

In Kooperation mit:
 bitkom e.V.
 BvD e.V.
 davit im DAV
 eco e.V.
 VPRT e.V.

ZEITSCHRIFT FÜR DATENSCHUTZ

ZD

Herausgeber: RA Prof. Dr. Jochen Schneider · Prof. Dr. Thomas Hoeren · Prof. Dr. Martin Selmayr · RA Dr. Axel Spies · RA Tim Wybitul

AUS DEM INHALT

- | | | |
|-----------------------------|------------|--|
| Datenschutzalltag | 101 | JYN SCHULTZE-MELLING
Ist die Ruhe nach dem Sturm nur die Ruhe vor dem Sturm? |
| Wirtschaftsauskunftei | 103 | RALF B. ABEL
Einmeldung und Auskunfteittigkeit nach DS-GVO und § 31 BDSG |
| „social watchdogs“ | 108 | KAI ENGELBRECHT
Informationsfreiheit zwischen Europischer Menschenrechtskonvention und Grundgesetz |
| Auskunftsrecht | 113 | EuGH: Korrigierte Prfungsarbeiten stellen personenbezogene Daten dar |
| Verletzung der Privatsphre | 115 | EuGH: Verleumdung im Internet |
| Datenverarbeitung | 118 | KG: Datenschutzanforderungen des sog. „App-Zentrums“ von Facebook |
| Nachmeldung | 124 | LG Lubeck: Datenbermittlung an Auskunfteien bei Datennderung |
| Verschwiegenheitswahrung | 126 | BFH: Verpflichtung von Rechtsanwlten zur Abgabe der Zusammenfassenden Meldung zur Umsatzsteuer trotz Schweigepflicht |
| Beschftigtendatenschutz | 127 | BAG: Zulssigkeit von berwachungsmanahmen durch Arbeitgeber |
| Sensible Daten | 134 | OVG Saarlouis: Videoberwachung in einer Apotheke |

www.zd-beck.de

Seiten 101–148
 8. Jahrgang 1. Mrz 2018
 Verlag C.H.BECK Mnchen

3/2018



In Kooperation mit:

bitkom - Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.

BvD - Berufsverband der Datenschutzbeauftragten Deutschlands e.V.

davit im DAV - Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein

eco - Verband der Internetwirtschaft e.V.

VPRT - Verband Privater Rundfunk und Telemedien e.V.



ZEITSCHRIFT FÜR DATENSCHUTZ

INHALT

3/2018 Seiten 101–148

	Editorial
Datenschutzalltag	101 JYN SCHULTZE-MELLING Ist die Ruhe nach dem Sturm nur die Ruhe vor dem Sturm?
	Beiträge
Wirtschaftsauskunftei	103 RALF B. ABEL Einmeldung und Auskunftstätigkeit nach DS-GVO und § 31 BDSG. Frage der Rechtssicherheit im neuen Recht
„social watchdogs“	108 KAI ENGELBRECHT Informationsfreiheit zwischen Europäischer Menschenrechtskonvention und Grundgesetz. Bedeutung der EGMR-Entscheidung in der Rs. Magyar Helsinki Bizottság für das deutsche Recht
	Rechtsprechung
Auskunftsrecht	113 EuGH: Korrigierte Prüfungsarbeiten stellen personenbezogene Daten dar Urteil vom 20.12.2017 – C-434/16 – Nowak/Data Protection Commissioner
Verletzung der Privatsphäre	115 EuGH: Verleumdung im Internet Urteil vom 17.10.2017 – C-194/16 – Bolagsupplysningen und Ilsjan
Datenverarbeitung	118 KG: Datenschutzerfordernissen des sog. „App-Zentrums“ von Facebook Urteil vom 22.9.2017 – 5 U 155/14
Behandlungsvertrag	123 OLG Hamm: Voraussetzung für eine Auskunft über behandelnde Klinikärzte Urteil vom 14.7.2017 – 26 U 117/16
Geschwindigkeitsüberwachung	123 LG Trier: Einsichtnahme in Messunterlagen einer Geschwindigkeitsmessanlage Beschluss vom 14.9.2017 – 1 Qs 46/17
Nachmeldung	124 LG Lübeck: Datenübermittlung an Auskunfteien bei nachträglicher Datenänderung Urteil vom 23.5.2017 – 3 O 325/15
Verschwiegenheitswahrung	126 BFH: Verpflichtung von Rechtsanwälten zur Abgabe der zusammenfassenden Meldung zur Umsatzsteuer trotz Schweigepflicht Urteil vom 27.9.2017 – XI R 15/15
Beschäftigtendatenschutz	127 BAG: Zulässigkeit von Überwachungsmaßnahmen durch Arbeitgeber Urteil vom 29.6.2017 – 2 AZR 597/16
Einsichtsrecht	129 LAG Hamm: Keine Anonymisierung der Bruttolohn-Listen nach § 80 BetrVG Beschluss vom 19.9.2017 – 7 TaBV 43/17

