Rat der
Europäischen Union

Brüssel, den 29. Januar 2018
(OR. en)

5702/18

DATAPROTECT 8
JAI 52
MI 53
DIGIT 8
DAPIX 11
FREMP 6
COMIX 30

ÜBERMITTLUNGSVERMERK

Absender:	Herr Jordi AYET PUIGARNAU, Direktor, im Auftrag des Generalsekretärs der Europäischen Kommission
Eingangsdatum:	26. Januar 2018
Empfänger:	Herr Jeppe TRANHOLM-MIKKELSEN, Generalsekretär des Rates der Europäischen Union
Nr. Komm.dok.:	COM(2018) 43 final
Betr.:	MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT Besserer Schutz und neue Chancen – Leitfaden der Kommission zur unmittelbaren Anwendbarkeit der Datenschutz-Grundverordnung ab 25. Mai 2018

Die Delegationen erhalten in der Anlage das Dokument COM(2018) 43 final.

Anl.: COM(2018) 43 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 24.1.2018
COM(2018) 43 final

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

Besserer Schutz und neue Chancen – Leitfaden der Kommission zur unmittelbaren Anwendbarkeit der Datenschutz-Grundverordnung ab 25. Mai 2018

Mitteilung der Kommission an das Europäische Parlament und den Rat

Besserer Schutz und neue Chancen – Leitfaden der Kommission zur unmittelbaren Anwendbarkeit der Datenschutz-Grundverordnung ab 25. Mai 2018

Einleitung

Am 6. April 2016 einigte sich die EU mit der Verabschiedung des Datenschutz-Reformpakets auf eine umfassende Reform ihres Datenschutzrahmens. Das Paket umfasst die Datenschutz-Grundverordnung (DS-GVO) [1], die die zwanzig Jahre alte Richtlinie 95/46/EG[2] (Datenschutzrichtlinie) ersetzt, und die Polizei-Richtlinie[3]. Am 25. Mai 2018 wird das neue EU-weite Datenschutzinstrument, die Datenschutz-Grundverordnung (nachstehend auch einfach „Verordnung"), unmittelbar anwendbar, zwei Jahre nach Annahme und Inkrafttreten.[4]

Die neue Verordnung wird das Individualrecht auf Schutz personenbezogener Daten besser schützen und trägt damit der Natur des Datenschutzes als Grundrecht der Europäischen Union Rechnung.[5]

Sie bietet ein einheitliches Regelwerk, das in den Rechtsordnungen der Mitgliedstaaten unmittelbar gilt, gewährleistet den freien Verkehr personenbezogener Daten zwischen den EU-Mitgliedstaaten und stärkt das Vertrauen und die Sicherheit der Verbraucher, zwei unerlässliche Elemente für einen echten digitalen Binnenmarkt. Auf diese Weise eröffnet die Verordnung der Wirtschaft, insbesondere kleineren Unternehmen, neue Möglichkeiten, auch durch klarere Regeln für die internationale Datenübermittlung.

Obwohl der neue Datenschutzrahmen auf den bestehenden Rechtsvorschriften aufbaut, wird er weitreichende Auswirkungen haben und in mancher Hinsicht erhebliche Anpassungen erfordern. Deshalb sieht die Datenschutz-Grundverordnung sieht einen Übergangszeitraum von 2 Jahren bis zum 25. Mai 2018 vor, um den Mitgliedstaaten und den Betroffenen Zeit zu geben, sich an den neuen Rechtsrahmen anzupassen.

In den letzten beiden Jahren haben alle Beteiligten – von den nationalen Verwaltungen und den nationalen Datenschutzbehörden bis hin zu den für die Verarbeitung Verantwortlichen und den Auftragsverarbeitern – eine Reihe von Maßnahmen ergriffen, um sicherzustellen, dass die Bedeutung und das Ausmaß der durch den neuen Datenschutz herbeigeführten Veränderungen gut verstanden werden und dass alle Akteure auf ihre Anwendung vorbereitet

---

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, ABl. L 119 vom 4.5.2016).

[2] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995).

[3] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89).

[4] Die Datenschutz-Grundverordnung ist seit dem 24. Mai 2016 in Kraft und gilt ab dem 25. Mai 2018.

[5] Artikel 8 der Charta der Grundrechte der Europäischen Union und Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union.

sind. Da der 25. Mai näher rückt, hält es die Kommission für sinnvoll, diese Arbeiten einer Bestandsaufnahme zu unterziehen und auszuloten, welche weiteren Schritte geeignet wären, um sicherzustellen, dass alle Voraussetzungen für ein erfolgreiches Inkrafttreten des neuen Rechtsrahmens vorhanden sind.[6]

In dieser Mitteilung werden

- die wichtigsten Neuerungen und Chancen, die sich durch die neuen EU-Datenschutzvorschriften eröffnet haben, in Erinnerung gerufen,
- die bisherigen Vorarbeiten auf EU-Ebene dargestellt,
- dargelegt, was die Europäische Kommission, die nationalen Datenschutzbehörden und die nationalen Behörden noch tun sollten, um die Vorbereitung auf einen erfolgreichen Abschluss zu bringen,
- und die Maßnahmen beschrieben, die die Kommission in den kommenden Monaten zu ergreifen beabsichtigt.

Parallel zur Annahme dieser Mitteilung startet die Kommission außerdem ein Online-Instrumentarium zur Unterstützung der Interessenträger bei der Vorbereitung auf die Anwendung der Verordnung und – mit Unterstützung der Vertretungen – eine Informationskampagne in den Mitgliedstaaten.

1. DER NEUE EU-DATENSCHUTZRAHMEN – BESSERER SCHUTZ UND NEUE CHANCEN

Die DS-GVO folgt nach wie vor dem Ansatz der Datenschutzrichtlinie, aber aufbauend auf den zwanzigjährigen Erfahrungen mit dem EU-Datenschutzrecht und der einschlägigen Rechtsprechung präzisiert und modernisiert sie die Datenschutzvorschriften. Sie enthält eine Reihe neuer Elemente, die den Schutz der Rechte des Einzelnen und der Unternehmen stärken. Diese werden nachstehend beschrieben.

- **Ein harmonisierter Rechtsrahmen, der zu einer einheitlichen Anwendung der Vorschriften führt, was sich positiv auf den europäischen digitalen Binnenmarkt auswirkt:** Die Richtlinie bietet ein einheitliches Regelwerk für Bürger und Unternehmen, was gegenüber der heutigen Situation, in der die EU-Mitgliedstaaten die Vorschriften der Richtlinie unterschiedlich umgesetzt haben, Abhilfe schafft. Um eine einheitliche und durchgängige Anwendung in allen Mitgliedstaaten zu gewährleisten, wird eine zentrale Anlaufstelle geschaffen.

- **Gleiche Wettbewerbsbedingungen für alle auf dem EU-Markt tätigen Unternehmen:** Mit der Verordnung werden Unternehmen mit Sitz außerhalb der EU verpflichtet, dieselben Vorschriften anzuwenden wie Unternehmen mit Sitz in der EU, wenn sie Waren und Dienstleistungen anbieten oder das Verhalten von Personen in der Union überwachen. Deshalb müssen Unternehmen von außerhalb der EU, die im Binnenmarkt tätig sind, unter bestimmten Umständen einen Vertreter in der EU benennen, an den sich Bürger und Behörden neben oder anstelle der im Ausland ansässigen Gesellschaft wenden können.

[6] https://ec.europa.eu/commission/sites/beta-political/files/letter-of-intent-2017_de.pdf.

- Ferner werden die **Grundsätze des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen** eingeführt. Sie setzen Anreize für innovative Lösungen, damit Datenschutzinteressen von Anfang an berücksichtigt werden.

- **Stärkung der Rechte des Einzelnen**: Mit der Verordnung werden neue Transparenzanforderungen eingeführt: Stärkung der Rechte auf Information, Zugang und Löschung – das „Recht auf Vergessenwerden". Verbot, Stillschweigen oder Untätigkeit dürfen nicht länger als Einwilligung betrachtet werden; vielmehr bedarf es einer eindeutigen bestätigenden Handlung. Kinder werden im Internet geschützt.

