Ausgabe 3 Juni 2025

Revisionspraxis PRev

Journal für Revision, IT-Sicherheit, SAP-Sicherheit und Datenschutz

Nicole Jekel
Effektive und effiziente Kommunikation mit KI: Mit KI auf den Punkt – oder darüber hinaus?

Lasse Grehl
Voice Deepfakes – Die neue Waffe im Cyberkrieg

Holger Stumm
Quantensichere Verschlüsselung aller digitalen Transaktionen: Geht das? Gibt es das? – Teil 1

Karsten Kinast
Der Weg des Vereinigten Königreichs nach dem Brexit: Datenschutzregulierung und -praktiken

Marco Di Filippo
Angriff der Maschinen – Wie Künstliche Intelligenz Cyberkriminellen „Superkräfte“ verleiht

Olaf Brandt
Aktuelle Tracking-Technologien und ihre rechtliche Bewertung

Sophie Schille
EU verschärft regulatorische Anforderungen an die Cybersicherheit digitaler Produkte

Rechtsprechung und Aktuelles zum Datenschutz

www.prev.de

ISSN 1862-9032

BOORBERG

Inhalt

Revision 4.0

Effektive und effiziente Kommunikation mit KI: Mit KI auf den Punkt – oder darüber hinaus? 104

Voice Deepfakes – Die neue Waffe im Cyberkrieg 109

Quantensichere Verschlüsselung aller digitalen Transaktionen: Geht das? Gibt es das? – Teil 1 117

Datenschutz

Der Weg des Vereinigten Königreichs nach dem Brexit: Datenschutzregulierung und -praktiken 124

Angriff der Maschinen – Wie Künstliche Intelligenz Cyberkriminellen „Superkräfte“ verleiht 133

Aktuelle Tracking-Technologien und ihre rechtliche Bewertung 139

EU verschärft regulatorische Anforderungen an die Cybersicherheit digitaler Produkte 144

Rechtsprechung und Aktuelles zum Datenschutz 147

Neue Bücher 151

Nachrichten 152

Seminare/Veranstaltungen 154

Impressum/Vorschau 156

Bestellen Sie hier die PRev im Abonnement

Datenschutz

Dr. Michael Foth

Liebe Leserinnen und Leser,

in seinem Beitrag „Der Weg des Vereinigten Königreichs nach dem Brexit: Datenschutzregulierung und -praktiken“ analysiert Karsten Kinast, wie Großbritannien seine Datenschutzstandards aufrechterhält und wie es sich in den globalen Datenschutzkontext einfügt.

Marco Di Filippo behandelt in seinem Beitrag „Angriff der Maschinen – Wie Künstliche Intelligenz Cyberkriminellen „Superkräfte“ verleiht“ ein hochaktuelles Thema: den Missbrauch von KI im Cyberraum. Durch intelligente Algorithmen werden digitale Angriffe präziser, schneller und schwerer zu erkennen. Der Beitrag zeigt eindrucksvoll, wie sich das Machtverhältnis zwischen Angreifern und Verteidigern verschiebt – und warum Aufklärung und Prävention wichtiger sind denn je.

Tracking-Technologien sind aus dem digitalen Alltag nicht mehr wegzudenken – gleichzeitig stehen sie zunehmend im Fokus datenschutzrechtlicher Debatten. Welche Verfahren sind zulässig? Wo verläuft die Grenze zwischen Analyse und Überwachung? Olaf Brandt widmet sich in seinem Beitrag „Aktuelle Tracking-Technologien und ihre rechtliche Bewertung“ genau diesen Fragen. Besonders im Fokus stehen neue Ansätze wie Cookie-loses-Session-Tracking und serverseitiger Datenaustausch mit Marketing-Plattformen. Diese Technologien ermöglichen es Unternehmen, ihre Ziele zu erreichen, ohne dabei die Privatsphäre der Nutzer zu gefährden. Sie bieten die Hoffnung auf eine harmonische Beziehung zwischen effektivem Tracking und konsequentem Datenschutz.

Mit dem Cyber Resilience Act (CRA) zieht die EU die Schrauben bei der Cybersicherheit digitaler Produkte deutlich an. Hersteller und Einführer stehen künftig in der Pflicht, Sicherheitsanforderungen über den gesamten Produktlebenszyklus hinweg zu erfüllen. In ihrem Kurzbeitrag „EU verschärft regulatorische Anforderungen an Cybersicherheit digitaler Produkte – Der Cyber Resilience Act“ gibt Sophie Schille einen kompakten Überblick über die neuen Regelungen, die zentralen Anforderungen und deren Auswirkungen auf Unternehmen.

Viele Erkenntnisse und Spaß beim Lesen wünscht Ihnen

Ihr
Dr. Michael Foth

Datenschutz

Karsten Kinast

Der Weg des Vereinigten Königreichs nach dem Brexit: Datenschutzregulierung und -praktiken

A. Einleitung

Seit dem Austritt aus der EU steht Großbritannien vor der Herausforderung, seine Datenschutzregulierung neu zu definieren.

Mit dem Brexit hat sich Großbritannien auch von der Datenschutzgrundverordnung (DSGVO) gelöst. Dennoch bleibt der britische IT-Sektor traditionell eng mit dem EU-Markt verbunden. Derzeit ist der Data Protection Act (DPA) von 2018 in Kraft, der in Kombination mit der UK-GDPR (General Data Protection Regulation) eine Angemessenheitsentscheidung der EU-Kommission rechtfertigt.

Die geplante Data (Use and Access) Bill (DUA Bill) markiert jedoch eine zunehmende Distanz zur DSGVO. Der Gesetzesentwurf zeigt durch verschiedene Änderungen, dass Großbritannien – ganz nach dem Vorsatz „take back control" – eigenständige Datenschutzstandards etablieren möchte. Dies wird unter anderem durch die Abschaffung der Pflicht zur Ernennung eines Datenschutzbeauftragten, reduzierte Dokumentationsanforderungen und die Einschränkung der Rechte betroffener Personen deutlich.[1]

1 Fischer, ZD-Aktuell 2023, 01157; Johannes, ZD-Aktuell 2023, 01137.

Insofern fällt Großbritannien im internationalen Vergleich auf. Das Land zielt offensichtlich darauf ab, die Anforderungen an den Datenschutz zu verringern und Unternehmen zu entlasten.[2]

Dieser Artikel beleuchtet die Entwicklung der britischen Datenschutzregulierung nach dem Brexit und untersucht, wie sich das Vereinigte Königreich von der EU-Datenschutzgrundverordnung entfernt. Es wird analysiert, welche neuen Gesetze und Reformen das Land einführen will und wie diese Unternehmen betreffen. Zudem werden die internationalen Auswirkungen der britischen Datenschutzpolitik analysiert und die Frage diskutiert, wie sich das Vereinigte Königreich im globalen Datenschutzkontext positioniert.

