Das neue Datenschutzrecht im Überblick

Daniel Nemmert Detlef Hühnlein Tina Hühnlein
Michael Rauh Stefan Baszanowski

ecsec GmbH, Sudetenstraße 16, D-96247 Michelau
vorname.nachname@ecsec.de

Zusammenfassung

Der vorliegende Beitrag liefert einen kompakten Überblick über die neuen datenschutzrechtlichen Rahmenbedingungen auf Basis der im letzten Jahr verabschiedeten „Datenschutz-Grundverordnung“ [DSGVO], der im Entwurf vorliegenden „ePrivacy-Verordnung“ [ePrivacy] und ausgewählten nationalen Datenschutzgesetzen, wie dem deutschen Bundesdatenschutzgesetz.

1 Einleitung

„Daten sind das Öl des 21. Jahrhunderts.“ – so oder so ähnlich fällt diese Aussage häufig, sobald es um Themen wie Big Data oder Spionage geht. Und tatsächlich beruht mittlerweile das Geschäftsmodell von vielen Unternehmen auf dem Sammeln oder Analysieren von Nutzerdaten oder -verhalten. Dabei spielen nicht nur offensichtliche Akteure, wie z. B. soziale Netzwerke und Suchmaschinen, deren Ziel es ist möglichst scharfe Profile ihrer einzelnen Nutzer zu erzeugen, eine wichtige Rolle, sondern auch die großen Werbenetzwerke, die ihrerseits diese und eigene Profile dafür nutzen, um möglichst treffsicher personalisierte Werbung an die jeweiligen Nutzer auszuliefern. Je detaillierter ein Profil ist, desto zielgerichteter kann Werbung geschaltet werden und desto teurer kann man den Werbeplatz für dieses Profil verkaufen. Konzerne mit diesem Geschäftsmodell sind häufig internationale Unternehmen (z. B. Google, Facebook und Amazon), die den Rahmen einer rein nationalen Regulierung ihrer Datenverarbeitung sprengen würden. Umso wichtiger war es, dass mit der Datenschutz-Grundverordnung europaweit harmonisierte Rahmenbedingungen für den Datenschutz entstanden sind, um für alle Bürgerinnen und Bürger in Europa ein angemessenes Datenschutzniveau zu gewährleisten. Auf dieser Grundlage und der so genannten ePrivacy-Verordnung („Verordnung über Privatsphäre und elektronische Kommunikation“) [ePrivacy] werden derzeit die nationalen Datenschutzgesetze, wie z. B. das deutsche Bundesdatenschutzgesetz, überarbeitet.

Der vorliegende Beitrag liefert in Abschnitt 2 einen Überblick über das ab Mai 2018 geltende Datenschutzrecht. Hierbei enthält Abschnitt 2.1 einen generellen Überblick über die europaweit gültige und bereits am 24. Mai 2016 in Kraft getretene Datenschutz-Grundverordnung [DSGVO]. In Abschnitt 2.2 findet sich ein Überblick über die momentan im Entwurf vorliegende ePrivacy-Verordnung [ePrivacy]. In Abschnitt 2.3 wird ein erster Blick in die Neufassung des Bundesdatenschutzgesetzes geworfen, welches an die Regelungen der DSGVO angepasst wurde. Abschnitt 3 geht auf die praktische Umsetzung der datenschutzrechtlichen An-

forderungen am Beispiel des SkIDentity-Dienstes ein, bevor die wesentlichen Aspekte des Beitrags in Abschnitt 4 kompakt zusammengefasst werden.

2 Das neue Datenschutzrecht für Europa

2.1 Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung [DSGVO] des Europäischen Parlaments und des Rates, hat eine Neuregelung der Vokabeln des Datenschutzes in ganz Europa zur Folge. Die DSGVO löst die alte EU-Datenschutzrichtlinie 95/46/EG [Ri95] endgültig ab und wird durch eine Verordnung ersetzt, die eher dem aktuellen Stand der Technik entspricht. Auch für den deutschen Datenschutz, seit langem einer der strengsten weltweit, hat dies Folgen. Mit Inkrafttreten der DSGVO am 24. Mai 2016 brach eine neue Ära des europäisch harmonisierten Datenschutzes an. Ab dem 25. Mai 2018 werden öffentliche und privatwirtschaftliche Organisationen auch für eine Überprüfung durch eine Aufsichtsbehörde nach der neuen Verordnung gerüstet sein müssen. Deutsche Dienstanbieter, die bisher konform zum Bundesdatenschutzgesetz (BDSG) waren, werden es daher nicht vermeiden können, entsprechende Änderungen an ihren bisherigen Modellen, Prozessen, Systemen und Verträgen vorzunehmen, um weiterhin mit den aktuellsten Regelungen zum Datenschutz im Einklang zu sein.