- **Einzelpersonen erhalten mehr Kontrolle über die sie betreffenden Daten.** Mit der Verordnung wird ein **neues Recht auf Datenübertragbarkeit** eingeführt, das es den Bürgern ermöglicht, von einem Unternehmen oder einer Organisation die Rückübertragung personenbezogener Daten zu verlangen, die sie diesem ihm bzw. ihr auf der Grundlage einer Einwilligung oder eines Vertrags zur Verfügung gestellt haben. Dieses Recht ermöglicht es auch, dass solche personenbezogenen Daten direkt an ein anderes Unternehmen oder eine andere Organisation übermittelt werden, wenn dies technisch machbar ist. Da es die direkte Übermittlung personenbezogener Daten von einem Unternehmen oder einer Organisation auf ein anderes/eine andere erlaubt, wird dieses Recht auch den freien Verkehr personenbezogener Daten in der EU fördern, die Blockade personenbezogener Daten vermeiden und den Wettbewerb zwischen Unternehmen fördern. Die Erleichterung des Wechsels zwischen verschiedenen Diensteanbietern wird die Entwicklung neuer Dienste fördern, wie in der Strategie für den digitalen Binnenmarkt anvisiert.

- **Besserer Schutz gegen Datenmissbrauch**: Die Datenschutz-Grundverordnung enthält umfassende Vorschriften zu Verletzungen des Schutzes personenbezogener Daten. Dort wird die „Verletzung des Schutzes personenbezogener Daten" definiert, und sie verpflichtet dazu, der Aufsichtsbehörde eine solche Verletzung binnen höchstens 72 Stunden zu melden, wenn diese voraussichtlich zu einem Risiko für die Rechte und Freiheiten des Einzelnen führt. Dann muss unter bestimmten Umständen die Person, deren Daten verletzt wurden, davon in Kenntnis gesetzt werden. Das bedeutet eine erhebliche Verbesserung gegenüber der heutigen Lage. Derzeit sind in der EU nur Anbieter elektronischer Kommunikationsdienste, Betreiber wesentlicher Dienste und Anbieter digitaler Dienste verpflichtet, Datenschutzverstöße gemäß der Datenschutzrichtlinie für elektronische Kommunikation[7] (Datenschutzrichtlinie für elektronische Kommunikation)

[7] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37). Nach Artikel 95 der Datenschutz-Grundverordnung erlegt diese natürlichen oder juristischen Personen keine zusätzlichen Verpflichtungen auf, soweit sie besonderen in der Richtlinie 2002/58/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen. Dies bedeutet zum Beispiel, dass Unternehmen, die unter die Datenschutzrichtlinie für elektronische Kommunikation fallen, eine Verletzung des Schutzes personenbezogener Daten nach Maßgabe dieser Richtlinie melden müssen, soweit der Verstoß eine Dienstleistung betrifft, die unter diese Richtlinie fällt. Die Datenschutz-Grundverordnung erlegt ihnen diesbezüglich keine zusätzlichen Verpflichtungen auf.

und der Richtlinie über die Sicherheit von Netz- und Informationssystemen[8] (NIS) zu melden.

- **Mit der Verordnung wird allen Datenschutzbehörden die Befugnis übertragen, Geldbußen gegen Verantwortliche und Auftragsverarbeiter zu verhängen.** Derzeit haben nicht alle Datenschutzbehörden diese Befugnis inne. Dies wird eine bessere Umsetzung der Vorschriften ermöglichen. Die Geldbußen können bis zu 20 Mio. EUR oder im Falle eines Unternehmens bis zu 4 % des weltweiten Jahresumsatzes betragen.

- **Mehr Flexibilität für die für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter, die personenbezogene Daten verarbeiten, aufgrund einer eindeutigen Zuweisung der Verantwortung (Grundsatz der Rechenschaftspflicht)**: Die Meldepflicht wird vom Grundsatz der Rechenschaftspflicht abgelöst. Dieser Grundsatz schlägt sich in abgestuften Verpflichtungen in Abhängigkeit von den Risiken (z. B. Anwesenheit eines Datenschutzbeauftragten oder Verpflichtung zu Datenschutz-Folgenabschätzungen) nieder. Es wird ein neues Instrument eingeführt, um das Risiko vor einem Beginn mit der Datenverarbeitung zu bewerten: die Datenschutz-Folgenabschätzung. Sie ist erforderlich, wenn die Verarbeitung zu einem hohen Risiko für die Rechte und Freiheiten des Einzelnen führen kann. Drei Fälle sind ausdrücklich als solche in der Verordnung aufgeführt: wenn ein Unternehmen systematisch und umfassend persönliche Aspekte einer Einzelperson bewertet (einschließlich Profiling), wenn es sensible Daten in großem Umfang verarbeitet oder öffentlich zugängliche Bereiche systematisch weiträumig überwacht. Die nationalen Datenschutzbehörden müssen die Listen der Fälle veröffentlichen, in denen eine Datenschutz-Folgenabschätzung erforderlich ist.[9]

- **Mehr Klarheit hinsichtlich der Pflichten der Auftragsverarbeiter und der Verantwortung der für die Verarbeitung Verantwortlichen bei der Auswahl eines Auftragsverarbeiters,**

- **und eine kohärentere und konsequentere Durchsetzung der Vorschriften:** Dazu zählt die Harmonisierung der Befugnisse der Datenschutzbehörden, auch in Bezug auf Geldbußen, und neue Vernetzungs- und Kooperationsmechanismen für diese Behörden.

- **Der durch die Verordnung garantierte Datenschutz bleibt auch außerhalb der EU erhalten, so dass sich die Bürgerinnen und Bürger auf ein hohes Schutzniveau verlassen können**[10]: Während der Aufbau der Vorschriften für die internationale Datenübermittlung in der Verordnung im Wesentlichen derselbe ist wie die der Richtlinie von 1995, wird mit der Reform deutlicher und einfacher festgelegt, wie sie anzuwenden sind. Außerdem werden neue Instrumente für die Datenübermittlung eingeführt. In Bezug auf die Angemessenheitsbeschlüsse enthält die Verordnung einen genauen und

---

[8] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1). Unternehmen, die unter die NIS-Richtlinie fallen, sollten Sicherheitsvorfälle melden, die beträchtliche oder erhebliche Auswirkungen auf die Erbringung einiger ihrer Dienstleistungen haben. Die Meldung von Sicherheitsvorfällen gemäß der NIS-Richtlinie erfolgt unbeschadet der Meldung von Verstößen im Sinne der Verordnung.

[9] Artikel 35 der Verordnung.

[10] Mitteilung der Kommission über den Austausch und den Schutz personenbezogener Daten in einer globalisierten Welt, COM (2017) 7 final.

detaillierten Katalog von Kriterien, die die Kommission bei der Beurteilung der Frage berücksichtigen muss, ob ein ausländisches System personenbezogene Daten angemessen schützt. Die Verordnung formalisiert ferner die Zahl alternativer Übermittlungsinstrumente, wie Standardvertragsklauseln und verbindliche interne Datenschutzvorschriften, und erweitert diese.

Die überarbeitete Verordnung für die Organe, Einrichtungen, Ämter und Agenturen der EU[11] die Verordnung über Privatsphäre und elektronische Kommunikation[12] („e-Datenschutzverordnung"), die sich derzeit im Gesetzgebungsverfahren befinden, werden sicherstellen, dass die EU über solide und umfassende Datenschutzvorschriften verfügt.[13]

2. BISHERIGE VORARBEITEN AUF EU-EBENE

Die erfolgreiche Anwendung der Verordnung erfordert die Zusammenarbeit zwischen allen am Datenschutz Beteiligten: Mitgliedstaaten, darunter öffentliche Verwaltungen, nationale Datenschutzbehörden, Unternehmen, Organisationen, die Daten verarbeiten, Bürgerinnen und Bürger und Kommission.

