Aktuelle Entwicklungen im Datenschutz und ihre Bedeutung für das IT-Management

Ralf Kneuper [1]

Abstract: Mit der Digitalisierung und Vernetzung von Diensten und Produkten steigt auch die Bedeutung des Datenschutzes für Organisationen und ihr IT-Management. Das wurde besonders sichtbar mit Beginn der Anwendbarkeit der DSGVO in 2018, aber auch danach gab es wesentliche neue Entwicklungen beim Datenschutz, die im Management derartiger Dienste und Produkte berücksichtigt werden müssen. Der vorliegende Beitrag gibt einen Überblick über die wichtigsten dieser Entwicklungen und ihre Bedeutung für das IT-Management. Betroffen hiervon sind in erster Linie die Nutzung von Cookies auf Webseiten sowie der Export von Daten in Staaten außerhalb der EU. Insbesondere das sogenannte „Schrems II-Urteil“ von 2020 hat durch die geforderten Einschränkungen beim Datenexport deutliche Auswirkungen auf das IT-Management, beispielsweise die Nutzung von Cloud-Diensten.

Keywords: Datenschutz; DSGVO; Schrems II-Urteil; TTDSG; Standardvertragsklauseln; Cookies

1 Aktuelle Entwicklungen im Datenschutz

1.1 Motivation und Hintergrund

Mit der Digitalisierung und Vernetzung von Diensten und Produkten steigt auch die Bedeutung des Datenschutzes für Organisationen und ihr IT-Management. Das wurde besonders sichtbar mit Beginn der Anwendbarkeit der DSGVO in 2018, aber auch danach gab es einige neue Entwicklungen, die im Management derartiger Dienste und Produkte berücksichtigt werden müssen. Der vorliegende Beitrag gibt einen Überblick über die wichtigsten dieser neuen Entwicklungen beim Datenschutz und ihre Bedeutung für das IT-Management. Die wichtigsten Entwicklungen betreffen dabei die Themen, bei denen es auch vorher schon viele Diskussionen gab, nämlich die Rahmenbedingungen für die Nutzung von Cookies (siehe Kap. 3) sowie den Export von Daten außerhalb der EU (genauer gesagt des EWR) (siehe Kap. 4). Einige der ursprünglich offenen Fragen wurden mittlerweile abschließend beantwortet, bei anderen Fragen sind die bisherigen Antworten sicher nur vorläufig und die Diskussionen werden in den nächsten Jahren weitergehen.

[1] IU Internationale Hochschule – Fernstudium, Kaiserplatz 1, 83435 Bad Reichenhall, ralf.kneuper@iu.org, https://orcid.org/0000-0003-3225-5895

Für eine umfassende Darstellung des Datenschutzes aus Sicht von Softwareentwicklung und IT, wenn auch teilweise noch vor den im Folgenden beschriebenen aktuellen Entwicklungen, siehe beispielsweise [Kn21].

1.2 Methodik

Grundlage dieser Arbeit ist eine Auswertung relevanter Mailinglisten, Blogs und PodCasts zu aktuellen Entwicklungen im Datenschutz mit anschließendem Literaturreview zur Vertiefung der angesprochenen Themen. Wissenschaftliche Literatur zu diesen aktuellen Entwicklungen existiert derzeit naturgemäß nur in geringem Umfang. Allerdings handelt es sich um ein Thema, bei denen verschiedene Organisationen hohes Interesse haben, dass die entsprechenden Informationen zumindest in Fachkreisen breit gestreut werden, so dass diese relativ leicht zu finden sind. Dabei handelt es sich beispielsweise um Veröffentlichungen der *Datenschutzkonferenz* (DSK), also dem Gremium der deutschen Datenschutz-Aufsichtsbehörden, verschiedener Datenschutz-Organisationen wie dem *Berufsverband der Datenschutzbeauftragten Deutschlands* (BvD) e.V. oder dem *NOYB-European Center for Digital Rights* („None Of Your Business"), sowie um Podcasts und Blogs von Verlagen bzw. Fachzeitschriften und von großen Kanzleien.

Fallbeispiel *Um die behandelten Themen anschaulicher zu machen, werden sie am Fallbeispiel eines fiktiven Fitness-Centers erläutert, in dem Daten von Kunden sowie von Mitarbeitern verarbeitet werden, außerdem solche Daten, die sich aus der Webpräsenz und den Präsenzen in verschiedenen sozialen Netzen ergeben. Das Fitness-Center hat bei der Einführung der DSGVO 2018 einen Datenschutzbeauftragten benannt und mit seiner Unterstützung die wesentlichen Anforderungen zum Datenschutz umgesetzt.*

2 Datenschutz-Anpassungs- und Umsetzungsgesetz EU (2. DSAnpUG-EU)

Parallel mit der DSGVO wurde das „Datenschutz-Anpassungs- und Umsetzungsgesetz EU" (DSAnpUG-EU) verabschiedet, das insbesondere die durch die DSGVO erforderliche Komplettüberarbeitung des Bundesdatenschutzgesetzes (BDSG), aber auch Anpassungen vieler anderer betroffener Gesetze, umsetzte. Das 2. Datenschutz-Anpassungs- und Umsetzungsgesetz EU (2. DSAnpUG-EU)[2] das am 26.11.2019 in Kraft trat, führte diese Anpassungen weiter und diente dazu, viele weitere Einzelregelungen zum Datenschutz in anderen Gesetzen und anderen Regelwerken anzupassen, beispielsweise in der Abgabenordnung oder dem IHK-Gesetz. Die für Unternehmen wichtigsten Änderungen betrafen erneut das Bundesdatenschutzgesetz (BDSG):

[2] Siehe http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl119s1626.pd

- Ein Datenschutzbeauftragter (DSB) muss nur noch benannt werden, wenn mindestens 20 (statt bis dahin zehn) Mitarbeiter regelmäßig mit der Verarbeitung personenbezogener Daten befasst sind.
- Einwilligungen von Mitarbeitern in die Verarbeitung ihrer persönlichen Daten dürfen auch in elektronischer Form statt bis dahin nur in Schriftform erfolgen.