Die zentralen Neuerungen der Datenschutz-Grundverordnung umfassen insbesondere den „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ (**Artikel 25**). Diese Begriffe sind jedoch eher unter den Bezeichnungen „Privacy by Design“ und „Privacy by Default“ bekannt. Dabei bedeuten diese beiden Prinzipien die Berücksichtigung des Datenschutzes von Anfang an und während der Entwicklung („by Design“) sowie das Setzen der datenschutzfreundlichsten Einstellungen als Voreinstellung einer Software oder eines Dienstes („by Default“). Außerdem legt die DSGVO größeren Wert auf die Sicherheit der Verarbeitung personenbezogener Daten (**Artikel 32**) und empfiehlt beispielsweise Verschlüsselung und Pseudonymisierung, ein Sicherheitskonzept, eine Notfallplanung und ein geeignetes Sicherheitsmanagement, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Im Gegensatz zu dem, was landläufig unter dem Begriff „IT-Sicherheit“ verstanden wird, nämlich der Schutz von Unternehmenswerten, kümmert sich der Datenschutz vor allem um den Schutz von natürlichen Personen im Falle der Verarbeitung ihrer persönlichen Daten durch einen Dritten. Es ist natürlich offensichtlich, dass der Schutz von personenbezogenen Daten damit auch in vielen Fällen ein wichtiger Unternehmenswert ist, da viele Unternehmen auf der einen Seite Daten von Kunden, aber auf der anderen Seite auch Daten der eigenen Mitarbeiter im Personalwesen verarbeiten. Ein Vorfall in diesem Bereich hat schnell einen katastrophalen Vertrauens- und Kundenverlust und mit dem Inkrafttreten der Datenschutz-Grundverordnung außerdem potenziell empfindliche Geldstrafen zur Folge.

Bei den Rechten, der von der Datenverarbeitung Betroffenen ist die DSGVO dem BDSG und der alten EU-Datenschutzrichtlinie sehr ähnlich. Auch sie enthält in Abschnitt 3 das Recht auf Berichtigung (**Artikel 16**), das Recht auf Löschung („Vergessenwerden“) (**Artikel 17**), das Recht auf Einschränkung der Verarbeitung (**Artikel 18**) und eine Mitteilungspflicht des Datenverarbeiters an den Betroffenen (**Artikel 19**).

Die DSGVO bietet in Bezug auf die Übermittlung von Daten an Drittländer eine potentiell schwere Schwachstelle. Nach **Artikel 45** Abs. 1 können Daten an Dritte übermittelt werden

„wenn die Kommission beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet.“ Unter diesen Bedingungen, wäre dann auch der EU-US Privacy Shield DGSVO konform. Da aber gerade die Unternehmen, die ihr Geschäftsmodell besonders auf die Verarbeitung personenbezogener Daten konzentrieren, ausgerechnet in den USA sitzen, kann durchaus bezweifelt werden, dass die DSGVO im Hinblick auf Facebook, Google und Co. das erhoffte höhere Datenschutzniveau für europäische Bürger bringt. Besonders deutlich wird dies in diesem Zusammenhang damit, dass Präsident Trump als eine der ersten Amtshandlungen eine Anordnung unterzeichnete, welche nur US-Bürgern, mit ständigem Wohnsitz in den USA, einen Schutz im Sinne des amerikanischen Privacy Acts zuspricht [Pe17]. Es muss also bezweifelt werden, dass gerade im Hinblick auf die von amerikanischen Anbietern dominierten sozialen und Werbenetzwerke die DSGVO ihre erhoffte Wirkung entfaltet.

In den folgenden Unterabschnitten werden ausgewählte Artikel der DSGVO genauer betrachtet.

2.1.1 Artikel 5 Grundsätze für die Datenverarbeitung

Die in der DSGVO festgelegten Grundsätze waren zum Großteil bereits in der alten EU-Datenschutzrichtlinie [Ri95] unter gleichen oder zumindest ähnlichen Stichworten beschrieben. Forderte die EU-Datenschutzrichtlinie [Ri95] bei manchen Grundsätzen noch, dass die Mitgliedsstaaten selbst geeignete Garantien vorsehen, werden diese künftig oft direkt in der DSGVO festgelegt:

- „**Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz**“ soll es von der Datenverarbeitung Betroffenen ermöglichen den Verarbeitungsprozess nachvollziehen zu können, was übermäßig komplizierte Formulierungen in Datenschutzbestimmungen der jeweiligen Dienstanbieter unterbindet; die Betonung der Transparenz ist neu und war bisher nicht in der EU-Datenschutzrichtlinie [Ri95] vorhanden.
- Der Grundsatz der „**Zweckbindung**“ legt fest, dass die erhobenen und zu verarbeitenden Daten nur zu einem eindeutigen und klar abgegrenzten Zweck verarbeitet werden dürfen.
- Mittels „**Datenminimierung**“ soll sichergestellt werden, dass nur höchstens die Menge an personenbezogenen Daten erhoben wird, die für den jeweiligen Dienst zum normalen Betrieb seines Angebots unbedingt nötig ist. Außerdem soll durch den Grundsatz der „**Speicherbegrenzung**“ gewährleistet werden, dass Daten nur so lange vorgehalten werden, wie es für die Verarbeitung nötig ist. Diese beiden Prinzipien lassen sich unter dem Begriff „**Datensparsamkeit**“ zusammenfassen.
- Ein Dienstanbieter hat außerdem auf die „**Richtigkeit**“ der von ihm verarbeiteten Daten zu achten. Falsche oder nicht aktuelle Daten sollen schnellstmöglich gelöscht oder berichtigt werden.
- Die Gewährleistung der „**Integrität und Vertraulichkeit**“ kann mit den identischen Begriffen in der Informationssicherheit gleichgesetzt werden.
- Eine Neuerung gegenüber etwa dem aktuellen Stand des BDSG ist die „**Rechenschaftspflicht**“. Mussten vorher noch die zuständigen Aufsichtsbehörden nachweisen, dass ein Datenverarbeiter gegen bestimmte Vorschriften verstößt, ist jetzt der Datenverarbeiter selbst in der Pflicht nachzuweisen, dass er sich an alle gängigen Regularien hält.