E-Mail-Adressen	131 LSG München: Anspruch auf Bekanntgabe von Kontaktdaten eines Sachbearbeiters Beschluss vom 11.9.2017 – L 7 AS 531/17 B ER
Informationsfreiheit	132 VerfGH Rheinland-Pfalz: Einschränkungen und Umfang des Zugangs zu amtlichen Informationen Beschluss vom 27.10.2017 – VGH B 37/16
Sensible Daten	134 OVG Saarlouis: Videoüberwachung in einer Apotheke Urteil vom 14.12.2017 – 2 A 662/17
Personenbezogene Daten	137 VGH München: Umfang der Auskunftspflicht nach Art. 10 BayDSG Beschluss vom 29.8.2017 – 5 ZB 16.2227
Geheimhaltungsschutz	139 OVG NRW: Öffentliche Belange nach § 3 Nr. 4 IFG Urteil vom 5.5.2017 – 15 A 1578/15
Geheimhaltung	141 VG Gelsenkirchen: Umfang des presserechtlichen Auskunftsanspruchs Beschluss vom 17.11.2017 – 17 L 2935/17
Löschung von Daten	143 VG Kassel: Befugnis zur Speicherung personenbezogener Daten durch Verfassungsschutzbehörde Urteil vom 19.9.2017 – 4 K 641/13.KS
Meta-Daten	144 VG Wiesbaden: Aktenvorlage an das Gericht bei elektronischen Akten Urteil vom 9.8.2017 – 6 K 808/17.WI.A
Internetblog	146 VG Berlin: Auskunftsanspruch für Telemedien mit journalistisch-redaktionellem Angebot Beschluss vom 23.6.2017 – VG 27 L 295.17
Patientendaten	148 LAG Baden-Württemberg: Kündigung wegen Verletzung der Verschwiegenheitsverpflichtung Urteil vom 11.11.2016 – 12 Sa 22/16 (Ls.)

III-IV Inhalt

V-XX ZD-Fokus

XX Impressum

Beilagenhinweis

Mit dieser Ausgabe verbreiten wir Beilagen von:

Verlag C.H.BECK oHG, München

Erich Schmidt Verlag GmbH & Co. KG, Berlin

Wir bitten unsere Leser um Beachtung!

<p>Sponsoren:</p>  <p>Kooperationspartner:</p>   <p>Medienpartner:</p>  	 <p>Fachtagungen</p> <p>Bildung • Fortbildung • Wissenschaft</p> <hr/> <p>Die Tagungsreihe zum Datenschutz</p> <p>Fachtagungen 2018 im hessischen Ministerium der Justiz in Wiesbaden:</p> <p>14.3.2018 „Datenschutz und Datensicherheit - Update 2018“</p> <p>21.3.18 „Datenschutz in Kliniken - Update 2018“</p> <p>22.3.18 „Datenschutz in der Medizin - Update 2018“</p> <p>Weitere Details und Anmeldung unter:</p> <p>www.esturias.de</p>	<p>Auszug der Referenten:</p> <ul style="list-style-type: none"> - Dr. Stefan Brink, Landesbeauftragter für den Datenschutz Baden-Württemberg - Sonja Wirtz, stellvertretende Leiterin des Bereichs Proaktiver Datenschutz beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz - Dr. Uwe K. Schneider, Fachanwalt für Medizinrecht und Lehrbeauftragter für Rechtsfragen der medizinischen Informatik an der Hochschule Heilbronn - Andreas Sachs, Referatsleiter IT-Sicherheit und technischer Datenschutz beim Bayerischen Landesamt für Datenschutzaufsicht - Markus Holzbrecher-Morys, Leiter der Arbeitsgruppe „Krankenhausinformationstechnik“ der DKG und stellvertretender Geschäftsführer des Dezernats „IT, Datenaustausch und eHealth“ - Thomas Mithlein, Vorstand GDD, Geschäftsführer der DMC Datenschutz Management & Consulting GmbH & Co. KG
--	---	--