B. Das Datenschutzgesetz im Vereinigten Königreich vor dem Brexit

I. Rückblick

Vor der DSGVO basierte das Datenschutzrecht im Vereinigten Königreich auf dem Data Protection Act 1998, der im Einklang mit der EU-Datenschutzrichtlinie 95/46/EG stand. Mit dem Inkrafttreten der DSGVO im Jahr 2018 wurde der Datenschutz im Vereinigten Königreich auf eine neue Grundlage gestellt. Um die europäischen Vorgaben national umzusetzen und EU-konforme Datenschutzstandards zu gewährleisten, verabschiedete das Vereinigte Königreich den DPA 2018. Dieser reformierte den Data Protection Act 1998 und sorgte für eine vollständige Harmonisierung des britischen Datenschutzrechts mit der DSGVO. Dieser ergänzte die DSGVO und passte sie an britische Gegebenheiten an, etwa durch Regelungen zu nationalen Sicherheitsbelangen oder spezifische Befugnisse des Information Commissioner's Office (ICO), die britische Aufsichtsbehörde. Damit war das britische Datenschutzrecht eng mit dem europäischen Regime verflochten, und Unternehmen in Großbritannien mussten sich an die strengen Vorgaben der DSGVO halten, insbesondere im Hinblick auf Datensicherheit, Rechte der Betroffenen und internationale Datentransfers.

II. Die Auswirkungen des Brexits auf die Datenschutzregulierung

Mit dem Brexit änderte sich die Rechtslage entscheidend. Durch den European Union (Withdrawal) Act 2018 übernahm das Vereinigte Königreich die DSGVO in nationales Recht, was zur Entstehung der sogenannten UK GDPR führte, einer an britische Bedürfnisse angepassten Version der europäischen Verordnung. Der Datenschutzstandard blieb zunächst weitgehend erhalten, um eine Angemessenheitsentscheidung der Europäischen Kommission zu gewährleisten, die es ermöglichen sollte, weiterhin personenbezogene Daten ungehindert zwischen der EU und Großbritannien zu transferieren.

Allerdings eröffnete der Brexit auch den Spielraum für eigenständige Gesetzesinitiativen, die das Datenschutzrecht flexibler gestalten sollten. Die britische Regierung verfolgt eine Datenschutzreform und strebt eine Abkehr von der DSGVO an. So soll der Datenschutz weniger bürokratisch gestaltet, Unternehmen entlastet und Datenschätze genutzt werden. Diese Reform sieht unter anderem die Abschaffung der Pflicht zur Benennung eines Datenschutzbeauftragten, verringerte Dokumentationspflichten und gelockerte Vorgaben für Datenschutz-Folgenabschätzungen vor. Dies zeigt die wachsende Divergenz zwischen britischem und europäischem Datenschutzrecht, die langfristig erhebliche Auswirkungen auf den Datentransfer und die Beziehungen zwischen der EU und Großbritannien haben könnte.

C. Das Datenschutzgesetz im Vereinigten Königreich nach dem Brexit

I. UK Data Protection Act 2018 (DPA 2018)

a. Inhalt des DPA 2018

Zum einen definiert der DPA 2018[3] wichtige Begriffe wie etwa den der „öffentlichen Gewalt" oder die Datenverarbeitung zu „öffentlichen Zwecken". Daneben werden auch die Durchsetzungsbefugnisse des ICO (Information Commissioner's Office) sowie spezielle Straftaten in Verbindung mit personenbezogenen Daten festgeschrieben. Im Übrigen bestimmt Anhang 1 weitere Rechtsgrundlagen für die Verarbeitung von besonderen Datenkategorien, während Anhänge 2 und 3 Ausnahmen von den Vorgaben der UK GDPR gestatten. Der DPA 2018 bietet auch besondere Regelungen für die Datenverarbeitung zur wissenschaftlichen Forschung und für statistische Zwecke.

b. Beziehung des DPA 2018 zur DSGVO

Der DPA 2018 trat parallel zur DSGVO am 25. Mai 2018 in Kraft und regelte den Schutz personenbezogener Daten. Er ersetzte das alte Gesetz von 1998 und sollte

2 Johannes, ZD-Aktuell 2023, 01137.

3 Data Protection Act 2018, abrufbar unter https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted, letzter Zugriff am 26.10.2024.

auch eine reibungslose Weitergeltung der DSGVO-Vorgaben nach Austritt aus der EU ermöglichen.[4] Der DPA 2018 wurde verabschiedet, um die DSGVO in nationales Recht zu integrieren und ergänzende Regelungen für Bereiche zu schaffen, die nicht vollständig durch die DSGVO abgedeckt wurden, wie etwa Strafverfolgung und nationale Sicherheit. Insofern setzt das Gesetz die DSGVO vergleichbar zum Bundesdatenschutzgesetz (BDSG) in nationales Recht um. In ähnlicher Wirkung ist das Gesetz bis heute mit einigen Anpassungen als Begleitgesetz für die UK GDPR in seiner aktuellen Fassung seit dem 1. Januar 2021 gültig.

II. Anpassungen nach dem Brexit: UK GDPR

Die DSGVO wurde gemäß Abschnitt 3 des European Union (Withdrawal) Act 2018 (EUWA 2018) durch die UK GDPR übernommen. Dieses Gesetz wurde für die Zeit nach dem Brexit geschaffen, um sicherzustellen, dass im Vereinigten Königreich weiterhin ein hohes Datenschutzniveau garantiert werden kann. Sie trat am 1. Januar 2021 in Kraft und regelt als Herzstück des britischen Datenschutzrechts, wie personenbezogene Daten verarbeitet werden dürfen. Inhaltlich ist die UK GDPR mit Ausnahme einiger Anpassungen weitgehend mit der DSGVO übereinstimmend.[5]

Die UK GDPR und die DSGVO teilen die gleichen Grundprinzipien, wie Fairness und Transparenz, Zweckbindung, Datenminimierung und Speicherbegrenzung. Zudem müssen Maßnahmen zur Sicherstellung der Integrität und Vertraulichkeit getroffen werden, um personenbezogene Daten zu schützen. Insbesondere bedarf es für die Verarbeitung personenbezogener Daten auch einer Rechtsgrundlage, wie etwa der Einwilligung.

