Datenschutzrechtlicher Handlungsbedarf 2016 für die deutsche Politik nach Verabschiedung der EU-DSGVO

Eine Empfehlung des Netzwerks Datenschutzexpertise

Stand: 9.5.2106

Ute Bernhardt
Elchdamm 56a, 13503 Berlin
030/280 466 95
bernhardt@netzwerk-datenschutzexpertise.de

Karin Schuler
Kronprinzenstr. 76, 53173 Bonn
0228/24 20 733
schuler@netzwerk-datenschutzexpertise.de

Ingo Ruhmann
Elchdamm 56a, 13503 Berlin
030/280 466 95
ruhmann@netzwerk-datenschutzexpertise.de

Dr. Thilo Weichert
Waisenhofstraße 41, 24103 Kiel
0431/971 97 42
weichert@netzwerk-datenschutzexpertise.de

www.netzwerk-datenschutzexpertise.de

Nach der Beschlussfassung über die Datenschutz-Grundverordnung (EU-DSGVO) durch den europäischen Gesetzgeber im April 2016 und nach deren Veröffentlichung im Amtsblatt der Europäischen Union (EU) (ABl. L 119/1 v. 04.05.2016) sind die Gesetzgeber der EU-Mitgliedstaaten aufgefordert, bis zum Inkrafttreten der EU-DSGVO am 25.05.2018 das geltende **nationale Datenschutzrecht** an die Vorgaben der Verordnung anzupassen.

Dies erfordert zunächst, diejenigen nationalen Regelungen, die durch die Normen der EU-DSGVO ersetzt werden, zum Zeitpunkt des Inkrafttretens 2018 **aufzuheben**. Nur so können Anwender sicher sein, in welchen Fällen das bisherige nationale Recht weiterhin Geltung hat und wann europäisches Recht anzuwenden ist.

Abschließende Regelungen finden wir in der EU-DSGVO im materiellen Recht, bei den Betroffenenrechten und insbesondere im Hinblick auf die staatliche Datenschutzaufsicht mit dem Kohärenzverfahren sowie im Bereich des Rechtsschutzes.

Hinsichtlich vieler materieller Regelungen, den Ausnahmen zu den Betroffenenrechten oder dem technisch-organisatorischen Datenschutz hat der EU-Gesetzgeber den nationalen Gesetzgebern die Möglichkeit eröffnet, bestehende **konkretisierende Normen** zu bewahren oder neue Regelungen zu erlassen, die sich im europarechtlichen Rahmen bewegen. Dies bedeutet z. B., dass im öffentlichen Bereich die in der Praxis bewährten bereichsspezifischen Regeln im deutschen Datenschutzrecht weitgehend beibehalten werden können und im Interesse der Kontinuität und der Rechtssicherheit auch beibehalten werden sollten.

Die vielfältigen **Öffnungsregelungen** für die nationalen Gesetzgeber sind nicht nur auf die Beseitigung bisheriger Regelungsdefizite beschränkt. Vielmehr besteht jetzt ein verbindlicher europäischer Rahmen, innerhalb dessen die deutsche Politik darüber hinaus grundrechts- und wirtschaftsstärkend tätig werden kann.

Es gibt nach wie vor Bereiche des deutschen Rechts mit **regulativen Defiziten,** die durch die EU-DSGVO nicht beseitigt wurden.

Dies ist der Fall beim unaufgelösten Konflikt zwischen **Berufsgeheimnissen und datenschutzrechtlich zulässigen Dienstleistungen im Auftrag, die insbesondere durch informationstechnische Dienstleister erbracht werden**. IT-Dienstleister, die z. B. Anwalts- oder Arztpraxissysteme administrieren oder hochkomplexe IT-Systeme in Krankenhäusern oder medizinischen Laboren verwalten, genießen nicht den in der Strafprozessordnung gesicherten Vertraulichkeitsschutz und unterliegen nicht der straf- und standesrechtlichen Schweigepflicht. Daher dürfte ein Berufsgeheimnisträger diesem Personenkreis nach dem derzeit geltenden Recht keinen Zugang zu Patienten- oder Klientendaten gewähren. Ist der Arzt oder Anwalt nicht selbst IT-fachkundig oder stellt einen IT-fachkundigen Gehilfen ein, ist eine fachkundige und datenschutzkonforme Pflege seiner informationstechnischen Systeme schlicht nicht möglich. Berufsgeheimnisträger stehen also vor der Alternative, sich entweder rechtswidrig zu verhalten oder ihre Aufgaben nicht ordnungsgemäß erledigen zu können. Der Gesetzgeber ist schon seit langem aufgefordert, die für die Pflege informationstechnischer Verfahren erforderlichen Offenbarungen zu erlauben und zugleich die Dienstleister rechtlich in den Kreis der Schweigeberechtigten und -verpflichteten einzubeziehen.