Herausgeber:

Prof. Dr. Thomas Hoeren, Direktor des Instituts für Informations-, Telekommunikations- und Medienrecht (ITM), Universität Münster – RA Prof. Dr. Jochen Schneider, Kanzlei SSW Schneider Schiffer Weihermüller, München – Prof. Dr. Martin Selmayr, Kabinettschef von Jean-Claude Juncker, Präsident der Europäischen Kommission, Brüssel/Direktor des Centrums für Europarecht, Universität Passau – RA Dr. Axel Spies, Morgan, Lewis & Bockius LLP, Washington, D.C./Frankfurt/M. – RA Tim Wybitul, FA Arbeitsrecht, Partner, Head of Compliance & Investigations Hogan Lovells, Frankfurt/M.

Wissenschaftsbeirat:

RAin Dr. Astrid Auer-Reinsdorff, FA IT-Recht, Berlin/Lissabon/Vorsitzende des Geschäftsführenden Ausschusses der Arbeitsgemeinschaft IT-Recht im DAV (davit) – Daniela Beaujean, Mitglied der Geschäftsleitung Recht und Regulierung/Justiziarin, Verband Privater Rundfunk und Telemedien e.V. (VPRT), Berlin – Dr. Stefan Brink, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Stuttgart – RAin Isabell Conrad, Kanzlei SSW Schneider Schiffer Weihermüller, München – RAin Susanne Dehmel, Mitglied der Geschäftsleitung Bitkom e.V., Berlin – Dr. Oliver Draf, LL.M., Leiter Datenschutz der Allianz Deutschland AG, München – RA Dr. Jens Eckhardt, FA IT-Recht, Düsseldorf/Vorstand (Recht) des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V. – Dr. Eugen Ehmann, Regierungsvizepräsident von Mittelfranken, Ansbach – RAin Prof. Dr. Sibylle Gierschmann, LL.M., Partnerin Kanzlei Taylor Wessing, München/Co-Leiterin Fachausschuss Datenschutz der Deutschen Gesellschaft für Recht und Informatik e.V. (DGRI) – RA Dr. Stefan Hanloser, München – Prof. Dr. Gerrit Hornung, LL.M., Inhaber des Lehrstuhls für Öffentliches Recht, IT-Recht und Umweltrecht, Universität Kassel – Prof. Dr. Jacob Joussem, Lehrstuhlinhaber für Bürgerliches Recht, Deutsches und Europäisches Arbeitsrecht und Sozialrecht, Ruhr-Universität Bochum – Thomas Kranig, Präsident des Bayerischen Landesamtes für Datenschutzaufsicht, Ansbach – RA Dr. Sebastian Kraska, externer Datenschutzbeauftragter, IITR GmbH, München – Prof. Dr. Thomas Petri, Der Bayerische Landesbeauftragte für den Datenschutz, München – Prof. Dr. Andreas Popp, M.A., Inhaber des Lehrstuhls für Deutsches und Europäisches Straf- und Strafprozessrecht, FB Rechtswissenschaft, Universität Konstanz – Prof. Dr. Alexander Roßnagel, Universitätsprofessor für Öffentliches Recht, Universität Kassel/Leiter der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) – RA Dr. Christian Schröder, Partner und Leiter des Fachbereichs IP/IT & Data Protection Practice Group in der Kanzlei ORRICK, HERRINGTON & SUTCLIFFE LLP, Düsseldorf – RA Dr. Jyn Schultze-Melling, LL.M., Executive Director Law, Ernst & Young Law GmbH, Berlin – Prof. Paul M. Schwartz, Professor der Rechtswissenschaft an der University of California – Berkeley Law School/Direktor des Berkeley Center for Law & Technology, USA – RA Thorsten Sörup, Aderhold Rechtsanwaltsgesellschaft mbH, Frankfurt/M. – Prof. Dr. Jürgen Taeger, Lehrstuhlinhaber für Bürgerliches Recht, Handels- und Wirtschaftsrecht sowie Rechtsinformatik, Universität Oldenburg/Vorsitzender der Deutschen Stiftung für Recht und Informatik (DSRI) – RA Florian Thoma, Senior Director, Global Data Privacy, Accenture AG, stv. Leiter des AK Datenschutz des Bitkom e.V. – Prof. Dr. Marie-Theres Tinnefeld, Professorin für Datenschutz und Wirtschaftsrecht, Hochschule München

