Zentren für
Kommunikation und
Informationsverarbeitung e.V.

Geschäftsstelle | c/o Freie Universität Berlin | Fabeckstraße 32 | 14195 Berlin

ZKI-Geschäftsstelle
c/o Freie Universität Berlin
Fabeckstraße 32
14195 Berlin

Tel.: 0049 30-2062262 0
Fax: 0049 30-2062262 98
geschaeftsstelle@zki.de

Ihr Ansprechpartner:
Torsten Prill
torsten.prill@zki.de

Autoren:
Johannes Nehlsen
Gernot Kirchner
Karola Möhring

European Commission

via Upload

07. February 2024

Stellungnahme des Vereins der „Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e.V. (ZKI)“ zur zweiten Evaluation der Datenschutz-Grundverordnung (DSGVO)

Einführung

Die Datenschutz-Grundverordnung (DSGVO) ist am 24. Mai 2016 in Kraft getreten und seit dem 25. Mai 2018 in allen Mitgliedstaaten der EU und aufgrund des Beschlusses des gemeinsamen EWR-Ausschusses vom 6. Juli 2018 auch in den EWR-Staaten verbindlich anwendbares Recht. Mit der DSGVO wurde das Datenschutzrecht in Europa vereinheitlicht und erlangte aufgrund des in der DSGVO vorgesehenen Marktortprinzips Strahlkraft über die Grenzen von Europa hinaus. Sie ist ein wichtiger Meilenstein beim Schutz personenbezogener Daten und soll harmonisierte Grundsätze für den Datenschutz festlegen sowie den freien Verkehr personenbezogener Daten im Binnenmarkt – insofern wird Art. 1 Abs. 1 a.E., Abs. 3 DSGVO gerne übersehen – gestalten. Auch wenn die DSGVO damit innerhalb von Europa das wichtigste Regelwerk für den Datenschutz und unmittelbar gültig und verbindlich ist, ist sie aufgrund zahlreicher Öffnungsklauseln nicht allein maßgeblich. Zum Teil ergänzen nationale Regelungen die DSGVO. Hinzu treten mitunter divergierende Rechtsauffassungen der jeweils zuständigen Aufsichtsbehörden, mit zum Teil ebenfalls auseinanderfallender Jurisprudenz, die es vor dem EuGH im Rahmen von Vorabentscheidungsverfahren wieder einzufangen und zu vereinheitlichen gilt. Durch geringfügige Anpassungen könnte zudem eine erhebliche bürokratische Entlastung ohne Abstriche beim Schutz der betroffenen natürlichen Personen erreicht werden.

Bankverbindung: DKB AG Berlin
Bankleitzahl: 120 300 00
Kontonummer: 2068120

IBAN: DE73 1203 0000 0002 0681 20
SWIFT BIC: BYLADEM1001

eingetragen im Vereinsregister
Berlin-Charlottenburg
Nr. 14209 Nz.

Vorstand: Torsten Prill (Vorsitzender, Finanzvorstand)
Dr. Inga Scheler (stellv. Vorsitzende)
Prof. Dr. Gudrun Oevel (stellv. Vorsitzende)
Dr. Rainer Bockholt
Daniel Bündgens
Dr. Karl Molter

ZKI e.V. als Vereinigung von IT-Zentren

Der Verein „Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e.V. (ZKI)“, als Vereinigung der IT-Zentren der Hochschulen, Universitäten und Forschungseinrichtungen in der Bundesrepublik Deutschland, widmet sich den für Hochschulen und Forschungseinrichtungen relevanten IT-Themen. Datenschutz ist ein omnipräsentes und komplexes Thema, das rechtliche, technische und anwendungsorientierte Belange vereint und vor allem Rechtssicherheit erfordert, um Wissenschaft und Forschung im Sinne des Schutzes personenbezogener Daten angemessen zu unterstützen und nicht unverhältnismäßig zu behindern.