Ein ähnlicher Konflikt besteht im Bereich der **wissenschaftlichen Forschung**. Deren Zugang zu personenbezogenen Daten ist vielfach legitim und wünschenswert, etwa wenn im Gesundheitsbereich gesellschaftlich relevante Erkenntnisse erzielt werden. Doch kann und darf im Interesse des Persönlichkeitsschutzes der Betroffenen dieser Zugang nur zugestanden werden, wenn diese Daten einer strengen Zweckbindung – auch gegenüber Polizei und Staatsanwaltschaft – unterworfen werden. Eine derartige Zweckbindung gilt derzeit für die meisten Forschenden nicht. Durch ein gesetzliches Forschungsgeheimnis könnten die von der EU-DSGVO geforderten angemessenen Garantien begründet werden.

In einer gesonderten Ausarbeitung hat das Netzwerk Datenschutzexpertise dargelegt, wie die EU-DSGVO den nationalen Gesetzgebern einen Regelungsrahmen zum Erlass eines **Beschäftigtendatenschutzgesetzes** lässt und wie dieser ausgefüllt werden sollte. Ein solches Gesetz wird in Deutschland von der Politik seit über 30 Jahren angekündigt, ohne dass dies jemals umgesetzt wurde. Inzwischen sind sich alle Expertinnen und Experten, insbesondere auch aus den Reihen der Arbeitgeber- und Arbeitnehmerschaft, darüber einig, dass die technologischen Entwicklungen in Richtung Wirtschaft 4.0 nur mit rechtssicheren Regelungen zum Beschäftigtendatenschutz gesellschaftliche Akzeptanz finden werden. Das Netzwerk Datenschutzexpertise hat zu dessen Gestaltung detaillierte Vorschläge gemacht.[1]

Die beispielhaft erwähnten rechtlichen Defizite sind seit Jahrzehnten bekannt, ohne dass sie von der Gesetzgebung behoben wurden. Durch diese Untätigkeit werden Beteiligte in rechtlicher Unsicherheit gehalten und in wissenschaftlichen, wirtschaftlichen und gemeinschaftsförderlichen Aktivitäten behindert. Im Ergebnis wird die Innovationskraft des **Wirtschafts- und Forschungsstandorts Deutschland** beeinträchtigt.

Über die Beseitigung von Regelungslücken hinaus ermöglicht die EU-DSGVO dem nationalen Gesetzgeber, innovativ zu agieren und dadurch den **digitalen Grundrechtsschutz voranzubringen**. So ist es möglich, in den mit Öffnungsklauseln versehenen Bereichen nationale Regelungen zu erlassen, die nicht nur anderen Mitgliedstaaten, sondern auch dem europäischen Normgeber als Vorbild dienen können. Innovationsbedarf besteht aber nicht nur hier, sondern in weiteren Bereichen der personenbezogenen Datenverarbeitung, die im Folgenden beispielhaft aufgeführt werden.

Deutschland hat wohl weltweit die größten Erfahrungen im Bereich der datenschutzrechtlichen **Zertifizierung und Auditierung**. Dies hat die Politik bisher nur in geringem Maße dazu veranlasst, diesen Bereich zu fördern und weiterzuentwickeln. In der EU-DSGVO sind nun entsprechende Instrumente rechtlich verankert (Art. 42, 43). Durch eine aktive Politik – etwa durch die staatliche Förderung von Zertifizierungsverfahren – kann die Entwicklung datenschutzfreundlicher Techniken und Verfahren im Interesse von Datenschutz und Wirtschaft vorangebracht werden, was die Stellung des deutschen Datenschutzes auf dem europäischen und dem globalen Markt stärken würde.

In Art. 22 der EU-DSGVO wird im Interesse der Wahrung digitaler Freiheiten und digitaler Souveränität der Einsatz von Profiling-, Scoring- und sonstigen, heute oft mit dem Modebegriff „**Big-Data"Analysen belegten Anwendungen** zur Vorbereitung automatisierter Einzelentscheidungen von der Ergreifung „angemessener Maßnahmen" abhängig gemacht. Durch eine Förderung gleichermaßen praktikabler

[1] http://www.netzwerk-datenschutzexpertise.de/dokument/besch%C3%A4ftigtendatenschutz

wie datenschutzfreundlicher Verfahren und deren normative und praktische Umsetzung würde sowohl die Entwicklung solcher Technologien vorangebracht als auch die Stärkung digitaler Grundrechte erfolgen. Stattdessen hat sich die Bundesregierung bisher insbesondere darauf konzentriert, den Datenschutz zum wirtschaftlichen Hindernis zu deklarieren und sich für eine Standardabsenkung einzusetzen.[2]

Sie wäre aber gefordert, **Synthesen zwischen Grundrechtsschutz und technologischen Erkenntnismöglichkeiten** zu suchen und hierfür gemeinsam mit den beteiligten Branchen, der Wissenschaft und Betroffenenorganisationen aus den Bereichen Daten- und Verbraucherschutz Lösungen zu erforschen, zu entwickeln und zu implementieren.