2.1.2 Artikel 7 Einwilligung in die Datenverarbeitung

Sofern die Verarbeitung auf einer Einwilligung beruht, muss der Verantwortliche nach **Artikel 7 (1)** nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat. Nach DGSVO reicht eine Handlung des Betroffenen, die seine Einwilligung in die Verarbeitung seiner Daten zu einem bestimmten Zweck nachweisbar macht [Ba16]. Dienstanbieter werden besonders mit Blick auf **Artikel 5** („Rechenschaftspflicht“) darauf achten müssen, dass sie jederzeit den Nachweis erbringen können, dass ein Nutzer der Verarbeitung zugestimmt hat. Außerdem hat die betroffene Person gemäß **Artikel 7 (3)** das Recht, ihre Einwilligung jederzeit zu widerrufen. Der Widerruf der Einwilligung muss jedoch genau so einfach sein, wie die Einwilligung selbst. Ein Dienstanbieter wird auch besonders im Blick auf die neuen und wesentlich höheren Strafen (Abschnitt 2.1.11) darauf achten müssen, dass eine Einwilligung nach allen Vorgaben der DSGVO gültig ist, darunter fällt auch insbesondere, dass die Datenschutzerklärung und Einwilligung in leicht verständlicher Sprache formuliert und der Zweck eindeutig ersichtlich ist (siehe **Erwägungsgrund (EG) 42**).

Die strengeren Anforderungen aus der DSGVO werden jedoch für Dienstanbieter nach **EG 171** möglicherweise keinen bürokratischen Albtraum bedeuten, da alte Einwilligungen, die gemäß der alten EU-Datenschutzrichtlinie [Ri95] abgegeben wurden, im Regelfall den Anforderungen an die Einwilligung der DSGVO entsprechen und deshalb nicht erneut eingeholt werden müssen [Ba16]. Problematisch könnte dies nur werden, wenn bisherige Einwilligungen nach BDSG nicht alle nach **Artikel 13** DSGVO geforderten Informationen enthalten (siehe [Ba16]). Der in **EG 171** erwähnte Fortbestand von alten Einwilligungen wird also bei vielen Dienstanbietern dennoch davon abhängen, ob die existierenden Einwilligungen den in **Artikel 13** und **EG 42** geforderten grundlegenden Anforderungen genügen.

2.1.3 Artikel 15 Auskunftsrecht der betroffenen Person

Genau wie in **§ 34 BDSG** („Auskunft an den Betroffenen“) bleibt das Recht auf Auskunft ein zentrales Recht der betroffenen Personen gegenüber einem Dienstanbieter. Die Rechte der Betroffenen werden jedoch umfassend erweitert. Die DSGVO gibt einem Betroffenen unteranderem das Recht auf Auskunft über die Kategorien der verarbeiteten personenbezogenen Daten. Darunter fällt z. B. die geplante Dauer der Speicherung der Daten oder zumindest die Kriterien für eine Festlegung dieser Dauer sowie das Bestehen eines Rechts auf Berichtigung, Löschung und Einschränkung der Verarbeitung sowie außerdem das Recht auf Widerspruch nach **Artikel 21** DSGVO („Widerspruchsrecht“).

Da es sich bei Artikel 15 um ein Recht eines Betroffenen handelt, gilt wie bei allen Artikeln zu Betroffenenrechten (**Artikel 12 – 22**), dass ein Verstoß gegen dieses Recht durch einen Dienstanbieter direkt in die Kategorie der hohen Bußgelder fällt (siehe Artikel 83 und Abschnitt 2.1.11).

2.1.4 Artikel 17 „Recht auf Vergessenwerden“

Das „Recht auf Vergessenwerden“ war vor einiger Zeit nach einem Gerichtsurteil des EuGH[1] in aller Munde und wurde, vor allem mit Blick auf das Internet und insbesondere Suchmaschinen, bisweilen auch kontrovers diskutiert. Die DSGVO garantiert dieses Recht nun Be-

[1] http://curia.europa.eu/juris/liste.jsf?language=de&num=C-131/12

troffenen durch einen eigenen Artikel hierzu, nachdem das Recht auf Löschung in der alten EU-Datenschutzrichtlinie nur Teil von Aufzählungen (z. B. [Ri95], Artikel 6, Abs. 1 d) war. **Artikel 17** bezieht sich dabei jedoch nicht nur auf das Internet, sondern generell auf alle Dienste, die personenbezogene Daten verarbeiten. Es werden also auch Anbieter „klassischer" Dienste zukünftig Mechanismen anbieten müssen, die innerhalb der Regeln dieses Artikels eine Löschung der Daten eines Betroffenen ermöglicht. Die Löschung kann unter bestimmten Umständen (Abs. 3) ausgesetzt werden.

2.1.5 Artikel 20 Datenportabilität

Neu ist das in **Artikel 20** festgelegte „Recht auf Datenübertragbarkeit", welches so manchem Dienst, der nicht ordentlich auf das Einsetzen der Anwendbarkeit der DSGVO vorbereitet ist, Probleme bereiten dürfte. Hiermit wird dem Betroffenen das Recht eingeräumt, seine zur Verfügung gestellten personenbezogenen Daten von einem Dienstanbieter „in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten" und diese anschließend ohne Behinderung durch den vorherigen Verantwortlichen anderweitig zu übermitteln. Ein mögliches Szenario hierfür wäre z. B. der Wechsel des Mobilfunkanbieters. Es bleibt abzuwarten welches Format (z. B. XML oder JSON) sich hier durchsetzen wird und wie kompatibel die strukturierten und maschinenlesbaren Austauschformate schlussendlich wirklich sein werden.