Daneben bestehen auch verschiedene DSGVO-ähnliche Betroffenenrechte, wie Auskunftsrechte oder Ansprüche auf Schadensersatz. Ein weiteres zentrales Recht ist die Widerspruchsmöglichkeit gegen die Verarbeitung, insbesondere gegen die Nutzung der Daten zu Zwecken der Direktwerbung. Die UK-GDPR regelt ebenfalls das Recht auf Schutz vor automatisierten Entscheidungen und Profiling, ähnlich wie die DSGVO.

Zudem können auch nach der UK-GDPR Verstöße mit hohen Geldstrafen geahndet werden, wobei die Sanktionen ähnlich streng sind wie bei der DSGVO. Die britische Datenschutzbehörde ist für die Überwachung und Durchsetzung der UK-GDPR zuständig. Eine erleichterte internationale Datenübertragung ist zu den gleichen Ländern möglich, für die auch die EU-Kommission Angemessenheitsbeschlüsse erlassen hat.

III. Unterschiede zur EU-Datenschutzgrundverordnung

Bislang stimmen die UK-GDPR und die DSGVO weitgehend überein. Bisher liegt der wesentliche Unterschied vor allem darin, dass die UK-GDPR ausschließlich im Vereinigten Königreich und für Unternehmen mit Sitz im Ausland, die personenbezogene Daten von UK-Bürgern verarbeiten, gilt. Die DSGVO findet hingegen weiterhin in der Europäischen Union Anwendung. Konsequent hierzu sind auch nicht mehr die Aufsichtsbehörden der einzelnen Mitgliedstaaten zuständig, sondern das ICO. Die wesentlichen Änderungen beziehen sich insofern insbesondere auf Streichungen von Passagen, die sich auf Mitgliedstaaten oder EU-Recht beziehen.[6]

Inhaltlich unterscheidet sich das britische Recht beispielsweise hinsichtlich des Mindestalters für die Einwilligung in die Verarbeitung von personenbezogenen Daten. Während EU-Bürger dies erst ab 16 Jahren können, ist eine Zustimmung durch Datenverarbeitung im Vereinigten bereits ab 13 Jahren möglich.

Anders als Mitgliedstaaten der EU kann das Vereinigte Königreich sein Datenschutzrecht nun auch jederzeit selbstständig ändern und ist nicht mehr an die Vorgaben der EU gebunden. EU-Mitgliedstaaten können nur in einzelnen Bereichen länderspezifische Anpassungen vornehmen, beispielsweise im Arbeitnehmerdatenschutz. In diesem Zusammenhang plant das Vereinigte Königreich nach dem Brexit mehr Flexibilität bei der Anpassung von Datenschutzbestimmungen an nationale Gegebenheiten.

IV. Reform der UK-GDPR: Bill No. 2

Im September 2021 hat das Ministerium für Digitales, Kultur und Sport (Department for Digital, Culture, Media and Sport, DCMS) erklärt, dass die Regierung ein öffentliches Konsultierungsverfahren zur Anpassung der Datenschutzregulierung gestartet hat. Dies führte zur Vorstellung der Data Protection and Digital Information (No. 2) Bill[7] (Bill No. 2) am 8. März 2023, die sowohl die UK-GDPR als auch den DPA 2018 anpassen soll. Die wesentlichen Grundprinzipien, Pflichten und Betroffenenrechte bleiben unberührt. Allerdings deuten die geplanten Änderungen darauf hin, dass sie zu einer Reduzierung der mit dem Verwaltungsaufwand verbun-

4 Stauch/Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Teil XV. Kap. 1 Großbritannien Rn. 13.

5 https://ico.org.uk/for-organisations/data-protection-and-the-eu/overview-data-protection-and-the-eu/, letzter Zugriff am 27.01.2025; Hofmann/Stach, ZD 2021, 3 (4).

6 Vgl. GDPR Keeling Schedule, abrufbar hier: https://assets.publishing.service.gov.uk/media/5a9d7430e5274a7bd3416ebd/2018-03-05_Keeling_Schedule.pdf, letzter Zugriff am 30.10.2024

7 https://publications.parliament.uk/pa/bills/cbill/58-03/0265/220265v2.pdf, letzter Zugriff am 18.11.2024.

denen Kosten, die für die Einhaltung der Datenschutzregeln für Unternehmen entstehen, führen sollen.[8] So sollen etwa Unternehmen die neuen Vorgaben nicht umsetzen müssen, wenn sie bereits DSGVO-konform agieren.[9]

Ein relevanter Unterschied liegt zudem in der Definition für anonymisierte personenbezogene Daten. So sollen nach Section 3A des Entwurfs Daten zwar für den Verantwortlichen als pseudonymisiert gelten und damit unter den Anwendungsbereich des Gesetzes fallen, aber unter bestimmten Voraussetzungen für andere Organisationen als vollständig anonym zu werten sein. Diese Erleichterung soll gelten, wenn die andere Organisation die für eine Identifizierung erforderlichen Informationen nicht im Rahmen der Datenverarbeitung erlangt hat oder erlangen könnte.[10]

Zudem wurden verschiedene Rechtfertigungsgrundlagen konkretisiert, damit eine Datenverarbeitung auch ohne Einwilligung einfacher möglich ist.[11] Exemplarisch für berechtigte Interessen werden beispielsweise Direktmarketing und Datenübertragungen im Unternehmen aufgelistet.[12] So soll es privilegierte berechtigte Interessen von Verantwortlichen geben, die in Anhang 1 des Entwurfs aufgelistet sind. Liegt ein solches Interesse vor, müssen Verantwortliche die sonst erforderliche Interessenabwägung nicht mehr vornehmen (Section 5 des Entwurfs). Bislang beschränkt sich die Liste auf öffentliche Interessen, wie etwa Notfälle, Strafprävention und die nationale Sicherheit. Allerdings soll das Innenministerium in einem speziellen Verfahren diesen Anhang erweitern können.[13]