Während die zweite Änderung weitgehend unproblematisch ist, führte die erste zu erheblichen Diskussionen, ob diese Änderung nicht statt der behaupteten Erleichterung für die betroffenen Unternehmen im Gegenteil die korrekte Umsetzung des Datenschutzes in der Praxis noch erschwere, da ja alle inhaltlichen Vorgaben unverändert geblieben sind, nur die interne Fachkompetenz eines DSB nicht mehr gefordert ist.[3]

Fallbeispiel *Das Fitness-Center hat drei Verwaltungsmitarbeiter, außerdem zwölf Mitarbeiter mit Zugriff auf die Mitgliederdatenbank (hauptsächlich Trainer) und sieben Mitarbeiter ohne solchen Zugriff (Reinigungskräfte etc.). Damit liegt es über der alten Grenze von zehn, aber unter der neuen Grenze von 20 Mitarbeitern, die regelmäßig mit der Verarbeitung von Personendaten befasst sind, und muss also keinen Datenschutzbeauftragten mehr benennen. Allerdings entschied es sich dafür, das trotzdem zu tun, damit dieser die Geschäftsführung entsprechend unterstützt. „Wir sind auch nicht verpflichtet, einen Steuerberater zu benennen, tun das aber trotzdem, weil es uns hilft."*

3 Umgang mit Cookies

Der Umgang mit Cookies auf Webseiten, insbesondere Tracking-Cookies, wird seit Jahren heftig diskutiert, da hier in besonderem Maße widersprüchliche Interessen auf einander treffen. Einerseits baut ein erheblicher Teil des Online-Marketings und indirekt auch die Finanzierung vieler Webseiten auf der Nutzung von Tracking-Cookies auf. Andererseits ist aus Sicht vieler Nutzer genau dieses Tracking nicht akzeptabel oder zumindest unerwünscht. Lange war umstritten, wie das Tracking aus Sicht des geltenden Datenschutzrechtes zu bewerten ist, aber hier hat es durch die sogenannten planet49-Urteile weitgehende Klarheit gegeben, siehe Kap. 3.1. Die Diskussion darüber, welche Regelungen in Bezug auf Tracking angemessen sind und inwieweit dieses erlaubt bzw. verboten werden sollte, läuft aber noch immer, wie sich das beispielsweise in der Verzögerung der in Kap. 3.3 beschriebenen ePrivacy-Verordnung der EU widerspiegelt.

3.1 Die planet49-Urteile

Zentrale Fragen aus Sicht des Datenschutzes in Bezug auf die Nutzung von Cookies bezogen sich nach Inkrafttreten der DSGVO darauf, wann man dafür eine Einwilligung

[3] Siehe beispielsweise https://www.bvdnet.de/presse/bvd-warnt-aufweichen-der-benennungspflicht-senkt-keine-buerokratie-sondern-erhoeht-sie/

der Besucher einer Webseite benötigt, und ob diese Einwilligung ggf. aktiv erteilt werden muss (Opt-In) oder ob es ausreicht, wenn die Besucher die Möglichkeit haben, das Setzen von Cookies abzuwählen (Opt-Out). Ein Teil der Unklarheit zumindest in Deutschland entstand dadurch, dass das deutsche Telemediengesetz (TMG) an dieser Stelle eine andere Aussage machte als die DSGVO, die Interpretation und die Priorität der beiden Aussagen aber nicht eindeutig war.

Eindeutig beantwortet wurden diese Fragen durch die sogenannten planet49-Urteile des Europäischen Gerichtshofes (EuGH) (Oktober 2019) und darauf aufbauend des Bundesgerichtshofes (BGH) (Mai 2020).[4] Mit diesen Urteilen wurde eindeutig geklärt, dass Cookies nur dann ohne ausdrückliche Einwilligung gesetzt werden dürfen, wenn sie für die Funktion der Webseite *technisch erforderlich* sind, beispielsweise um Daten in einem Warenkorb zu verwalten oder um die Authentifizierung, die Sprachauswahl oder andere Einstellungen umzusetzen. Dienen Cookies dagegen „der Erstellung von Nutzerprofilen zum Zwecke der Werbung, indem das Verhalten des Nutzers im Internet erfasst und zur Zusendung darauf abgestimmter Werbung verwendet werden soll“, dann ist eine Einwilligung mit Opt-In erforderlich. Diese Einwilligung muss *informiert* und *für den konkreten Fall* erteilt werden, d.h. wenn „die beanstandete Gestaltung der Einwilligungserklärung darauf angelegt ist, den Verbraucher mit einem aufwendigen Verfahren der Auswahl von in der Liste aufgeführten Partnerunternehmen zu konfrontieren, um ihn zu veranlassen, von dieser Auswahl abzusehen“, dann ist auch eine erteilte Einwilligung gemäß dem BVG-Urteil nicht gültig und das Unternehmen kann sich nicht auf die Einwilligung berufen.

Auch bei technisch erforderlichen Cookies ist eine entsprechende *Information* der Webseitenbesucher notwendig, aber eben keine Einwilligung. Bei der Umsetzung dieser Anforderungen wird erfahrungsgemäß oft übersehen, dass die *Information* gegeben werden muss (bzw. die Einwilligung eingeholt werden muss), *bevor* der jeweilige Cookie gesetzt wird, Cookies also nicht gleich beim ersten Anzeigen der Webseiten gesetzt werden dürfen.