Deutsche Hochschulen, Universitäten und Forschungseinrichtungen unter Zugzwang

Deutsche Hochschulen, Universitäten und Forschungseinrichtungen sind in zweifacher Hinsicht von der DSGVO betroffen, zum einen als wissenschaftliche Einrichtungen und zum anderen auch als Verwaltungseinrichtungen. Der Schutz personenbezogener Daten ist zu Recht als Grundrecht der Europäischen Union (Art. 8 Charta der Grundrechte der Europäischen Union – GRCh / Art. 16 Abs. 1 Vertrag über die Arbeitsweise der Europäischen Union – AEUV) ausgestaltet und ein von allen Verantwortlichen zu achtendes hohes Gut. In der Praxis geraten deutsche Hochschulen, Universitäten und Forschungseinrichtungen aber zunehmend unter permanenten Zugzwang, indem bspw. aufwändige Prüfprozesse vor der Einführung digitaler Tools eingehalten werden und regelmäßig neue und zum Teil divergierende Entscheidungen der Aufsichtsbehörden und Gerichte zu berücksichtigen sind. Dies führt zunehmend zu mangelnder Planbarkeit und Verlässlichkeit und schafft Rechtsunsicherheit.

Unwägbarkeiten im internationalen Datentransfer

Forschung und Lehre finden weltweit statt und sind stark internationalisiert. Für die Forschung wurde zwar eine Öffnungsklausel sowie verschiedene Privilegierungstatbestände geschaffen, diese lässt jedoch die Verpflichtungen aus Kapitel V der DSGVO unberührt.

Die wenigen bestehenden Angemessenheitsbeschlüsse der EU-Kommission decken den Bereich Forschung und Lehre häufig nicht ab. Diese Einschränkung gilt insbesondere für forschungsstarke Länder wie die Vereinigten Staaten von Amerika und Japan, da beispielweise das EU-US Data Privacy Framework nur Organisationen unter der Aufsicht der FTC (Federal Trade Commission) bzw. des DOT (Department of Transportation) erfasst und damit grundsätzlich keine öffentlichen Universitäten. Es wäre daher zu begrüßen, wenn die EU-Kommission spezifische Standarddatenschutzklauseln für Lehr- und Forschungskooperationen entwickelt bzw. deren Entwicklung anregt. Ergänzend sollte auch Forschung zur Lösung von Regelungskonflikten zwischen dem Datenschutzrecht von Drittstaaten und dem Europäischen Wirtschaftsraum initiiert werden.

Im Hinblick auf Art. 48 DSGVO, der die Übermittlung personenbezogener Daten beispielsweise an ausländische Sicherheitsbehörden erlaubt, steht der Abschluss weiterer internationaler Übereinkünfte wie etwa Rechtshilfeabkommen weiterhin aus. Bestehende Rechtshilfeabkommen sind regelmäßig komplex ausgestaltet, erfassen aber nur zum Teil ausdrücklich die Übermittlung personenbezogener Daten. Zudem lässt Art. 48 DSGVO offen, ob und in welchem Umfang der Ersuchte zu prüfen hat, inwiefern im ersuchenden Drittland ein angemessenes Schutzniveau vorhanden ist. Insbesondere im Hinblick auf die

Rechtsprechung des EuGH, z.B. die Entscheidung „Schrems II“ (Urteil v. 16. Juli 2020 – C-311/18), und die Kritik an ausländischen Sicherheitsgesetzen und fehlenden Rechtsschutzmöglichkeiten für betroffene natürliche Personen ist eine Weiterentwicklung erforderlich.

Verbesserungspotentiale

Herstellerverantwortung

Im Hinblick auf die Weiterentwicklung der DSGVO sollten neben den (gemeinsamen) Verantwortlichen und Auftragsverarbeitern auch die Hersteller Pflichten aus der DSGVO erfüllen müssen, insbesondere im Hinblick auf die Art. 24, 25 und 32 DSGVO sowie für die datenschutzrechtliche Bewertung gemäß Klausel 14 des Anhangs zum Beschluss der EU-Kommission vom 4. Juni 2021/914. Die Erfüllung dieser Anforderungen sollte dann auch für die Rechenschaftspflicht der Verantwortlichen ausreichend sein, gerade auch vor dem Hintergrund der Einführung neuer Technologien (bspw. KI-Anwendungen). Letztere werden in Zukunft zunehmend und mitunter ausschließlich als SaaS-Angebote am Markt verfügbar sein und entziehen sich damit der Einflussnahme der Einrichtungen, so dass anzuregen ist, die datenschutzrechtlichen Verantwortlichkeiten zum Teil auf die Hersteller derartiger Angebote zu verlagern und durchsetzbare Pflichten diesen gegenüber auszugestalten. Bspw. Art. 25 DSGVO könnte hierfür angepasst und im Sinne einer Herstellverantwortlichkeit in Anlehnung an das EU-Produkthaftungsrecht ausgestaltet werden. Hersteller, welche kommerziell Produkte zur Verarbeitung personenbezogener Daten auf dem europäischen Binnenmarkt anbieten, müssen, sofern sie die Mittel und Zwecke der Datenverarbeitung für spätere Anwender unabänderlich und losgelöst vom konkreten Einsatzzweck festlegen, selbständig in die Verantwortung genommen werden können. Wegweisende Ansatzpunkte hierfür bietet bspw. der Cyber Resilience Act betreffend die Cybersicherheit, dessen Erwägungen ebenfalls für eine Novellierung der DSGVO Früchte tragen könnten.

