(Hrsg.): Digitale Marktplätze und Plattformen,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2018 87

Die DSGVO auf der Zielgeraden

Stand ausgewählter Anforderungen an Marktplätze/Plattformen wenige Monate vor dem Wirksamwerden

Klaus Gennen

Abstract: Die Datenschutz-Grundverordnung (DSGVO[1]) trat im Mai 2016 in Kraft und wird am 25.5.2018 wirksam. Aufgrund vieler sog. Öffnungsklauseln und unbestimmter Rechtsbegriffe bestehen erhebliche Unsicherheiten für Unternehmen/Institutionen bei der Umsetzung. Zwar geben Datenschutz-Institutionen Handreichungen zur DSGVO heraus und Deutschland verfügt bereits über ein neues Bundesdatenschutzgesetz (BDSG). Viele Fragen zur Umsetzung sind aber noch ungeklärt. Der Beitrag beschreibt ausgewählte Anforderungen der DSGVO, die für Marktplätze/Plattformen relevant werden, u.a. die Grundsätze zu Data protection by Design und by Default (Art. 25[2]) sowie die Auswirkungen auf bestehende Einwilligungen und Vereinbarungen zur Auftrags(daten)verarbeitung, die vor dem 25.5.2018 getätigt wurden bzw. entstanden sind.

Keywords: DSGVO, BDSG-neu, Data protection by Design, Data protection by Default, ePrivacy-VO, technisch-organisatorische Maßnahmen, Plattform, Marktplatz, Datenschutz, Recht auf Löschung, Einwilligung, Auftragsdatenvereinbarung, Auftragsverarbeitung.

1 Einleitung

Unternehmen und Institutionen stehen vor der Herausforderung, zum Wirksamwerden der DSGVO Geschäftsprozesse, die mit personenbezogenen Daten („pbD“) zu tun haben, umzustellen, die zum Datenschutz (“DS“) notwendigen technischen und organisatorischen Maßnahmen („TOM“) zu treffen und ein DS-Managementsystem mit entsprechenden Kontroll- und Steuerungsmechanismen zu etablieren – und dies alles ausreichend zu dokumentieren, um die Einhaltung der DSGVO gegenüber der Behörde nachweisen zu können (sog. Rechenschaftspflicht). Soweit der DS, insbes. bei KMU, bisher stiefmütterlich behandelt wurde, hat sich die Einstellung unter dem Druck künftig enormer Bußgelder geändert. Dennoch haben erst 13% der Unternehmen DSGVO-Konformitätsprojekte umgesetzt oder damit begonnen und nur 19% der Unternehmen gehen davon aus, die notwendigen Maßnahmen fristgerecht umzusetzen (Stand 9/2017, Bitkom-Studie[3]). Passgenaue Hilfestellung vonseiten der Aufsichtsbehörden fehlt nach Ansicht der Verantwortlichen,

[1] VO (EU) 2016/679 des Europäischen Parlaments und des Rates v. 27.4.2016 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, S. 1–88.

[2] Artikelbezeichnungen ohne Kennzeichnung sind solche der DSGVO, §§ solche des BDSG-neu.

[3] https://www.bitkom.org/Presse/Presseinformation/Jedes-dritte-Unternehmen-hat-sich-noch-nicht-mit-der-Datenschutzgrundverordnung-beschaeftigt.html.

auch wenn zunehmend Handreichungen zur DSGVO ausgegeben werden. Die Öffnungsklauseln in der DSGVO wurden i.W. durch das als Teil des DSAnpUG-EU[4] erlassene neue Bundesdatenschutzgesetz („BDSG-neu“) befüllt. Es bleiben jedoch zahlreiche Unklarheiten, was die Umsetzung im Detail betrifft.

Für Kommunikationsdienste wie z.B. Marktplätze/Plattformen, hat die EU Lücken im DS ausgemacht. Daher soll es parallel zur DSGVO auch die ePrivacy-VO[5] geben – diese befindet sich nach dem Beschluss des EU-Parlaments vom 26.10.2017 weiterhin im Gesetzgebungsverfahren und wird wohl nicht rechtzeitig zum 25.5.2018 nicht in Kraft treten. Das hat nach einer Ansicht zur Folge, dass die bisherigen DS-Vorschriften der §§ 12 ff TMG[6] zum DS auf Webseiten, insbes. zum Tracking über Cookies, neben der DSGVO weiter gelten (vgl. Art. 95, Erwägungsgrund [„EG“] 173). Nach anderer Auffassung soll an deren Stelle die DSGVO gelten und der Betreiber kann auf Grundlage eines sog. „berechtigten Interesses“ nach Art. 6 Abs. 1 lit. f) eine Analyse des Nutzerverhaltens durchführen, sofern hierfür ein legitimes, rechtmäßiges Interesses des Verantwortlichen besteht und die Interessen der betroffenen Person nicht überwiegen.

