Nachfolgend finden sich alle 24 Beiträge des EUDataP-Weihnachtskalenders 2015. Ab dem 17.12.2015 beziehen sich die Beiträge auf die offizielle konsolidierte Fassung der Datenschutz-Grundverordnung nach den Trilogverhandlungen.

1. Dezember 2015

Was versteht die Datenschutz-Grundverordnung eigentlich unter „personenbezogenen Daten“?

Art. 4 Abs. 1 bzw. Abs. 2 DS-GVO definieren diesen, für die Anwendbarkeit des Datenschutzrechts so wichtigen Begriff. Dabei gehen alle drei Vorschläge der DS-GVO davon aus, dass es sich hierbei um Informationen handeln soll, die sich auf die sogenannte „betroffene Person“ beziehen.

Dies ist eine „bestimmte“ natürliche Person. Juristische Personen können sich also nicht auf den Schutz der DS-GVO berufen. Ausreichend ist jedoch auch, wenn diese natürliche Person „bestimmbar“ ist. Wann genau diese Bestimmbarkeit der betroffenen Person gegeben ist, da gehen die Vorschläge jedoch auseinander. So verlangt das Parlament etwa die Möglichkeit der direkten oder indirekten Identifizierung (!). Für den Rat und die Kommission ist ausreichend, dass die natürliche Person unter Zuhilfenahme und Zuordnung zu Kennnummern, Standortdaten oder einer OnlineKennung bestimmt werden kann. Die Voraussetzung der Identifizierung (Parlament) scheint jedoch dem Wortlaut nach höhere Anforderungen zu stellen.

Was sind Online-Kennungen? Nach Erwägungsgrund 24 (sowohl Kommission als auch Rat) handelt es sich dabei zum Beispiel um IP-Adressen oder Cookie-Kennungen. Jedoch stellen beide Versionen der Datenschutz-Grundverordnung im selben Erwägungsgrund klar, dass allein etwa die IP-Adresse (selbst wenn sie unter den Begriff der Online-Kennung fällt), für sich betrachtet noch kein personenbezogenes Datum darstellt. Zu diesem wird sie erst dann, wenn in Kombination/zusammen mit eindeutigen Kennungen betroffene Personen identifiziert (Achtung: Hier verweisen die Kommission und der Rat jeweils dann also doch auf die Voraussetzung der Identifizierung, die das Parlament in Art. 4 selbst verlangt) werden können.

Das Parlament schlägt zudem vor, in Art. 4 Abs. 2a DS-GVO den Begriff der „pseudonymisierten Daten“ zu definieren. Der Rat hingegen möchte in Art. 4 Abs. 3b DS-GVO die „Pseudonymisierung“, also den Vorgang selbst, definieren.

Etwas unklar scheinen die Entwürfe von Rat und Parlament mit Blick auf die Frage zu sein, ob denn “pseudonymisierte Daten” auch personenbezogene Daten sind. Art. 4 Abs. 2a DSG-VO der Parlamentsversion etwa sieht vor: “”pseudonymisierte Daten” personenbezogene Daten, die…”. Dem Wortlaut nach handelt es sich also um personenbezogene Daten. Ansonsten hätte man auch Formulierungen wie “Daten” oder “Informationen” wählen können. Art. 4 Abs. 3b DS-GVO der Ratsversion definiert die “Pseudonymiserung” als “Verarbeitung personenbezogener Daten”. Dies ist nicht wirklich überraschend, denn es liegen personenbezogene Daten vor, die nun pseudonymisiert werden sollen. Die Frage ist eher, was für das Ergebnis der Pseudonymisierung gilt. Diesbezüglich scheint der Rat davon auszugehen, dass pseudonymisierte Daten keinen Personenbezug aufweisen. Denn das Ergebnis der Pseudonymisierung soll sein, “dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können”.

2. Dezember 2015

Die Auftragsdatenverarbeitung und die DS-GVO

Art. 26 DS-GVO aller drei Entwürfe befasst sich mit dem „Auftragsverarbeiter". Eine Datenverarbeitung im Auftrag kann entweder auf der Grundlage eines Vertrages zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter oder aber auf der Grundlage eines

Rechtsaktes erfolgen (Art. 26 Abs. 2 DS-GVO). Der Rat möchte zudem als Grundlage eine Auftragsdatenverarbeitung auch nationale Vorschriften der Mitgliedstaaten aufnehmen.

Mit Blick auf die Kontrollbefugnisse des für die Verarbeitung Verantwortlichen möchte das Parlament vorsehen, dass der Auftragsverarbeiter Nachprüfungen bei sich vor Ort verpflichtend zulassen muss (Art. 26 Abs. 2 h) DS-GVO).

Kommission und Parlament möchten vorsehen, dass die per Gesetz in dem Vertrag zur Auftragsdatenverarbeitung zu regelnden Rechte und Pflichten zu „dokumentieren" sind, wobei sie auf keine spezielle Form dieser Dokumentation eingehen. Der Rat hingegen möchte vorsehen, dass der Vertrag „schriftlich abzufassen" ist (Art. 26 Abs. 3 DS-GVO), was jedoch auch in einem elektronischen Format erfolgen könne.

Zudem ist darauf hinzuweisen, dass die Anwendbarkeit der DS-GVO nicht mehr allein (wie derzeit etwa im BDSG) von dem Sitz des für die Verarbeitung Verantwortlichen oder dessen Niederlassung abhängig gemacht wird. Alle drei Entwürfe sehen in Art. 3 Abs. 1 DS-GVO vor, dass die Verordnung auf die Verarbeitung personenbezogener Daten Anwendung findet, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Auftragsverarbeiters in der Union erfolgt. Darüber hinausgehend möchte das Parlament die Verordnung auch dann zur Anwendung bringen, wenn ein Auftragsverarbeiter nicht in der Union niedergelassen ist, jedoch von in der Union ansässigen Personen Daten verarbeitet, mit dem Zweck, diesen Personen Waren oder Dienstleistungen anzubieten (Art. 3 Abs. 2 DS-GVO). Auch in Drittstaaten ansässige Auftragsverarbeiter ohne eine Niederlassung im europäischen Wirtschaftsraum würden also, bei Erfüllung der Voraussetzungen, dem Anwendungsbereich der DS-GVO unterliegen.

Auch möchte das Parlament in seinem Entwurf die Pflichten zur Einführung technisch und organisatorischer Maßnahmen und Verfahren, durch die sichergestellt werden soll, dass die Verarbeitung den Anforderungen der DS-GVO genügt (Datenschutz durch Technik; Privacy by Design) auf Auftragsverarbeiter erstrecken (Art. 23 Abs. 1 DS-GVO).

Zudem soll nach allen drei Entwürfen eine Person, der wegen einer rechtswidrigen Verarbeitung oder einer anderen mit der DS-GVO nicht zu vereinbarenden Handlung (!) (so zumindest Kommission und Parlament) ein Schaden entstanden ist, direkte Schadensersatzansprüche gegen den Auftragsverarbeiter haben (Art. 77 Abs. 1 DS-GVO).

3. Dezember 2015

Zur Datenübermittlung in Drittstaaten

Nach dem Urteil des Europäischen Gerichtshofs zu Safe Harbor, ist diese Thematik natürlich besonders „heiß". Wie genau die finalen Vorschriften der Datenschutz-Grundverordnung zur Übermittlung personenbezogener Daten in Drittstaaten (also außerhalb des europäischen Wirtschaftsraums) aussehen werden, bleibt daher, vorbehaltlich etwaiger Anpassung nach dem Urteil des Europäischen Gerichtshofs, abzuwarten.

Dem Grunde nach wird es jedoch ähnliche Vorgaben geben, wie sie schon derzeit innerhalb der Datenschutzrichtlinie existieren. So soll die EU-Kommission die Möglichkeit besitzen, Angemessenheitsentscheidung zu treffen. Alternativ können Datenübermittlung auch auf der Grundlage von Standardvertragsklauseln oder unternehmensinternen Vorschriften (BCR) erfolgen.