2.1.6 Artikel 25 Privacy by Design & Default

Artikel 25 der DSGVO etabliert die in der deutschen Übersetzung mit „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen" etwas sperrig übersetzten Prinzipien „Privacy by Design" und „Privacy by Default" als zentrale Ziele des europäischen Datenschutzes. Das Ziel dieses Artikels ist eine Berücksichtigung datenschutzrelevanter Aspekte direkt zu Beginn der Erstellung eines neuen Produktes. Außerdem sollten die datenschutzfreundlichsten Einstellungen die Grundeinstellung sein. Ein Nutzer muss also selbst aktiv werden, wenn er ein niedriges Datenschutzniveau möchte. Ähnlich wie im alten Bundesdatenschutzgesetz sollen hier Maßnahmen umgesetzt werden, die dem Stand der Technik entsprechen und ein angemessenes Schutzniveau etablieren. Dabei muss das Schutzniveau auf jeden Fall dem Schutzbedarf der verarbeiteten Daten entsprechen. Entsteht einem Betroffenen durch die Verarbeitung von kritischeren Daten ein höheres Risiko, so muss das Risiko durch die verantwortliche Stelle oder den Auftragsdatenverarbeiter minimiert werden und kann nicht, wie beispielsweise bei der Implementierung eines Informationssicherheitsmanagementsystems, durch die Organisation akzeptiert werden.

2.1.7 Artikel 28 Auftragsverarbeiter

Artikel 28 der DSGVO ersetzt zukünftig § 11 BDSG. Eine der Neuerungen ist, dass Verträge zur Auftragsdatenverarbeitung zukünftig auch in elektronischer Form abgeschlossen werden können. Nach aktueller Einschätzung des LdA Bayern [Ba161] „gilt [für den Inhalt des Vertrags] weitestgehend das Gleiche wie bisher", wobei zukünftig eine Auflistung der nach **Artikel 32** (siehe Abschnitt 2.1.8) nötigen Maßnahmen Bestandteil des Vertrags sein wird.

Neu ist außerdem, dass ein Auftragsverarbeiter nun nach **Artikel 28 (10)** DSGVO automatisch als für die Daten *Verantwortlicher* (mit allen dazugehörigen Pflichten) gilt, wenn er die ihm überlassenen Daten zusätzlich zu einem anderen Zweck verarbeitet [Ba161].

2.1.8 Artikel 32 Sicherheit der Verarbeitung

Artikel 32 DSGVO ist das Äquivalent zu § 9 der alten Fassung des BDSG, einschließlich der Anlage zu Satz 1. Damit werden auch Probleme, die sich bei der Anwendung des Paragraphen ergaben, behoben, indem beispielsweise Prozesse und Verfahren für die sichere Datenverarbeitung gefordert werden. Durch die DSGVO wird die Etablierung eines Managementprozesses (z. B. der vielen ISO-Normen zugrundeliegende „Plan, Do, Check, Act"-Zyklus) auch im Bereich des Datenschutzes verpflichtend, mit der sich auch die Forderung nach regelmäßiger Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen (TOM) verbinden lässt. Über diesen etablierten Prozess lässt sich außerdem die geforderte Gewährleistung des adäquaten Schutzniveaus leichter realisieren. Die zu wählenden TOMs müssen im Hinblick auf den Schutzbedarf der jeweils verarbeiteten Daten angemessen sein.

Eine geeignete Maßnahme ist hier z. B. die Pseudonymisierung von Daten natürlicher Personen. Jedoch gelten nach **EG 26** pseudonymisierte Daten nur dann als nicht schutzbedürftig, wenn sie nicht durch die Zusammenführung mit weiteren Informationen einer bestimmten Person zugeordnet werden können. Pseudonymisierung hilft jedoch bereits, das Risiko für eine betroffene natürliche Person zu senken und unterstützt Dienstanbieter bei der Einhaltung der datenschutzrechtlichen Pflichten. Personenbezogene Daten sollten daher grundsätzlich in verschlüsselter Form vorliegen. Bei weiteren Maßnahmen handelt es sich beispielsweise um „die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen" (**Artikel 32 (1) b)** DSGVO), was durch ein entsprechendes Sicherheitskonzept sichergestellt werden kann. Natürlich sollten personenbezogene Daten nach einem Zwischenfall auch möglichst schnell wiederherstellbar sein. Durch die Bestimmung von Eintrittswahrscheinlichkeiten und der Schwere der Folgen für eine natürliche Person von möglichen Zwischenfällen soll außerdem für jede Datenverarbeitung die Höhe des Risikos bestimmt werden.

Basierend auf den Ergebnissen der Risikoanalyse werden schließlich Datenschutzmaßnahmen ausgewählt, die sich aus den verschiedenen Schutzmöglichkeiten wie Pseudonymisierung, Verschlüsselung und Transparenz bei der Verarbeitung der Daten zusammensetzen. Darüber hinaus entsteht mit ISO/IEC FDIS 29151 („Code of practice for personally identifiable information protection") derzeit eine datenschutzspezifische Fassung der ISO/IEC 27002.

2.1.9 Artikel 35 Datenschutz-Folgenabschätzung

Im internationalen Bereich bereits länger als „**Privacy Impact Assessment**" bekannt, ist eine Datenschutz-Folgeabschätzung (DSFA) kein neues Vorgehen. Für den deutschen Datenschutz ist es jedoch, auch weil es bisher im BDSG nicht gefordert wird, ein komplett neues Gebiet. Eine DSFA muss vor allem dann durchgeführt werden, wenn Art, Umfang oder Zweck der Verarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen bieten. Nach **Artikel 35 (7)** enthält eine DSFA mindestens eine Beschreibung der Verarbeitungsvorgänge inklusive des Zweckes der Verarbeitung sowie eine Bewertung der Risiken für Rechte und Freiheiten der Betroffenen. Außerdem muss eine hinreichende Bewertung der Notwendigkeit der Datenverarbeitung im Hinblick auf den vorgesehen Zweck erfolgen. Sobald die Bewertung abgeschlossen ist, müssen entsprechende Maßnahmen (Garantien, Sicherheitsvorkehrungen und Verfahren) zur Risikominimierung etabliert werden.