In der DSGVO sollte eine ausdrückliche Rechtsgrundlage für aufsichtsbehördliche Produktwarnungen geschaffen und die Art. 57 Abs. 1 lit. b) i.V.m. Art. 58 Abs. 3 lit. b) DSGVO entsprechend konkretisiert werden, ob und in welchem Rahmen Aufsichtsbehörden vor nicht datenschutzkonformen Produkten warnen dürfen und welche Konsequenzen damit für Verantwortliche und Hersteller verbunden sind.

Diensteanbieterverantwortung

Der Anwendungsbereich der DSGVO ist für Anbieter, die den Verpflichtungen der ePrivacy-Richtlinie (Richtlinie 2002/58/EG) unterliegen, weiterhin aufgrund von Art. 95 DSGVO eingeschränkt. Diese gelten zudem regelmäßig insbesondere aufgrund der Vertraulichkeitspflicht der ePrivacy-Richtlinie (Art. 5 ePrivacy-Richtlinie / § 3 TTDSG – Fernmeldegeheimnis) als berechtigte Empfänger. Die mit Inkrafttreten der DSGVO vorgesehene Änderung und Überprüfung der ePrivacy-Richtlinie, um die Kohärenz mit der DSGVO zu gewährleisten (173. Erwägungsgrund), steht weiterhin aus und sollte zeitnah mit dem Abschluss der Verhandlungen zur und einer Inkraftsetzung der ePrivacy-Verordnung vollzogen werden. Im Zuge dessen könnte bspw. auch über eine neue, über das Vertraulichkeitsgebot des Datenschutzes hinausgehende Verpflichtung z.B. für Anbieter von Cloud-Diensten, Social-Media-Diensten oder Torwächtern („Gatekeeper“ im Verständnis des Digital Markets Acts) nachgedacht werden. Insbesondere sollte im Rahmen einer Novellierung der DSGVO im Rahmen von Art. 26, 28 DSGVO eine klare Abgrenzung erfolgen, unter welchen Voraussetzungen von einer gemeinsamen Verantwortlichkeit, einer Auftragsverarbeitung

oder einer getrennten alleinigen Verantwortlichkeit im Verhältnis zu Diensteanbietern im Sinne der ePrivacy-Richtlinie bzw. ePrivacy-Verordnung ausgegangen werden muss. Rechtsunsicherheiten und Abgrenzungsschwierigkeiten bestehen derzeit beispielsweise bei der Nutzung von cloudbasierten Videokonferenzdiensten, welche mitunter verbundene Dienstleistungen (bspw. Aufzeichnungen, Upload-Funktionen etc.) anbieten, welche über das reine Anbieten einer Telekommunikationsdienstleistung hinausgehen.

Reduktion von Umsetzungsaufwänden

Der Umsetzungsaufwand für die Verantwortlichen könnte ohne Einschränkungen für die betroffenen natürlichen Personen bspw. durch folgende Maßnahmen reduziert werden:

- Die Anonymisierung von personenbezogenen Daten sowie die damit verbundenen Vorkehrungen sollten in der DSGVO geregelt werden. Insbesondere sollte eine eindeutige Positionierung zum relativen oder absoluten Personenbezug von Daten getroffen und klargestellt werden, ob und in welcher Form nach der erfolgten Anonymisierung auch zukünftig noch Prüfpflichten im Rahmen einer Risikobewertung ausgelöst werden können, insbesondere wenn nicht ausgeschlossen werden kann, dass bspw. mittels neuer Technologien die Anonymisierung später aufgehoben werden könnte. Die DSGVO sollte zugleich ein ausdrückliches Verbot beinhalten, den Versuch zu unternehmen, eine Anonymisierung wieder aufzuheben.
- Der Inhalt der Auftragsverarbeitungsverträge sollte gesetzlich geregelt und nur die Anlagen Gegenstand der Vereinbarung zwischen Verantwortlichen und Auftragsverarbeitern sein. Art. 28 Abs. 7 DSGVO könnte entsprechend angepasst und die Standardvertragsklauseln der Kommission als verbindlich vorgesehen werden. In Bayern ist dies für den behördlichen Bereich durch Art. 38 BayDiG bereits umgesetzt, weitere gegebenenfalls auch auseinanderfallende nationale Regelungen drohen, wenn in der DSGVO keine dahingehende Harmonisierung vorgesehen wird.
- Im Falle einer gemeinsamen Verantwortlichkeit sollte auf die gesetzlich zwingende Notwendigkeit einer Vereinbarung nach Art. 26 DSGVO verzichtet werden. Verantwortliche sind bereits aus eigenem Interesse und wegen der drohenden gesamtschuldnerischen Haftung (Art. 82 Abs. 4 DSGVO) in der Praxis daran interessiert, entsprechende Vereinbarungen zur Abgrenzung der internen Verantwortlichkeiten zu schließen. Es besteht in diesem Fall auch ohne interne vertragliche Regelung eine gemeinsame Verantwortlichkeit der Verantwortlichen gegenüber den Betroffenen. Anstelle des zwingenden Vertragsabschlusses sollte Art. 26 DSGVO analog zum derzeitigen Art. 28 Abs. 7 DSGVO ergänzt und die Möglichkeit für die Kommission geschaffen werden, (unverbindliche) Standardvertragsklauseln betreffend die gemeinsame Verantwortlichkeit zu erlassen. Art. 26 Abs. 2 S. 2 DSGVO sollte gestrichen und die Informationspflichten gemäß Art. 13, 14 DSGVO um konkret offenzulegende Informationen betreffend die gemeinsame Verantwortlichkeit ergänzt werden.
- Anlagen mit Musterdokumenten zur DSGVO, bspw. betreffend die Dokumentationspflichten aus Art. 5, 12-14, 24, 25, 30 und 32 DSGVO, wobei zwischen einem öffentlichen und einem nicht öffentlichen Teil differenziert werden sollte. Ein weiteres offizielles Musterdokument könnte für die Durchführung einer Datenschutzfolgenabschätzung gemäß Art. 35 DSGVO sowie für die Durchführung eines Transfer Impact Assessment (TIA) im Rahmen der Art. 44 ff. DSGVO erstellt und

veröffentlicht werden. Allgemeingültige Muster könnten sowohl die Datenqualität der Dokumentation erhöhen und damit auch den Prüfaufwand für Aufsichtsbehörden reduzieren als auch die Verantwortlichen spürbar entlasten.

- Die Einführung von standardisierten Bildsymbolen für betroffene Personen gemäß Art. 12 Abs. 7, 8 DSGVO sollte weiter vorangetrieben und abgeschlossen werden. Insbesondere sollte die Möglichkeit der Nutzung von standardisierten Bildsymbolen nicht nur auf die Art. 13, 14 DSGVO beschränkt werden, sondern auch in anderen Bereichen (bspw. Art. 34, 44 ff. DSGVO) Anwendung finden können.
- Mit einer Mustereinwilligung ähnlich der Muster-Widerrufsbelehrung im Sinne von Anhang I zur Richtlinie 2011/83/EU (Verbraucherrechte-Richtlinie) könnte Rechtssicherheit insbesondere auch betreffend die Frage der zur Verfügung zu stellenden Mindestinformationen innerhalb der Einwilligung erzielt werden. Letzteres gilt entsprechend für eine Musterwiderspruchsbelehrung im Sinne von Art. 21 Abs. 4 DSGVO.
- Mit klaren gesetzlichen Vorgaben zur Fristberechnung könnten Verantwortliche wesentlich entlastet werden, bspw. betreffend die konkrete Anwendung der Verordnung (EWG, Euratom) Nr. 1182/71 des Rates vom 3. Juni 1971 zur Festlegung der Regeln für die Fristen, Daten und Termine in Bezug auf die Meldepflicht aus Art. 33 DSGVO.
- In Art. 13, 14 DSGVO sollte klargestellt werden, dass es nicht darauf ankommt, dass die Daten unmittelbar bei der betroffenen Person erhoben werden oder nicht, sondern dass entscheidend ist, ob die betroffene Person von der Datenerhebung Kenntnis erhält. Zumindest sollte geprüft werden, ob die Ausnahmetatbestände des Art. 14 Abs. 5 DSGVO auch in Art. 13 Abs. 4 DSGVO verankert werden können.
- In Art. 33 DSGVO sollte klargestellt werden, dass nicht jedes Risiko für die Rechte und Freiheiten natürlicher Personen eine Meldepflicht gegenüber der Aufsichtsbehörde auslöst, da sich im Rahmen einer Negativprüfung Risiken bei der Verletzung des Schutzes personenbezogener Daten regelmäßig nicht gänzlich ausschließen lassen. In der Praxis führen derartige Meldung aber kaum zu einer Verbesserung des Schutzes personenbezogener Daten, sondern in einer Vielzahl von Fällen lediglich zu einer bürokratischen Mehrbelastung für die Verantwortlichen, welche von der eigentlichen operativen Auseinandersetzung mit der Verletzung und dem Ergreifen geeigneter Schutzmaßnahmen abhalten, diese zumindest auch verzögern kann.
- Die Möglichkeit der Zuständigkeit einer federführenden Aufsichtsbehörde sollte nicht auf grenzüberschreitende Verarbeitungsvorgänge gemäß Art. 56 DSGVO beschränkt bleiben, sondern auch auf nationale Verarbeitungsvorgänge Anwendung finden. Letzteres gilt insbesondere in dem für deutsche Hochschulen, Universitäten und Forschungseinrichtungen bedeutsamen Bereich der gemeinsamen Verantwortlichkeit im Sinne von Art. 26 DSGVO, im Rahmen derer die verbindliche Benennung einer federführenden Aufsichtsbehörde ermöglicht werden sollte.