2 Ausgewählte Anforderungen für Marktplätze und Plattformen

DS auf Marktplätzen/Plattformen kann die Verantwortlichen auf unterschiedliche Arten berühren, je nach Art der Vermarktung der angebotenen Ware oder Dienstleistung. Von besonderer Bedeutung werden die Anforderungen rund um den Onlinehandel sein, die die Erhebung von pbD erforderlich machen. Verantwortliche müssen sich insbes. auf erhöhte Anforderungen an die Information anlässlich der Erhebung von pbD einstellen („transparente Information“, vgl. Art. 12 bis 14, §§ 32 ff), dürfen nur die notwendigen pbD erheben, müssen sich mit umfangreichen Dokumentationspflichten anfreunden (vgl. z.B. Art. 5 Abs. 2, 24, 30, 32) und müssen die Neuerungen bei der Auftragsverarbeitung (Art. 28) umsetzen. Zudem sind bei der Nutzung von Arbeitsmitteln, zB. Software („SW“) für Plattformen, die Prinzipien „Privacy by Design“ (DS durch Technikgestaltung) und „Privacy by Default“ (DS-freundliche Voreinstellungen) zu beachten (Art. 25).

2.1 Data protection by Design und by Default

Ziel von Data protection by Design ist die Verarbeitung möglichst weniger pbD („Datensparsamkeit“). Sowohl auf technischer als auch auf administrativer Ebene sollen die mög-

[4] G. zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU) v. 30.6.2017 (BGBl. I S. 2097)

[5] Bezeichnung voraussichtlich „VO des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektr. Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (VO über Privatsphäre und elektronische Kommunikation)“, besteht bisher nur im Entwurf.

[6] Telemediengesetz v. 26.2.2007 (BGBl. I S. 179), zul. geänd. d. Art. 1 des G. v. 28.9.2017 (BGBl. I S. 3530)

lichen DS-Funktionen in die SW eingearbeitet werden und das Risiko künftiger DS-kritischer Entwicklungen, die aus dem Einsatz technischer Systeme herrühren, minimieren. Zu beachten sind nach Art. 25 Abs. 1 der Stand der Technik, womit der Beurteilungsmaßstab dynamisch, ferner die Implementierungskosten, womit der Verantwortliche auch wirtschaftliche Gesichtspunkte berücksichtigen darf, und natürlich Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die Risiken für die betroffenen Personen. Als eine typische Maßnahme nennt die DSGVO ausdrücklich die Pseudonymisierung. Zwar trifft die Norm den Verantwortlichen und zwingt ihn zum Einsatz entsprechender Arbeitsmittel; dieser wird daher aber künftig nur noch solche Arbeitsmittel erwerben und einsetzen, die die entsprechenden Grundsätze wahren. Also wird SW, die diesen Anforderungen nicht genügt, unverkäuflich werden.

Hierneben ist der Grundsatz der Data protection by Default zu beachten, d.h. die Notwendigkeit DS-freundlicher Voreinstellungen in der SW. Damit sind bei Online-Diensten Maßnahmen gemeint, die sicherstellen, dass nur solche pbD verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind. Das meint insbes. die Menge der erhobenen pbD, den Umfang der Verarbeitung und die Speicherfrist, als auch für die Zugänglichkeit der Daten. Dem Nutzer des Online-Dienstes steht es jedoch frei sich, z.B. SW-layer-weise, eine umfangreichere Verarbeitung seiner pbD zuzulassen – es muss aber seine Entscheidung sein. Die Datenhoheit soll mithin weitestgehend beim Nutzer des Online-Dienstes liegen. Um solche DS-freundlichen Voreinstellungen nutzen und anbieten zu können, müssen diese wiederum in der SW vorgesehen sein, was SW, die so etwas nicht vorsieht, wiederum unverkäuflich machen dürfte.