2.1 Maßnahmen der Europäischen Kommission

Kurz nach Inkrafttreten der Verordnung Mitte 2016 hat sich die Kommission mit den Behörden der Mitgliedstaaten, den Datenschutzbehörden und den Interessenträgern in Verbindung gesetzt, um die Anwendung der Verordnung vorzubereiten und mit Unterstützung und Beratung zu begleiten.

a) Unterstützung der Mitgliedstaaten und ihrer Behörden

Die Kommission arbeitet eng mit den Mitgliedstaaten zusammen, um ihre Vorbereitungstätigkeit während des Übergangszeitraums zu unterstützen. So soll größtmögliche Kohärenz gewährleistet werden. Zu diesem Zweck hat die Kommission eine Expertengruppe eingesetzt, die die Mitgliedstaaten bei ihren vorbereitenden Arbeiten begleiten soll. Die Gruppe dient als Forum, in dem die Mitgliedstaaten ihre Erfahrungen und ihr Fachwissen austauschen können.[14] Sie ist bereits dreizehn Mal zusammengetroffen. Zudem hat die Kommission bilaterale Treffen mit den Behörden der Mitgliedstaaten abgehalten, um Fragen zu erörtern, die auf nationaler Ebene auftraten.

---

[11] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG, COM(2017) 8 final.

[12] Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), COM(2017) 10 final.

[13] Bis zur Annahme und Anwendung der e-Datenschutzverordnung gilt die Richtlinie 2002/58/EG als *lex specialis*.

[14] Eine vollständige Liste der Sitzungen und Tagesordnungen sowie Zusammenfassungen der Erörterungen und einen Überblick über den aktuellen Stand der Rechtsetzung in den einzelnen Mitgliedstaaten finden Sie unter http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3461.

b) Unterstützung der Datenschutzbehörden und Einrichtung des Europäischen Datenschutzausschusses

Die Kommission unterstützt aktiv die Arbeiten der Datenschutzgruppe nach Artikel 29, auch um einen reibungslosen Übergang zum Europäischen Datenschutzausschuss zu ermöglichen.[15]

c) Internationale Datenschutzpolitik

Die Verordnung wird die Möglichkeiten der EU verbessern, ihre Datenschutzwerte aktiv nach außen zu vertreten. Zudem erleichtert sie die Datenströme, indem sie die weltweite Konvergenz der Rechtssysteme fördert.[16] Die Datenschutzvorschriften der EU werden auf internationaler Ebene zunehmend als Grundlage für einige der höchsten Datenschutznormen weltweit anerkannt. Das Übereinkommen Nr. 108 des Europarates, das einzige rechtsverbindliche multilaterale Instrument im Bereich des Schutzes personenbezogener Daten, wird ebenfalls modernisiert. Die Kommission arbeitet daran, dass es die gleichen Grundsätze widerspiegelt, wie sie in den neuen EU-Datenschutzvorschriften verankert sind, und leistet damit ihren Beitrag zu einheitlich hohen Datenschutznormen. Die Kommission wird sich aktiv dafür einsetzen, dass der modernisierte Wortlaut des Übereinkommens rasch angenommen wird, damit die EU Vertragspartei werden kann.[17] Die Kommission ermutigt Nicht-EU-Länder, das Übereinkommen Nr. 108 des Europarats und sein Zusatzprotokoll zu ratifizieren.

Zudem führen auch einige Länder und regionale Organisationen außerhalb der EU, in unserer unmittelbaren Nachbarschaft ebenso wie in Asien, Lateinamerika oder Afrika, neue Datenschutzvorschriften ein bzw. aktualisieren bestehende Vorschriften, um die Chancen der globalen digitalen Wirtschaft zu nutzen und der wachsenden Nachfrage nach mehr Datensicherheit und Schutz der Privatsphäre zu begegnen. Auch wenn in der Herangehensweise der einzelnen Länder und der Regulierungsintensität Unterschiede bestehen, so gibt es doch dafür, dass die Verordnung zunehmend als Modell und Inspirationsquelle fungiert.[18]

In diesem Zusammenhang setzt die Kommission ihre internationale Datenschutzpolitik im Einklang mit ihrer Mitteilung vom Januar 2017[19] fort, indem sie sich aktiv mit wichtigen Handelspartnern in Ost- und Südostasien engagiert, um die Möglichkeiten etwaiger Angemessenheitsbeschlüsse auszuloten.[20]

---

[15] So wird die Kommission dem Datenschutzausschuss die Möglichkeit einräumen, das Binnenmarkt-Informationssystem (IMI) für die Kommunikation zwischen seinen Mitgliedern zu nutzen.

[16] Reflexionspapier „Die Globalisierung meistern“ (COM (2017) 240).

[17] Übereinkommen des Europarats vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV Nr. 108) und Zusatzprotokoll von 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr (SEV Nr. 181). Das Übereinkommen steht Nichtmitgliedern des Europarats offen und wurde bereits von 51 Ländern (darunter auch von Uruguay, Mauritius, Senegal und Tunesien) ratifiziert.

[18] Siehe z. B. Data Protection Standards of the Ibero-American States’, http://www.redipd.es/documentacion/common/Estandares_eng_Con_logo_RIPD.pdf

[19] COM(2017) 7.

[20] COM (2017) 7, a.a.O., S. 10-11.

So steht die Kommission unter anderem in Verhandlungen mit Japan, um die von Präsident Juncker und Premierminister Abe in ihrer gemeinsamen Erklärung vom 6. Juli 2017[21] in Aussicht gestellte gegenseitige Bestätigung eines angemessenen Schutzniveaus bis Anfang 2018 zu verwirklichen. Im Hinblick auf einen möglichen Angemessenheitsbeschluss wurden auch Gespräche mit Südkorea aufgenommen. Ein Angemessenheitsbeschluss würde den freien Datenverkehr mit den betreffenden Drittländern sicherstellen und gleichzeitig gewährleisten, dass bei der Übermittlung personenbezogener Daten aus der EU in diese Länder ein hohes Schutzniveau gilt.

Gleichzeitig arbeitet die Kommission mit den Interessenträgern zusammen, um das Instrumentarium, das die Verordnung für die internationale Datenübertragung zur Verfügung stellt, durch Entwicklung alternativer Übermittlungsmechanismen auszuschöpfen, die an die besonderen Bedürfnisse bestimmter Wirtschaftszweige und/oder Unternehmen angepasst sind.[22]

d) Einbeziehung von Interessenträgern

Die Kommission hat eine Reihe von Veranstaltungen organisiert, um sich mit den Betroffenen ins Benehmen zu setzen.[23] Für das erste Quartal 2018 ist ein neuer Workshop für Verbraucher geplant. Gezielte sektorale Diskussionen in Bereichen wie Forschung und Finanzdienstleistungen fanden ebenfalls statt.

Die Kommission hat darüber hinaus eine aus Vertretern der Zivilgesellschaft und der Wirtschaft sowie aus Wissenschaft und Praxis von Forschung und Lehre und Unternehmensvertretern bestehende DS-GVO-Gruppe ins Leben gerufen. Diese Gruppe wird die Kommission insbesondere bei der Frage beraten, wie ein angemessenes Maß an Sensibilisierung der Interessenträger erreicht werden kann.[24]

Schließlich hat die Europäische Kommission mit ihrem Rahmenprogramm für Forschung und Innovation „Horizont 2020“[25] Maßnahmen zur Entwicklung von Instrumenten finanziert, mit denen die wirksame Anwendung der Vorschriften der Verordnung im Hinblick auf die Einwilligung und die Privatsphäre wahrende Methoden zur Datenanalyse (z. B. mehrseitige Verschlüsselung und homomorphe Verschlüsselung) unterstützt werden sollen.

2.2 Maßnahmen der Artikel 29-Datenschutzgruppe und des Europäischen Datenschutzausschusses

Die Datenschutzgruppe nach Artikel 29, die alle nationalen Datenschutzbehörden und den Europäischen Datenschutzbeauftragten vereint, spielt bei der Vorbereitung der Anwendung der Verordnung durch die Herausgabe von Leitlinien für Unternehmen und andere Beteiligte eine Schlüsselrolle. Als Durchsetzungsstellen und direkte Ansprechpartner für die

---

[21] http://europa.eu/rapid/press-release_STATEMENT-17-1917_de.htm.
[22] COM (2017) 7, a.a.O., S. 10-11.
[23] Zwei Workshops mit der Industrie im Juli 2016 und im April 2017, zwei Rundtischgespräche mit Wirtschaftsvertretern im Dezember 2016 und im Mai 2017, einen Workshop zu Gesundheitsdaten im Oktober 2017 und einen Workshop mit KMU-Vertretern im November 2017.
[24] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537&Lang=DE.
[25] https://ec.europa.eu/programmes/horizon2020/h2020-sections

Betroffenen sind die nationalen Datenschutzbehörden am besten in der Lage, zusätzliche Rechtssicherheit in Bezug auf die Auslegung der Verordnung zu schaffen.