Neu ist jedoch etwa, dass Art. 43 Abs. 2 DS-GVO konkrete Vorgaben an den Inhalt von BCR macht.

Mit Blick auf die gesetzlichen Ausnahmen für Datenübermittlungen in Drittstaaten (wenn also kein Angemessenheitsbeschluss existiert und auch keine Standardvertragsklauseln oder BCR genutzt werden), legt Art. 44 DS-GVO die Voraussetzungen fest. So soll, wie auch derzeit, eine Datenübermittlung auf der Grundlage einer Einwilligung der betroffenen Person möglich sein.

Interessant ist insoweit, dass Kommission und Parlament allein die „Zustimmung“ zur Datenübermittlung verlangen, während der Rat darüber hinausgehend eine „ausdrückliche“ Einwilligung verlangt.

Weiterhin soll eine Datenübermittlung auch zur Durchführung eines Vertrages zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen erlaubt sein.

Die Entwürfe von Kommission und Rat sehen zudem die Möglichkeit einer Übermittlung für den Fall vor, wenn diese zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen erforderlich ist. Einschränkend darf eine solche Übermittlung jedoch nicht häufig, massiv (so die Kommission) oder in großem Maßstab (so der Rat) erfolgen. Der Rat möchte in seinem Entwurf zudem mögliche entgegenstehende Interessen und Grundrechte der betroffenen Personen einbeziehen, welche in diesem Fall der Datenübermittlung nicht überwiegen dürften.

Es stellt sich auch die Frage, was mit den derzeit existierenden Entscheidungen der EU-Kommission zu den Standardvertragsklauseln geschieht. Nach dem Entwurf der Kommission bleiben diese so lange in Kraft bis sie von der Kommission selbst geändert ersetzt oder aufgehoben wurden (Art. 41 Abs. 8 DS-GVO). Das Parlament möchte jedoch eine Ablauffrist einführen und betreffende Kommissionsentscheidungen sollen fünf Jahre nach Inkrafttreten der DS-GVO unwirksam werden.

4. Dezember 2015

Die Datenschutz-Grundverordnung und das Medienprivileg

Seit der Entscheidung des Europäischen Gerichtshofs in der Sache „Google Spain“ ist unter anderem auch die Frage nach der Regulierung und eventuell Einschränkung der Presse- oder allgemeiner Medienfreiheit durch das Datenschutzrecht stärker in den Fokus gerückt. Der Europäische Gerichtshof hat in seinem Urteil ausdrücklich darauf verwiesen, dass Webseitenbetreiber, deren Artikel in einer Suchergebnisliste verlinkt sind, sich (je nach Einzelfall) hinsichtlich des betreffenden Artikels auf der eigenen Website auf das Medienprivileg und damit umfassende Ausnahmen im Datenschutzrecht berufen können.

In der Datenschutz-Grundverordnung soll sich Art. 80 mit dieser Thematik befassen. Den derzeit geltenden Regelungen folgend hat die Kommission vorgeschlagen, dass die Mitgliedstaaten in ihren nationalen Gesetzen Abweichungen und Ausnahmen von den Regelungen der DS-GVO vorsehen sollen, wenn personenbezogene Daten allein (!) zu journalistischen, künstlerischen oder literarischen Zwecken verarbeitet werden (Art. 80 Abs.

1 DS-GVO). Das Parlament verzichtet auf das Erfordernis einer Datenverarbeitung allein zu journalistischen, künstlerischen oder literarischen Zwecken und verlangt von den Mitgliedstaaten die Schaffung entsprechender Ausnahmen bzw. Abweichungen „wann immer dies notwendig ist“ um das Recht auf Schutz der Privatsphäre mit den für die Freiheit der Meinungsäußerung geltenden Vorschriften in Einklang zu bringen. Auch der Rat nimmt in seinem Vorschlag Abstand von der Voraussetzung, dass eine Datenverarbeitung allein zu journalistischen, künstlerischen oder literarischen Zwecken erfolgen müsse. Zudem verweist der Rat in seiner Position zusätzlich auf das Recht auf Informationsfreiheit, welches mit dem Recht auf Schutz personenbezogene Daten in den nationalen Regelungen der Mitgliedstaaten in Einklang zu bringen ist.

Möglicherweise werden wir also in Zukunft in Europa wenig einheitliche Vorgaben zum Umgang mit personenbezogenen Daten für journalistische, künstlerische und literarische Zwecke vorfinden. Grundsätzlich scheint die Tendenz der Entwürfe der DS-GVO dahin zu gehen, Ausnahmen und Abweichungen von den datenschutzrechtlichen Regelungen schon früher eingreifen zu lassen, als dies derzeit der Fall ist.

Hinzuweisen ist noch auf den Umstand, dass der Rat in Erwägungsgrund 121 Ausnahmen und Abweichungen von den Vorgaben der Datenschutz-Grundverordnung insbesondere dann für geboten hält, wenn es um die Verarbeitung personenbezogener Daten im audiovisuellen Bereich sowie in Nachrichten- und Pressearchiven geht.

Zudem fordern alle drei Entwürfe in Erwägungsgrund 121, dass Begriffe, die sich auf das Recht auf freie Meinungsäußerung und das Recht, Informationen zu empfangen beziehen, weit auszulegen sind. Das Parlament möchte zudem klarstellen, dass diese weite Auslegung unabhängig davon geboten ist, welche Medien für die Inanspruchnahme dieser Grundrechte genutzt werden.

5. Dezember 2015

Datenschutz für Kinder

Erstmals soll es in der Datenschutz-Grundverordnung auch spezielle Vorgaben zum Umgang mit personenbezogenen Daten von Kindern geben. Erwägungsgrund 29 aller drei Entwürfe spricht davon, dass die personenbezogenen Daten von Kindern besonderen Schutz genießen müssten.

Unter dem geltenden Datenschutzrecht ist insbesondere nicht geklärt, ab welchem Alter Kinder selbstbestimmt über die Verarbeitung personenbezogener Daten entscheiden können. Eine feste Altersgrenze existiert nicht. Dies könnte sich mit der Datenschutz-Grundverordnung ändern.

So schlägt das Parlament vor, dass eine Einwilligung in eine Datenverarbeitung, die im Zusammenhang mit dem Angebot von Waren und Dienstleistungen an ein Kind steht, bis zur Vollendung dessen 13. Lebensjahres durch die Eltern oder den rechtlichen Vertreter abgegeben werden muss.

Art. 8 DS-GVO befasst sich insgesamt mit der Verarbeitung personenbezogener Daten von Kindern. Ein „Kind“ soll nach Art. 4 Abs. 18 DS-GVO der Entwürfe der Kommission und des Parlaments jede Person bis zur Vollendung des 18. Lebensjahres sein. Der Rat möchte diese Definition löschen.

Wenn die Einwilligung für die Verarbeitung personenbezogener Daten eines Kindes durch die Eltern oder einen anderen vertretungsberechtigten erfolgt, so hat der für die Verarbeitung

verantwortliche angemessene Anstrengungen zu unternehmen, um zu prüfen, dass die Einwilligung tatsächlich durch den Träger der elterlichen Verantwortung erteilt wurde (Art. 8 Abs. 1 der Entwürfe der Kommission und des Parlaments bzw. Art. 8 Abs. 1a des Ratsentwurfs).

6. Dezember 2015

Das Recht auf Vergessenwerden in der Datenschutz-Grundverordnung

Wie bereits hinlänglich bekannt, soll im Rahmen der DS-GVO ein sogenanntes „Recht auf Vergessenwerden“ für Betroffene das Licht der Welt erblicken. Der Europäische Gerichtshof hat dieses Recht (zumindest in gewissem Umfang) in seinem Google Spain-Urteil bereits aus der geltenden Datenschutzrichtlinie abgeleitet.