Datennutzung durch die Aufsichtsbehörden für Verantwortliche

Die Aufsichtsbehörden erhalten viele Daten von den für die Verarbeitung Verantwortlichen und den Auftragsverarbeitern, stellen diese aber nur selten der Öffentlichkeit zur Verfügung. Es wäre z. B. wertvoll,

die Maßnahmen der für die Verarbeitung Verantwortlichen zu kennen, die sich nach einem Datenschutzvorfall als wirksam für den Schutz der betroffenen Personen erwiesen haben, sofern und soweit keine berechtigten Geheimhaltungsinteressen der betroffenen Verantwortlichen entgegenstehen. Art. 59 DSGVO sollte verbindliche Vorgaben für die Erstellung des Jahresberichtes der Aufsichtsbehörden beinhalten, so dass auch eine Vergleichbarkeit mit anderen Berichten sichergestellt ist.

Darüber hinaus werden viele Entscheidungen von den Aufsichtsbehörden getroffen. Diese werden jedoch in der Regel nicht veröffentlicht und stehen damit anderen Verantwortlichen, welche gegebenenfalls gleichgelagerte Verarbeitungstätigkeiten planen oder durchführen, nicht zur Verfügung. Anders verhält es sich mit den vom Europäischen Datenschutzausschuss veröffentlichten Datenschutzentscheidungen, die bereits zu ersten wertvollen Forschungsergebnissen geführt haben und den Verantwortlichen wie den Auftragsverarbeitern Orientierung bieten. Dies sollte auch auf nationaler Ebene fortgesetzt und aufsichtsbehördliche Entscheidungen anonymisiert veröffentlicht werden. Unterstützen könnte hierbei eine verpflichtende Transparenzregelung für aufsichtsbehördliches Handeln, welches beispielsweise das Vorhalten einer Transparenzplattform mit veröffentlichungspflichtigen Informationen und anonymisierten Entscheidungen vorsieht.

Harmonisierung für mehr Rechtssicherheit

Die DSGVO enthält eine Vielzahl von Öffnungsklauseln, die es ermöglichen, in bestimmten Bereichen nationale Gesetzgebungsspielräume zu nutzen. So kann ein EU-Mitgliedstaat die DSGVO milder, ein anderer dagegen strenger ausgestalten. Dies kann zu einer Benachteiligung derjenigen führen, die sich an die strengeren Vorschriften im Rahmen der Öffnungsklauseln der DSGVO halten müssen. Dies kann einer Harmonisierung entgegenstehen und zu Wettbewerbsverzerrungen führen. Vor diesem Hintergrund sollte bei einer Novellierung der DSGVO geprüft werden, inwiefern Öffnungsklauseln weiter reduziert, die zugrunde liegenden Regelungsbereiche verpflichtend in der DSGVO ausgestaltet und damit eine einheitliche Anwendung der DSGVO sichergestellt werden können.

