wesentliche Punkte hinsichtlich geltend gemachter Schadensersatzansprüche aus:

1. Die Veröffentlichung der Daten im Internet sei nicht durch die Beklagte, sondern einen unbekannten Dritten vorgenommen worden und sei somit nicht als Verstoß der Beklagten zu werten.
2. Da es unklar geblieben ist, wodurch das Datenleck verursacht wurde, sei eine Kausalität des etwaigen Verstoßes für den Datenvorfall und damit den Schaden des Klägers nicht feststellbar. Es bliebe Spekulation, ob der Vorfall durch andere Sicherheitsmaßnahmen hätte verhindert werden können.
3. DSGVO fordert lediglich angemessene und dem Stand der Technik entsprechende Sicherheitsmaßnahmen. Auf das Ergreifen einer bestimmten Maßnahme würde kein Anspruch bestehen, so dass das Nichtergreifen einer bestimmten Maßnahme auch keinen Schadensersatz begründen könne.
4. Aus dem Nichtabschluss von Verträgen zur gemeinsamen Verantwortlichkeit entstehen betroffenen Personen ebenfalls keine Schadensersatzansprüche. Es sei nicht ersichtlich, worin der Schaden der betroffenen Person liegen solle, wenn Verträge nicht geschlossen sein sollten.

Rechtlicher Schutz von Unternehmen bei Hackerangriffen

Das Urteil des Landgerichts Frankfurt am Main vom 18. September 2020 stärkt von Hackerangriffen betroffenen Unternehmen erfreulicherweise den Rücken. Erneut wird bekräftigt, dass Anspruchsteller für die Anspruchsgrundlagen beweis- und darlegungsbelastet sind sowie, dass nicht jeder Verstoß gegen datenschutzrechtliche Vorschriften automatisch zu einem Schaden der betroffenen Personen führt. Sofern Unternehmen somit trotz angemessener und technisch auf aktuellem Stand Sicherheitsmaßnahmen Opfer von Hackerangriffen werden, ist ein geltend gemachter Unterlassungs- und Schadensersatzanspruch auf seine Berechtigung hin zu prüfen. In der Regel dürften diese nicht berechtigt sein. Unternehmen, welche Opfer von Cyber-Attacken geworden sind, tun somit auch in dieser Hinsicht gut daran, sich professionelle Rechtsberatung einzuholen bevor Ansprüche von betroffenen Personen einfach erfüllt werden.

Franziska Ladiges, Frankfurt am Main
f.ladiges@skwschwarz.de

Internet? Metaverse!

Wir werden derzeit Zeugen einer (r)evolutionären Entwicklung, die unseren Alltag – wie die Dampfmaschine oder das Smartphone – drastisch verändern wird.

Die vergangenen Monate des Lockdowns und Social Distancings aufgrund der Coronakrise verfrachteten einen Großteil unseres Arbeits- und Soziallebens rasend schnell in die digitale Welt. Wir bekamen einen ansatzweisen Ausblick auf das mögliche real-virtuelle Hybrid-Leben in nicht allzu ferner Zukunft: Wie wir arbeiten, Freunde treffen, spielen, shoppen oder Konzerte besuchen werden. Wie jene Monate gezeigt haben, waren es vor allem auch Computerspiele, die ihren Nutzer:innen während der Coronakrise ermöglichten, sich trotz physischer Distanz zu treffen und Gemeinsames zu erleben.

Das Metaverse: Die Puzzleteile liegen bereit

Heute erledigen wir bereits einen Großteil digital: Dank Cloud-Systemen und Instant Messengern können wir von überall arbeiten; bei Twitter geht daher kein Angestellter mehr ins Büro. Viele treffen ihre Freunde online; früher in Chats, heute in „Fortnite“: Dort trat im April dieses Jahres der Rapper Travis Scott auf, und seine 12 Millionen Zuschauer saßen dabei nicht stumm auf den Rängen,

sondern konnten während seiner Performance miteinander und innerhalb der Spielewelt interagieren. Im März öffnete in „Minecraft“ die „Uncensored Library“ der Reporter ohne Grenzen ihre Türen, um jungen Menschen in aller Welt unabhängigen Zugang zu Informationen zu ermöglichen. Die Onlinewelt verlagert also nicht nur bereits Bekanntes – wie Lebensmitteleinkäufe – aus der Realität in den digitalen Raum. Sie schafft und erfüllt auch vollkommen neue Bedürfnisse.

Kurioserweise wirkt all das aber zugleich auch veraltet: Am Ende sitzt noch immer ein Mensch vor einem Bildschirm, wie vor einem Fenster in die digitale Welt, deren Teil er letztlich nicht ist. Und auch, wenn die technischen Zugangshürden (etwa dank Neuerungen wie Cloudgaming) immer weiter sinken, benötigt er oder sie eine Vielzahl von Systemen und Programmen; etwa einen Browser zum Shoppen, eine VoD-Plattform für Filme, eine Konsole oder Gaminglauncher zum Spielen. Zugleich sind weit überwiegend die „wirkliche“ und die „digitale“ Welt noch immer getrennt – Frau / Mann spielt zeitgleich entweder auf dem Platz oder in „FIFA 20“ Fußball, trifft Freunde entweder in der Bar oder in „Fortnite“, heiratet in der Kirche oder in „Animal Crossing: New Horizons“. Und wirkt das genannte Travis Scott-Konzert nicht doch (noch) etwas wie ein interaktives Musikvideo?

