Stellungnahme

des Deutschen Anwaltvereins durch den Ausschuss Informationsrecht

Zur Teilnahme an der öffentlichen Konsultation des Europäischen Datenschutz Ausschusses (EDSA)

Zum Entwurf von Leitlinien 4/2019 zu Artikel 25 DSGVO, „Data protection by design and by default“ (DPbDD) des EDSA

Stellungnahme Nr.: 2/2020 Brüssel, im Januar 2020

Mitglieder des Ausschusses

- RA Dr. Helmut Redeker, Bonn (Vorsitzender und Berichterstatter)
- RA Dr. Simon Assion, Frankfurt am Main
- RAin Dr. Christiane Bierekoven, Köln
- RAin Isabell Conrad, München
- RA Dr. Malte Grützmacher, LL.M., Hamburg
- RA Prof. Niko Härting, Berlin
- RA Peter Huppertz, LL.M, Düsseldorf
- RAin Birgit Roth-Neuschild, Karlsruhe
- RA Dr. Robert Selk, LL.M. (EU), München
- RA Prof. Dr. Holger Zuck, Stuttgart

Zuständig in der DAV-Geschäftsführung

- RAin Nicole Narewski, Berlin

Ansprechpartnerin in Brüssel

- Nicolas Schaeffer, Ass. iur.

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
EU-Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV mit seinen über 63.000 Mitgliedern vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.

1.

Der Informationsrechtsausschuss des Deutschen Anwaltvereins begrüßt es ausdrücklich, dass im Entwurf der Leitlinien an mehreren Stellen (u.a. Rn. 85) festgestellt wird, dass schon bei der Softwarebeschaffung und den dabei durchgeführten Ausschreibungen darauf geachtet werden muss, dass die Software so gestaltet wird, dass der Verantwortliche die Grundsätze des Art. 25 DSGVO einhalten kann. Eine datenschutzgerechte Gestaltung der verwendeten Software ist ein zentraler Teil der technischen Gestaltung des Softwareschutzes. Die Softwareanbieter müssen hier vertraglich in die Pflicht genommen werden. Dies ist nur durch eine entsprechende Leistungsbeschreibung in Ausschreibungen und Beschaffungsverträgen möglich.

2.

Der Entwurf beschäftigt sich ausgiebig mit dem Stand der Technik und den Anforderungen, die sich daraus ergeben, dass der Verantwortliche im Rahmen des Datenschutzes durch Technikgestaltung technisch und organisatorisch diesen Stand der Technik berücksichtigen muss. Sehr richtig bemerkt der Entwurf auch, dass sich dieser Stand laufend mit der technischen Entwicklung verändert, und der Anwender bei der Beurteilung, was Stand der Technik ist, den regelmäßigen technischen Fortschritt beachten muss. Es fehlt aber jeder Hinweis, wie zu einem konkreten Zeitpunkt der jeweilige Stand der Technik festzustellen ist.

Der Entwurf erwähnt zwar in Rn. 18, dass der Begriff auch in anderen EU-Vorschriften vorkommt und verweist auf umweltrechtliche Regelungen. Er macht aber noch nicht einmal klar, dass der Begriff in der DSGVO in gleicher Weise wie im Umweltrecht zu verstehen ist. Das deutsche Recht enthält im Umweltrecht (§ 3 Abs. 6 BImSchG) eine Definition des Standes der Technik, nach der der Stand der Technik der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen ist,

der die praktische Eignung der Maßnahmen zur Erreichung des (im BImSchG umweltrechtlichen, in er DSGVO datenschutzrechtlichen) Zweckes als gesichert erscheinen lässt. Diese Definition bezieht sich auf EU-rechtliche Vorschriften. In der datenschutzrechtlichen Literatur wird davon gesprochen, dass mit dem Stand der Techniken diejenigen Maßnahmen gemeint sind, die auf gesicherten Erkenntnissen beruhen und in der Praxis in ausreichendem Maß zur Verfügung stehen (Kühling/Buchner/*Hartung,* Art. 25 DSGVO, Rn. 21: Pall/Pauly/*Martini,* Art. 25 DSGVO Rn. 39d). Letztendlich geht es um fortschrittliche, aber in der Praxis schon verfügbare und in gewissem Umfang bewährte Techniken zur Erreichung datenschutzrechtlicher Ziele. Ob der EDSA den Begriff auch so versteht, bleibt unklar. Hier ist eine Präzisierung des Begriffs für die Praxis wichtig.