Mit ISO/IEC FDIS 29134[2] entsteht derzeit ein einschlägiger ISO-Standard zu diesem Thema.

2.1.10 Artikel 42 Zertifizierung

Artikel 42 legt die Rahmenbedingungen für eine Zertifizierung auf Basis der DSGVO fest. Dabei werden die Aufsichtsbehörden dazu angehalten, die Einführung von geeigneten Zertifizierungsverfahren zu unterstützen. Eine erfolgreiche Zertifizierung eines Unternehmens mindert jedoch nicht die Verpflichtung des Verantwortlichen und berührt außerdem ausdrücklich nicht die Aufgaben und Befugnisse der Aufsichtsbehörden (**Artikel 42 (4)**). Dabei können sich Unternehmen sowohl von den Aufsichtsbehörden als auch von anderen akkreditierten Zertifizierungsstellen eine Zertifizierung erteilen lassen. Eine Zertifizierung ist maximal drei Jahre gültig, kann aber „unter denselben Bedingungen verlängert werden, sofern die einschlägigen Voraussetzungen weiterhin erfüllt werden“ (**Artikel 42 (7)**).

2.1.11 Artikel 83 Geldbußen

Artikel 83 legt die Höhe der zu verhängenden Bußgelder fest, die schnell empfindliche Höhen erreichen können. Selbst bei nach DSGVO geringeren Verstößen, wenn z. B. keine geeigneten Sicherheitsmaßnahmen nach Stand der Technik implementiert wurden, drohen Geldstrafen von bis zu 10 Mio. Euro bzw. im Fall eines Unternehmens bis zu 2 % des weltweiten Jahresumsatzes. Bei Verstößen gegen die zentralen Grundsätze der Verordnung (Artikel 5, 6, 7 und 9) oder gegen die Betroffenenrechte (Artikel 12 bis 22) erhöht sich die Höhe der Geldbuße auf bis zu 20 Mio. Euro oder im Falle eines Unternehmens auf bis zu 4 % des weltweiten Jahresumsatzes. Sollte das zu bestrafende Unternehmen Teil einer Unternehmensgruppe sein, so ist, basierend auf **EG 150,** nicht nur das unmittelbar verantwortliche Unternehmen, sondern die gesamte Unternehmensgruppe zu belangen [Bay162].

2.2 ePrivacy-Verordnung

Die ePrivacy-Verordnung [ePrivacy] ist per Definition eine Konkretisierung der DSGVO. Ein Vergleich zwischen verschiedenen Entwürfen der Verordnung deutet jedoch darauf hin, dass die ePrivacy-Verordnung zentrale Punkte der DSGVO teilweise deutlich abschwächen könnte. War im von POLITICO „geleakten“ Entwurf vom Dezember 2016 [Po16] in **Artikel 10** noch davon die Rede, dass eine Endanwendung als Voreinstellung dritten Parteien verbieten soll Daten zu speichern und zu verarbeiten, fordert der aktuelle Entwurf nur noch, dass „Software die Möglichkeit bieten muss […] zu verhindern, dass Dritte Informationen in der Endeinrichtung eines Endnutzers speichern oder bereits in der Endeinrichtung gespeicherte Informationen verarbeiten.“ [ePrivacy] Die neue Version schwächt also das zentrale Prinzip „Privacy by Default“ der DSGVO entsprechend ab. Ist der Betroffene durch die DSGVO noch standardmäßig dadurch geschützt, dass die datenschutzfreundlichsten Einstellungen bereits ohne sein Zutun festgelegt waren, liegt es nun in der Verantwortung des Betroffenen die Einstellungen auf das von ihm gewünschte Niveau anzupassen. Zwar gibt die Version von Januar 2017 immer noch vor, dass die Software während der Installation den Betroffenen über die verfügbaren Datenschutzeinstellungen informieren muss, jedoch muss hierbei nicht mehr automatisch die strikteste Einstellung vorausgewählt sein.

[2] Guidelines for privacy impact assessment

2.2.1 Artikel 6 Erlaubte Verarbeitung von Kommunikationsdaten

Die ePrivacy-Verordnung erlaubt in **Artikel 6** die Verarbeitung von (durch **Artikel 5** zunächst grundsätzlich vertraulichen) Kommunikationsdaten (im Folgenden „Daten“) durch Betreiber von Kommunikationsnetzen nur für den Zeitraum der Übertragung und für die Fehleranalyse im Kommunikationsnetz. Des Weiteren dürfen Kommunikationsmetadaten und -inhalte u.a. zum Zwecke der Rechnungsstellung verarbeitet werden oder aber, wenn der Betroffene explizit in die Verarbeitung für bestimmte Zwecke zustimmt. Handelt es sich bei dem vorgesehenen Zweck allerdings um einen Vorgang, der auch durch die Verarbeitung von anonymisierten Informationen erreicht werden kann, müssen diese dafür genutzt werden.