Art. 17 DS-GVO sieht in allen drei Entwürfen ein „Recht auf Löschung“ und in den Entwürfen von Kommission und Rat auch das „Recht auf Vergessenwerden“ vor. Dem Grunde nach unterschiedlich ist jedoch bereits die Voraussetzung ausgestaltet, wann ein für die Verarbeitung Verantwortlicher diesem Recht zur Geltung verhelfen muss. Nach den Vorschlägen von Kommission und Parlament hat die betroffene Person das Recht von dem für die Verarbeitung Verantwortlichen die Löschung von personenbezogenen Daten und die Unterlassung jeglicher weiteren Verbreitung dieser Daten zu verlangen. In diesen Entwürfen handelt es sich also um einen Anspruch, den der Betroffene geltend machen muss. Im Entwurf des Rates wird der für die Verarbeitung Verantwortliche direkt verpflichtet personenbezogene Daten zu löschen. Die Geltendmachung des Anspruchs ist hier also nicht erforderlich.

Nach dem Entwurf des Parlaments hat die betroffene Person zudem das Recht, von Dritten die „Löschung aller Querverweise auf diese personenbezogenen Daten bzw. aller Kopien davon“ zur verlangen.

Nach allen drei Entwürfen hängt der Anspruch bzw. die Verpflichtung von gewissen Voraussetzungen ab. Unter anderem, dass die Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind oder die Datenverarbeitung ursprünglich auf der Grundlage einer Einwilligung erfolgte, die von der betroffenen Person widerrufen wird und keine andere Rechtsgrundlage für die Verarbeitung existiert.

Das Parlament möchte den Anspruch des Betroffenen zudem davon abhängig machen, dass der für die Verarbeitung verantwortliche in der Lage ist, zu überprüfen, ob die Person, die die Löschung der Daten beantragt, tatsächlich die betroffene Person ist. Gegebenenfalls müsste der für die Verarbeitung Verantwortliche also zunächst einmal noch mehr personenbezogene Daten verarbeiten, um sicherzustellen und prüfen zu können, ob der Anspruchsteller nicht ein Dritter ist.

Zudem sieht Art. 17 Abs. 2 bzw. 2a DS-GVO in allen drei Entwürfen auch Regelungen dazu vor, was der für die Verarbeitung Verantwortliche unternehmen muss, wenn er die Daten öffentlich gemacht hat. Nach dem Entwurf der Kommission muss er alle vertretbaren Schritte unternehmen, um Dritte, die diese Daten verarbeiten, darüber zu informieren, dass die betroffene Person die Löschung aller Querverweise auf diese personenbezogenen Daten verlangt. Das Parlament macht diese Pflicht des für die Verarbeitung Verantwortlichen zusätzlich davon abhängig, dass die Daten „ohne Vorliegen eines Rechtfertigungsgrundes“ öffentlich gemacht wurden. Die Verpflichtung greift also im Entwurf des Parlaments erst nach Erfüllung einer weiteren Voraussetzung, geht dann jedoch inhaltlich über den Vorschlag der

Kommission hinaus, indem der für die Verarbeitung Verantwortliche auch dazu verpflichtet wird, alle zumutbaren Maßnahmen zu ergreifen, „um die Daten zu löschen und bei Dritten löschen zu lassen“. Eine reine Information von Dritten würde danach nicht ausreichen. Auch im Entwurf des Rates ist allein eine Pflicht zur Information von Dritten (explizit sogar nur von anderen für die Datenverarbeitung Verantwortlichen) vorgesehen.

7. Dezember 2015

Arbeitnehmerdatenschutz und die DS-GVO

Das Thema „Beschäftigtendatenschutz“ spielt in der Praxis eine wichtige Rolle. Gesetzliche Anläufe in Deutschland, einen umfassenden Regulierungsrahmen zu etablieren, sind bislang gescheitert. Art. 82 DS-GVO aller drei Entwürfe befasst sich in der Datenschutz-Grundverordnung mit der Verarbeitung personenbezogener Daten im Kontext eines Arbeitsverhältnisses.

Nach dem Entwurf der Kommission können Mitgliedstaaten in den Grenzen der DS-GVO per nationalem Gesetz die Verarbeitung personenbezogener Arbeitnehmerdaten im Beschäftigungskontext regeln, wobei beispielhaft einige Zwecke der möglichen Datenverarbeitung aufgelistet sind (Einstellung, Erfüllung des Arbeitsvertrages, Planung und Organisation der Arbeit oder auch Gesundheit und Sicherheit am Arbeitsplatz). Das Parlament wandelt in seinem Entwurf diese Vorgaben nur leicht ab, indem es etwa verlangt, dass nationale Vorschriften im Einklang mit den Regelungen der DS-GVO stehen und stets den Grundsatz der Verhältnismäßigkeit berücksichtigen müssen. Interessant ist jedoch die weitergehende Konkretisierungsanforderung an nationale Regelungen (Art. 82 Abs. 1a DS-GVO), wonach der Zweck der Verarbeitung mit dem Grund, wegen dem die Daten erhoben wurden, in Zusammenhang stehen muss und auch nur auf den Beschäftigungskontext beschränkt bleiben darf. Ausdrücklich ist eine Profilerstellung oder auch nur eine Verwendung der im Beschäftigungskontext erhobenen Daten für sekundäre Zwecke nicht gestattet. Nicht ganz klar ist, was mit den „sekundären“ Zwecken gemeint ist. Man wird wohl davon ausgehen können, dass davon alle anderen Zwecke außer jene mit Bezug auf den Beschäftigungskontext umfasst sind.

Nach dem Entwurf des Rates können die Mitgliedstaaten sowohl durch Rechtsvorschriften als auch durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Datenverarbeitung im Beschäftigungskontext vorsehen.

Eine „heiße“ Thematik im Arbeitnehmerdatenschutz ist oft die Frage nach der Wirksamkeit von Einwilligungen der Arbeitnehmer. Diesbezüglich sieht der Ratsentwurf vor (Art. 82 Abs. 3 DS-GVO), dass die Mitgliedstaaten durch nationale Rechtsvorschriften die Bedingungen festlegen können unter denen personenbezogene Daten im Beschäftigungskontext auf der Grundlage einer Einwilligung verarbeitet werden dürfen. In der Folge könnten sich also in den verschiedenen Mitgliedstaaten der Europäischen Union ganz differenzierte Anforderungen an eine datenschutzrechtliche Einwilligung im Beschäftigungskontext ergeben. Multinationale Unternehmen, mit Arbeitnehmern in vielen verschiedenen Staaten, müssten diese verschiedenen nationalen Vorgaben dann beachten.

Interessant ist zudem der Vorschlag des Parlaments (Art. 82 Abs. 1d DS-GVO), ein „eingeschränktes“ Konzernprivileg für die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe zu etablieren. Eingeschränkt deshalb, weil sich dieses Konzernprivileg nur auf personenbezogene Beschäftigtendaten bezieht und die Übermittlung für den Geschäftsbetrieb relevant und der Abwicklung von zweckgebundenen Arbeits- oder

Verwaltungsvorgängen dienen muss. Daneben möchte das Parlament klarstellen, dass Regelungen zur Nutzung bzw. zum Umfang der Nutzung von Telefon, E-Mail und Internet auch zu privaten Zwecken durch Kollektivvereinbarungen geschaffen werden können (Art. 82 Abs. 1c d) DS-GVO). Auch wenn eine private Nutzung erlaubt ist, darf der Arbeitgeber Verkehrsdaten insbesondere zur Gewährleistung der Datensicherheit und zur Sicherstellung des ordnungsgemäßen Betriebs verarbeiten.

8. Dezember 2015

Datensicherheit: die technischen und organisatorischen Maßnahmen

Art. 30 DS-GVO behandelt das Thema der „Sicherheit der Verarbeitung“. Vergleichbar ist diese Vorschrift in etwa mit dem derzeit geltenden § 9 BDSG. Etwas spezifischer als derzeit vorgegeben, umfasst die Verpflichtung, technische und organisatorische Maßnahmen zu treffen, das Erfordernis der Geeignetheit dieser Maßnahmen, welche von den jeweils gegebenen Risiken der Datenverarbeitung und auch der Art der zu schützenden personenbezogenen Daten abhängt (so die Entwürfe der Kommission und des Parlaments).