Section 2 des Entwurfs erhält eine Konkretisierung zum Forschungsbegriff, der Innovation fördern soll[14]. Hiernach soll alles als wissenschaftlicher Zweck gelten, was vernünftigerweise als wissenschaftlich bezeichnet werden kann. Ob die Forschung öffentlich oder privat finanziert ist oder einen kommerziellen Zweck hat, soll nicht von Bedeutung sein.[15] Exemplarisch werden hierfür Bezüge zur Technologieentwicklung, Grundlagenforschung oder angewandten Wissenschaft aufgelistet, solange sie „vernünftigerweise als wissenschaftlich bezeichnet werden können". Forschung im Gesundheitsbereich ist allerdings nur dann wissenschaftlich, wenn sie zu öffentlichen Interessen erfolgt. Damit übernimmt die Bill No. 2 einen Großteil der Erwägungsgründe der DSGVO unmittelbar in den Gesetzestext. Wenn das Forschungsprivileg greift, müssen Verantwortliche die Mitteilungspflicht gegenüber Betroffenen nicht mehr einhalten, wenn die Daten direkt bei ihnen zu Forschungszwecken erhoben wurden und dies einen unverhältnismäßigen Aufwand darstellen würde.[16] Insgesamt soll die Reform auch zu einer Verbesserung des Gesundheits- und Sozialwesens durch einfacheren Zugang zu Daten sorgen.[17]

Zur Benennung eines Datenschutzbeauftragten sollen außerdem nur Behörden und Organisationen, die in Risikobereichen tätig sind, verpflichtet werden[18]. Auch müssen nach dem Entwurf Verantwortliche und Auftragsverarbeiter, die keinen Sitz im Vereinigten Königreich haben, keinen dort ansässigen Vertreter bestimmen.[19]

Außerdem soll das Auskunftsverweigerungsrecht nach Art. 12 Abs. 5 DSGVO zukünftig nicht mehr bei „offenkundig unbegründet oder exzessiven", sondern bei „lästigen oder exzessiven" Anträgen greifen.

Auch die Verwendung von Cookies soll durch Gesetzesänderung erleichtert werden.[20] Es soll etwa eine Ausnahme von der Zustimmungspflicht geben, wenn statistische Daten verarbeitet werden, um etwa die Webseite an Nutzerpräferenzen anzupassen oder Sicherheitsupdates durchzuführen.[21]

V. Data Use and Access (DUA) Bill

Mit dem Regierungswechsel in Großbritannien kam auch ein neuer Vorschlag für ein geändertes Datenschutzrecht. Insofern wurde am 3. Oktober 2024 der Entwurf der neuen Data Use and Access (DUA) Bill ins Parlament eingebracht. Am 19. November 2024 fand die zweite Lesung statt. Im Anschluss geht es nun in die sogenannte Ausschussphase.

Ziel ist es, das enorme Potential, das in Daten schlummert, auszuschöpfen. Bei dem neuen Gesetzesentwurf handelt es sich um eine an die neuen Regierungsziele angepasste Version der Bill No. 2. Dabei wurden insbesondere die wesentlichen Bausteine, die diesen Vorschlag ausgemacht haben, beibehalten.[22]

Es gibt aber auch einige relevante Abweichungen zur vorherigen Version. Zum einen stärkt der neue Vorschlag die Rechtsgrundlage des berechtigten Interesses.

8 Etteldorf, ZD-Aktuell 2023, 01131; Johannes, ZD-Aktuell 2023, 01137; ZD-Aktuell 2022, 01171.
9 Johannes, ZD-Aktuell 2023, 01137.
10 Johannes, ZD-Aktuell 2023, 01137.
11 Etteldorf, ZD-Aktuell 2023, 01131.
12 Etteldorf, ZD-Aktuell 2023, 01131.
13 Johannes, ZD-Aktuell 2023, 01137.
14 ZD-Aktuell 2022, 01171.
15 Etteldorf, ZD-Aktuell 2023, 01131.
16 Johannes, ZD-Aktuell 2023, 01137.
17 The Queen's Speech 2022, S. 57, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1074113/Lobby_Pack_10_May_2022.pdf.
18 Etteldorf, ZD-Aktuell 2023, 01131.
19 Johannes, ZD-Aktuell 2023, 01137.
20 Etteldorf, ZD-Aktuell 2023, 01131.
21 Johannes, ZD-Aktuell 2023, 01137.
22 https://dma.org.uk/article/dua-vs-dpdi-spot-the-difference#:~:text=The%20DUA%20Bill%20builds%20on,enhances%20market%20competition%20and%20innovation, letzter Zugriff am 17.12.2024.

Insbesondere gibt er verschiedene Beispiele, für welche Datengruppen dies zulässig sein soll, wie etwa Cybersicherheitsmaßnahmen oder Direktmarketing.[23] Damit will Großbritannien bezüglich einiger bereits in den Erwägungsgründen der DSGVO genannten Datenkategorien mehr Rechtssicherheit für Unternehmen schaffen. Zudem soll es spezielle Smart Data Vorgaben geben, um einen vereinfachten Datenaustausch mit autorisierten Organisationen zu fördern. Ziel ist es, die Wettbewerbsfähigkeit datenintensiver Branchen zu stärken.[24]

Zudem sollen die Weiterentwicklung digitaler Verifikationssysteme und die Einführung nationaler Sicherheitsvorkehrungen für Zertifizierungen sichere digitale Identitäten fördern und die Datensicherheit stärken. Allerdings soll der Außenminister befugt sein, eine Zertifizierung aufgrund der nationalen Sicherheit ablehnen zu können. Eine wesentliche Änderung gibt es auch in Bezug auf Transparenzpflichten. Nach der DUA Bill sollen zukünftig Verantwortliche in bestimmten Ausnahmefällen nicht mehr verpflichtet sein, über eine Datenverarbeitung zu Forschungs- und Statistikzwecken zu unterrichten. Das ist beispielsweise der Fall, wenn dies mit unverhältnismäßig hohen Kosten verbunden wäre.[25]