2.2.2 Artikel 7 Speicherung und Löschung von Daten

Eine Speicherung oder Verarbeitung von Daten ist grundsätzlich nur im Einklang mit den Vorgaben aus der DSGVO möglich. Datenverarbeiter sollen mit **Artikel 7** darauf verpflichtet werden, Kommunikationsmetadaten zu löschen oder zu anonymisieren, sobald diese für die Datenübermittlung nicht mehr benötigt werden. Ausgeschlossen hiervon sind Metadaten, die zu Abrechnungszwecken genutzt werden. Diese können weiterhin für die im jeweils nationalen Recht der Mitgliedsstaaten verankerten Fristen (beispielsweise für die Anfechtung einer Rechnung) gespeichert werden.

2.2.3 Artikel 8 Schutz der Daten auf Endgeräten von Nutzern

Artikel 8 untersagt die Erhebung von personenbezogenen Daten über einen Endnutzer, sofern dieser nicht ausdrücklich in die Erhebung der Daten eingewilligt oder wenn diese Daten nicht für den Betrieb des vom Nutzer gewünschten Dienstes nötigt sind.

Außerdem wird dem Dienstanbieter die Speicherung von Informationen über das Endgerät untersagt, wie sie z. B. beim Verbindungsaufbau mit Angeboten im Internet anfallen. Ausgenommen hiervon ist die Speicherung erlaubt sofern diese Daten für den initialen Aufbau der Verbindung notwendig sind, jedoch auch dann nur für die Dauer, die für eine erfolgreiche Durchführung des Durchgangs nötig ist. Sollte ein Dienstanbieter die längere Speicherung dieser Informationen vorsehen, muss er hierfür jedoch den Nutzer entsprechend **Artikel 13 DSGVO** (Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person) vor der Erhebung der Daten informieren und die Datenverarbeitung nach **Artikel 32 DSGVO** (Abschnitt 2.1.8) absichern. Interessanterweise wird in **Artikel 8 (3)** die Möglichkeit gegeben, diese Information mittels standardisierten Bildsymbolen in klarer Form anzubieten, für deren Entwicklung bzw. für das Anstoßen der Entwicklung in **Artikel 8 (4)** der europäischen Kommission die Befugnis erteilt wird. Klare und allgemein verständliche Bildsymbole haben das Potential Endnutzer mehr für Datenschutz zu sensibilisieren und ihnen bewusst zu machen, in welche Art von Verarbeitung zu welchem Zweck sie gerade einwilligen.

2.2.4 Artikel 9 Einwilligung

Für die Einwilligung gelten grundsätzlich die Bestimmungen, die in **Artikel 7 DSGVO** (siehe Abschnitt 2.1.2) festgelegt wurden. Die Einwilligung kann nach **Artikel 9 (2)** vermutlich auch durch eine Einstellung im Browser des Nutzers erfolgen. Dies hätte zur Folge, dass etwa die „Do-Not-Track“-Funktion deutlich gestärkt werden könnte, da Internetseiten die Angabe dieser Option zukünftig verpflichtend berücksichtigen müssten. Browser müssen als Konsequenz so konfigurierbar sein, dass sie z. B. Cookies der besuchten Seite akzeptieren, Third-

Party-Cookies jedoch ablehnen. Für die Werbeindustrie könnte dies weitreichende Folgen haben, da sie nicht wie bisher, den „Do Not Track"-Header schlicht ignorieren können. Gleichzeitig dürfte dieser Artikel jedoch auch das Ende der teils aufdringlichen Cookie Warnungen auf Webseiten sein, da Cookies von der aufgerufenen Seite nach **Artikel 9** ohnehin in den meisten Fällen keine Warnung mehr benötigen dürften und die Behandlung von Cookies von Drittanbietern in die Verantwortung der Nutzer bzw. Browserhersteller übergeben werden würde. Eine Einwilligung in die Verarbeitung von Daten ist zukünftig also womöglich ganz formlos nicht nur durch das Setzen oder Entfernen eines Hakens in den Einstellungen eines Browsers möglich, sondern auch bereits dadurch, dass ein Nutzer eine Software einfach mit den vorgegebenen Einstellungen betreibt. **Artikel 9 (3)** verpflichtet den Verantwortlichen dazu, den von der Verarbeitung Betroffenen alle 6 Monate darauf hinzuweisen, dass er seine Einwilligung in die Verarbeitung seiner Daten jederzeit widerrufen kann.

2.2.5 Artikel 10 Informationen und Einstellungsmöglichkeiten

Wie bereits oben beschrieben, stellt **Artikel 10** im Entwurf vom Januar 2017 eine Abkehr vom Prinzip „Privacy by Design and Default" dar, dem in der DSGVO noch ein kompletter Artikel gewidmet wurde (**Artikel 25 DSGVO**). Software muss während der Installation lediglich über die möglichen Einstellungen zum Datenschutz informieren und vom Nutzer eine Entscheidung verlangen, statt wie bisher direkt die datenschutzfreundlichste Option vorausgewählt zu haben.

2.3 Das neue Bundesdatenschutzgesetz

Nach dem Inkrafttreten der europäischen Datenschutz-Grundverordnung am 24. Mai 2016 ist es nötig geworden, das deutsche Bundesdatenschutzgesetz an die neuen Gegebenheiten anzupassen. Die DSGVO gibt hierbei einen relativ engen Rahmen vor, der jedoch an einigen Stellen Öffnungsklauseln für nationale Regelungen anbietet.

Der „Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU)" [Ge17] der Bundesregierung vom 24. Februar 2017 ist die in dieser Form wohl mittlerweile endgültige Fassung der Anpassung des BDSG an die DSGVO.

Genau wie die vorangegangenen Entwürfe gibt es an diesem Entwurf erneut deutliche Kritik von vielen Seiten, die sich vor allem darauf konzentriert, dass der Entwurf versucht die Vorgaben der DSGVO zu ignorieren, um eigene nationale Fakten zu schaffen, die in der Regel die Vorgaben aus der DSGVO abschwächen sollen [Ne17].