Leitlinien/Arbeitsunterlagen der Datenschutzgruppe nach Artikel 29 mit Blick auf die Einführung der Datenschutz-Grundverordnung[26]	
Recht auf Datenübertragbarkeit	Angenommen am 4./5. April 2017
Datenschutzbeauftragte	
Benennung der federführenden Aufsichtsbehörde	
Datenschutz-Folgenabschätzung	Angenommen am 3./4. Oktober 2017
Geldbußen	Angenommen am 3./4. Oktober 2017
Profilerstellung	Laufende Arbeiten
Verletzung personenbezogener Daten	Laufende Arbeiten
Einwilligung	Laufende Arbeiten
Transparenz	Laufende Arbeiten
Zertifizierung und Akkreditierung	Laufende Arbeiten
Angemessenheit	Laufende Arbeiten
Verbindliche interne Datenschutzvorschriften für die für die Verarbeitung Verantwortlichen	Laufende Arbeiten
Verbindliche interne Datenschutzvorschriften für Auftragsverarbeiter	Laufende Arbeiten

Die Datenschutzgruppe nach Artikel 29 arbeitet an der Aktualisierung bestehender Stellungnahmen, auch in Bezug auf die Instrumente für die Übermittlung von Daten an Nicht-EU-Länder.

Da kohärente und einheitliche Leitlinien für die Wirtschaftstätigen unerlässlich sind, müssen die derzeitigen Leitlinien auf nationaler Ebene entweder aufgehoben oder mit den entsprechenden Leitlinien der nach Artikel 29 eingesetzten Arbeitsgruppe/des Europäischen Datenschutzausschusses in Einklang gebracht werden.

Die Kommission misst der Tatsache, dass diese Leitlinien vor der endgültigen Fertigstellung einer öffentlichen Konsultation unterzogen werden, große Bedeutung bei. Dabei müssen die Beiträge der Beteiligten so präzise und konkret wie möglich sein, da der Datenschutzgruppe nach Artikel 29 so bewährte Verfahren und branchenspezifische Besonderheiten zur Kenntnis gebracht werden können. Die endgültige Verantwortung für diese Leitlinien liegt weiterhin bei der Datenschutzgruppe nach Artikel 29 bzw. dem künftigen Europäischen Datenschutzausschuss, und die Datenschutzbehörden werden auf sie Bezug nehmen, wenn sie die Verordnung durchsetzen.

[26] Alle angenommenen Leitlinien sind abrufbar unter: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

Die Leitlinien sollten im Lichte der Entwicklungen und Praktiken geändert werden können. Deshalb sollten die Datenschutzbehörden eine Kultur des Dialogs mit allen Beteiligten, einschließlich Unternehmen, pflegen.

Das letzte Wort bei Fragen der Auslegung und Anwendung der Verordnung haben natürlich die Gerichte auf nationaler und EU-Ebene.

3. WEITERE SCHRITTE FÜR EINE ERFOLGREICHE VORBEREITUNG

3.1 Mitgliedstaaten: Fertigstellung des Rechtsrahmens auf nationaler Ebene

Die Verordnung gilt unmittelbar in allen Mitgliedstaaten.[27] Dies bedeutet, dass sie unabhängig von den nationalen Rechtsvorschriften bindend ist: Bürger, Unternehmen, öffentliche Stellen und andere Organisationen, die Daten verarbeiten, können sich in der Regel unmittelbar auf ihre Bestimmungen berufen. Dennoch müssen die Mitgliedstaaten im Einklang mit der Verordnung die erforderlichen Schritte ergreifen, um ihre Rechtsvorschriften durch die Aufhebung und Änderung bestehender Rechtsvorschriften, die Einrichtung nationaler Datenschutzbehörden[28], die Benennung einer Akkreditierungsstelle[29] und Kollisionsnormen für die Abwägung zwischen Meinungsfreiheit und Datenschutz[30] anzupassen.

Darüber hinaus bietet die Verordnung den Mitgliedstaaten die Möglichkeit, die Anwendung der Datenschutzbestimmungen in bestimmten Bereichen zu konkretisieren: öffentlicher Sektor[31], Beschäftigung und soziale Sicherheit[32], Gesundheitsvorsorge und Arbeitsmedizin, öffentliche Gesundheit[33], im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke[34], nationale Kennziffern[35], Zugang der Öffentlichkeit zu amtlichen Dokumenten[36] und Geheimhaltungspflichten[37]. Darüber hinaus werden die Mitgliedstaaten durch die Verordnung ermächtigt, für genetische

---

[27] Artikel 288 AEUV.
[28] Artikel 54 Absatz 1 DS-GVO.
[29] Artikel 43 Absatz 1 DS-GVO sieht vor, dass die Mitgliedstaaten den Zertifizierungsstellen zwei mögliche Akkreditierungsmethoden anbieten, nämlich durch die gemäß den Datenschutzvorschriften errichteten nationalen Datenschutzbehörde und/oder durch die gemäß der Verordnung (EG) Nr. 765/2008 über Akkreditierung und Marktüberwachung benannte nationale Akkreditierungsstelle. Die im Rahmen der Verordnung (EG) Nr. 765/2008 anerkannte Europäische Kooperation für die Akkreditierung (European Cooperation for Accreditation, im Folgenden „EA“), in der nationale Akkreditierungsstellen zusammenarbeiten, und die Aufsichtsbehörden der Datenschutz-Grundverordnung sollten zu diesem Zweck eng zusammenarbeiten.
[30] Artikel 85 Absatz 1 DS-GVO.
[31] Artikel 6 Absatz 2 DS-GVO.
[32] Artikel 88 und 9 Absatz 2 Buchstabe b DS-GVO. In der europäischen Säule sozialer Rechte heißt es ferner, dass „Arbeitnehmer das Recht auf den Schutz ihrer persönlichen Daten im Rahmen eines Beschäftigungsverhältnisses haben“. (2017/C 428/09, ABl. C 428 vom 13.12.2017, S. 10-15).
[33] Artikel 9 Absatz 2 Buchstaben h und i DS-GVO.
[34] Artikel 9 Absatz 2 Buchstabe j DS-GVO.
[35] Artikel 87 DS-GVO.
[36] Artikel 86 DS-GVO.
[37] Artikel 90 DS-GVO.

Daten, biometrische Daten und Gesundheitsdaten weitere Bedingungen, einschließlich Beschränkungen, aufrechtzuerhalten oder einzuführen.[38]

Den einschlägigen Maßnahmen der Mitgliedstaaten werden durch zwei Vorschriften Grenzen gesetzt:

1. Artikel 8 der Charta, wonach alle nationalen Vorschriften die Anforderungen des Artikel 8 der Charta erfüllen müssen (und damit die der Verordnung, die sich auf Artikel 8 der Charta stützt), und
2. Artikel 16 Absatz 2 AEUV, nach dem die nationalen Rechtsvorschriften den freien Verkehr personenbezogener Daten in der EU nicht berühren können.

Die Verordnung bietet die Gelegenheit, die rechtlichen Rahmenbedingungen im Sinne von weniger einzelstaatlichen Vorschriften und mehr Klarheit für die Wirtschaftstätigen zu vereinfachen.