Axel Spies USA: Repräsentantenhaus verlängert Spionagebefugnisse nach Sec. 702 FISA

ZD-Aktuell 2018, 05932

Das US-Repräsentantenhaus hat am 11.1.2018 nach einer hitzigen Debatte beschlossen, ein wichtiges außenpolitisches Überwachungsprogramm zu erneuern. Die Debatte war geprägt von teils widersprüchlichen Twitter-Botschaften von Präsident Trump über seine Unterstützung. Im Zusammenhang mit den Enthüllungen des Whistleblowers Edward Snowden ist die überwiegend geheime Tätigkeit des FISA-Gerichts einer breiten Öffentlichkeit bekannt geworden.

Die Erneuerung von Section 702 des Foreign Intelligence Surveillance Act (FISA), mit der die US-Sicherheitsbehörden (NSA u.a.) Informationen über Ziele im Ausland sammeln können, wurde mit 256 zu 164 Stimmen angenommen. Der Gesetzentwurf geht nun zur Abstimmung in den Senat, wo mit wenig Widerstand gerechnet wird. Das Gesetz ist auf sechs Jahre befristet.

Der Kongress hatte das Gesetz im Jahr 2008 mit einer automatischen Auslauffrist (Sunset Provision) in Kraft gesetzt, um ein ehemals geheimes Überwachungsprogramm zu legalisieren, das nach den Terroranschlägen vom 11. September geschaffen wurde. Seine Befürworter argumentieren, dass es ein wichtiges Werkzeug ist, um Terroranschläge zu verhindern. Der Gesetzentwurf, der vom Repräsentantenhaus angenommen wurde, erlaubt weiterhin den Zugriff auf eine Schlüsseldatenbank mit Suchbegriffen, um (auch) Informationen über Amerikaner abzufragen, allerdings nicht als direkte Ziele der Ermittlungen. Für die Durchführung der Kommunikation von Amerikanern gibt es wegen des Schutzes des 4. Verfassungszusatzes (4th Amendment) Rechtsschranken. Die Ermittler müssen einen hinreichenden Anhaltspunkt (probable cause) vor dem FISA-Gericht geltend machen, wenn sie den eigentlichen Inhalt dieser Kommunikationen sehen wollen.

Trump-Tweets stiften vor Abstimmung Verwirrung

Die Verwirrung vor der Abstimmung war groß, weil Präsident Trump in einem

Tweet am Morgen das FISA-Programm angriff – trotz der offiziellen Unterstützung seiner Regierung für die Verlängerung. Er behauptete, das FISA-Programm sei benutzt worden, um seinen Wahlkampf auf der Grundlage eines „falschen“ Trump-Dossiers „zu überwachen und [das Programm] zu missbrauchen.“ Trumps Widerstand hielt jedoch nicht lange an. Später am Morgen veröffentlichte er einen Folge-Tweet, in dem er klarstellte, dass er Änderungen am Gesetz anstrebe, und seine Unterstützung für das Überwachungsprogramm aussprach. Zuvor hatte das US-Repräsentantenhaus einen Alternativentwurf abgelehnt, der dem FBI strengere Beschränkungen auferlegt hätte. Am selben Tag stimmte das Repräsentantenhaus den alternativen FISA-Plan des libertären US-Abgeordneten Amash ab, der den Behörden weitergehende Spionage-Beschränkungen auferlegt hätte.

Auswirkungen in der EU?