Fallbeispiel *Auf seiner Webpräsenz hatte auch das Fitness-Center ein Werbebanner integriert, auf dem Werbung Dritter gegen Provision über einen entsprechenden Dienst angezeigt wurde. Nach dem planet49-Urteil des BGH schaltete das Fitness-Center auf seiner Webpräsenz ein sogenanntes Cookie-Banner vor, damit Besucher zuerst über die gesetzten technisch erforderlichen Cookies informiert werden, und außerdem entscheiden müssen, ob sie die Nutzung von Tracking-Cookies erlauben, damit auf sie zugeschnittene Werbung angezeigt werden kann. Allerdings ist das Fitness-Center mit dieser Lösung unzufrieden, denn abgesehen von den geringeren Werbeeinnahmen sind auch die*

[4] Siehe https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2020&nr=106314&pos=1&anz=68. Oft ist nur vom BVG-Urteil als „dem“ planet49-Urteil die Rede, aber genau genommen gab es mit dem genannten EuGH-Urteil ein weiteres Urteil mit im Kern den gleichen Aussagen.

Besucher der Webpräsenz, also meist derzeitige oder potentielle Kunden, genervt von derartigen Cookie-Banners, und beschweren sich darüber.

Derzeit gibt es noch viele Webseiten, die die genannten Regelungen nicht oder unvollständig erfüllen und beispielsweise mit vorausgefüllten Einwilligungskästchen arbeiten, Cookies zu Unrecht als technisch erforderlich deklarieren, oder die Schaltfläche zur Einwilligung deutlich herausgehoben, die Schaltfläche zur Ablehnung dagegen schwer sichtbar darstellen („Nudging“) [GS21]. Daher gab es hierzu in 2020/21 eine gemeinsame Prüfaktion der deutschen Datenschutz-Aufsichtsbehörden[5], außerdem eine umfangreiche Aktion der österreichischen Datenschutzorganisation NOYB, bei der 10.000 Websites geprüft wurden und schließlich 422 formelle Beschwerden bei den jeweils zuständigen Aufsichtsbehörden eingereicht wurden.[6] Für Unternehmen und ihr IT-Management bleibt zu konstatieren, dass gerade ein unangemessener Umgang mit Cookies und anderen personenbezogenen Daten auf der Webseite auch nach außen deutlich sichtbar ist, mit einem entsprechend hohen Risiko von Konsequenzen wie Bußgeldern oder negativer Presse.

3.2 Das „Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG)“

Das „Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG)“[7] tritt zum 01.12.2021 in Kraft und passt eine Reihe von gesetzlichen Regelungen zum Datenschutz in Telekommunikation und Telemedien an. Dazu zählt u.a. auch die Bereitstellung von Webseiten. Mit diesem Gesetz werden das Telemediengesetz TMG und das Telekommunikationsgesetz TKG abgelöst. Insbesondere passt das TTDSG die Rechtslage in Deutschland (etwas verspätet) in Bezug auf den Opt-In bei Cookies-Einwilligungen an die Vorgaben der ePrivacy-Richtlinie der EU von 2002 (Richtlinie 2002/58/EG) und der Cookie-Richtlinie von 2009 (Richtlinie 2009/136/EG) sowie die Aussagen der planet49-Urteile an. Praktisch ändert sich daher durch das Gesetz nur wenig.

Daneben definiert das TTDSG die Rahmenbedingungen für Dienste zum Einwilligungsmanagement, die prinzipiell die Nutzung der ungeliebten Cookie-Banner ablösen oder zumindest reduzieren könnten. Hier bleibt abzuwarten, ob und wann es solche Dienste geben wird, und ob die Webseitenbetreiber sie dann auch nutzen werden. Potentiell könnte dies mittel- oder langfristig zu einer wesentlichen Vereinfachung beim Umgang mit Cookies sowohl für die Webseitenbetreiber als auch die Besucher dieser Webseiten führen, aber kurzfristig haben diese Regelungen sicher keine Auswirkungen auf das IT-Management von Organisationen. Andererseits hat sich aber die einfache

[5] Siehe https://www.datenschutz.de/laenderuebergreifende-pruefung-einwilligungen-auf-webseitenvon-medienunternehmen-sind-meist-unwirksam-nachbesserungen-sind-erfor
agement

[6] Siehe https://noyb.eu/de/noyb-reicht-422-formelle-dsgvo-beschwerden-gegen-cookie-banner-wahnsinn-ein

[7] http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1982.pdf

Lösung mit der Do-Not-Track Einstellung, die im Wesentlichen dem gleichen Zweck diente, nicht durchgesetzt, da sie von der Werbewirtschaft in der Breite nicht akzeptiert wurde.

3.3 Die ePrivacy-Verordnung der EU

Die ePrivacy-Verordnung (ePrivacyVO) der EU sollte eigentlich parallel mit der DSGVO verabschiedet werden und in Kraft treten, musste aber aufgrund der starken Interessenkonflikte zurückgestellt werden. Anfang 2021 hat sich zumindest der Rat der EU auf eine gemeinsame Position geeinigt, so dass einerseits Hoffnung besteht, dass diese Verordnung in absehbarer Zeit verabschiedet werden kann, andererseits aber auch bereits gravierende Kritik am aktuellen Stand geäußert wird. Ein konkreter Zeitpunkt für eine Verabschiedung der ePrivacyVO ist aber derzeit (Oktober 2021) nicht absehbar.

Für Unternehmen stellt sich damit aktuell die Aufgabe, diese Entwicklung zu beobachten, um ggf. zügig reagieren zu können, wenn die Verordnung dann tatsächlich verabschiedet wird.

Diese ePrivacyVO wird dann die Vorgänger-Richtlinien der EU, die ePrivacy-Richtlinie sowie die Cookie-Richtlinie, ablösen, die ja in Deutschland gerade erst durch das TTDSG umgesetzt werden, so dass dieses Gesetz dann voraussichtlich wieder angepasst werden muss.

3.4 Weitere Entwicklungen zum Umgang mit Cookies

Neben den beschriebenen größeren Anpassungen gab es in den letzten Jahren auch einige kleinere Entwicklungen, die in erster Linie die Nutzung bestimmter, allerdings weit verbreiteter Produkte betreffen.