D. Herausforderungen und Unsicherheiten im Umgang mit der EU

I. Status der Angemessenheitsentscheidung der EU-Kommission

Mit Mitteilung vom 9. Januar 2018 hat die EU-Kommission verkündet, dass das Vereinigte Königreich ab dem 3. März 2019 – soweit es kein anderes Austrittsdatum geben soll – als Drittland zu bewerten sei.[26] Deshalb hat die EU-Kommission am 28.06.2021 einen Angemessenheitsbeschluss für das Vereinigte Königreich genehmigt. Darin bestätigt sie, dass die UK ein im Wesentlichen der DSGVO entsprechendes Datenschutzniveau hat. Dies ermöglicht, dass – abgesehen von einigen wenigen Ausnahmen – personenbezogene Daten wie zuvor frei zwischen dem Vereinigten Königreich und den EU-Mitgliedstaaten ausgetauscht werden können.[27]

23 https://dma.org.uk/article/dua-vs-dpdi-spot-the-difference#:~:text=The%20DUA%20Bill%20builds%20on,enhances%20market%20competition%20and%20innovation, letzter Zugriff am 17.12.2024.
24 https://dma.org.uk/article/dua-vs-dpdi-spot-the-difference#:~:text=The%20DUA%20Bill%20builds%20on,enhances%20market%20competition%20and%20innovation, letzter Zugriff am 17.12.2024.
25 https://dma.org.uk/article/dua-vs-dpdi-spot-the-difference#:~:text=The%20DUA%20Bill%20builds%20on,enhances%20market%20competition%20and%20innovation, letzter Zugriff am 17.12.2024.
26 Hoeren, MMR 2018, 53, 53.
27 https://ico.org.uk/for-organisations/data-protection-and-the-eu/overview-data-protection-and-the-eu/, letzter Zugriff am 27.11.2024.

Zuvor hatte das Europäische Parlament jedoch Bedenken kundgetan. Diese bezogen sich insbesondere auf die umfangreiche Sammlung von personenbezogenen Daten durch den britischen Geheimdienst. Die Kommission hielt dem entgegen, dass aufgrund von Klagemöglichkeiten und unabhängigen Kontrollstellen ein hinreichender Schutz garantiert sei.[28]

II. Auswirkungen auf den Datentransfer zwischen dem Vereinigten Königreich und der EU

Für Übertragungen im Rahmen des Angemessenheitsbeschlusses gelten spezifische Bedingungen. Erstens muss das Vereinigte Königreich sein Datenschutzniveau weiterhin aufrechterhalten, was regelmäßig von der Europäischen Kommission überprüft wird. Sollte das Vereinigte Königreich seine Datenschutzgesetze in einer Weise ändern, die das Schutzniveau senkt – wie gegebenenfalls durch eine baldige Datenschutzreform – kann der Angemessenheitsbeschluss widerrufen, ausgesetzt oder eingeschränkt werden. Zweitens bleibt der Angemessenheitsbeschluss befristet und ist zunächst auf vier Jahre, also bis zum 27. Juni 2025, ausgelegt. Eine Verlängerung ist möglich, falls das Datenschutzniveau im Vereinigten Königreich weiterhin als angemessen erachtet wird.[29]

Zusätzlich unterliegt die Übertragung personenbezogener Daten zwischen der EU und dem Vereinigten Königreich besonderen Datenschutzvorkehrungen im Bereich der nationalen Sicherheit und Strafverfolgung. Der Angemessenheitsbeschluss enthält Schutzmechanismen, um sicherzustellen, dass die Daten von EU-Bürgern vor unrechtmäßiger staatlicher Überwachung oder unzureichenden Schutzmaßnahmen geschützt sind. Zudem ist die grenzüberschreitende Datenübertragung zum Zwecke der Immigrationskontrolle nicht vom Angemessenheitsbeschluss umfasst.[30]

III. Rechtliche und wirtschaftliche Risiken für Unternehmen und Privatpersonen

Solange der Angemessenheitsbeschluss noch Gültigkeit hat, kann ein internationaler Datenverkehr weiterhin unter vereinfachten Bedingungen erfolgen. Sobald allerdings die ersten von Großbritannien geplanten Änderungen des Datenschutzrechts erfolgen werden, besteht die Gefahr, dass die EU-Kommission den Beschluss widerruft. Dann müssten Unternehmen erweiterte Vorsichtsmaßnahmen treffen. Für Unternehmen

28 ZD-Aktuell 2021, 05280.
29 Heermann, ZD-Aktuell 2022, 01254.
30 https://ico.org.uk/for-organisations/data-protection-and-the-eu/overview-data-protection-and-the-eu/, letzter Zugriff am 27.11.2024.

mit Niederlassungen im Vereinigten Königreich oder auf diesen Markt ausgerichteten Dienstleistungen oder Geschäftspartnern mit dortigem Sitz bedeutet dies, dass sie gegebenenfalls bereits vereinbarte Verträge aktualisieren müssen. Andererseits müssen Unternehmen, die Kunden in der EU ansprechen, aufgrund des Marktortprinzips weiterhin die DSGVO beachten.[31]

Der durch den Angemessenheitsbeschluss ermöglichte freie Datenfluss wäre beendet. Dies hätte für Unternehmen die Folge, dass sie plötzlich gezwungen wären, alternative Maßnahmen wie Standardvertragsklauseln (SCCs) oder verbindliche Unternehmensrichtlinien (Binding Corporate Rules) zu implementieren, um weiterhin Daten in das Vereinigte Königreich rechtmäßig übertragen zu können. Dieser Prozess ist oft zeit- und kostenintensiv und birgt das Risiko, dass Unternehmen zeitweilig keine rechtlich abgesicherte Grundlage für die Datenübermittlung haben. Dies könnte insbesondere kleine und mittelständische Unternehmen finanziell belasten. Darüber hinaus kann ein plötzlicher Widerruf des Beschlusses zu Unterbrechungen in datenintensiven Geschäftsprozessen und zur Verlangsamung des internationalen Handels führen, was wiederum wirtschaftliche Verluste zur Folge haben könnte. Besonders belastend könnte sich das auf Unternehmen im Bereich von FinTech und E-Commerce auswirken. Für Organisationen, die es nicht schaffen, eine Lösung für die komplexere Datenschutzsituation zu finden, drohen empfindliche Geldbußen und Sanktionen sowohl durch die europäischen Aufsichtsbehörden als auch durch das ICO.