Als Beispiel soll hier **§ 33 BDSG-neu** „Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden" heran gezogen werden. **§ 33 BDSG-neu** Abs. 1 weitet die in Artikel 23 DSGVO festgelegten möglichen Beschränkungen der in **Artikel 13 DSGVO** festgelegten Informationspflichten durch nationale Stellen anscheinend weiter aus. Möglicherweise genügt nach dem aktuellen Entwurf bereits eine Gefährdung für „die ordnungsgemäße Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben" einer öffentlichen Stelle als Begründung für ein Unterlassen der Informationspflicht. Auch die Anwendbarkeit von **Artikel 23 DSGVO** (Beschränkung der Informationspflicht) auf Fälle der öffentlichen Sicherheit wird im aktuellen Entwurf des neuen BDSG bereits anwendbar, sobald „die öffentliche Sicherheit oder **Ordnung**" gefährdet würde. Die Auswei-

tung auf den Bereich der öffentlichen Ordnung schränkt die Informationspflicht für öffentliche Stellen möglicherweise weiter ein.

Dies erscheint dadurch, dass bereits eine Gefährdung der Aufgabenerfüllung einer öffentlichen Stelle als Begründung für ein Unterlassen der Informationspflicht genügt, als eine Lockerung der Vorgaben der DSGVO.

§ 35 BDSG-neu „Recht auf Löschung" schränkt das in **Artikel 17 DSGVO** beschriebene Recht auf Löschung eher auf das „Recht auf Berichtigung der Verarbeitung" (Artikel 18 DSGVO) ein; und entspricht damit zunächst in der aktuellen Fassung eher der aktuell noch gültigen Fassung alten des BDSG. Außerdem wird auch nach der Neuregelung des BDSG noch die bisherige Rechtsprechung gültig bleiben. In dieser wird z. B. die Beschränkung des Rechts auf Löschung sehr streng ausgelegt und bezieht sich auf mittlerweile eher exotische Fälle wie die Speicherung auf permanenten Datenträgern wie etwa Lochkarten oder Magnetbänder, was für heutige Speichermethoden kaum noch anwendbar erscheint, da hier Löschung und Sperrung in der Regel den gleichen Aufwand bedeuten dürften. Es deutet jedoch alles darauf hin, dass es auch weiterhin kein absolutes Recht auf Löschung für einen Betroffenen geben wird.

Es wird sich also im Laufe der Zeit zeigen müssen, ob die bisherige Rechtsprechung in Verbindung mit der Neuregelung des bezüglich der Rechte der Betroffenen und Pflichten der Verantwortlichen weiter Bestand hat, oder, wie von manchen Kritikern vermutet [Kr17], relativ schnell vor dem europäischen Gerichtshof landen wird.

3 Umsetzung der DSGVO durch SkIDentity-Dienstes

In diesem Abschnitt soll zum Schluss noch kurz ein Überblick darüber gegeben werden, wie beispielsweise der SkIDentity-Dienst schon heute die Anforderungen der GDSVO erfüllt. Während die Nutzung eines Dienstes für das Identitätsmanagement für den Nutzer oftmals mit der teilweisen Aufgabe der Kontrolle über seine Identitätsdaten einhergeht und prominente Anbieter von modernen Single Sign-On Lösungen regelmäßig für ihren Umgang mit personenbezogenen Daten kritisiert werden, soll am Beispiel des SkIDentity-Dienstes gezeigt werden, wie im Einklang mit den Anforderungen der Datenschutz-Grundverordnung und der e-Privacy-Richtlinie ein sehr datenschutzfreundliches Identitätsmanagement-System umgesetzt werden kann.

Während die Identitätsdaten der Benutzer bei klassischen Systemen für das Identitätsmanagement in einer zentralen Datenbank vorgehalten werden, wird bei SkIDentity bewusst ein anderer, dezentraler Ansatz verfolgt. Hierbei werden die personenbezogenen Daten ausschließlich in kryptographisch geschützter Form, als so genannte „Cloud Identität", auf dem System des Nutzers abgelegt (**Artikel 25 DSGVO**).

Für die Anmeldung an Online-Diensten werden aus den Identitätsdaten des Nutzers datenschutzfreundliche Pseudonyme gebildet und nur solche Daten zu einem angeschlossenen Online-Dienst übertragen, die vom Online-Dienst für einen bestimmten Geschäftszweck benötigt werden (**Artikel 5 DSGVO**) und für die der Nutzer explizit in die Übertragung eingewilligt hat (**Artikel 7** und **25 DSGVO**).

Das Auskunftsrecht gemäß **Artikel 15 DSGVO** und das Recht auf Löschung (**Artikel 17 DSGVO)** kann der Nutzer direkt im Rahmen des von SkIDentity angebotenen Identitätsmanagements wahrnehmen. Das Recht auf Datenübertragbarkeit (**Artikel 20 DSGVO**)

wird durch die Bereitstellung der Identitätsdaten in Form von XML- oder JSON-basierten Datenstrukturen gewährleistet.

SkIDentity ist im Informationsverbund „Secure Cloud Infrastructure (SkIDentity)“ vom Bundesamt für Sicherheit in der Informationstechnik nach ISO/IEC 27001 auf Basis von IT-Grundschutz [BSIIGZ02502016] zertifiziert worden. Dies belegt insbesondere, dass im Einklang mit **Artikel 32 DSGVO** ein sehr hohes Sicherheitsniveau bei der Verarbeitung von personenbezogenen Daten gewährleistet wird.