Das deutsche System der Datenschutzaufsicht ist durch zum Teil unterschiedliche Rechtsauffassungen und dementsprechend heterogene Maßnahmen in den einzelnen Bundesländern und dem Bund gekennzeichnet, da im föderalen System der Bundesrepublik Deutschland die Aufsicht auf die einzelnen Bundesländer und den Bund (18 Datenschutzaufsichtsbehörden ohne Kirchen und Medien) verteilt ist. Die anderen EU-Mitgliedstaaten zeichnen sich dagegen durch eine einheitliche und zentrale Datenschutzaufsicht aus. Insofern stellt Deutschland in Europa eine Besonderheit dar. Dies erleichtert zwar den Zugang zu den lokalen Datenschutzbehörden und erlaubt es landesspezifische Besonderheiten in der Rechtsanwendung zu berücksichtigen, kann aber im Ergebnis die effektive Durchsetzung eines am Schutz der personenbezogenen Daten der betroffenen Personen orientierten Datenschutzes schwächen und zu einer unterschiedlichen Anwendungspraxis des eigentlich harmonisierten Regelwerks führen. Grundlegendes Ziel der DSGVO ist die Harmonisierung zwischen den EU-Ländern, um ein einheitliches Datenschutzrecht im EU-Raum zu schaffen und gleichzeitig die Rechtsposition der betroffenen Personen zu stärken. Die DSGVO sollte entsprechend zur Mitgliedschaft im Europäischen Datenschutzausschuss (vgl. Art. 68 Abs. 4 DSGVO) Regelungen vorsehen, die trotz eines föderal gestalteten Aufsichtssystems eine einheitliche nationale Rechtsanwendungspraxis schafft, sofern und soweit in einem Mitgliedstaat mehr als eine Aufsichtsbehörde für die Überwachung der Anwendung der Datenschutzvorschriften zuständig ist.

Zentren für
Kommunikation und
Informationsverarbeitung e.V.

Zusammenfassung

Das erklärte Ziel der DSGVO, die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten zu schützen (Art. 1 Abs. 1, 2 DSGVO), wurde grundsätzlich unter Zugrundelegung des Verständnisses von Art. 8 GRCh und Art. 16 Abs. 1 AEUV erreicht. Das in Deutschland vom BVerfG geprägt Verständnis vom Schutz personenbezogener Daten als Ausprägung des Allgemeinen Persönlichkeitsrechtes und damit als in praktische Konkordanz zu anderen Grundrechten zu setzendes Grundrecht findet sich darin jedoch nur begrenzt wieder, was insbesondere in der Praxis dazu führte, dass Dinge aufgrund des vermeintlich abwägungsresistenten Datenschutzgrundrechtes nicht getan werden. Datenschutz muss und soll jedoch gerade nicht zu einer Verhinderungskultur beitragen, sondern dazu führen, dass Dinge richtig gemacht werden.

Vor diesem Hintergrund darf insbesondere auch das zweite erklärte Ziel der DSGVO nicht aus dem Fokus gerückt werden, namentlich der freie Verkehr personenbezogener Daten in der Europäischen Union, welcher aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden darf (Art. 1 Abs. 3 DSGVO). Misst man den Erfolg der DSGVO allein an diesem Zielmaßstab, dann müsste die eingangs formulierte Aussage relativiert werden, auch wenn man aus Sicht der deutschen Hochschulen, Universitäten und Forschungseinrichtungen an manches instituts- und die Grenzen eines Mitgliedstaats überschreitendes Forschungsprojekt denkt, welches aufgrund von zu einseitig verstandenen Datenschutzbedenken und damit einhergehender Rechtsunsicherheit bei der praktischen Anwendung der DSGVO gar nicht erst weiterverfolgt worden ist.

Rechtsunsicherheiten und widersprüchliche Auslegungen der Datenschutzvorschriften innerhalb Europas und zwischen den Aufsichtsbehörden sollten durch eine verbesserte Vollzugspraxis und Harmonisierung sowohl im geschriebenen Recht als auch in der Rechtsanwendung ausgeglichen werden. Kohärenz und Rechtsangleichung auch auf nationaler Ebene durch Abbau der Öffnungsklauseln sollten daher neben dem Bürokratieabbau oberste Priorität bei der aktuellen Evaluierung der DSGVO haben.

Der ZKI als Vereinigung der IT-Zentren der Hochschulen, Universitäten und Forschungseinrichtungen in der Bundesrepublik Deutschland begrüßt eine weiterführende Harmonisierung, um mehr Rechtssicherheit zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr personenbezogener Daten zu schaffen.