Der Rat möchte in seinem Entwurf das Prinzip des risikobasierten Ansatzes (welcher im Entwurf des Rates für die DS-GVO ohnehin verstärkt Bedeutung erlangt) festschreiben und verlangt daher, dass technische und organisatorische Maßnahmen zudem unter Berücksichtigung der Zwecke der Datenverarbeitung sowie der Wahrscheinlichkeit und der Höhe des Risikos für die persönlichen Rechte und Freiheiten der Betroffenen umgesetzt werden. Ausdrücklich verweist der Entwurf des Rates zudem beispielhaft auf eine Pseudonymisierung personenbezogener Daten.

Im Entwurf des Parlaments wird zudem ein Maßnahmenkatalog etabliert, der an die Vorgaben der derzeitigen Anlage zu § 9 S. 1 BDSG erinnert (Art. 30 Abs. 1a DS-GVO). Interessant hierbei ist, dass die in Bezug genommene „Sicherheitspolitik“ im Parlamentsentwurf die durch technische und obligatorische Maßnahmen zu etablierenden „Fähigkeiten“ verpflichtend vorzuschreiben scheint. Denn dem Wortlaut nach umfasst die Sicherheitspolitik „folgendes“ und nicht etwa „unter anderem“ oder „beispielsweise“ folgendes. In Art. 30 Abs. 2 DS-GVO stellt das Parlament zudem das durch die Implementierung technischer und organisatorischer Maßnahmen „zumindest“ zu bewirkende Ergebnis dar. So muss mit den Maßnahmen sichergestellt werden, dass nur ermächtigte Personen für rechtlich zulässige Zwecke Zugang zu Person bezogenen Daten erhalten. Zudem muss die Umsetzung eines Sicherheitskonzepts für die Verarbeitung personenbezogene Daten gewährleistet sein.

Der Rat möchte dem für die Verarbeitung Verantwortlichen als auch dem Auftragsverarbeiter zu dem aufgeben, „Schritte zu unternehmen“, um sicherzustellen, dass ihnen unterstellte Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des für die Datenverarbeitung Verantwortlichen verarbeiten (Art. 30 Abs. 2b DS-GVO).

Von der Kommission im Originalentwurf vorgesehene Möglichkeiten zum Erlass delegierter Rechtsakte oder von Durchführungsbestimmungen wurden von Rat und Parlament gestrichen.

9. Dezember 2015

Dokumentationspflichten: was wird aus dem schönen Verfahrensverzeichnis?

Nach allen drei Entwürfen der DS-GVO haben sowohl der für die Verarbeitung Verantwortliche als auch der Auftragsverarbeiter gewisse Dokumentationspflichten (Art. 28 DS-GVO).

Nach dem Entwurf der Kommission sind die der Zuständigkeit des für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters unterliegenden Verarbeitungsvorgänge zu dokumentieren. Das Parlament möchte die Dokumentationspflicht dahingehend präzisieren, dass die verpflichteten Stellen eine Dokumentation für den Zweck vorhalten und auch aktualisieren müssen, um die Anforderungen der DS-GVO zu erfüllen. Danach muss also nur dokumentiert werden, was tatsächlich auch gesetzlich gefordert wird (beispielsweise der Nachweis einer erteilten Einwilligung). Der Rat möchte die allgemeine Dokumentationspflicht zunächst nur auf den für die Verarbeitung Verantwortlichen begrenzen. Nach Art. 28 Abs. 2a DS-GVO des Ratsentwurfs sind jedoch auch Auftragsverarbeiter dazu verpflichtet, eine Aufzeichnung zu allen Kategorien von den im Auftrag durchgeführten Tätigkeiten der Verarbeitungen personenbezogener Daten zu führen. Der inhaltliche Umfang der Dokumentationspflicht ist in diesem Fall jedoch eingeschränkt.

Interessant ist, wie die drei Entwürfe die Frage behandeln, was genau zu dokumentieren ist. So sieht der Kommissionsentwurf in Abs. 2 eine Liste von Informationen vor, die der zuvor benannten allgemeinen Dokumentationspflicht unterfallen. Der Parlamentsentwurf entgegen nimmt ausdrücklich eine Unterscheidung zu der allgemeinen Dokumentationspflicht in Abs. 1 vor und verlangt in Abs. 2 „darüber hinaus“ eine Dokumentation von weiteren näher aufgeführten Informationen.

Der Rat und die Kommission möchten in ihren Entwürfen zudem eine Ausnahmeregelung für KMUs vorsehen (Art. 28 Abs. 4 b) DS-GVO). Die in den Abs. 1 und 2 aufgestellten Verpflichtungen für eine Dokumentation gelten danach nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen. Der Rat möchte diesbezüglich jedoch eine Rückausnahme vorsehen, nämlich für den Fall, dass die vorgenommene Datenverarbeitung aufgrund ihrer Art, ihres Umfangs, ihrer Umstände oder ihrer Zwecke voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen birgt.

Mit Blick auf die tatsächlich zu dokumentierenden Informationen lässt sich beispielhaft anmerken, dass etwa Rat und Kommission es als ausreichend erachten, wenn die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten dokumentiert werden. Das Parlament möchte verlangen, dass „Name und Kontaktdaten“ für die Verarbeitung Verantwortlichen, denen personenbezogene Daten mitgeteilt werden, zu dokumentieren sind.

10. Dezember 2015

Der Datenschutzbeauftragte in der DS-GVO

Kommission und Parlament möchten, unter gewissen Voraussetzungen, die Pflicht für verantwortliche Stellen und Auftragsverarbeiter vorsehen, einen Datenschutzbeauftragten zu benennen (Art. 35 DSGVO). Der Ratsentwurf möchte eine solche Pflicht auf europäischer Ebene nicht vorgeben bzw. überlässt dies den nationalen Rechtsvorschriften.

Die Kommission möchte die Bestellungspflicht unter anderem davon abhängig machen, ob eine öffentliche Einrichtung personenbezogene Daten verarbeitet oder aber ein Unternehmen, welches 250 oder mehr Mitarbeiter beschäftigt. Abweichend hiervon verlangt das Parlament eine Bestellung, wenn eine Datenverarbeitung von einer juristischen Person

durchgeführt wird und sich diese Datenverarbeitung auf mehr als 5000 betroffene Personen innerhalb von zwölf Monaten bezieht.

Alle drei Entwürfe sehen explizit die Möglichkeit vor, dass eine Gruppe von Unternehmen einen gemeinsamen bzw. Hauptdatenschutzbeauftragten ernennen kann.

Kommission und Parlament möchten zudem verpflichtend vorschreiben, für welchen Mindestzeitraum ein Datenschutzbeauftragter zu bestellen ist. Die Kommission verlangt eine Bestellung für mindestens zwei Jahre (Art. 35 Abs. 7 DS-GVO). Das Parlament sogar eine Bestellung für vier Jahre, wenn es sich um einen Beschäftigten des für die Verarbeitung Verantwortlichen handelt oder auch für zwei Jahre, wenn die Tätigkeit durch einen externen Dienstleister erfüllt wird.

Auch wenn die drei Entwürfe die Pflicht zur Bestellung des Datenschutzbeauftragten unterschiedlich regeln, so stellen sie doch gewisse Anforderungen an die Qualifikation des Datenschutzbeauftragten (Art. 35 Abs. 5 DS-GVO). So ist die jeweilige Person nach Maßgabe ihrer beruflichen Qualifikation und insbesondere ihres Fachwissens, dass sie auf dem Gebiet des Datenschutzrechts und der einschlägigen Praktiken (so Kommission und Parlament) bzw. der Datenschutzpraxis (so der Rat) besitzt, auszuwählen. Zudem muss die Fähigkeit zur Erfüllung der in Art. 37 DS-GVO gesetzlich vorgegebenen Aufgaben gegeben sein.