3.4.1 Google Analytics

Schon seit vielen Jahren in der Diskussion ist die Nutzung von Google Analytics und ähnlicher Systeme für die Analyse der Webseitennutzung. Hier hat die DSK im Mai 2020 einen Beschluss gefasst, unter welchen Rahmenbedingungen sie die Nutzung von Google Analytics als vereinbar mit der DSGVO ansieht.[8] Zentrale Bedingung ist dabei, dass Google Analytics nur bei *aktiver Einwilligung* der Webseitenbesucher genutzt werden darf, da dabei deren personenbezogene Daten gesammelt und auch an Google gesendet werden.

Neben dem hier betrachteten Umgang mit Cookies stellt auch der mit Google Analytics verbundene Datenexport in die USA aus Datenschutzsicht ein Problem dar, das in Kap. 4

[8] Siehe https://www.datenschutzkonferenz-online.de/media/dskb/20200526_beschluss_hinweise_zum_einsatz_von_google_analytics.pdf

näher betrachtet wird. Auch hier gilt, dass es einerseits noch viele Verstöße gegen diese Regelungen gibt (auch wenn diese in den letzten Jahren zumindest subjektiv gesehen deutlich weniger geworden sind), andererseits aber für Außenstehende (Mitbewerber, Aufsichtsbehörden, verärgerte Kunden etc.) leicht erkennbar sind und daher ein hohes Entdeckungsrisiko haben.

Fallbeispiel *Nach der Veröffentlichung des DSK-Beschlusses bat das Fitness-Center seinen DSB um Unterstützung bei der Umsetzung. Dieser empfahl allerdings, statt Google Analytics das ähnliche Werkzeug Matomo Analytics zu nutzen, bei dem die Analyse-Ergebnisse sehr ähnlich sind, wobei aber deutlich weniger personenbezogene Daten erfasst und verarbeitet werden. Bei entsprechender Konfiguration kann man sogar auf die Nutzung von Cookies und dementsprechend Cookie-Bannern verzichten, verliert dabei allerdings die Zuordnung verschiedener Besuche des gleichen Nutzers auf der Webseite. Da diese durch vom Benutzer gelöschte Cookies etc. sowieso nur eingeschränkt möglich ist, entschied sich das Fitness-Center dafür, auf Matomo Analytics umzusteigen.*

3.4.2 Google Federated Learning of Cohorts (FLoC)

Keine direkte rechtliche Auswirkung, voraussichtlich aber starke praktische Auswirkungen auf alle Unternehmen, die Online-Marketing betreiben, hat die Ankündigung von Google, 3rd-Party-Cookies im Chrome-Browser nicht mehr zuzulassen, sondern stattdessen mit Hilfe von „Federated Learning of Cohorts (FLoC)“ eine Datenschutz-freundlichere Möglichkeit einzuführen, um Werbung jeweils bei wahrscheinlich interessierten Benutzern zu platzieren [Go].

Allerdings gibt es auch an dieser Lösung erhebliche Kritik, u.a. wegen des Risikos, dass damit die Monopolstellung von Google weiter ausgebaut wird [Cy21].

4 Auftragsverarbeitung und Datenexport außerhalb der EU

4.1 Datenexport in der DSGVO

Wichtige Werkzeuge für das IT-Management sind die Vergabe von Dienstleistungen an Anbieter im Ausland (Offshoring) sowie die Nutzung von Cloud-Diensten, bei denen die Anbieter ebenfalls oft ihren Sitz im Ausland haben.

In den meisten Fällen betrifft das auch personenbezogene Daten und deren Verarbeitung, und die Nutzung dieser Dienstleistungen fällt damit unter die Regelungen des Datenschutzes.

Solange der Sitz der Anbieter innerhalb des Geltungsbereiches der DSGVO ist, ist das unproblematisch und es gelten die gleichen Regelungen wie bei einer Verarbeitung im eigenen Land. Schwieriger wird es bei Anbietern außerhalb des Geltungsbereiches der

DSGVO, dem sogenannten Datenexport in Drittländer, denn hier besteht grundsätzlich das Risiko, dass in dem jeweiligen Land kein angemessenes Datenschutzniveau besteht und die Daten daher bei Übertragung an den Dienstleister nicht angemessen geschützt wären.

Um das zu verhindern, sind in der DSGVO Mechanismen definiert, wie ein angemessenes Schutzniveau sichergestellt und nachgewiesen werden kann. In erster Linie handelt es sich dabei um:

- einen Angemessenheitsbeschluss der EU-Kommission, mit dem diese bestätigt, dass das Datenschutzniveau in einem bestimmten Land als mit dem der EU vergleichbar bewertet wird.[9]
- Standardvertragsklauseln („Standard Contractual Clauses“ (SCC)), also ein von der EU-Kommission vordefiniertes Vertragswerk für den Datenexport.
- verbindliche interne Datenschutzvorschriften („Binding Corporate Rules“ (BCR)), also ein internes Vertragswerk einer länderübergreifenden Unternehmensgruppe, das von der zuständigen Aufsichtsbehörde genehmigt wurde.

Bei der Anwendung dieser Mechanismen gab es nun, ausgelöst in erster Linie durch das im Folgenden beschriebene Schrems II-Urteil, wichtige Änderungen mit Auswirkungen auf das IT-Management.

Wichtig für international aufgestellte Unternehmen ist, dass die hier beschriebenen Vorgaben auch innerhalb eines Unternehmens oder Konzerns gelten, d.h. beispielsweise auch für Datentransfers an eine außerhalb der EU sitzende Mutter- oder Tochtergesellschaft. Man spricht daher davon, dass es in diesem Zusammenhang kein Konzernprivileg gibt [SS21].