Bei der Anpassung ihrer innerstaatlichen Rechtsvorschriften müssen die Mitgliedstaaten der Tatsache Rechnung tragen, dass alle nationalen Maßnahmen, die die unmittelbare Wirkung der Verordnung behindern oder ihre gleichzeitige einheitliche Anwendung in der gesamten EU gefährden würden, gegen die Verträge verstoßen.[39]

Die Wiederholung des Verordnungswortlauts in innerstaatlichen Rechtsvorschriften (z. B. Wiederholung der Begriffsbestimmungen oder der Rechte des Einzelnen) ist ebenfalls verboten, es sei denn, solche Wiederholungen sind aus Gründen der Kohärenz und der Verständlichkeit für die Betroffenen unbedingt erforderlich.[40] Die Wiedergabe des Verordnungswortlauts in einzelstaatlichen Präzisierungsvorschriften sollte nur in Ausnahmefällen vorkommen und gerechtfertigt sein; sie darf nicht dazu verwendet werden, um zusätzliche Bedingungen oder Auslegungen zu ergänzen.

Die Auslegung der Verordnung ist Sache der europäischen Gerichte (der nationalen Gerichte und letztlich des Europäischen Gerichtshofs) und nicht des einzelstaatlichen Gesetzgebers. Letzterer kann daher weder den Wortlaut der Verordnung kopieren, sofern dies nicht angesichts der Kriterien der Rechtsprechung erforderlich sein sollte, noch zusätzliche Bedingungen für die im Rahmen der Datenschutz-Grundverordnung unmittelbar geltenden Vorschriften einfügen. Andernfalls wären die Wirtschaftstätigen in der gesamten Union erneut mit einer Fragmentierung konfrontiert und würden nicht wissen, welche Vorschriften sie einzuhalten haben.

Bislang haben nur zwei Mitgliedstaaten die einschlägigen nationalen Rechtsvorschriften bereits erlassen.[41] Die übrigen Mitgliedstaaten befinden sich in unterschiedlichen Stadien ihres Gesetzgebungsverfahrens[42] und planen die Verabschiedung der Rechtsvorschriften bis

---

[38] Artikel 9 Absatz 4 DS-GVO.

[39] Rs. 94/77 *Fratelli Zerbone Snc/Amministrazione delle finanze dello Stato* ECLI:EU:C:1978:17 und 101.

[40] Erwägungsgrund 8 DS-GVO.

[41] Österreich (http://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2017_I_120/BGBLA_2017_I_120.pdf); Deutschland (https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D__1513091793362).

[42] Einen Überblick über den Stand der Gesetzgebungsverfahren in den einzelnen Mitgliedstaaten siehe unter http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3461

zum 25. Mai 2018. Es ist wichtig, den Wirtschaftstätigen genug Zeit einzuräumen, um sich auf alle Bestimmungen vorzubereiten, die sie einzuhalten haben.

Treffen die Mitgliedstaaten nicht oder verspätet die gemäß der Verordnung erforderlichen Maßnahmen, oder verwenden die dort vorgesehenen Spezifikationsklauseln in einer Weise, die der Verordnung zuwiderläuft, wird die Kommission die ihr zur Verfügung stehenden Instrumente einschließlich des Vertragsverletzungsverfahrens nutzen.

3.2 Verantwortung der Datenschutzbehörden für die uneingeschränkte Arbeitsfähigkeit des neuen unabhängigen Europäischen Datenschutzausschuss

Es ist von wesentlicher Bedeutung, dass das neue durch die Verordnung geschaffene Gremium, der Europäische Datenschutzausschuss[43], der der Datenschutzgruppe nach Artikel 29 nachfolgt, ab dem 25. Mai 2018 voll arbeitsfähig ist.

Der Europäische Datenschutzbeauftragte als die Datenschutzbehörde, die für die Beaufsichtigung von Organen und Einrichtungen der EU zuständig ist, stellt im Interesse von Synergien und Arbeitseffizienz das Sekretariat des Ausschusses. In den vergangenen Monaten hat der Europäische Datenschutzbeauftragte damit begonnen, entsprechende Vorbereitungen zu treffen.

Der Europäische Datenschutzausschuss wird im Zentrum des Datenschutzes in Europa stehen. Er wird zu einer einheitlichen Anwendung des Datenschutzrechts beitragen und eine solide Grundlage für die Zusammenarbeit zwischen den Datenschutzbehörden, einschließlich des Europäischen Datenschutzbeauftragten, bieten. Der Europäische Datenschutzausschuss wird nicht nur Leitlinien zur Auslegung der Kernkonzepte der Datenschutz-Grundverordnung herausgeben, sondern auch verbindliche Entscheidungen über Streitigkeiten im Zusammenhang mit der grenzüberschreitenden Verarbeitung treffen. Dadurch wird die einheitliche Anwendung der EU-Vorschriften gewährleistet und verhindert, dass ein und derselbe Fall in den einzelnen Mitgliedstaaten unterschiedlich behandelt wird.

Die reibungslose und effiziente Arbeit des Europäischen Datenschutzausschusses ist daher eine Voraussetzung für das reibungslose Funktionieren des gesamten Systems. Mehr denn je wird der Europäische Datenschutzausschuss eine gemeinsame Datenschutzkultur unter allen nationalen Datenschutzbehörden herbeiführen müssen, um sicherzustellen, dass die Vorschriften der Verordnung einheitlich ausgelegt werden. Die Verordnung fördert die Zusammenarbeit zwischen den Datenschutzbehörden, indem sie ihnen die Instrumente zur wirksamen und effizienten Zusammenarbeit bietet: sie werden insbesondere in der Lage sein, gemeinsame Maßnahmen zu ergreifen, im Einvernehmen zu entscheiden und Meinungsverschiedenheiten zu lösen, die sie im Zusammenhang mit der Auslegung der Verordnung im Ausschuss haben könnten. Hierzu können sie Stellungnahmen und verbindliche Beschlüsse fassen. Die Kommission fordert die Datenschutzbehörden auf, für die neuen Vorschriften Verantwortung zu übernehmen und ihre Abläufe, Finanzierung und Arbeitskultur entsprechend anzupassen, um die neuen Rechte und Pflichten zu erfüllen.

---

[43] Der Europäische Datenschutzausschuss wird eine EU-Einrichtung mit eigener Rechtspersönlichkeit sein, die für die einheitliche Anwendung der Verordnung zuständig ist. Er setzt sich aus den Leitern der einzelnen Datenschutzbehörden und dem Europäischen Datenschutzbeauftragten oder deren Vertretern zusammen.

3.3 Mitgliedstaaten: Bereitstellung der erforderlichen finanziellen und personellen Ressourcen für die nationalen Datenschutzbehörden

Die Einrichtung völlig unabhängiger Aufsichtsbehörden in jedem Mitgliedstaat ist von wesentlicher Bedeutung, um den Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten in der EU zu gewährleisten.[44] Die Aufsichtsbehörden können die individuellen Rechte und Freiheiten nicht wirksam schützen, es sei denn, sie handeln völlig unabhängig. Wird die Unabhängigkeit und die wirksame Ausübung ihrer Befugnisse nicht gewährleistet, so hat dies weitreichende negative Auswirkungen auf die Durchsetzung der Datenschutzvorschriften.[45]

Die Verordnung gießt das Erfordernis, dass jede Datenschutzbehörde völlig unabhängig handeln muss, in geltendes Recht.[46] Sie stärkt die Unabhängigkeit der nationalen Datenschutzbehörden, vereinheitlicht ihre Befugnisse europaweit und versetzt sie so in die Lage, wirksam Beschwerden nachzugehen, Untersuchungen durchzuführen, verbindliche Entscheidungen zu treffen und wirksame und abschreckende Sanktionen zu verhängen. Außerdem wird ihnen die Befugnis übertragen, gegen für die Verarbeitung Verantwortliche oder Auftragsverarbeiter Geldbußen in Höhe von bis zu 20 Mio. EUR oder im Falle von Unternehmen bis zu 4 % des weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs zu verhängen, je nachdem, welcher der Beträge höher ist.

Die Datenschutzbehörden sind die natürlichen Gesprächspartner und der erste Ansprechpartner für die breite Öffentlichkeit und für Unternehmen und Verwaltungen in Fragen der Verordnung. Die Aufgabe der Datenschutzbehörden besteht darin, die für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter zu informieren und die Öffentlichkeit für die Risiken, Regeln, Garantien und Rechte bei der Datenverarbeitung zu sensibilisieren. Allerdings sollten die für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter von den Datenschutzbehörden nicht die Art maßgeschneiderter, individuell zugeschnittener juristischer Beratung erwarten, zu der nur ein Rechtsanwalt oder ein Datenschutzbeauftragter in der Lage ist.