Die Auswirkungen der Verlängerung auf den EU-US-Datenverkehr dürften sich in Grenzen halten. Seit Jahren ist FISA in der Kritik, weil in Brüssel und anderswo in der EU befürchtet wird, dass die US-Regierung Datenbanken von EU-Bürgern anlegt und diese im Ausland überwacht. Dies war auch ein Kritikpunkt bei der Einführung des EU-US-Privacy-Shield (s. Weichert, ZD 2016, 209; Molnár-Gábor/Kaffenberger, ZD 2017, 18, 23), den auch die EU-Kommission in ihren ersten jährlichen Bericht zum Privacy Shield vom 18.10.2017 ausdrücklich benannt hat, allerdings ohne der US-Regierung ernste Konsequenzen anzudrohen:

„Die bevorstehende Debatte über die Wiederzulassung von Section 702 des Foreign Intelligence Surveillance Act (FISA) bietet der US-Administration und dem Kongress eine einzigartige Gelegenheit zur Stärkung des Datenschutzes nach FISA. In diesem Zusammenhang hofft die Kommission, dass der Kongress in Erwägung ziehen wird, den Schutz, der von der Präsidentenrichtlinie (28) in Bezug auf Nicht-US-Personen in der FISA geboten wird, gesetzlich zu verankern, um die Stabilität und Kontinuität dieser Schutzmaßnahmen zu gewährleisten. Alle weiteren Reformen, sowohl in Bezug auf materielle Beschränkungen als auch in Bezug auf Verfahrensgarantien, sollten im Sinne von PPD-28 durchgeführt wer-

den und somit unabhängig von der Staatsangehörigkeit oder dem Wohnsitzstaat Schutz bieten.“

Auch wenn diese vagen Hoffnungen sich nunmehr zerschlagen haben, bringt die Verlängerung von Section 702 für die Bewertung nicht viel Neues. Die europäischen Geheimdienste profitieren indirekt von FISA für ihre Terroristenverfolgung zusammen mit den US-Behörden. Es bleibt abzuwarten, ob der *EuGH* bei einem Urteil zum Privacy Shield-Framework oder zu den EU-Standardvertragsklauseln auf die FISA-Verlängerung Bezug nimmt oder sie sogar als „casus belli“ einstuft, um die bestehenden transatlantischen Regeln für EU-rechtswidrig zu erklären.

■ Vgl. auch *Spies*, MMR 2007, Heft 10, XV; ZD-Aktuell 2015, 04668; *Spies*, ZD-Aktuell 2013, 03608; *ders.*, ZD-Aktuell 2012, 02957 und zum US-Patriot Act *Voigt/Klein*, ZD 2013, 16 ff.; ferner *Tinnefeld*, ZD-Aktuell 2013, 03164; zu Datentransfers *Schmitz/von Dall'Armi*, ZD 2016, 217; zum Privacy Shield *Weichert*, ZD 2016, 209 und *Smagon*, ZD 2016, 55.

Dr. Axel Spies

ist Rechtsanwalt in der Kanzlei Morgan Lewis & Bockius in Washington DC und Mitherausgeber der ZD.

Thomas Hoeren EU-Kommission: Entwurf einer VO über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der EU ZD-Aktuell 2018, 05930

Die *EU-Kommission* beschäftigt sich zurzeit nicht nur mit dem Datenschutz, sondern mit sonstigen rechtlichen Beschränkungen für nicht-personenbezogene Daten. Insbesondere will sie gegen Versuche einzelner Staaten vorgehen, solche Daten auf dem Gebiet des eigenen Nationalstaats verpflichtend vorrätig zu halten. Die *Kommission* plant daher zu dem Thema einen Verordnungsvorschlag (COM/2017/0495 final – 2017/0228 (COD)), auf Grund dessen zahlreiche territoriale Beschränkungen auch in Deutschland fallen.

Im Weiteren wird der Verordnungsvorschlag vorgestellt und anhand einzelner Regelungen problematisiert.