Zu diesen Aufgaben gehören unter anderem: Unterrichtung und Beratung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters zu bestehenden rechtlichen Pflichten, sowohl nach der DS-GVO als auch nach nationalen Datenschutzvorschriften; Überwachung der Umsetzung (so Kommission und Parlament) bzw. der Einhaltung (so der Rat) der Strategien für den Schutz personenbezogener Daten und der Vorgaben der DS-GVO und anderer Datenschutzvorschriften der Union oder der Mitgliedstaaten (so der Rat); Tätigkeit als Ansprechpartner für die jeweils zuständige Aufsichtsbehörde.

Selbst wenn es also am Ende zu der vom Rat präferierten Lösung kommen sollte, dass auf europäischer Ebene keine Pflicht zur Bestellung besteht, sondern dies den Mitgliedstaaten in ihrem nationalen Recht überlassen bleibt, müssen dennoch die Anforderungen an die Fähigkeiten der Person des Datenschutzbeauftragten und ihren Aufgabenumfang in der DS-GVO berücksichtigt werden.

11. Dezember 2015

Das Recht auf Datenübertragbarkeit

Art. 18 der Entwürfe von Kommission und Rat sehen das „Recht auf Datenübertragbarkeit“ vor. Das Parlament möchte dieses Recht im Rahmen des Auskunftsanspruchs in Art. 15 verorten.

Nach den Entwürfen von Kommission und Rat soll die betroffene Person das Recht haben, die sie betreffenden personenbezogenen Daten, die sie zuvor einem für die Verarbeitung Verantwortlichen zur Verfügung gestellt bzw. bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten (die Kommission spricht von einem gängigen elektronischen Format). Deutlich wird hier bereits, dass ich dieses Recht nur gegen einen für die Verarbeitung Verantwortlichen richtet.

Nach dem Entwurf des Rates hat die betroffene Person danach ein Recht, diese Daten einem anderen für die Verarbeitung Verantwortlichen zu übermitteln. Die Kommission spricht in ihrem Entwurf davon, dass die betroffene Person das Recht hat, die Daten in ein anderes

System zu überführen, ohne zu spezifizieren, welche Stelle der Empfänger der Daten sein kann.

Wichtig ist zudem, dass sowohl Kommission und Rat vorschreiben, dass die Übermittlung der Daten durch den für Verarbeitung Verantwortlichen, bei dem die Daten liegen, nicht behindert werden darf. Beide Entwürfe schweigen sich jedoch darüber aus, ob die empfangende Stelle gewisse Voraussetzungen aufstellen darf, die die Übermittlung behindern würden.

Zudem möchte der Rat den Anwendungsbereich von Art. 17 einschränken und das Recht auf Datenübertragbarkeit dann nicht gelten lassen, wenn eine Datenverarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in der Ausübung öffentlicher Gewalt erfolgt (Abs. 2a). Sowohl Kommission und Rat beschränken den Anwendungsbereich von Art. 17 weiterhin auf Datenverarbeitungen, die auf der Grundlage einer Einwilligung oder eines Vertrages erfolgen.

Wie erwähnt, integriert das Parlament das Recht auf Datenübertragbarkeit in Art. 15 Abs. 2a DS-GVO. Danach hat die betroffene Person das Recht, von dem für die Verarbeitung Verantwortlichen eine Kopie der zur Verfügung gestellten personenbezogenen Daten in einem „interoperablen gängigen elektronischen“ Format zu verlangen. Zudem darf sie auch nach dem Vorschlag des Parlaments hierbei nicht von dem für die Verarbeitung Verantwortlichen, von denen die Daten herausgegeben werden, behindert werden.

Im Unterschied zu Kommission und Rat verlangt das Parlament jedoch, dass, soweit es technisch machbar und verfügbar ist, die Daten auf Verlangen der betroffenen Person unmittelbar von dem für die Verarbeitung Verantwortlichen an einen anderen für die Verarbeitung Verantwortlichen übermittelt werden. Das Parlament sieht also durchaus eine Situation vor, in der die Daten direkt zwischen zwei verantwortlichen Stellen übermittelt werden können, ohne dass die betroffene Person die Daten als Zwischenstelle erhält.

12. Dezember 2015

Die Einwilligung in der DS-GVO

Nach allen drei Entwürfen stellt die datenschutzrechtliche Einwilligung auch in Zukunft eine Grundlage für die Verarbeitung personenbezogene Daten dar (Art. 6 Abs. 1 a) DS-GVO). Nach den Entwürfen von Kommission und Parlament muss die betroffene Person die Einwilligung für einen oder mehrere genau festgelegte Zwecke abgeben. Der Entwurf des Rates fordert darüber hinausgehend, dass die betroffene Person ihre „unmissverständliche“ Einwilligung gegeben hat.

In Art. 4 Abs. 8 DS-GVO aller drei Entwürfe soll die Einwilligung definiert werden. Nach dem Vorschlag der Kommission handelt es sich dabei um „jede ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgte explizite Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen Handlung “. Der Entwurf des Parlaments streicht den Terminus „explizit“ und ersetzt ihn durch „ausdrücklich“. Der Ratsentwurf wiederum streicht sowohl den Terminus „explizit“ als auch „ausdrücklich“.

In Art. 7 DS-GVO werden in allen drei Entwürfen die Bedingungen für eine wirksame Einwilligung näher spezifiziert. Nach den Entwürfen von Parlament und Kommission trägt der für die Verarbeitung verantwortliche die Beweislast dafür, dass die betroffene Person ihre Einwilligung für eindeutig festgelegte Zwecke erteilt hat. Nach dem Entwurf des Rates muss der für die Verarbeitung Verantwortlichen nachweisen können, dass die betroffene Person ihre unmissverständliche Einwilligung erteilt hat. In allen drei Entwürfen wird vorgesehen,

dass das Erfordernis (so Kommission und Parlament) bzw. das Ersuchen (so der Rat) um die Einwilligung äußerlich erkennbar von anderen Sachverhalten getrennt wird bzw. zu unterscheiden ist, wenn die Einwilligung durch eine schriftliche Erklärung erfolgen soll die noch andere Sachverhalte betrifft. In allen drei Entwürfen geht es hier also um eine deutliche Hervorhebung bzw. Abgrenzung der datenschutzrechtlichen Einwilligung von übrigen Texten, wenn von der auch für die Einwilligung relevanten Erklärung weitere Sachverhalte umfasst sind.

Alle drei Entwürfe sehen vor, dass die betroffene Person das Recht hat, ihre Einwilligung jederzeit zu widerrufen (Art. 7 Abs. 3 DS-GVO). Vergangene Datenverarbeitungen werden durch einen Widerruf jedoch nicht berührt, er wirkt also nur ex-nunc. Der Rat möchte zusätzlich vorsehen, dass die betroffene Person vor Abgabe der Einwilligung über das Widerrufsrecht informiert wird. Das Parlament möchte darüber hinausgehend vorsehen, dass die betroffene Person darüber informiert wird, wenn ein Widerruf zu einer Einstellung der erbrachten Dienstleistungen oder der Beendigung der Beziehung zu dem für die Verarbeitung Verantwortlichen führen kann.

13. Dezember 2015

Profiling und Nutzungsanalyse

Art. 20 DS-GVO aller drei Entwürfe befasst sich mit der Thematik des sog. Profiling. Nach dem Entwurf der Kommission hat eine natürliche Person das Recht, nicht einer auf einer rein automatisierten Verarbeitung von Daten basierenden Maßnahme unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie maßgeblich beeinträchtigt. Ähnlich umschreibt der Ratsentwurf, dass eine betroffene Person das Recht hat, nicht einer allein auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden. Bei genauem Vergleich der beiden Entwürfe fällt auf, dass der Kommissionsentwurf auf „Maßnahmen“ abzielt, wohingegen der Ratsentwurf eine „Entscheidung“ erwähnt. Der Anwendungsbereich des Kommissionsentwurfs dürfte vom Wortlaut her daher weiter sein, da Maßnahmen ja nicht unbedingt eine vorherige Entscheidung erfordern.