Für Privatpersonen liegt das größte Risiko bei einer Absenkung des Datenschutzstandards in einer erhöhten Gefahr für Datenschutzvorfälle und Datenmissbrauch bei oder durch privatrechtliche Unternehmen und in einer erhöhten Gefahr der staatlichen Überwachung im Vereinigten Königreich. Sollte es zu einer zu starken Aufweichung des Datenschutzniveaus kommen, besteht die Gefahr, dass personenbezogene Daten von EU-Bürgern schlechter vor unbefugten Zugriffen durch staatliche oder private Organisationen geschützt sind.

E. Einfluss des Brexits auf die internationale Datenschutzposition Großbritanniens

I. Großbritanniens Bestrebungen zur Schaffung von Datenschutzabkommen

Das Vereinigte Königreich hat verschiedene Datenschutzabkommen mit Ländern außerhalb der EU abgeschlossen oder in Planung, um den internationalen Datenfluss zu erleichtern. Die Angemessenheitsentscheidungen beruhen ähnlich wie die der EU auf einer Bewertung, ob das Datenschutzniveau in diesen Ländern mit dem des Vereinigten Königreichs kompatibel ist, und ermöglichen einen freien Datentransfer.[32]

Neben den EU-Mitgliedstaaten bestehen solche Abkommen auch zu den weiteren Ländern des Europäischen Wirtschaftsraums (EEA), also zu Norwegen, Irland und Liechtenstein.[33] Daneben existieren auch Datenschutzabkommen mit den Ländern, für die auch die EU-Kommission einen Angemessenheitsbeschluss erlassen hat.[34]

Zudem arbeitet das Vereinigte Königreich laut eigener Aussage daran, Datenschutzvereinbarungen mit weiteren Ländern, wie etwa Australien, Singapur, Kolumbien und Indien, zu etablieren[35]. Schon die Vereinbarung mit Südkorea von November 2022 zeigt, dass das Vereinigte Königreich bei der Schaffung neuer internationaler Abkommen einen flexibleren Ansatz verfolgt als die EU[36]. So sollen die wirtschaftlichen Vorteile von internationalen Datenflüssen besser ausgeschöpft werden. Dies könnte dazu führen, dass Großbritannien Abkommen mit Ländern schließt, deren Datenschutzniveau von den EU-Standards abweicht, was sich langfristig negativ auf die Angemessenheitsentscheidung der EU auswirken könnte.

II. Das Potenzial für internationale Partnerschaften

Die Anpassung des britischen Datenschutzrechts durch aktuelle Gesetzesentwürfe könnte zu einer deutlichen Änderung der Gesetzeslage führen. Möglicherweise würde dann eine erneute Prüfung des Angemessenheitsbeschlusses zu einer Ablehnung eines vergleichbar hohen Schutzniveaus führen. Sollte in den kommenden Jahren die EU-Kommission deshalb diesen Status aberkennen, könnte dies zur Stärkung der wirtschaftlichen Beziehungen mit anderen Ländern führen. Die britische Datenschutzlinie zeigt bereits jetzt im inter-

31 Heermann, ZD-Aktuell 2022, 01254

32 https://www.gov.uk/government/publications/uk-approach-to-international-data-transfers/international-data-transfers-building-trust-delivering-growth-and-firing-up-innovation, letzter Zugriff am 10.12.2024.

33 https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-transfers-a-guide/, letzter Zugriff am 10.12.2024.

34 https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-transfers-a-guide/, letzter Zugriff am 10.12.2024.

35 https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-transfers-a-guide/, letzter Zugriff am 10.12.2024.

36 https://www.gov.uk/government/news/uk-finalises-landmark-data-decision-with-south-korea-to-help-unlock-millions-in-economic-growth, letzter Zugriff am 10.12.2024.

nationalen Kontext im Vergleich zur EU einen deutlich flexibleren Ansatz.

Insofern besteht die Möglichkeit, dass sich international agierende Unternehmen in der Zukunft vermehrt an das Vereinigte Königreich statt an Organisationen mit Sitz in der EU wenden. Gerade in Anbetracht eines möglichen Datenschutzabkommens mit den Vereinigten Staaten von Amerika könnte dies ein enormer Vorteil sein. Die Europäische Kommission versucht seit Jahren einen erfolgreichen Angemessenheitsbeschluss für die USA zu verabschieden. Bislang ist der letzte Anstoß im Rahmen des EU-US-Datenschutzrahmens noch gültig. Allerdings besteht die Möglichkeit, dass der EuGH ihn, genau wie seine Vorgänger, für ungültig erklärt. Eine Absenkung des britischen Datenschutzniveaus könnte deshalb die Vereinbarung eines entsprechenden Abkommens erleichtern. Langfristig könnte dies auf wirtschaftlicher Ebene zu einer Abkehr US-amerikanischer Unternehmen von der EU hin zu britischen Vertragspartnern führen.

III. Rolle des Vereinigten Königreichs im globalen Datenschutzkontext

Das Vereinigte Königreich spielt im globalen Datenschutzkontext eine doppelte Rolle: Einerseits orientiert es sich zumindest bislang weiterhin an den strengen Standards der DSGVO (UK GDPR), um internationale Datenübertragungen zu erleichtern und wettbewerbsfähig zu bleiben. Andererseits verfolgt das Land zunehmend eigene Ansätze, die das Datenschutzrecht flexibler an die Bedürfnisse von Wirtschaft und Innovation anpassen sollen. Ein besonderes Augenmerk ist in diesem Zusammenhang auf die geplante Datenschutzreform zu legen. Diese Balance zwischen der Aufrechterhaltung eines hohen Datenschutzniveaus und der Schaffung eines unternehmensfreundlichen Regulierungsumfelds positioniert das Vereinigte Königreich als potenziellen Vermittler zwischen unterschiedlichen Datenschutzregimen, wie denen der EU, der USA und anderer großer Wirtschaftsblöcke. Allerdings birgt diese Strategie Risiken, insbesondere im Hinblick auf die zukünftige Anerkennung des Datenschutzniveaus durch internationale Partner.