Aus dem Vorschlag COM/2017/0495 final – 2017/0228 (COD)

Artikel 6: Übertragung von Daten

1. Die *Kommission* fördert und erleichtert auf Unionsebene die Entwicklung von Verhaltensregeln für die Selbstregulierung, um Leitlinien für bewährte Verfahren zur Erleichterung des Anbieterwechsels aufzustellen und damit vor Abschluss eines Vertrags über die Datenspeicherung und -verarbeitung hinreichend ausführliche, eindeutige und transparente Informationen in Bezug auf folgende Fragen geben:

■ die Prozesse, technischen Anforderungen, Fristen und Entgelte, die für einen beruflichen Nutzer gelten, der zu einem anderen Anbieter wechseln oder Daten zurück in seine eigenen IT-Systeme übertragen möchte; dies umfasst auch die Prozesse und den Ort von Datensicherungen, die verfügbaren Datenformate und -träger, die erforderliche IT-Konfiguration und die Mindestnetzbandbreite, die Vorlaufzeit vor Beginn des Übertragungsprozesses und die Zeitspanne, in der die Daten für eine Übertragung verfügbar bleiben, sowie die Garantien für den Zugang zu den Daten im Falle der Insolvenz des Anbieters;

■ die betrieblichen Anforderungen für den Anbieterwechsel oder die Übertragung von Daten in einem strukturierten, gängigen und maschinenlesbaren Format, die dem Nutzer für den Wechsel oder die Übertragung der Daten genügend Zeit lassen.

2. Die *Kommission* hält die Anbieter dazu an, die in Absatz 1 genannten Verhaltensregeln innerhalb eines Jahres nach dem Beginn der Anwendung dieser Verordnung wirksam umzusetzen.

3. Die *Kommission* überprüft die Entwicklung und wirksame Anwendung solcher Verhaltensregeln und die tatsächliche Bereitstellung von Informationen seitens der Anbieter spätestens zwei Jahre nach dem Beginn der Anwendung dieser Verordnung.

Aus der Begründung des Vorschlags

Um dieses Potenzial freizusetzen, werden mit dem vorliegenden Vorschlag folgende Fragen angegangen:

■ die Verbesserung der grenzüberschreitenden Mobilität nicht-personenbezogener Daten im Binnenmarkt, die heute in vielen Mitgliedstaaten noch durch Lokalisierungsbeschränkungen

oder Rechtsunsicherheit auf den Märkten begrenzt ist;

■ die Gewährleistung, dass die Befugnisse der zuständigen Behörden, zu ordnungspolitischen Kontrollzwecken (wie Überprüfungen und Audits) Zugang zu Daten zu verlangen und zu erhalten, unberührt bleiben;

■ die Erleichterung des Anbieterwechsels und der Übertragung von Daten für die beruflichen Nutzer von Datenspeicherungs- oder sonstigen Datenverarbeitungsdiensten, ohne dadurch die Diensteanbieter übermäßig zu belasten oder die Marktbedingungen zu verfälschen.

Erläuterungen

1. Nationale Beschränkungen des öffentlichen Rechts: Artikel 4 legt den Grundsatz des freien Verkehrs nicht-personenbezogener Daten in der Union fest. Dieser Grundsatz verbietet jegliche Datenlokalisierungsaufgaben (DLA), es sei denn, diese sind aus Gründen der öffentlichen Sicherheit gerechtfertigt. Festgelegt werden ferner die Überprüfung bestehender Auflagen, die Mitteilung verbleibender oder neuer Auflagen an die *Kommission* sowie Transparenzmaßnahmen. Das richtet sich also gegen staatliche Sonderwege und hilft etwa tk-rechtlich bei Sonderauflagen, was die Daten im „Internet of Things“ angeht. Es dürfte allerdings unverhältnismäßig sein, alle anderen Gründe für den Erlass von Datenlokalisierungsaufgaben außer für „öffentliche Sicherheit“ per se für illegitim zu erklären. Damit würde den Mitgliedstaaten künftig eine Berufung auf alle anderen anerkannten Rechtfertigungsgründe (öffentliche Ordnung, Gesundheit oder andere zwingende Gründe des Allgemeinwohls) versagt werden.

Deutschland muss alle in deutschen Rechts- oder Verwaltungsvorschriften enthaltenen DLA innerhalb von 18 Monaten nach Veröffentlichung der Verordnung aufheben oder gegenüber der *Kommission* rechtfertigen. Überprüft werden müssen u.a. die steuer- und handelsrechtlichen Buchführungs- und Aufbewahrungspflichten, soweit sie die Datenspeicherung im Ausland an Bewilligungen oder Bedingungen knüpfen, wie etwa § 146 Abs. 2 AO, § 14b Abs. 2 UStG, § 41 Abs. 1 EStG und § 257 Abs. 1, 3 HGB.