Die nationalen Datenschutzbehörden spielen somit eine zentrale Rolle, aber das relative Ungleichgewicht zwischen den ihnen in den verschiedenen Mitgliedstaaten zugewiesenen personellen und finanziellen Mitteln kann ihre wirksame Arbeit und letztendlich die nach der Verordnung erforderliche vollständige Unabhängigkeit gefährden. Es kann auch die Fähigkeit der Datenschutzbehörden zur Ausübung von Kompetenzen wie ihrer Ermittlungsbefugnisse beeinträchtigen. Die Mitgliedstaaten sind aufgefordert, ihren rechtlichen Verpflichtungen nachzukommen und die nationalen Datenschutzbehörden mit den personellen, technischen und finanziellen Ressourcen und Räumlichkeiten sowie der Infrastruktur auszustatten, die für die wirksame Wahrnehmung ihrer Aufgaben und die Ausübung ihrer Befugnisse erforderlich sind.[47]

---

[44] Erwägungsgrund 117; siehe auch bereits Erwägungsgrund 62 der Richtlinie 95/46.
[45] Mitteilung der Kommission an das Europäische Parlament und an den Rat - Stand des Arbeitsprogramms für eine bessere Durchführung der Datenschutzrichtlinie, COM(2007) 87 final vom 7. März 2007.
[46] Artikel 52 DS-GVO.
[47] Artikel 52 Absatz 4 DS-GVO.

3.4 Unternehmen, Behörden und andere Organisationen, die Daten verarbeiten: Vorbereitung auf die Anwendung der neuen Vorschriften

Die Verordnung hat an den Kernkonzepten und -grundsätzen der Rechtsvorschriften zum Datenschutz, die 1995 eingeführt wurden, nichts Wesentliches geändert. Die große Mehrheit der für die Verarbeitung Verantwortlichen und der Auftragsverarbeiter wird, sofern sie bereits im Einklang mit den geltenden EU-Datenschutzvorschriften stehen, ihre Datenverarbeitungsvorgänge nicht wesentlich ändern müssen, um der Verordnung nachzukommen.

Die Verordnung wirkt sich überwiegend auf Wirtschaftsbeteiligte aus, deren Kerngeschäft die Verarbeitung von und/oder der Umgang mit sensiblen Daten ist, und auf diejenigen, die regelmäßig und systematisch Einzelpersonen in großem Maßstab beobachten. Diese werden höchstwahrscheinlich einen Datenschutzbeauftragten benennen, eine Datenschutz-Folgenabschätzung durchführen und Datenschutzverstöße melden müssen, wenn die Rechte und Freiheiten des Einzelnen gefährdet sind. Wirtschaftsbeteiligte, insbesondere KMU, deren Kerntätigkeit nicht in einer mit hohen Risiken verbundenen Datenverarbeitung besteht, werden in der Regel nicht den besonderen Verpflichtungen der Verordnung unterliegen.

Es ist wichtig, dass die für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter ihre Verarbeitungsabläufe gründlich überprüfen, um klar erkennen zu können, welche Daten zu welchem Zweck und auf welcher Rechtsgrundlage gespeichert sind (z. B. Cloud-Umgebung, Unternehmen im Finanzsektor). Sie müssen auch die bestehenden Verträge bewerten, insbesondere die Verträge zwischen Verantwortlichen und Auftragsverarbeitern, die Möglichkeiten für internationale Übermittlungen und die allgemeinen Rahmenbedingungen (welche IT- und organisatorischen Maßnahmen sind vorhanden), einschließlich der Benennung eines Datenschutzbeauftragten. Wichtig wäre es, dass die Führungsebene an solchen Überprüfungen beteiligt ist, ihren Beitrag leistet und regelmäßig unterrichtet und zu Änderungen der Datenpolitik des Unternehmens konsultiert wird.

Zu diesem Zweck greifen einige Unternehmen auf Übereinstimmungsprüflisten (intern oder extern) zurück, involvieren Beratungsfirmen und Anwaltskanzleien und suchen nach Produkten, die die Anforderungen des Datenschutzes durch Technik und datenschutzfreundliche Voreinstellungen erfüllen. Jeder Sektor muss branchenspezifische, auf das eigene Geschäftsmodell zugeschnittene Vorkehrungen treffen.

Unternehmen und andere Organisationen, die Daten verarbeiten, können die neuen in der Verordnung vorgesehenen Instrumente wie Verhaltenskodizes und Zertifizierungsverfahren auch nutzen, um die Einhaltung der Vorschriften nachzuweisen. Es handelt sich um an der Basis entwickelte Konzepte, die von der Wirtschaft, von Verbänden oder anderen Organisationen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, und die bewährte Verfahren oder wichtige Entwicklungen in einer bestimmten Branche widerspiegeln oder die über das erforderliche Niveau des Datenschutzes bei bestimmten Produkten und Dienstleistungen informieren können. Die Verordnung sieht einen gestrafften Regelkanon für solche Mechanismen vor und berücksichtigt dabei die Marktgegebenheiten (z. B. Zertifizierung durch eine Zertifizierungsstelle oder durch eine Datenschutzbehörde).

Während Großunternehmen sich aktiv auf die Anwendung der neuen Vorschriften vorbereiten, sind viele KMU noch nicht in vollem Umfang über die künftigen Datenschutzbestimmungen informiert.

Kurz gesagt, die Wirtschaftstätigen sollten sich auf die neuen Regeln vorbereiten und anpassen und die Datenschutz-Grundverordnung als

- Chance, ihre Datenverarbeitung in Ordnung zu bringen,
- als Verpflichtung zur Entwicklung privatsphären- und datenschutzfreundlicher Produkte und zum Aufbau einer neuen Beziehung zu ihren Kunden auf der Grundlage von Transparenz und Vertrauen und
- als Gelegenheit zu begreifen, ihre Beziehungen zu den Datenschutzbehörden durch Rechenschaftspflicht und antizipative Regelbefolgung neuzugestalten.

3.5 Unterrichtung der Interessenträger, insbesondere der Bürgerinnen und Bürger sowie der kleinen und mittleren Unternehmen.

Der Erfolg der Verordnung hängt davon ab, dass die neuen Regeln allen, die von ihnen betroffen sind (Unternehmen und andere Organisationen, die Daten verarbeiten, Behörden und Bürger) bekannt sind. Auf nationaler Ebene ist es in erster Linie Aufgabe der Datenschutzbehörden, das Bewusstsein zu schärfen und gegenüber Verantwortlichen, Auftragsverarbeitern und Einzelpersonen als erster Ansprechpartner zu fungieren. Als Durchsetzungsinstanzen für Datenschutzvorschriften in ihrem Hoheitsgebiet sind die Datenschutzbehörden auch am besten in der Lage, der Wirtschaft und dem öffentlichen Sektor die von der Verordnung eingeführten Änderungen zu erläutern und die Bürger mit ihren Rechten vertraut zu machen.

Die Datenschutzbehörden haben damit begonnen, die Beteiligten entsprechend dem jeweiligen nationalen Ansatz zu informieren. Einige halten Seminare mit staatlichen Verwaltungen auch auf regionaler und kommunaler Ebene sowie Workshops mit verschiedenen Wirtschaftszweigen ab, um für die wichtigsten Bestimmungen der Verordnung zu sensibilisieren. Einige bieten spezifische Schulungsprogramme für Datenschutzbeauftragte an. Die meisten von ihnen haben Informationsmaterial in verschiedenen Formaten (Checklisten, Videos usw.) in Ihrem Internet-Angebot.

Allerdings sind den Bürgerinnen und Bürgern die Änderungen und der verbesserte Rechtsschutz, den ihnen die neuen Datenschutzvorschriften bieten, noch nicht ausreichend bekannt. Die Initiative Schulungs- und Sensibilisierungsinitiative, die von den Datenschutzbehörden in Gang gesetzt wurde, sollte fortgesetzt und intensiviert werden, wobei ein besonderer Schwerpunkt auf KMU gelegt werden sollte. Die nationalen sektoralen Verwaltungen können die Arbeit der Datenschutzbehörden unterstützen und deren Beiträge nutzen, um selber unterschiedliche Interessenträger anzusprechen.