Das Bild setzt sich zusammen

Visionäre träumten deshalb schon seit langem von einem Ort, der die wirkliche und digitale Welt in Echtzeit vereint, oft genannt das Metaverse. Der Begriff geht auf Neal Stephenson’s Roman „Snow Crash“ aus den 90er Jahren zurück. Dort fliehen die Protagonisten der Handlung aus der Realität immer wieder in das Metaversum, einer Mischung zwischen Internet und MMORPG (Massively Multiplayer Online Role-Playing Game), und bewegen sich dort mithilfe von Avataren. Der Roman „Ready Player One“ und dessen Kinofilm-Visualisierung geben ein moderneres Beispiel und einen Eindruck, wie sich das anfühlen kann.

Nach heutigem Verständnis beschreibt das Metaverse im Wesentlichen einen virtuell-realen Raum, der sämtliche virtuellen Welten als Weiterentwicklung des Internets umfasst. Der allen Menschen ermöglicht, sich live in eine voll funktionierende Wirtschaft einzubringen. Der Blogger und Investor Matthew Ball vergleicht in seinem Essay die heutige digitale Welt mit einem Einkaufszentrum mit unzähligen Shops, deren Produkte weder mit derselben Währung bezahlt noch miteinander zugleich benutzt werden können. Im Metaverse hingegen sollen Daten, digitale Gegenstände und Inhalte untereinander vollkommen kompatibel sein. Eine am Kurfürstendamm erworbene Luxusuhr kann vielleicht künftig auch in Counterstrike oder beim Besuch eines Konzerts – ob digital oder analog – getragen oder verkauft/getauscht werden. Hier soll jede:r erschaffen, besitzen, investieren und verkaufen und für eine undefinierbare Fülle von „Arbeit“ belohnt werden, welche weder allein digital noch analog erbracht werden soll. Was genau das Metaverse letztendlich aber sein wird, lässt sich zum jetzigen Zeitpunkt kaum erahnen und wird auch entsprechend diskutiert. Um sich ihm zu nähern, hilft Matthew Balls‘ Negativabgrenzung zu dem, was das Metaverse nicht ist:

1. Es ist keine virtuelle Welt wie beispielsweise „Second Life“ oder „World of Warcraft“. Beide erweitern nicht unser jetziges „Universum“, sondern sind letztlich nur virtuelle, in sich geschlossene Räume.
2. Aus demselben Grund sind auch Spiele oder Virtual Reality, wie wir sie heute kennen, kein Metaverse. Auch hier hat der Mensch lediglich das simulierte Gefühl, sich in einer digitalen Welt zu befinden. Das Metaverse mag zwar einige spielähnliche Ziele haben und Spiele einschließen, es ist aber selbst kein Spiel und orientiert sich auch nicht an bestimmten Zielen.
3. Genauso wenig ist es ein virtueller Themenpark wie in „Rick and Morty“ oder ein neuer Appstore – es dient nicht nur dem Spaß und der Unterhaltung.

Das Metaverse ist also vielmehr eine virtuelle Manifestation der Realität mit gegenseitigen Wechselwirkungen, wie wir sie eben aus „Ready Player One“ oder „Matrix“ kennen. Und es steht außer Frage, dass es nicht nur die digitale, sondern auch große Teile der physischen Welt sowie alle Dienste und Plattformen für immer revolutionieren wird.

Gaming als Urknall?

Wie „Fortnite“ oder „Minecraft“ zeigen, ist Ursprung und Motor auf dem Weg zum Metaverse vor allem auch die Gamingindustrie. Das ist wenig überraschend, bedient sie doch eine Zielgruppe mit den höchsten technischen Ansprüchen und Möglichkeiten. Die Schlagzahl der Veröffentlichung von neuen Tools und Puzzlesteinen ist immens. Der Druck aus dieser Branche für die anderen Player ist daher

mittlerweile hoch. Wem es gelingt, in naher Zukunft welche technischen Standards zu setzen, bleibt abzuwarten.

Und wie wird sich irgendwann die Existenz des Metaverse retoure auf die Gamingindustrie und insbesondere auf den Esport auswirken? Die Entwicklung der letzten Jahre, Esport aus dem Internet in reale Arenen zu holen, kehrt sich vielleicht wieder um. In einer Arena einem Spieler auf einer Leinwand beim Spielen zuzuschauen, wirkt heute (jedenfalls in Europa) noch neu, in wenigen Jahren aber vielleicht schon angestaubt, wenn der Zuschauer dem Wettkampf auch live auf bzw. in der Map zuschauen kann. Mit fortschreitender technischer Entwicklung wird auch die schon jetzt eigentlich wenig sinnvolle Trennung zwischen „echtem“ und „elektronischen“ Sport immer mehr verschwimmen – gut möglich, dass ein Shooter in einem Metaverse physisch anstrengender wird als heute jedes reale Fußballspiel. Die eigentlich nur noch hierzulande geführte und ermüdende Debatte, ob Esport ein „Sport“ ist, erledigt sich spätestens dann vielleicht von selbst.

Blicken wir schließlich einmal kurz zurück zu den Anfängen des Internets: Es wurde Mitte der 90iger Jahre ernsthaft diskutiert, ob das Internet ein rechtsfreier Raum sei, in dem die geltenden Gesetze keine Anwendung finden könnten. Allein die Diskussion ist heute nicht mehr vorstellbar, und sie wird auch für die nächste Evolutionsstufe – das Metaverse – nicht mehr wiederaufstehen. Die rechtlichen Herausforderungen werden vielfältig und uns an vielen Stellen zum Umdenken zwingen, manche neue Regelungen hervorrufen, aber ansonsten wird das gelten, was im realen Leben schon lange die beste Strategie ist: rechtliche Themen erkennen und smart lösen. Stay tuned.

Sandra Sophia Redeker, Berlin
s.redeker@skwschwarz.de
Tobias Voßberg, Berlin
t.vossberg@skwschwarz.de