2.2 Recht auf Löschung, Art. 17, § 35 und Recht auf Datenportabilität, Art. 20

Dem BDSG in dieser Weise unbekannt, jedoch durch die Rechtsprechung eingeführt, ist der Grundsatz des Rechts auf Löschung (Vergessenwerden). Die betroffene Person hat das Recht, alle über sie gespeicherten pbD von dem Verantwortlichen löschen zu lassen. Jedoch schränkt § 35 Abs. 1 BDSG-neu den Löschungsanspruch des Nutzers ein, wenn wegen der besonderen Art der Speicherung eine Löschung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich und gleichzeitig das Interesse der betroffenen Person an der Löschung als gering anzusehen ist. In diesem Fall soll dann das Recht auf Einschränkung der Verarbeitung (früher: Sperren) gegeben sein (Art. 18). Hier zeigt sich das Problem, dass ein Löschen von Daten in einer Vielzahl von Systemen bisher schlichtweg technisch nicht vorgesehen ist. Auch hier bedarf es eines technischen Nachrüstens, damit Plattformbetreiber bzw. deren Subunternehmer den Anforderungen genügen.

Will der Betroffene einen Provider wechseln, mit dem er vertraglich verbunden ist, zB. einen Plattformbetreiber, hat er nach Art. 20 das Recht, die pbD in einem strukturierten, gängigen und maschinenlesbaren Format herausgegeben zu erhalten, und hat insbes. das Recht, diese einem anderen Verantwortlichen ohne Behinderung durch bisherigen Betreiber zu übermitteln. Damit müssen Marktplatz- und Plattformsysteme künftig Schnittstellen zur Datenbereitstellung enthalten.

2.3 Fortgeltung von Alt-Einwilligungen und Anpassungsbedarf bei Vereinbarungen zur Auftragsdatenverarbeitung (ADV)

Für Verantwortliche stellt sich die Frage, ob Einwilligungen (nunmehr Art. 7) fortgelten, die unter der bisherigen Rechtslage abgegeben wurden. Hierzu findet sich lediglich in EG 171 Satz 3 die Aussage, dass erteilte Einwilligungen unter der DSGVO fortgelten, sofern sie der Art nach den Bedingungen der DSGVO entsprechen. Auch wenn es sich bei einem EG nicht um den eigentlichen Gesetzestext handelt, diese Aussage mithin nicht unmittelbar geltendes Recht ist, wird es kaum vertretbar sein, gegen die Fortgeltung von Einwilligungen zu argumentieren, solange die Anforderungen der DSGVO eingehalten wurden[7]. Eine besondere Herausforderung wird es jedoch sein, im Zweifel darzulegen, dass die Einwilligung nach Maßgabe der DSGVO hinreichend informiert erfolgte. Ungeachtet dessen müssen Plattformbetreiber die bisherigen Muster für Einwilligungserklärungen für künftige Nutzer vorsorglich überarbeiten – auch wenn noch nicht klar ist, wie die ePrivacy-VO sich insoweit auswirken wird.

Die Vorschriften zur Auftragsdatenverarbeitung nach § 11 BDSG („ADV“), künftig Auftragsverarbeitung („AV“) haben sich nach Art. 28 in Teilen nennenswert geändert, auch wenn die gesetzlichen Pflichtinhalte weitgehend gleich geblieben sind. So haften für den Fall eines Datenschutzverstoßes Verantwortlicher und Auftragsverarbeiter als Gesamtschuldner (Art. 79). Auch sind die Unterstützungspflichten des Auftragserarbeiters bei der sog. Datenschutz-Folgenabschätzung neu (Art. 28 Abs. 3 lit. f). Auch die Regelungen zur Einschaltung von Subunternehmern wurden strenger. In Anbetracht der erheblichen Bußgelder sollten die an einer AV Beteiligten ein Interesse daran haben, bestehende Vereinbarungen hinsichtlich der veränderten Rechtslage nachzubessern.

3 Praktische Umsetzung der Anforderungen

Die Umsetzung der neuen Anforderungen hat auf verschiedenen Ebenen zu erfolgen, technisch wie organisatorisch. Ein DS-Managementsystem, das diese Bezeichnung verdient, ist zu etablieren. Dabei werden insbesondere die erheblich gestiegenen Dokumentationspflichten erhöhte Anforderungen stellen, die für viele Verantwortliche zeitgerecht kaum noch zu umzusetzen sind.

[7] Siehe Kreis der Landesdatenschutzbeauftragten und der Bundesdatenschutzbeauftragten, vgl. https://www.lda.bayern.de/media/dk_einwilligung.pdf.