4.2 Das Schrems II-Urteil

Als Schrems II-Urteil[10] bezeichnet man ein Urteil des Europäischen Gerichtshofs (EuGH) vom Juli 2020, benannt nach dem österreichischen Datenschutzaktivisten Max Schrems, der das Verfahren durch seine Beschwerde bei der irischen Aufsichtsbehörde gegen den Transfer seiner Daten durch Facebook aus Europa in die USA angestoßen hatte.[11] Im Kern des Urteils hat der EuGH den auf den Privacy Shield-Regelungen basierenden Angemessenheitsbeschluss für die USA für ungültig erklärt. Grund für diese Entscheidung war, dass staatliche Stellen und Nachrichtendienste in den USA aus Sicht des EuGH zu viele Möglichkeiten haben, auf die Daten zuzugreifen, und es keine ausreichenden Rechtsmittel dagegen gibt. Diese Entscheidung betrifft insbesondere viele Cloud-Dienste,

[9] Eine vollständige Liste dieser Angemessenheitsbeschlüsse ist unter https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en veröffentlicht.
[10] https://curia.europa.eu/juris/liste.jsf?language=de&num=C-311/18
[11] Man spricht hier vom Schrems II-Urteil, da es bereits ein Vorgängerurteil des EuGH gab, mit dem die damalige Safe-Harbor-Regelung, Vorgänger des Privacy Shield, für ungültig erklärt worden war.

die in den USA basiert sind und bei denen die Daten auf Basis von Privacy Shield in die USA transferiert wurden. Auf Grund dieses Urteils müssen alle Datentransfers in die USA, die bislang auf Grundlage dieser Regelungen durchgeführt wurden, auf eine neue Rechtsgrundlage gestellt werden, typischerweise die SCC. Die SCC wurden vom EuGH ausdrücklich als weiterhin mögliche Rechtsgrundlage akzeptiert, allerdings unter der Voraussetzung, dass mit den SCC (oder analog auch den BCR) unter den rechtlichen und sonstigen Rahmenbedingungen im Zielland tatsächlich ein ausreichendes Schutzniveau erreicht wird. Dies muss in einem ersten Schritt systematisch bewertet werden, wofür sich mittlerweile der Begriff eines „Transfer Impact Assessments" (TIA) etabliert hat. Bei Bedarf müssen zusätzliche Maßnahmen wie die Verschlüsselung der Daten (geeignet, sofern die Daten im Zielland nur gespeichert werden) ergriffen werden. Eine ausführliche Diskussion derartiger Maßnahmen wurde vom European Data Protection Board (EDPB) zusammengetragen, dem Gremium der europäischen Datenschutz-Aufsichtsbehörden [Eu21].

Auch wenn das Urteil sich direkt nur auf den Datentransfer in die USA bezieht, hat es Auswirkungen weit darüber hinaus, denn die Aussagen im Urteil sind sehr grundsätzlich und auch auf Datentransfers in andere Staaten anzuwenden.

Fallbeispiel *Nach dem Schrems II-Urteil überprüfte das Fitness-Center seine Auftragsverarbeitungsverträge daraufhin, inwieweit diese betroffen waren. Kriterium dafür war in erster Linie, ob die Verträge das Privacy Shield als Grundlage verwendeten, aber auch, ob es andere Verträge mit Anbietern außerhalb der EU gab. Bei den meisten Verträgen hatten die Vertragspartner ihren Sitz in der EU und unterlagen also direkt der DSGVO.*

Bei einem der genutzten Cloud-Anbieter lief der Vertrag auf Basis von Privacy Shield. Dieser Anbieter reagierte aber kurzfristig von sich aus und bot eine neue Auftragsverarbeitungsvereinbarung auf Basis der SCC an, die dann auch sofort akzeptiert wurde. Schwieriger war die Durchführung eines TIA mit der Klärung, welche zusätzlichen technischen und organisatorischen Maßnahmen für die Anbieter mit Sitz außerhalb der EU erforderlich waren, um hier ein angemessenes Datenschutzniveau sicherzustellen, insbesondere da es sich um Anbieter handelte, die wesentlich größer waren als das Fitness-Center, und es daher in der Praxis kaum Möglichkeit gab, Maßnahmen gegen den Willen der Anbieter durchzusetzen. Bei dem genutzten Cloud-Speicherdienst wurde vereinbart, dass die Daten dort in Zukunft nur noch in verschlüsselter Form abgelegt werden, und entsprechende Maßnahmen zur Umsetzung dieser Vereinbarung wurden umgesetzt. Dies dauerte einige Monate, auch wenn die Vorgaben des Schrems II-Urteils streng genommen sofort hätten umgesetzt werden müssen, aber das war praktisch nicht umsetzbar. Bei der Nutzung von MS Office 365 wurde im Rahmen der TIA analysiert, welche Daten dort abgelegt wurden und wie kritisch diese aus Datenschutzsicht zu bewerten sind.

Das führte dazu, dass einige Daten, beispielsweise einzelne Attribute in der Kundenübersicht, gelöscht wurden, weil sie nicht unbedingt notwendig waren. Andere

Attribute, beispielsweise über gesundheitliche Einschränkungen der Besucher des Fitness Centers, wurden aus der Übersicht herausgezogen und in eine separate und verschlüsselte Datei übertragen. Die noch in MS Office 365 verbleibenden Daten wurden als wenig kritisch betrachtet und daher das verbleibende Risiko akzeptiert. Auch wenn das datenschutzrechtlich als grenzwertig beurteilt wurde, war die Einschätzung, dass dieses Vorgehen gerade noch vertretbar sei.