Der Parlamentsentwurf sieht vor, dass jede natürliche Person das Recht hat, dem Profiling zu widersprechen und die betroffene Person über dieses Recht in deutlich sichtbarer Weise zu unterrichten ist. Der Parlamentsentwurf definiert in Art. 4 Abs. 3a DS-GVO das Profiling als jede Form automatisierter Verarbeitung personenbezogener Daten, die zu dem Zweck vorgenommen wird, bestimmte personenbezogene Aspekte zu bewerten oder insbesondere die Leistungen der betroffenen Person oder ihr Verhalten zu analysieren. Eine ähnliche Definition findet sich in Art. 4 Abs. 12a DS-GVO des Ratsentwurfs.

Interessant ist die unterschiedliche Herangehensweise der drei Entwürfe an das Thema Profiling. So sehen der Entwurf der Kommission und des Rates ein Recht der betroffenen Personen vor, einer Maßnahme bzw. einer Entscheidung nicht unterworfen zu werden. Nach dem Entwurf des Parlaments können betroffene Person durchaus einer solchen Maßnahme bzw. Entscheidung unterworfen werden, sie besitzen dann eben nur ein Widerspruchsrecht.

Nach dem Entwurf des Rates besitzt die betroffene Person das entsprechende Recht jedoch nicht, wenn die Entscheidung für den Abschluss oder die Erfüllung eines Vertrages erforderlich ist oder aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten zugelassen wird und diese Rechtsvorschriften geeignete Schutzmaßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person vorsehen (Art. 20 Abs. 1a DS-GVO). Eine Ausnahme sei ebenfalls dann gelten, wenn die betroffene Person ausdrücklich (!) eingewilligt hat.

Die Entwürfe von Kommission und Parlament sehen hingegen in Abs. 2 Voraussetzungen vor, wann ein Profiling betroffener Personen überhaupt erst gestattet ist. Diese Voraussetzungen gelten jedoch nur dann, wenn es sich um Maßnahmen handelt, durch die sich rechtliche Konsequenzen für die betroffene Person oder ähnliche erhebliche Auswirkungen auf die Interessen, Rechte oder Freiheiten der betroffenen Person ergeben (so der Entwurf des Parlaments). Erlaubt es ein Profiling danach, wenn es für den Abschluss oder die Erfüllung eines Vertrages erforderlich ist und dieser Abschluss oder die Erfüllung auf Wunsch der betroffenen Person erfolgt ist. Das Parlament stellt als zusätzliche Voraussetzungen auf, dass geeignete Maßnahmen ergriffen wurden, um die berechtigten Interessen der betroffenen Person zu wahren, wohingegen die Kommission das Ergreifen geeigneter Maßnahmen alternativ zu der Voraussetzung des Wunsches der betroffenen Person ausgestaltet. Nach beiden Entwürfen ist das Profiling auch dann erlaubt, wenn dies ausdrücklich aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten gestattet ist oder die betroffene Person eingewilligt hat (anders jedoch als der Entwurf des Rates, wird hier keine ausdrückliche Einwilligung verlangt).

Das Parlament möchte zudem vorsehen (Abs. 5), dass sich ein Profiling, welches Maßnahmen zur Folge hat, durch die sich rechtliche Konsequenzen für die betroffene Person ergeben, nicht ausschließlich oder vorrangig auf eine automatisierte Verarbeitung stützen darf und stets eine persönliche Prüfung enthalten muss.

14. Dezember 2015

Informationspflichten gegenüber betroffenen Personen

Alle drei Entwürfe der DS-GVO sehen in Art. 14 gewisse Informations- bzw. Unterrichtungspflichten des für die Verarbeitung Verantwortlichen vor, die bei der Erhebung personenbezogener Daten zu erfüllen sind. Insgesamt lässt sich feststellen, dass die zu erteilenden Informationen weitaus genauer und auch umfangreicher geregelt sind, als dies derzeit der Fall ist. Zu den verpflichten zu erteilenden Informationen (im Internet oder in einer App etwa in der Form einer Datenschutzerklärung) gehören unter anderem:

Name und Kontaktdaten des für die Verarbeitung Verantwortlichen und auch des Datenschutzbeauftragten; die Zwecke, für die Daten verarbeitet werden; die jeweilige Rechtsgrundlage der Datenverarbeitung (dies kann bedeuten, dass in einer Datenschutzerklärung zu verschiedenen Datenverarbeitungsprozessen auch Informationen zu unterschiedlichen Rechtsgrundlagen erteilt werden müssen).

Parlament und Kommission möchten zudem verpflichtend vorsehen, dass noch unter anderem folgende Informationen erteilt werden: die Dauer, für die die personenbezogenen Daten gespeichert werden bzw. die Kriterien für die Festlegung der Dauer; das Bestehen eines Rechts auf Auskunft sowie Berichtigung oder Löschung; das Bestehen eines Beschwerderechts bei der Datenschutzbehörde; die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten. Das Parlament verlangt in seinem Entwurf zudem, dass aussagekräftige Informationen über die Logik einer automatisierten Datenverarbeitung erteilt werden.

Der Entwurf des Rates geht einen etwas anderen Weg. Zum einen bestehen verpflichtend zu erteilende Informationen. Zudem ist je nach Einzelfall abhängig, ob der für die Datenverarbeitung Verantwortliche eventuell weitere Informationen erteilen muss (Art. 14 Abs. 1a DS-GVO). Diese sollen dann erteilt werden, wenn sie unter Berücksichtigung der besonderen Umstände und Rahmenbedingungen, unter denen die personenbezogenen Daten verarbeitet werden, „notwendig sind, um eine faire und transparente Verarbeitung zu

gewährleisten“. Zu diesen Informationen gehören unter anderem: die Benennung der berechtigten Interessen, die von dem für die Verarbeitung Verantwortlichen verfolgt werden, wenn er seine Datenverarbeitung auf Art. 6 Abs. 1 f) DS-GVO stützt; die Empfänger oder Kategorien von Empfängern; die Absicht, personenbezogene Daten an einen Empfänger in einem Drittland zu übermitteln; wenn die Verarbeitung auf eine Einwilligung beruht, die Information über das Bestehen des Rechts, die Einwilligung jederzeit zu widerrufen; das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde.

Insgesamt dürfte also der Katalog an zu erteilenden Informationen weitaus umfangreicher und detaillierter ausfallen, als dies bei vielen Datenschutzerklärungen derzeit der Fall ist. Daneben bestehen zudem Informationspflichten, wenn die personenbezogenen Daten nicht direkt bei der betroffenen Person erhoben werden.

15. Dezember 2015

Das Auskunftsrecht in der DS-GVO

In Art. 15 aller drei Entwürfe soll das Auskunftsrecht der betroffenen Personen vorgesehen werden. Kommission und Parlament möchten regeln, dass betroffene Personen das Auskunftsrecht „jederzeit“ in Anspruch nehmen können. Der Rat möchte einschränkend vorsehen, dass die Ausübung nur „in angemessenen Abständen“ dafür jedoch ausdrücklich „unentgeltlich“ erfolgen darf.

Zu beachten ist, dass das Auskunftsrecht in allen drei Entwürfen zweigeteilt ist, wobei sich diese Zweiteilung in der Praxis häufig nicht auswirken wird. Denn alle drei Entwürfe sehen als erste Stufe des Auskunftsrechts eine bloße „Bestätigung“ vor, dass personenbezogene Daten verarbeitet werden. Ist dies der Fall, so hat der für die Verarbeitung verantwortliche eine in Art. 15 inhaltlich näher spezifizierte Auskunft zu erteilen. Das Parlament möchte zu dem generell vorsehen, dass die Auskunft und die in ihr enthaltenen Informationen in einfacher und verständlicher Sprache zu erfolgen haben.