3.

Ein weiteres, in der Praxis für die Auswahl geeigneter technischer und organisatorischer Datenschutzmaßnahmen im Rahmen von Art. 25 DSGVO, aber auch zur Erfüllung der Pflichten nach Art. 32 DSGVO wichtiges Kriterium sind die Kosten der Implementierung der notwendigen Maßnahmen.

Der Entwurf geht auf dieses Kriterium ein, verkürzt aber seine Bedeutung maßgeblich. Er führt zwar richtig aus, dass der Verantwortliche diese Kosten in den Blick nehmen solle. Er führt auch richtig aus, dass zu diesen Kosten auch der zeitliche Aufwand der Mitarbeiter gehöre. Diese Ausführungen geben aber nur betriebswirtschaftliche Selbstverständlichkeiten wieder. Ein ordentlich geführtes Unternehmen wird die Kosten in der vom Entwurf vorgeschlagenen Art und Weise ermitteln. Der Entwurf verweist dann aber hinsichtlich der Auswirkungen dieser Überlegungen nur darauf, dass der Verantwortliche die Kosten so zu kontrollieren hat, dass die datenschutzrechtlichen Risiken gemindert und die datenschutzrechtlichen Prinzipien gewahrt sind (Rn. 24). In der Zusammenfassung wird unter Rn. 86 noch klarer ausgeführt, dass die Verantwortlichen wegen dieser Vorgaben ihre Technologieprovider verpflichten sollten, die Kosten der Lösung klar und transparent darzustellen.

Die Bedeutung des Kriteriums „Kosten der Implementierung“ in Art. 25 und 32 DSGVO geht aber weit über solche für Unternehmen generell geltende Hinweise hinaus. Die Kosten der Implementierung sind vielmehr im Rahmen einer Verhältnismäßigkeitsprüfung zu betrachten: Der datenschutzrechtliche Mehrwert einer nach Art. 25 DSGVO zu treffenden Maßnahme ist ins Verhältnis zu den Kosten zu

setzen. Dies heißt nicht, dass wegen der Kosten gar keine Maßnahmen zu treffen sind oder nicht bei großen Gefahren auch teure Maßnahmen erforderlich sind. Selbstverständlich müssen auch immer die Datenschutzgrundsätze des Art. 5 und die die Betroffenenrechte der Art. 12 – 20 DSGVO gewahrt bleiben. Es muss aber eine Abwägung zwischen dem Nutzen der Maßnahme und ihren Kosten erfolgen. Je nach datenschutzrechtlichem Gefährdungspotential und Wirksamkeit der Maßnahme sind unterschiedlich teure Maßnahmen zu treffen. Es kann dabei zwar sein, dass bei großen datenschutzrechtlichen Risiken auch sehr teure und sehr wirksame Maßnahmen erforderlich sind, die sogar bestimmte Verfahren finanziell unmöglich machen. Bei geringeren Risiken sind aber oft auf weniger teure Maßnahmen erforderlich. Dabei ist Maßstab der Auswahl nicht die konkret vom Verantwortlichen erwogene Maßnahme. Gibt es preiswertere, gleich wirksame Maßnahmen sind diese der Verhältnismäßigkeitsprüfung zu Grunde zu legen (so z.B. auch Kühling/Buchner/*Hartung,* Art. 25 DSGVO Rn. 22); Plath/*Plath,* Art. 25 DSGVO, Rn. 13; Paal/Pauly/*Martini,* Art. 25 DSGVO Rn. 42)
Diese auch grundrechtlich gebotene Abwägung der notwendigen Maßnahmen kommt im Entwurf nicht zum Ausdruck. Der Entwurf muss dies stärker betonen.

4.
Die Ausführungen zur "Fairness" unter Rn. 64 haben aus Sicht des Ausschuss kaum noch datenschutzrechtlichen Gehalt. Sie beschäftigen sich mit der Zulässigkeit von Lock-In-Technologie oder in Beispiel 2 mit der Frage, wie ein Unternehmen seine Kunden mit den vertraglich geschuldeten Leistungen versorgen soll. Es geht um Verbraucherschutz im Allgemeinen und um fairen Wettbewerb zwischen Unternehmen. Es ist nicht erkennbar, wie die (politisch meist zutreffenden) Ausführungen des Entwurfs mit der DSGVO begründet werden können.