4.3 Brexit und „Five Eyes“

Für UK gab es nach einigem Hin und Her (nicht nur beim Datenschutz) im Juni 2021, also gerade rechtzeitig zum Auslaufen der Brexit-Übergangsvereinbarungen, einen Angemessenheitsbeschluss der EU. Ein solcher Angemessenheitsbeschluss nach Art. 45 DSGVO bestätigt, dass im jeweiligen Land ein angemessenes Datenschutzniveau herrscht und ein Transfer personenbezogener Daten in das Land unter den gleichen Rahmenbedingungen möglich ist wie innerhalb der EU. Einerseits war ein solcher Beschluss zu erwarten, da Datenschutz im UK ja bis einige Monate vorher als Mitglied der EU noch selbstverständlich als angemessen akzeptiert war. Andererseits ist UK eines der sogenannten Five-Eyes-Länder (die anderen sind USA, Kanada, Australien und Neuseeland) und die Kritik aus dem Schrems II-Urteil des EuGH ist teilweise auch hier anwendbar. Für Unternehmen bedeutet das, dass der Datenexport nach UK derzeit aus Datenschutzsicht problemlos möglich ist, es aber ein nennenswertes Risiko gibt, dass ein ähnliches Urteil diese Situation in absehbarer Zeit ändert und für das UK dann im Wesentlichen die gleichen Regeln gelten wie für die USA.

Verschärft wurde dieses Risiko dadurch, dass es einige Wochen nach diesem Angemessenheitsbeschluss Aussagen aus der britischen Regierung gab, dass man die Regeln zum Umgang mit Cookies gegenüber den bisherigen, aus der DSGVO übernommenen Regeln ändern wolle [Ka21]. Auch wenn diese Änderung noch akzeptabel erscheint, gibt es Befürchtungen, dass dies ein Dammbruch sei und weitere Änderungen die Angemessenheit des bestätigten Datenschutzniveaus aushöhlen könnten.

4.4 Neue Standardvertragsklauseln

Die Standardvertragsklauseln (SCC) enthalten ein von der EU-Kommission vordefiniertes Vertragswerk für den Datenexport in Drittländer. Da diese noch aus der Zeit vor der DSGVO stammten und dementsprechend veraltet waren, wurden sie im Juni 2021 aktualisiert und an die DSGVO sowie die im Schrems II-Urteil formulierten Anforderungen angepasst. Die alten Klauseln dürfen seit dem 28.09.2021 nicht mehr für neue Verträge verwendet werden, bestehende Verträge können noch bis Ende 2022 weiter genutzt werden und müssen bis dahin auf die neuen Klauseln angepasst[12] werden.

[12] Diese neuen Klauseln sind veröffentlicht unter https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/

Aus den neuen Standardvertragsklauseln ergeben sich teilweise deutlich höhere datenschutzrechtliche Anforderungen beim Export von Daten in Drittländer außerhalb der EU, beginnend mit der Forderung nach einem Transfer Impact Assessment (TIA). Hierbei sind insbesondere die im Schrems-II-Urteil genannten Risiken zu betrachten, die auch der Empfänger der Daten nicht unter Kontrolle hat. Neben den beschriebenen SCC für den Datenexport außerhalb der EU wurden auch optionale Standardvertragsklauseln für die Arbeit mit Auftragnehmern innerhalb der EU definiert, es in der Vergangenheit nicht gab. Diese sind optional, sollten aber in Verhandlungen zwischen Auftraggebern und Auftragnehmern zumindest berücksichtigt werden und können dann als Hilfestellung bei der Formulierung geeigneter eigener Auftragsverarbeitungsverträge dienen.

Fallbeispiel *Nachdem die neuen SCC veröffentlicht wurden, überprüfte das Fitness-Center erneut seine Auftragsverarbeitungsverträge. Zwar gibt es für Auftragnehmer mit Sitz in der EU jetzt die neuen optionalen SCC, aber das Fitness-Center sah für diese Fälle keinen Grund, die Verträge umzustellen.*

Anders war die Situation bei den Auftragnehmern, die ihren Sitz außerhalb der EU hatten, die ja schon nach dem Schrems II-Urteil identifiziert worden waren. In einem Fall lief die Zusammenarbeit ursprünglich auf der Basis von Privacy Shield, war dann auf die SCC umgestellt worden. Bei diesen Auftragnehmern entschied sich das Unternehmen dafür, kurzfristig bei den bestehenden Verträgen zu bleiben, mit den Auftragnehmern aber Kontakt aufzunehmen und abzustimmen, wann und wie man auf die neuen SCC umstellen sollte.

4.5 Home Office, Videokonferenzen, MS Office 365 etc.

Auch wenn es bei den Themen Home Office, Videokonferenzen, MS Office 365 etc. in den letzten Jahren keine expliziten rechtlichen Änderungen gab, so waren sie doch sehr im Fokus der Diskussion und auch der Aufsichtsbehörden, da die verwendeten Werkzeuge zum großen Teil auf Cloud-Diensten von Anbietern von außerhalb der EU basieren, gleichzeitig auf Grund der Corona-Epidemie aber intensiv genutzt wurden. Es gelten dabei im Wesentlichen die gleichen Regelungen zum Datenexport wie oben beschrieben, allerdings mit teilweise sehr unterschiedlichen Interpretationen der gleichen Regelungen auch zwischen den verschiedenen Aufsichtsbehörden, was die Umsetzung für Unternehmen besonders erschwert.[13]

Fallbeispiel *Schon seit einigen Jahren nutzt das Fitness-Center MS Office 365 für seine Office-Anwendungen. Außerdem bot es einige seiner Kurse online über einen US-amerikanischen Anbieter an, als Vor-Ort-Kurse auf Grund der Corona-Epidemie nicht mehr stattfinden konnten.Der DSB des Unternehmens verfolgte daher die Diskussionen*

[13] Siehe beispielsweise die Pressemitteilung von mehreren, aber eben nicht allen, Landesdatenschutzbeauftragten unter https://www.datenschutz.de/microsoft-office-365-bewertung-der-datenschutzkonferenz-zu-undifferenziert-nachbesserungen-gleichwohl-geboten/

zur Rechtslage für diese Dienste, und kam zu folgenden Empfehlungen, die dann auch umgesetzt wurden:

- MS Office 365 kann vorerst weiterhin genutzt werden, wobei darauf zu achten ist, dass die entsprechenden Optionen genutzt werden, um das System möglichst datenschutzfreundlich zu konfigurieren und die mögliche Nutzung von Daten durch Microsoft auf ein Minimum zu beschränken. Dabei ist die weitere Entwicklung, insbesondere eventuelle neue Aussagen der Datenschutzkonferenz (DSK), zu beobachten.
- Die Nutzung des Videokonferenzsystems ist problematisch, aber es ist zumindest kurzfristig schwierig, zu einem anderen Anbieter zu wechseln. Daher muss auch hier die Nutzung des Systems datenschutzfreundlich konfiguriert werden auf Basis der entsprechenden Orientierungshilfe der DSK [Ko20]. Außerdem sollten andere Anbieter mit Serverstandorten innerhalb der EU evaluiert werden, inwieweit deren Dienste ebenfalls die Anforderungen erfüllen.