Unter anderem muss über folgende Informationen Auskunft erteilt werden:

Die Verarbeitungszwecke, wobei das Parlament zusätzlich vorsehen möchte, dass die Verarbeitungszwecke für jede Kategorie personenbezogener Daten aufgeschlüsselt werden müssen. Parlament und Kommission möchten zudem, dass Informationen über die Kategorien personenbezogener Daten, die verarbeitet werden erteilt werden. Zudem über die Empfänger oder Kategorien von Empfängern, an die die personenbezogenen Daten weitergegeben werden, speziell bei Empfängern in Drittländern. Auch Informationen über die Dauer, für die die personenbezogenen Daten gespeichert werden, sollen zumindest nach dem Entwurf der Kommission erteilt werden. Das Parlament möchte alternativ die Information darüber ausreichen lassen, welche Kriterien für die Festlegung der Speicherdauer angewendet werden. Der Rat möchte vorsehen, dass die Information über die Speicherfrist erteilt wird, wenn dies möglich ist. Etwas schwammig scheint die Verpflichtung des Parlaments zu sein, auch über die Tragweite der Verarbeitung und die mit ihr angestrebt den Wirkungen zu informieren. Das Parlament möchte zudem die Information auf die Logik einer automatisierten Datenverarbeitung erstrecken.

Zum Verfahren selbst möchte der Rat vorsehen, dass ein Anspruch auf eine Kopie der zu erteilenden Informationen nicht besteht, wenn eine solche Kopie nicht zur Verfügung gestellt werden kann, ohne personenbezogene Daten anderer betroffener Personen oder vertrauliche Daten des für die Verarbeitung Verantwortlichen offen zu legen.

16. Dezember 2015

Benachrichtigungspflicht bei Verletzung des Schutzes personenbezogener Daten

In den Art. 31 und 32 DS-GVO soll in allen drei Entwürfen eine Benachrichtigungspflicht, sowohl an die Aufsichtsbehörde als auch an die betroffene Person, für den für die Verarbeitung Verantwortlichen statuiert werden.

Nach dem Entwurf der Kommission soll die Meldung an die Aufsichtsbehörde ohne unangemessene Verzögerung nach Möglichkeit innerhalb von 24 Stunden nach Verstellung der Verletzung erfolgen. Der Entwurf des Parlaments sieht eine „unverzügliche“ Meldung vor. Der Rat sieht die Pflicht zur Meldung ohne „unangemessene Verzögerung“ vor, die nach Möglichkeit innerhalb von 72 Stunden nach Verstellung der Verletzung erfolgen soll. Der Rat möchte zudem direkt die Voraussetzungen einer Meldung in Art. 31 Abs.1 DS-GVO regeln und diese daher nicht bei jeder Verletzung des Schutzes personenbezogener Daten vorschreiben. Die Meldung soll dann erfolgen, wenn eine Verletzung des Schutzes personenbezogener Daten vorliegt, die voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge hat, wobei als Beispiele Diskriminierung, Identitätsdiebstahl, Betrug, finanzielle Verluste oder Rufschädigung genannt werden. Zudem sieht der Rat eine Ausnahme von der Meldepflicht vor, wenn nämlich nach Art. 32 DS-GVO auch eine Meldung an die betroffene Person nicht erforderlich ist.

Alle drei Entwürfe sehen zudem in Abs. 1 eine Pflicht des Auftragsverarbeiters vor, den für die Verarbeitung Verantwortlichen zu informieren, wenn eine Verletzung des Schutzes personenbezogener Daten festgestellt wird, wobei das Parlament eine „unverzügliche“ Meldung erfordert und der Rat diese „ohne ungebührliche Verzögerung“ verlangt.

In Abs. 3 werden die Mindestangaben festgeschrieben, die in der Meldung an die Aufsichtsbehörde enthalten sein müssen. Hierzu gehört unter anderem, eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten mit Angaben der Kategorien und der Zahl der betroffenen Personen oder auch Name und Kontaktdaten des Datenschutzbeauftragten. Kommission und Parlament möchten zudem Empfehlungen für Maßnahmen zur Eindämmung etwaiger negativer Auswirkungen als verpflichtende Informationen vorsehen.

Zudem ist der für die Verarbeitung verantwortliche nach Abs. 4 verpflichtet etwaige Verletzungen des Schutzes personenbezogener Daten zu dokumentieren. Die Dokumentation hat vor allem den Zweck, im Nachhinein der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen des Art. 31 DS-GVO zu ermöglichen.

In Art. 32 DS-GVO sehen alle drei Entwürfe die Pflicht zur Benachrichtigung der betroffenen Personen vor. Diese steht jedoch unter der Voraussetzung, dass eine Wahrscheinlichkeit besteht, dass der Schutz der personenbezogenen Daten oder der Privatsphäre der betroffenen Personen durch eine festgestellte Verletzung beeinträchtigt wird. So zumindest die Entwürfe von Kommission und Parlament. Der Rat möchte die Benachrichtigungspflicht der Betroffenen davon abhängig machen, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge hat.

17. Dezember 2015

Rechtsmittel gegen Aufsichtsbehörden

In Art. 74 DS-GVO wird das Recht jeder natürlichen oder juristischen Person auf einen gerichtlichen Rechtsbehelf gegen sie betreffende Entscheidungen einer Aufsichtsbehörde festgeschrieben. Es wird ausdrücklich nicht von dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter, sondern umfassender von „juristischen Personen“ gesprochen. Interessant ist, dass nur von einem Rechtsbehelf gegen eine „Entscheidung“ der Aufsichtsbehörde sprechen. Ein Rechtsbehelf in der Situation, wenn eine Datenschutzbehörde keine Entscheidung fällt, eine solche Entscheidung jedoch von der natürlichen oder juristischen Person verlangt wird, ist nicht erwähnt. Dies relativiert sich jedoch in Abs. 2, wenn auf das Recht jeder betroffenen Person auf einen gerichtlichen Rechtsbehelf hingewiesen wird, um die Aufsichtsbehörde zu verpflichten, im Fall einer Beschwerde tätig zu werden. Nicht abgedeckt ist jedoch die Konstellation, in der etwa ein Unternehmen oder eine betroffene Person eine Behörde verpflichten möchte, einen bestimmten Verwaltungsakt zu unterlassen, um die in diesen gerichtlich vorgehen zu können. Abs. 2 betrifft allein die Situation, dass eine Behörde Ermittlungen nicht aufnimmt oder über den Fortgang einer Beschwerde nicht informiert.

Der Rechtsbehelf muss unbeschadet eines anderweitigen administrativen oder außergerichtlichen Rechtsbehelfs existieren. Zudem muss die betreffende Entscheidung „rechtsverbindlichen“ Charakter besitzen.

In Abs. 3 wird europaweit verbindlich festgeschrieben, dass für Verfahren gegen eine Aufsichtsbehörde die Gerichte des Mitgliedstaates zuständig sind, in dem die Aufsichtsbehörde ihren Sitz hat.

Nach Art. 76 DS-GVO soll die betroffene Person das Recht erhalten, Einrichtungen, Organisationen oder Verbände damit zu beauftragen, die in Art. 74 genannten Rechte im Namen einer oder mehrerer betroffener Personen auszuüben. Umfasst ist hiervon also auch ein gerichtliches Vorgehen gegen eine Aufsichtsbehörde. Zudem muss es zu den satzungsmäßigen Zielen der Einrichtung gehören, die Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz personenbezogener Daten zu schützen.

18. Dezember 2015

Data protection by design and by default

Nach Art. 23 Abs. 1 soll der für die Verarbeitung Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel der Datenverarbeitung als auch während der Datenverarbeitung selbst angemessene technische und organisatorische Maßnahmen umsetzen. Dabei hat er unter anderem folgende Aspekte zu beachten: den Stand der Technik; die Kosten der Umsetzung; die Natur, Reichweite und Zwecke der Datenverarbeitung; die Risiken der Datenverarbeitung für die Rechte und Freiheiten der Betroffenen.