IV. Politische und rechtliche Entwicklungen seit dem Brexit

a. Änderungen und Erweiterungen der Datenschutzgesetzgebung seit 2020

Die geplanten Änderungen deuten darauf hin, dass Großbritannien zukünftig neben dem Schutz personenbezogener Daten auch wirtschaftliche Interessen berücksichtigen möchte.[37] Das deutet auf eine Entwicklung vom „Datenschutzrecht" zum „Datenrecht" hin, das insbesondere auch finanzielle Aspekte an der Nutzung solcher Daten beachten möchte. Insofern findet eine Annäherung zu Grundsätzen der US-amerikanischen Einstellung zum Thema Datenschutz statt.[38]

b. Die Rolle der britischen Datenschutzbehörde ICO (Information Commissioner's Office)

Die Datenschutzreform enthält auch Anpassungen zur Rolle der britischen Datenschutzbehörde. Geplant ist, die Rolle des ICO zu modernisieren, um zu gewährleisten, dass es effektiv gegen Datenschutzverstöße vorgehen kann.[39] Hierzu soll insbesondere eine Änderung der Befugnisse stattfinden.[40] Zudem hat das ICO erst kürzlich ein Audit Framework gestartet, das Unternehmen als Werkzeug zur Überprüfung der Befolgung der datenschutzrechtlichen Vorgaben helfen soll.[41]

c. Neue politische Agenden und ihre möglichen Auswirkungen auf den Datenschutz

Die britische Regierung verfolgt nach dem Brexit eine datenschutzpolitische Agenda, die auf mehr Flexibilität und wirtschaftlicher Wettbewerbsfähigkeit basiert. Ein zentrales Ziel ist es, internationale Datenflüsse durch flexiblere Angemessenheitsentscheidungen zu fördern. Gleichzeitig könnten diese neuen Ansätze potenziell Konflikte mit der EU hervorrufen, wenn die britischen Datenschutzstandards als unzureichend angesehen werden. Solche Spannungen könnten die bestehende Angemessenheitsentscheidung der EU für das Vereinigte Königreich gefährden, was wirtschaftliche und rechtliche Unsicherheiten für Unternehmen zur Folge hätte.

37 Etteldorf, ZD-Aktuell 2023, 01131.
38 Etteldorf, ZD-Aktuell 2023, 01131.
39 The Queen's Speech 2022, S. 57, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1074113/Lobby_Pack_10_May_2022.pdf, letzter Zugriff am 27.11.2024.
40 ZD-Aktuell 2022, 01171.
41 https://ico.org.uk/for-organisations/advice-and-services/audits/data-protection-audit-framework/, letzter Zugriff am 27.11.2024.

V. Praxisbeispiele: Unternehmen und die Realität des Datenschutzes in Großbritannien

I. Datenschutz-Compliance und Herausforderungen für britische Unternehmen

Da bislang noch keine wesentlichen Änderungen des Datenschutzrechts vorgenommen wurden, hält sich der organisatorische Anpassungsaufwand für britische Unternehmen noch in Grenzen. Praktische Probleme zeigen sich wie auch in EU-Mitgliedstaaten regelmäßig bei der Umsetzung von Maßnahmen zur Gewährleistung der Datensicherheit und der Wahrung von Betroffenenrechten. Beispielsweise fällt es kleinen und mittleren Unternehmen häufig schwer, mit der Komplexität der gesetzlichen Vorgaben Schritt zu halten. Zudem müssen Unternehmen, die neue Technologien wie Künstliche Intelligenz einsetzen, auch hierbei stets die Befolgung des Datenschutzes sicherstellen. In Zukunft könnte sich für britische Unternehmen im Vergleich zu solchen mit Sitz in der EU insofern ein Vorteil ergeben, dass diese die Vorgaben der EU-Verordnung für Künstliche Intelligenz nicht befolgen müssen. In Anbetracht aktueller Gesetzesvorhaben und einer erhöhten Flexibilität Großbritanniens bei Angemessenheitsentscheidungen besteht allerdings ein Spannungsfeld mit EU-Vorgaben. Unternehmen müssen darauf vorbereitet sein, ihre Compliance-Strategien anzupassen, falls es zu Änderungen der Datenschutzbeziehungen zwischen der EU und Großbritannien kommt.

Praxisprobleme ließen sich in letzter Zeit vermehrt in Bezug auf Verstöße im Bereich des Direktmarketings feststellen. So hat das ICO in den letzten Monaten eine Vielzahl von Bußgeldern gegen Unternehmen erlassen. Zum Beispiel verhängte die Datenschutzbehörde am 12. Dezember 2024 ein Bußgeld in Höhe von 170.000 Pfund gegen Breathe Services Ltd und 120.000 Pfund gegen Money Bubble Ltd. Gegenstand des Vorwurfs sind ordnungswidrige Spam-Anrufe, die, ohne dass eine vorliegende Einwilligung bewiesen werden konnte, durchgeführt wurden.[42]

II. Datenschutz in Start-ups und KMUs

Der Datenschutz stellt für britische Start-ups, kleine und mittlere Unternehmen (KMUs) ebenso wie in Mitgliedstaaten der EU eine Herausforderung dar. Die Einhaltung des britischen Datenschutzrechts erfordert oft beträchtliche Ressourcen, die in kleineren Unternehmen begrenzt sind. Besonders gravierend können Datenschutzverstöße sein, die in hohen Bußgeldern enden, da sie gerade KMUs mit wenig Gewinn und hohem Umsatz besonders stark treffen können. Gerade wenn Start-ups schnell wachsen, kann eine Herausforderung darin liegen, auch mit der wachsenden Menge an personenbezogenen Daten weiterhin verantwortungsvoll umzugehen.

Dabei müssen insbesondere Sicherheitsmaßnahmen etabliert werden, um den Schutz personenbezogener Daten zu gewährleisten.[43] Beschwerden über KMUs gehen am häufigsten ein über unzureichende Auskünfte, Sicherheitsmängel, fehlerhafte Daten, Datenweitergabe, rechtswidrige Marketingpraktiken, Überschreitung der Speicherfristen und die Missachtung der Zweckbindung.[44]

Organisationen müssen beachten, dass es sich bei Datenschutz nicht um eine einmalig zu erledigende Aufgabe handelt.[45] Vielmehr müssen Unternehmen dauerhaft die Einhaltung der Sicherheitsstandards überprüfen und gegebenenfalls nachbessern. Zudem fällt eine Vielzahl der Bußgelder gegenüber KMUs aufgrund von Verstößen im Bereich des Direktmarketings an.[46] In diesem Zusammenhang muss besonders darauf geachtet werden, neben allgemeinem Datenschutz auch besondere Vorschriften wie „Privacy Electronic Communications Regulations" zu beachten.[47] Diese regeln den Schutz der Privatsphäre in der elektronischen Kommunikation, insbesondere bei Cookies, Online-Tracking, elektronischer Werbung und Telemarketing.