5 Entwicklungen außerhalb der EU

Für größere Unternehmen, die auch außerhalb der EU aktiv sind, ist zu berücksichtigen, dass auch in anderen Ländern neue Datenschutzgesetze eingeführt wurden oder in Vorbereitung sind. Manche davon sind stark an der DSGVO orientiert (z.B. Brasilien, Schweiz), bei anderen ist die Ähnlichkeit geringer (Kalifornien) oder die Schwerpunkte liegen an anderer Stelle (Indien).

6 Bewertung der aktuellen Entwicklungen zum Datenschutz

Nach diesem Überblick über die aktuellen Entwicklungen im Datenschutz stellt sich die Frage, wie diese zu bewerten sind. Für die DSGVO gab es Mitte 2020 eine Evaluation durch die EU-Kommission [Eu20], wie bereits in Art. 97 DSGVO festgelegt. Dabei kam die EU-Kommission zum Ergebnis, dass es keinen Handlungsbedarf gibt. Viele andere Autoren haben diese Evaluation dagegen zum Anlass genommen, Kritikpunkte sowie Handlungsbedarfe zusammenzutragen, so beispielsweise [JJ20, RG20, Sc20, We20].

Im Folgenden sind die wichtigsten Kritikpunkte an der DSGVO und den aktuellen Entwicklungen des Datenschutzes insgesamt zusammengetragen.

- Nervende Cookie-Banner: Aus Sicht vieler Benutzer sind Cookie-Banner wahrscheinlich der Punkt, an dem sie am meisten Berührung mit dem Datenschutz haben, und gleichzeitig für viele eine nervende Pflichtübung, bei der sie sowieso ohne nachzudenken alle gefragten Cookies akzeptieren, d.h. die Banner verfehlen in vielen Fällen ihren Zweck. Hier besteht großer Bedarf an neuen, besseren Lösungen, die einen Kompromiss zwischen den beteiligten Interessengruppen

herstellen und für alle akzeptabel sind. Ob die im TTDSG definierten Dienste zum Einwilligungsmanagement einen solchen Kompromiss darstellen, bleibt abzuwarten.

- Schwierige Nutzung von Cloud-Diensten: Aus Sicht vieler Unternehmen stellen die mit dem Schrems II-Urteil definierten Regelungen ein großes Problem dar, da diese die Nutzung von vielen Cloud-Diensten wesentlich erschweren. Andere Beteiligte sehen gerade darin ein Zeichen für die große Abhängigkeit der europäischen Unternehmen und für die unzureichende digitale Autonomie der EU, die mit Ansätzen wie der europäischen GAIA-X-Cloud adressiert werden sollte. Hierbei handelt es sich aber in erster Linie um wirtschaftspolitische Fragen, die nur begrenzt auch Fragen des angemessenen Datenschutzes sind.

- Wachsende Beschränkungen für die Nutzung von Tracking-Mechanismen, insbesondere Cookies: Hier sind die Meinungsunterschiede je nach Sichtweise besonders groß, ob es sich hierbei in erster Linie um eine Gefährdung des Geschäftsmodells für viele verbreitete Webangebote handelt oder um einen notwendigen Schutz der Privatsphäre der Internet-Nutzer.

- „One size fits all“: Im Kern gelten die Vorgaben zum Datenschutz unabhängig von der Größe der verantwortlichen Organisation, unabhängig davon, ob es sich beispielsweise um einen kleinen Sportverein handelt oder einen Großkonzern, dessen Geschäftsmodell auf der Sammlung und Auswertung persönlicher Daten basiert. Diese Einheitlichkeit ist sehr zwiespältig zu bewerten, denn einerseits haben große Organisationen natürlich wesentlich mehr Ressourcen, um die gewünschte Verarbeitung juristisch korrekt zu gestalten und trotzdem ihre Ziele zu erreichen und die Regelungen des Datenschutzes zum Umgehen. Kleine Organisationen benötigen dagegen schon für die grundlegende Einhaltung der Vorgaben des Datenschutzes anteilmäßig sehr viel mehr Ressourcen. Andererseits wäre es nicht schlüssig, warum die gleichen personenbezogene Daten bei einer kleinen Organisation weniger geschützt werden sollten als bei einer großen.

- Ungenügende Vereinheitlichung: Ein wesentliches Ziel der DSGVO war die Vereinheitlichung der Vorgaben des Datenschutzes und ihrer Umsetzung, aber dies wurde nur sehr begrenzt erreicht. Dies betrifft u.a. die unterschiedlichen nationalen Ergänzungen und Konkretisierungen der DSGVO, in Deutschland durch das Bundesdatenschutzgesetz und eine Vielzahl anderer Regelungen. Ein viel diskutiertes Beispiel für die unterschiedliche Interpretation und Umsetzung sind die 18 verschiedenen Aufsichtsbehörden alleine in Deutschland, die häufig uneinig sind, wie beispielsweise beim Thema MS Office 365. Ein weiteres Beispiel für die uneinheitliche Umsetzung der gleichen Regelungen ist die Kritik an Irland und seiner Datenschutzaufsichtsbehörde, der häufig nachgesagt wird, die DSGVO-Vorgaben nicht ernsthaft durchzusetzen.[14]

[14] Siehe beispielsweise https://www.heise.de/news/DSGVO-Kritik-an-Irland-als-Europas-Flaschenhals-mit-Zahlen-untermauert-6191701.html