4. NÄCHSTE SCHRITTE

In den kommenden Monaten wird die Kommission weiterhin aktiv die Vorbereitung auf die Anwendung der Datenschutz-Grundverordnung unterstützen.

a) Zusammenarbeit mit den Mitgliedstaaten

Die Kommission wird ihre Zusammenarbeit mit den Mitgliedstaaten im Vorfeld des Inkrafttretens der DS-GVO im Mai 2018 fortsetzen. Ab Mai 2018 wird sie beobachten, wie die Mitgliedstaaten die neuen Vorschriften anwenden, und erforderlichenfalls geeignete Maßnahmen treffen.

b) Neue Online-Leitlinien in allen EU-Sprachen und Sensibilisierungsmaßnahmen

Die Kommission stellt praktische Anleitungen[48] zur Verfügung, um Unternehmen, insbesondere KMU, Behörden und der Öffentlichkeit dabei zu helfen, die neuen Datenschutzvorschriften einzuhalten und von ihnen zu profitieren.

Die Leitlinien werden in Form eines in allen EU-Sprachen verfügbaren praktischen Online-Informationsangebots bereitgestellt. Dieses Online-Angebot wird regelmäßig aktualisiert und soll drei Hauptzielgruppen ansprechen: Bürger, Unternehmen (insbesondere KMU) und andere Organisationen sowie öffentliche Verwaltungen. Zum bereitgestellten Material gehören Fragen und Antworten mit praktischen Beispielen und Links zu verschiedenen Informationsquellen (z. B. Artikel der Datenschutz-Grundverordnung; Leitlinien der Artikel 29-Datenschutzgruppe bzw. des Europäischen Datenschutzausschusses und Materialien, die auf nationaler Ebene entwickelt wurden).

Die Kommission wird ihr Online-Informationsangebot auf der Grundlage der eingegangenen Rückmeldungen und unter Berücksichtigung neuer Fragen, die sich aus der Umsetzung ergeben, regelmäßig aktualisieren.

Die Leitlinien werden durch gezielte Informationsmaßnahmen Unternehmen und Öffentlichkeit in allen Mitgliedstaaten verbreitet.

Da die Verordnung weitergehende individuelle Rechte vorsieht, wird die Kommission ferner Sensibilisierungsmaßnahmen durchführen und sich an Veranstaltungen in den Mitgliedstaaten beteiligen, um die Bürger über die Vorteile und Auswirkungen der Verordnung zu informieren.

c) Finanzielle Unterstützung für nationale Informations- und Sensibilisierungsmaßnahmen

Die Kommission unterstützt nationale Sensibilisierungs- und Informationsmaßnahmen mittels Finanzhilfen für interne Schulungen von Datenschutzbehörden, Verwaltungen, Angehörigen der Rechtsberufe und Datenschutzbeauftragten.[49]

Rund 1,7 Mio. EUR werden für sechs Begünstigte bereitgestellt, die mehr als die Hälfte der EU-Mitgliedstaaten abdecken. Die Finanzierung richtet sich an die lokalen Behörden, einschließlich ihrer Datenschutzbeauftragten, an die Datenschutzbeauftragten von Behörden und aus der Privatwirtschaft sowie an Richter und Rechtsanwälte. Die Finanzhilfen werden für die Ausarbeitung von Schulungsmaterial für Datenschutzbehörden, Datenschutzbeauftragte und andere Fachkräfte sowie für die Ausbildung von Ausbildern verwendet.

---

[48] Die Leitlinien werden zu einem besseren Verständnis der EU-Datenschutzvorschriften beitragen, aber nur der Text der Verordnung selbst ist rechtlich bindend. Folglich kann nur die Verordnung Rechte und Pflichten für den Einzelnen begründen.

[49] Finanzhilfen auf der Grundlage des Programms "Rechte und Unionsbürgerschaft“ 2016)https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/rec/calls/rec-data-2016.html#c,topics=callIdentifier/t/REC-DATA-2016/1/1/1/default-group&callStatus/t/Forthcoming/1/1/0/default-group&callStatus/t/Open/1/1/0/default-group&callStatus/t/Closed/1/1/0/default-group&+identifier/desc).

Die Kommission hat auch eine Aufforderung zur Einreichung von Vorschlägen speziell für die Zielgruppe der Datenschutzbehörden gerichtet. Die betreffende Schulungsinitiative wird mit einem Gesamtbudget von bis zu 2 Mio. EUR ausgestattet sein und die Datenschutzbehörde bei der Ansprache von Interessenträgern unterstützen.[50] Ziel ist es, die von den Datenschutzbehörden im Zeitraum 2018-2019 ergriffenen Maßnahmen zur Sensibilisierung der Unternehmen, insbesondere der KMU, und zur Beantwortung von Fragen zu 80 % mitzufinanzieren. Diese Mittel können auch zur Sensibilisierung der Öffentlichkeit eingesetzt werden.

d) Bewertung der Notwendigkeit, die Ermächtigungen der Kommission in Anspruch zu nehmen

Die Verordnung[51] berechtigt die Kommission zum Erlass von Durchführungsrechtsakten oder delegierten Rechtsakten, um die Umsetzung der neuen Vorschriften weiter zu unterstützen. Die Kommission wird diese Ermächtigungen nur dann in Anspruch nehmen, wenn ein eindeutiger Mehrwert nachgewiesen werden kann, und nachdem sie die Ansichten der Beteiligten eingeholt hat. Die Kommission wird sich insbesondere – gestützt auf eine Studie, die an externe Sachverständige in Auftrag gegeben wurde, sowie auf Beiträge und Gutachten der am Ende des Jahres 2017 eingesetzten Multi-Stakeholder-Gruppe zu diesem Thema – mit der Frage der Zertifizierung befassen. Die Arbeiten der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) im Bereich der Cybersicherheit werden in diesem Zusammenhang ebenfalls von Bedeutung sein.

e) Übernahme der Verordnung in das EWR-Abkommen

Die Kommission wird ihre Gespräche mit den drei EFTA-Staaten (Island, Liechtenstein und Norwegen) fortsetzen, um die DS-GVO in das EWR-Abkommen aufzunehmen.[52] Erst wenn die Übernahme der Verordnung in das EWR-Abkommen in Kraft getreten ist, können personenbezogene Daten zwischen EU- und EWR-Ländern in gleicher Weise ungehindert fließen wie zwischen den EU-Mitgliedstaaten.

f) Austritt des Vereinigten Königreichs aus der EU

Im Rahmen der Verhandlungen über ein Austrittsabkommen zwischen der EU und dem Vereinigten Königreich auf der Grundlage von Artikel 50 des Vertrags über die Europäische Union verfolgt die Kommission das Ziel, dass die am Tag vor dem Austritt geltenden Bestimmungen des Unionsrechts über den Schutz personenbezogener Daten auf im Vereinigten Königreich befindliche personenbezogene Daten, die vor dem Widerruf

---

[50] http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/rec/topics/rec-rdat-trai-ag-2017.html

[51] Delegierte Rechtsakte zur Bestimmung der Informationen, die durch Bildsymbole darzustellen sind, und der Verfahren für die Bereitstellung standardisierter Bildsymbole (Artikel 12 Absatz 8 DS-GVO); Delegierte Rechtsakte zur Festlegung der Anforderungen an datenschutzspezifische Zertifizierungsverfahren (Artikel 43 Absatz 8 DS-GVO); Durchführungsrechtsakte, mit denen technische Standards für Zertifizierungsverfahren und Datenschutzsiegel und -prüfzeichen sowie Mechanismen zur Förderung und Anerkennung dieser Zertifizierungsverfahren und Datenschutzsiegel und -prüfzeichen festgelegt werden (Artikel 43 Absatz 9 DS-GVO); Durchführungsrechtsakte zur Festlegung des Formats und der Verfahren für den Informationsaustausch über verbindliche interne Datenschutzvorschriften zwischen Verantwortlichen, Auftragsverarbeitern und Aufsichtsbehörden (Artikel 47 Absatz 3 DS-GVO); Durchführungsrechtsakte für Form und Verfahren der gegenseitigen Amtshilfe und für den elektronischen Informationsaustausch zwischen den Aufsichtsbehörden (Artikel 61 Absatz 9 und Artikel 67 DS-GVO).