Dass SkIDentity auch alle sonstigen Anforderungen für eine Auftragsdatenverarbeitung gemäß **Artikel 28 DSGVO** erfüllt, wird durch die Zertifizierung gemäß des „Trusted Cloud Datenschutz-Profil“ [TUVIT5529] mit der höchsten Schutzklasse III nachgewiesen.

4 Zusammenfassung und Ausblick

Mit der DSGVO wurde ein wichtiger Schritt zu einem europaweit harmonisierten Datenschutz gegangen, der das Datenschutzniveau im Mittel in Europa spürbar anheben dürfte. Jedoch gefährdet der bereits vorhandene EU-US Privacy Shield die Stärke der Verordnung noch bevor diese durch Aufsichtsbehörden angewandt werden kann. Außerdem droht mit der ePrivacy-Verordnung eine erste Aufweichung der DSGVO. Auch der neue Entwurf des BDSG lässt anscheinend Versuche erkennen, den bisher im weltweiten Vergleich außerordentlich starken deutschen Datenschutz abzuschwächen. Die ePrivacy-Verordnung und die Novelle des BDSG sind jedoch derzeit noch nicht komplett final. Dies lässt hoffen, dass die verbindliche Anwendbarkeit der DSGVO wirklich zur Folge hat, dass in Zukunft zumindest in ganz Europa ein einheitliches Niveau bezüglich des Datenschutzes herrscht und dieser rechtliche Rahmen nicht durch Nebenverordnungen und nationale Sonderbestimmungen aufgeweicht oder ausgehebelt wird.

Das Beispiel SkIDentity zeigt, dass bei datenschutzfreundlichen Systemen, die schon vor der Verabschiedung der DSGVO die einschlägigen Aspekte des Datenschutzes ernst genommen und insbesondere auch die Prinzipien „**Privacy by Design and by Default**“ berücksichtigt hatten, durch die DSGVO kein wesentlicher Änderungsbedarf besteht bzw. entstehen wird.

Referenzen

[Ba161] Bayerisches Landesamt für Datenschutzaufsicht. (26. Oktober 2016). *Auftragsverarbeitung nach der DS-GVO.* Von EU-Datenschutz-Grundverordnung (DS-GVO): https://www.lda.bayern.de/media/baylda_ds-gvo_10_processor.pdf abgerufen

[Ba16] Bayerisches Landesamt für Datenschutzaufsicht. (26. Oktober 2016). *Einwilligung nach der DS-GVO.* Abgerufen am 2017 von EU-Datenschutz-Grundverordnung (DS-GVO): https://www.lda.bayern.de/media/baylda_ds-gvo_9_consent.pdf

[Bay162] Bayerisches Landesamt für Datenschutzaufsicht. (01. September 2016). *Sanktionen nach der DS-GVO.* Abgerufen am 2017

[BSIIGZ02502016] BSI-IGZ-0250-2016. (kein Datum). ISO 27001 Zertifikat auf der Basis von IT-Grundschutz. *Secure Cloud Infrastructure (SkIDentity)* . https://www.skidentity.de/fileadmin/Ecsec-files/pub//BSI-IGZ-0250.pdf.

[Ge17] Gesetzentwurf der Bundesregierung. (2017. Feburar 2017). *Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU)* . https://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/entwurf-datenschutz-grundverordnung.pdf.

[Kr17] Krempl, S. (1. Februar 2017). *heise online*. Abgerufen am 12. Juni 2017 von Neues Datenschutzgesetz: Bundesregierung hebelt Bürgerrechte und Kontrollbefugnisse aus: https://www.heise.de/newsticker/meldung/Neues-Datenschutzgesetz-Bundesregierung-hebelt-Buergerrechte-und-Kontrollbefugnisse-aus-3614529.html

[Ne17] *Netzpolitik.org*. (09. März 2017). Abgerufen am 2017. Juni 12 von Kommentar: Das neue Bundesdatenschutzgesetz – ein postfaktisches Gesetz: https://netzpolitik.org/2017/kommentar-das-neue-bundesdatenschutzgesetz-ein-postfaktisches-gesetz/

[Po16] *Politico.* (Dezember 2016). Abgerufen am 15. März 2017 von EU ePrivacy Regulation leak: http://www.politico.eu/wp-content/uploads/2016/12/POLITICO-e-privacy-directive-review-draft-december.pdf

[Ri95] 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. (24. Oktober 1995). http://data.europa.eu/eli/dir/1995/46/oj.

[Pe17] Schaar, P. (28. Januar 2017). *heise online*. Abgerufen am 12. Juni 2017 von https://www.heise.de/newsticker/meldung/Analyse-Amerika-mauert-sich-ein-Privacy-Shield-vor-dem-Aus-3609712.html: https://www.heise.de/newsticker/meldung/Analyse-Amerika-mauert-sich-ein-Privacy-Shield-vor-dem-Aus-3609712.html

[TUVIT5529] TUVIT-5529.16. (kein Datum). Trusted Cloud Datenschutzprofil für Cloud-Dienste (TCDP). *SkIDentity, Version 2.0, im Betriebsmodus Klassik* . https://www.tuvit.de/fileadmin/Content/TUV_IT/zertifikate/de/5529UD_s.pdf.

[DSGVO] 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 . (27. April 2016). *(Datenschutz-Grundverordnung)* . http://data.europa.eu/eli/reg/2016/679/oj.

[ePrivacy] Vorschlag für eine über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG. (10. Januar 2017). *(Verordnung über Privatsphäre und elektronische Kommunikation)* . https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.