- Unzureichende Rechtssicherheit durch Interpretationsschwierigkeiten und mangelnde Durchsetzung: Verbunden mit der ungenügenden Vereinheitlichung ist die von fast allen Beteiligten kritisierte Rechtsunsicherheit beim Datenschutz. Hier gibt es zwar durch die im vorliegenden Beitrag beschriebenen Urteile und zusätzlichen Regelungen insgesamt eine Verbesserung, aber die Unsicherheit ist weiterhin hoch und stellenweise sogar noch gewachsen, insbesondere in Bezug auf den angemessenen Umgang mit Cloud-Diensten. Kritisch zu bewerten ist dabei auch, dass der weitaus überwiegende Teil der Datenschutzverstöße nicht geahndet wird, wie jeder Internetnutzer regelmäßig sieht. Dementsprechend ist für viele Organisationen die Motivation gering, sich selbst zu beschränken und die relevanten gesetzlichen Anforderungen zu erfüllen, wenn doch „alle anderen das auch nicht tun“.
- Erhöhte Grenze für die Benennung eines DSB: Die im 2. DSAnpUG-EU erhöhte Grenze führt einerseits zu einer leichten Annäherung an die EU-Regelung. De facto führt diese Änderung andererseits zumindest bei einem Teil der betroffenen Unternehmen dazu, dass sie die weiterhin gültigen Regelungen zu geringerem Anteil umsetzen, da ihnen jetzt die benötigte Kompetenz fehlt.

7 Zusammenfassung und Ausblick

Das Datenschutzrecht ist ein Themengebiet, das sich in einer relativ schnellen Entwicklung befindet, u.a. deshalb, weil hier widerstrebende Interessen der Beteiligten aufeinandertreffen. Für Unternehmen (und andere Organisationen) bedeutet das, dass sie diese Entwicklung laufend beobachten, um nach Bedarf darauf zu reagieren, insbesondere natürlich, wenn sie personenbezogene Daten in einem Rahmen verarbeiten, der bereits sehr in der Diskussion ist, wie der weitreichenden Nutzung von Cookies oder dem Datentransfer nach außerhalb der EU. Es ist damit zu rechnen, dass es gerade bei diesen Themen auch weiterhin viel Bewegung geben wird, beispielsweise in Bezug auf die Gestaltung der Cookie-Banner, mit denen Einwilligungen der Webseitenbesucher zum Einsatz von Cookies eingeholt werden. Die Nutzung von operativen Daten für statistische und ähnliche Auswertungen, üblicherweise verbunden mit einer nur begrenzt erlaubten Zweckänderung der Daten, ist ein weiteres Thema, bei dem noch viel Klärungsbedarf besteht und das ggf. genau beobachtet werden sollte, um nach Bedarf reagieren zu können. Unabhängig von dieser rechtlichen Sichtweise sollten Organisationen aber immer daran denken, dass sie Daten ihrer Kunden, Mitarbeiter, Webseitenbesucher etc. im Vertrauen darauf bekommen, dass sie damit angemessen und fair umgehen. Selbst wenn die Verarbeitung dieser Daten im konkreten Fall juristisch gerade noch akzeptabel ist, kann sie zu einem Vertrauensverlust mit entsprechenden Folgen führen.

Literaturverzeichnis

[Cy21] Cyphers, B.: Google´s FLoC Is a Terrible Idea, https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea, Stand: 10.08.21.

[Eu20] European Commission - Data protection as a pillar of citizens' empowermentand the EU's approach to the digital transition - two years of application of the General Data Protection Regulation, https://ec.europa.eu/info/sites/default/files/1_en_act_part1_v6_1.pdf, Stand: 10.08.21.

[Eu21] European Data Protection Board (EDPB): Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf, Stand: 10.08.21.

[Go] Google Research & Ads: Evaluation of Cohort Algorithms for the FLoC API, https://raw.githubusercontent.com/google/ads-privacy/master/proposals/FLoC/FLOC-Whitepaper-Google.pdf, Stand: 10.08.21.

[GS21] Grombacher, S.; Straub, T.: Alles akzeptieren oder Einstellung(en) ändern? – zum Stand der Praxis bei der Nutzung von Cookies. In (Gesellschaft für Informatik e.V. (GI), Hrsg.): 2021 Computer Science & Sustainability. Berlin, S. 963–977, 2021.

[JJ20] Jaspers, A.; Jacquemain, T.: Datenschutz-Grundverordnung – Praxiserfahrungen und Evaluation. Datenschutz und Datensicherheit 44/20, S. 297–301, 2020.

[Ka21] Kafsack, H.: Erst der Brexit, jetzt die Cookies, https://www.faz.net/aktuell/wirtschaft/grossbritannien-will-cookie-hinweise-im-internet-einschraenken-17504630.html, Stand: 10.08.21.

[Kn21] Kneuper, R.: Datenschutz für Softwareentwicklung und IT - Eine praxisorientierte Einführung, Springer Vieweg, 2021.

[Ko20] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz): Orientierungshilfe Videokonferenzsysteme, https://www.datenschutzkonferenz-online.de/media/oh/20201023_oh_videokonferenzsysteme.pdf, Stand: 10.08.21.

[RG20] Roßnagel, A.; Geminn, C.: Datenschutz-Grundverordnung verbessern - Änderungsvorschläge aus Verbrauchersicht, Nomos, 2020.

[Sc20] Schulz, S.: Die Evaluation der DSGVO. Datenschutz und Datensicherheit 44/20, S. 302–306, 2020.

[SS21] Schulte, L.; Schmale, J.: Vertragliche Absicherung internationaler Datentransfers. Datenschutz und Datensicherheit 45/21, S. 46–54, 2021.

[We20] Weichert, T.: Die DSGVO, ein – ganz guter – Anfang. Datenschutz und Datensicherheit 44/20, S. 293–296, 2020.