[52] Zum Stand der Verhandlungen siehe http://www.efta.int/eea-lex/32016R0679.

verarbeitet wurden, weiterhin Anwendung finden.[53] Zum Beispiel sollten die betroffenen Personen weiterhin das Recht auf Information, auf Auskunft, auf Berichtigung, auf Löschung, auf Einschränkung der Verarbeitung, auf Datenübertragbarkeit sowie auf Widerspruch gegen die Verarbeitung und das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, nach Maßgabe der einschlägigen Bestimmungen des am Austrittsdatum geltenden Unionsrechts genießen. Die oben genannten personenbezogenen Daten sollten nicht länger aufbewahrt werden, als es für die Zwecke, für die die personenbezogenen Daten verarbeitet wurden, erforderlich ist.

Vorbehaltlich etwaiger Übergangsbestimmungen in einem etwaigen Austrittsabkommen gelten ab dem Austrittstermin für das Vereinigte Königreich die EU-Vorschriften für die Übermittlung personenbezogener Daten in Drittländer.[54]

g) Bestandsaufnahme im Mai 2019

Ab dem 25. Mai 2018 wird die Kommission die Anwendung der neuen Vorschriften genau verfolgen und bereit sein, Maßnahmen zu ergreifen, falls nennenswerte Probleme auftreten. Ein Jahr nach Inkrafttreten der Verordnung (2019) wird die Kommission eine Veranstaltung organisieren, um Bilanz über die Erfahrungen der verschiedenen Akteure bei ihrer Umsetzung zu ziehen. Dem wird sich ein Bericht anschließen, den die Kommission bis Mai 2020 zur Bewertung und Überprüfung der Datenschutz-Grundverordnung vorlegen muss. Im Mittelpunkt dieses Berichts werden insbesondere die internationale Datenübermittlung und die für die Arbeit der Datenschutzbehörden geltenden Bestimmungen über Zusammenarbeit und Kohärenz stehen.

Fazit

Am 25. Mai treten EU-weit neue einheitliche Datenschutzvorschriften in Kraft. Die neuen Datenschutzvorschriften werden für Einzelpersonen, Unternehmen, öffentliche Verwaltungen und andere Organisationen gleichermaßen erhebliche Verbesserungen bewirken. Sie bieten der EU zudem die Möglichkeit, im Bereich des Schutzes personenbezogener Daten weltweit eine Führungsrolle zu übernehmen. Die Reform kann jedoch nur erfolgreich sein, wenn alle Beteiligten ihre Verpflichtungen und Rechte wahrnehmen.

Seit der Verabschiedung der Verordnung im Mai 2016 hat die Kommission im Hinblick auf die Anwendung der neuen Vorschriften aktiv mit allen betroffenen Akteuren – Regierungen, nationalen Behörden, Unternehmen, Zivilgesellschaft – zusammengearbeitet. Es wurden erhebliche Anstrengungen unternommen, um eine umfassende Sensibilisierung und Vorbereitung zu gewährleisten, aber es bleibt noch einiges zu tun. Die Vorbereitungen in den Mitgliedstaaten und unter den verschiedenen Akteuren kommen unterschiedlich rasch voran. Darüber hinaus ist die Kenntnis der mit den neuen Vorschriften verbundenen Vorteile und Chancen nicht überall gleich ausgeprägt. Insbesondere bei KMU besteht weiterer Sensibilisierungs- und Unterstützungsbedarf im Hinblick auf erforderliche Anpassungen an die neuen Regeln.

---

[53] https://ec.europa.eu/commission/publications/position-paper-use-data-and-protection-information-obtained-or-processed-withdrawal-date_en

[54] Siehe die Bekanntmachung der Kommission zu den Folgen des Austritts des Vereinigten Königreichs aus der EU für die Datenschutzregeln (http://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=49245).

Die Kommission fordert daher alle betroffenen Akteure auf, ihre laufenden Arbeiten zu intensivieren, um die einheitliche Anwendung und Auslegung der neuen Vorschriften in der gesamten EU zu gewährleisten und Unternehmen und Bürger gleichermaßen zu sensibilisieren. Sie wird diese Bemühungen finanziell und administrativ unterstützen und zur Sensibilisierung der Öffentlichkeit beitragen, insbesondere durch die Einführung ihres Online-Informationsangebots.

Daten sind die wertvollste Ressource der heutigen Wirtschaft und aus unserem Alltag nicht mehr wegzudenken. Die neuen Vorschriften bieten sowohl den Unternehmen als auch der Öffentlichkeit eine einzigartige Chance. Die Unternehmen, insbesondere die kleineren Unternehmen, werden von einem innovationsfreundlichen einheitlichen Regelwerk profitieren und ihre Datenverarbeitung auf Vordermann bringen können, um das Vertrauen der Verbraucher wiederherzustellen und es in der gesamten EU als Wettbewerbsvorteil zu nutzen. Die Bürgerinnen und Bürger werden von dem besseren Schutz personenbezogener Daten profitieren und besser kontrollieren können, wie die Daten von den Unternehmen verarbeitet werden.

In einer modernen Welt mit einer florierenden digitalen Wirtschaft müssen die Europäische Union und ihre Bürger und Unternehmen dafür gerüstet sein, die Vorteile der Datenwirtschaft zu nutzen und ihre Konsequenzen zu begreifen. Die neue Verordnung enthält die erforderlichen Instrumente, um Europa fit für das 21. Jahrhundert zu machen.

Folgende weitere Maßnahmen sind vorgesehen:

Gegenüber den Mitgliedstaaten:

- Die Kommission wird weiter mit den Mitgliedstaaten zusammenarbeiten, um die Kohärenz bei der Anwendung der Verordnung zu fördern und die Fragmentierung zu begrenzen, wobei der Spielraum zu berücksichtigen ist, den die neuen Vorschriften den Mitgliedstaaten belassen.

- Nach Mai 2018 wird die Kommission die Anwendung der Verordnung in den Mitgliedstaaten aufmerksam beobachten und erforderlichenfalls geeignete Maßnahmen, einschließlich der Einleitung von Vertragsverletzungsverfahren, ergreifen.

Gegenüber den Datenschutzbehörden:

- Bis Mai 2018 wird die Kommission die Arbeit der Datenschutzbehörden im Rahmen der Artikel 29-Datenschutzgruppe und beim Übergang zum künftigen Europäischen Datenschutzausschuss unterstützen. Ab Mai 2018 wird sie ihren Beitrag zu den Arbeiten des Europäischen Datenschutzausschusses leisten.

- 2018-2019 wird die Kommission Sensibilisierungsmaßnahmen von Datenschutzbehörden auf nationaler Ebene (ab Mitte 2018 durchgeführte Projekte) mit insgesamt bis zu 2 Mio. EUR kofinanzieren.

Gegenüber den Interessenträgern:

- Die Kommission wird ein Online-Instrument zur praktischen Anleitung auf den Weg bringen, das Fragen und Antworten für Bürger, Unternehmen und Verwaltungen enthält. Die Kommission beabsichtigt, diese Leitlinien durch gezielte

Informationskampagnen für die Unternehmen und die Öffentlichkeit im Vorfeld bis Mai 2018 und auch danach besser bekannt zu machen.

- 2018 und darüber hinaus wird die Kommission aktiv mit den Beteiligten insbesondere im Rahmen der Multi-Stakeholder-Gruppe zusammenarbeiten, um ihre Rückmeldungen zur Umsetzung der Datenschutz-Grundverordnung und zum Bekanntheitsgrad der neuen Regeln einzuholen.

Gegenüber sämtlichen Akteure:

- Im Zeitraum 2018-2019 wird die Kommission prüfen, ob es notwendig ist, von ihrer Befugnis Gebrauch zu machen, delegierte Rechtsakte oder Durchführungsrechtsakte zu erlassen.

- Im Mai 2019 wird die Kommission die Verordnungspraxis einer Bestandsaufnahme unterziehen. 2020 wird sie einen Bericht über die Anwendung der neuen Vorschriften vorlegen.