Zudem müssen Unternehmen auch Gebühren (so genannte „data protection fees") an die Datenschutzbehörde zahlen, falls keine entsprechende Ausnahme greift. Dies gilt auch für KMUs, die darauf achten sollten, dass diese Zahlung regelmäßig wiederholt werden muss.[48] Die Gebühr beschränkt sich jedoch für Unternehmen mit bis zu 250 Mitarbeitern oder einem jähr-

42 https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/12/rogue-companies-receive-fines-totalling-290k-for-making-millions-of-nuisance-calls/, letzter Zugriff am 23.12.2024.

43 https://ico.org.uk/for-organisations/advice-for-small-organisations/whats-new/blogs/data-protection-fines-why-they-happen-and-how-to-avoid-them/; letzter Zugriff am 31.12.2024.

44 https://ico.org.uk/for-organisations/advice-for-small-organisations/frequently-asked-questions/getting-started-with-data-protection/#receivescomplaint, letzter Zugriff am 31.12.2024.

45 https://ico.org.uk/for-organisations/advice-for-small-organisations/whats-new/blogs/data-protection-fines-why-they-happen-and-how-to-avoid-them/, letzter Zugriff am 31.12.2024.

46 https://ico.org.uk/for-organisations/advice-for-small-organisations/whats-new/blogs/data-protection-fines-why-they-happen-and-how-to-avoid-them/, letzter Zugriff am 31.12.2024.

47 https://ico.org.uk/for-organisations/advice-for-small-organisations/whats-new/blogs/data-protection-fines-why-they-happen-and-how-to-avoid-them/; letzter Aufruf 31.12.2024.

48 https://ico.org.uk/for-organisations/advice-for-small-organisations/whats-new/blogs/data-protection-fines-why-they-happen-and-how-to-avoid-them/, letzter Zugriff am 31.12.2024.

lichen Umsatz von bis zu 36 Millionen Pfund auf 40 oder 60 Pfund jährlich.[49]

VI. Fazit

Der Datenschutz in Großbritannien steht vor einer spannenden und herausfordernden Zukunft, insbesondere nach dem Brexit. Die regulatorischen Anpassungen zeigen, dass das Land einerseits seine Verpflichtungen gegenüber der DSGVO aufrechterhalten möchte, andererseits jedoch zunehmend auf Flexibilität und Eigenständigkeit setzt, etwa durch die geplante Datenschutzreform. Die Balance zwischen wirtschaftlicher Innovationsförderung und dem Schutz individueller Rechte bleibt eine zentrale Herausforderung.

Im Vergleich zu den untersuchten Ländern dieser Beitragsreihe Südamerika, Asien und Afrika weist Großbritannien ein deutlich gereifteres Datenschutzregime auf, geprägt von europäischer Rechtstradition und einem hohen Schutzniveau. Während Südamerika, etwa mit Brasilien und seiner „Lei Geral de Proteção de Dados“ (LGPD), ähnliche Fortschritte macht, sind manche asiatische und afrikanische Länder stärker durch länderspezifische Faktoren wie begrenzte Ressourcen, fehlende Regulierung oder technologische Abhängigkeit geprägt. Großbritannien hebt sich durch seine rechtliche Stabilität und institutionellen Kapazitäten ab, doch seine globalen Ambitionen im Datenschutz müssen sich in einem Umfeld behaupten, das zunehmend von geopolitischen und technologischen Dynamiken geprägt ist.

Ein kritischer Ausblick zeigt, dass Großbritannien Gefahr laufen könnte, durch eigenständige Datenschutzgesetze von der EU-Datenschutzlandschaft abzuweichen. Dies könnte die Beziehungen zu Handelspartnern erschweren, insbesondere, wenn die EU die Angemessenheitsentscheidung über Großbritannien in Frage stellt. Ebenso birgt die stärkere Fokussierung auf Innovation, wie in der DUA Bill vorgesehen, das Risiko, Datenschutzrechte zugunsten wirtschaftlicher Interessen zu verwässern.

Langfristig wird sich zeigen, ob Großbritannien in der Lage ist, Datenschutzstandards zu setzen, die sowohl wirtschaftliche Interessen fördern als auch den Schutz der Bürgerrechte bewahren. Die Gefahr besteht, dass ein zu flexibles Datenschutzregime zu Unsicherheiten führt und das Vertrauen der Bürger sowie internationaler Partner mindert. Nur durch eine ausgewogene Strategie, die sowohl technologischen Fortschritt als auch Grundrechte berücksichtigt, kann das Land seine Rolle als Vorreiter im Datenschutz behaupten.

49 https://ico.org.uk/for-organisations/advice-for-small-organisations/frequently-asked-questions/getting-started-with-data-protection/#receivescomplaint, letzter Zugriff am 31.12.2024.

Rechtsanwalt **Dr. Kinast** ist Gründer und geschäftsführender Gesellschafter von KINAST Rechtsanwälte. Er ist Externer Datenschutzbeauftragter zahlreicher nationaler und internationaler Großkonzerne, Banken und Versicherungen sowie Organisationen der Kirche und öffentlichen Hand. Weiterhin berät Herr Dr. Kinast als Externer Compliancebeauftragter diverse Unternehmen der verschiedensten Branchen.

Wettbewerbsvorteile.

Outsourcing
Ökonomische Hintergründe, Einsatzfelder, Rechtsfragen und Gestaltungshinweise

von Dr. Jürgen Niebling, Rechtsanwalt, und Dipl.-Jurist Univ. Julius Rübartsch, Wiss. Mitarbeiter

2025, 5., überarbeitete Auflage, 106 Seiten, € 19,–

Das Recht der Wirtschaft

ISBN 978-3-415-07709-6

BOORBERG
RICHARD BOORBERG VERLAG
BESTELLUNG@BOORBERG.DE TEL 0711/7385-343 FAX 0711/7385-100

SC0525