Die defizitäre **Ausstattung der Datenschutzaufsichtsbehörden** hat zu großen Vollzugsdefiziten beim Datenschutz geführt. Die Behörden können schon seit langem weder ihrem Beratungs- noch ihrem Kontrollauftrag hinreichend wirksam nachkommen. Dies führt nicht nur zu massiven Grundrechtsverletzungen, sondern auch zu starken Marktverzerrungen. Die EU-DSGVO sieht in Art. 83 nun erstmals adäquate Sanktionsmöglichkeiten bei Datenschutzverstößen vor. Mit einer stark verbesserten Ausstattung der Datenschutzaufsicht müssen nicht nur die erwähnten Defizite abgebaut werden, sondern der Staat kann zugleich Sanktionsgelder zur teilweisen Refinanzierung der zusätzlichen Investitionen verwenden. Da insbesondere nichteuropäische Firmen, etwa aus den USA, von den Konsequenzen wirksamer Kontrollen betroffen wären, könnte dies zudem die datenschutzkonform agierende Wirtschaft im eigenen Land stärken: ungerechtfertigte Marktvorteile durch datenschutzverletzende Geschäftsmodelle würden so abgebaut.

Politische Organe der Bundesrepublik haben sich während der Diskussion über die EU-DSGVO u. a. dadurch hervorgetan, dass sie die Schaffung eines europaweit harmonisierten Datenschutzes behinderten, indem sie vorgeblich das **hohe deutsche Datenschutzniveau** durch die EU-DSGVO nicht reduziert sehen wollten. Nachdem der europäische Gesetzgeber den Mitgliedstaaten nun einen großen Handlungsspielraum belassen hat, ist die Bundesrepublik aufgefordert, diesen Spielraum im Sinne ihrer eigenen Argumentation zu nutzen. Leider muss festgestellt werden, dass die Bundesregierung – im Widerspruch hierzu – durch ihre im Bereich des Datenschutzes und der Informationssicherheit getätigten personellen, organisatorischen und rechtlichen Maßnahmen oft das genaue Gegenteil praktizierte.

Das Netzwerk Datenschutzexpertise fordert den Bundesgesetzgeber, also insbesondere die Bundesregierung und den Bundestag, aber auch die Parlamente und Regierungen der Länder, dazu auf, im Rahmen ihrer jeweiligen Zuständigkeit die durch die EU-DSGVO eröffneten Möglichkeiten zur Stärkung des digitalen Grundrechtsschutzes, der wirtschaftlichen Leistungsfähigkeit und des allgemeinen Wohls zu nutzen. Dazu sollten kurzfristig die gesetzgeberischen und administrativen Schritte eingeleitet werden, mit denen Deutschland seine Position als **Pionier für den globalen Datenschutz** zurückerlangen kann.

Das ursprünglich verfolgte Ziel, den Datenschutz nicht nur europaweit sondern auch über **alle Anwendungsgebiete** hinweg einheitlich zu regeln, wird mit der EU-DSGVO nicht erreicht. Art und Umfang der Öffnungsregeln reduzieren die zersplitterte deutsche Regelungslandschaft nicht. Neben

[2] http://www.netzwerk-datenschutzexpertise.de/file/140/download?token=6F9NbVAD

der Bearbeitung der oben dargelegten Themen ist es ist daher eine unumgängliche Fleißaufgabe für den Gesetzgeber, eine Bestandsaufnahme vorzunehmen, um die Auswirkungen der EU-DSGVO auf alle betroffenen Spezialgesetze systematisch und vollständig zu erfassen. Hierbei sollte gleichzeitig erfasst werden, welche national bereits geregelten Themen durch die EU-DSGVO überhaupt nicht thematisiert werden, wie z.B. Fragen der Videoüberwachung. Die Ergebnisse dieser Bestandsaufnahme sollte veröffentlicht werden, um die Diskussion über notwendige Anpassungsschritte transparent und sachbezogen führen zu können.

Der deutsche Gesetzgeber sollte außerdem nicht darauf warten, dass die Diskussion über gesetzliche Anpassungserfordernisse, Auslegungs- und Anwendbarkeitsabgrenzung von selbst in Gang kommt. Vielmehr sollte er auf Grundlage seiner Bestandsaufnahme einen **Fahrplan** entwickeln und von sich aus eine angemessene Beteiligung der Zivilgesellschaft an dieser Gestaltungsaufgabe vorsehen und einfordern.