Zu den angemessenen Maßnahmen zählt das Gesetz unter anderem die Pseudonymisierung. Zudem sollen solche Maßnahmen umgesetzt werden, die der Verwirklichung von Datenschutzprinzipien, wie etwa Datenminimierung bzw. -sparsamkeit dienen. Sinn und Zweck dieser Maßnahmen soll nach dem Gesetz sein, die Voraussetzungen der DS-GVO selbst zu erfüllen und die Rechte der Betroffenen zu schützen.

Im Endeffekt dient also das Prinzip „Data protection by design and by default“ nichts anderen, als der Rechtmäßigkeit der Datenverarbeitung. Diese Rechtmäßigkeit muss aber ohnehin hergestellt sein. Ein besonderer, darüber hinausgehende Nutzen bzw. Sinn wird in der Vorschrift nicht genannt.

Zudem soll der für die Verarbeitung Verantwortliche angemessene technische und organisatorische Maßnahmen umsetzen, die per Voreinstellung (by default) dafür sorgen, dass nur jene personenbezogene Daten verarbeitet werden, die für den konkreten Zweck erforderlich sind. Diese Voreinstellung soll sich auf den Umfang der Daten, den Umfang der Datenverarbeitung selbst, die Dauer ihrer Speicherung und den Zugang zu ihnen beziehen. Auch diese Vorgabe ist kein besonderes „Plus“ an Datenschutz, sondern findet sich in dem altbekannten Prinzip des Erforderlichkeitsgrundsatzes.

Diese Maßnahmen sollen zudem sicherstellen, dass personenbezogenen Daten nicht standardmäßig ohne einen „Eingriff“ bzw. „Intervention“ des Betroffenen einer unbestimmten Anzahl von Personen zugänglich gemacht werden. Interessant ist insoweit die Verwendung des Begriffs „Eingriff“. Eine Einwilligung der betroffenen Person ist ausweislich des Wortlauts nicht erforderlich.

19. Dezember 2015

Strafen und Bußgelder in der DS-GVO

Art. 79 legt fest, dass jede nationale Aufsichtsbehörde bei der Verhängung von Bußgeldern darauf zu achten hat, dass diese in jedem Einzelfall wirksam, verhältnismäßig und gleichzeitig abschreckend sind.

Lange wurde darüber diskutiert, in welcher Höhe Bußgelder in Zukunft ausgesprochen werden können. Abs. 3 legt eine Grenze von 10 Millionen € bzw. 2 % des weltweiten Jahresumsatzes eines Unternehmens für dort benannte Verstöße fest. Abs. 3a erhöht diese Grenze für Verletzungen von dort aufgezählten Pflichten auf 20 Millionen € bzw. 4 % des weltweiten Jahresumsatzes eines Unternehmens. Abs. 2a beinhaltet eine Liste an Faktoren, die bei der Verhängung des Bußgeldes durch die Behörde zu berücksichtigen sind und Einfluss auf dessen Höhe haben können. Hierzu gehört etwa die Art und Schwere des Verstoßes, ob eine fahrlässige oder vorsätzliche Handlung zu dem Verstoß führte und auch, ob bereits zuvor gegen Vorgaben der DS-GVO verstoßen wurde.

Interessant ist, dass Verstöße gegen Art. 22 der DS-GVO anscheinend nicht bußgeldbewehrt sind. Art. 22 beschreibt allgemein die Verpflichtung des für die Verarbeitung Verantwortlichen technische und organisatorische Maßnahmen einzusetzen um sicherzustellen und nachweisen zu können, dass die Verarbeitung personenbezogener Daten in Übereinstimmung mit der DS-GVO erfolgt. Bei Art. 22 handelt es sich also nicht um technische und organisatorische Maßnahmen die der Datensicherheit dienen sollen. Vielmehr geht es um solche Maßnahmen die allgemein dazu dienen, die Vorgaben der Verordnung einzuhalten. Ein Verstoß hiergegen ist also nicht bußgeldbewehrt.

Hinzuweisen ist noch darauf, dass die höchsten Bußgelder etwa für Verstöße gegen die Vorgaben zur wirksamen Einholung einer Einwilligung oder auch zur Einhaltung der Vorgaben für die Verarbeitung personenbezogener Daten auf der Grundlage eines Vertrages oder auf der Grundlage berechtigter Interessen ausgesprochen werden können. Hiervon auch umfasst sind die Voraussetzungen für einen wirksamen Datentransfer in Drittstaaten.

Nach Abs. 3b bleibt es jedem Mitgliedstaat selbst überlassen, festzulegen, inwiefern Bußgelder auch gegen öffentliche Stellen verhängt werden können.

Mit Blick auf die Erfüllung von Straftatbeständen durch Verletzungen der Vorgaben der DS-GVO verweist diese in Art. 79b auf die nationalen Regelungen der Mitgliedstaaten. Diese müssen selbst festlegen, inwieweit ein bußgeldbewährtes Vergehen eventuell auch strafrechtliche Konsequenzen haben kann.

20. Dezember 2015

Das eingeschränkte Konzernprivileg kommt. Ein bisschen.

Bekanntlich enthält das geltende Datenschutzrecht kein Konzernprivileg. Mutter und Töchtergesellschaften eines Konzerns werden daher jeweils als eigene Stellen angesehen und müssen entweder ein Vertrag zur Auftragsdatenverarbeitung abschließen oder für einen Datentransfer untereinander eine rechtliche Grundlage vorweisen.

Zwar wird sich an dieser datenschutzrechtlichen Lage in Zukunft dem Grunde nach nichts ändern, jedoch könnte ein Erwägungsgrund in der DS-GVO in Zukunft dafür sorgen, dass die Übermittlung zwischen zwei für die Verarbeitung Verantwortlichen Stellen innerhalb eines Konzerns etwas leichter fällt bzw. die Rechtfertigung erleichtert. Nach Erwägungsgrund 38a kann (!) ein berechtigtes Interesse für eine Datenübermittlung zwischen konzernverbundenen Unternehmen für Zwecke der internen Verwaltung (wozu ausdrücklich sowohl Mitarbeiter- als auch Kundendaten gehören) bestehen. Die DS-GVO legt damit zwar nicht verbindlich fest, dass für diese Zwecke stets ein berechtigtes Interesse existiert. Jedoch zeigt Erwägungsgrund 38a, dass gerade wenn es um eine Übermittlung für die benannten Zwecke innerhalb eines Konzerns geht, ein berechtigtes Interesse bestehen kann.

Zumindest dürfte es für Unternehmen mit diesem gesetzgeberischen Zugeständnis und der Anerkennung eines legitimen Interesses zur Datenübermittlung innerhalb eines Konzerns in Zukunft leichter sein zu argumentieren, dass entsprechende Transfers rechtmäßig sind, auch ohne Einwilligung des Kunden oder des Mitarbeiters. Die Praxis wird dann jedoch zeigen müssen, was unter dem Begriff „interne Verwaltung“ genau zu verstehen ist. Beispiele könnten Abrechnungen, die Vertragsverwaltung aber eventuell auch der Betrieb von CRM-Systemen sein.

21. Dezember 2015

Umfang der Einwilligung: jeder Zweck und jede Verarbeitung = eine Einwilligung?

Bekanntlich wird auch in Zukunft die Einwilligung eine mögliche Grundlage für die Verarbeitung personenbezogener Daten darstellen (Art. 6 Abs. 1 (a) DS-GVO). Art. 7 DS-GVO regelt zudem weitere Voraussetzungen, die eine Einwilligung erfüllen muss, um wirksam zu sein.

Erwägungsgrund 25 erläutert etwas genauer, was der europäische Gesetzgeber als Form einer wirksamen Einwilligung ansieht und was nicht. So kann etwa das Anklicken einer Box auf einer Webseite ausreichend sein oder auch die Auswahl bestimmter technischer Einstellungen bei der Nutzung von Informationsdiensten (was sich z.B. auf Browsereinstellungen beziehen könnte).

Nicht ausreichend soll jedoch ein Schweigen des Betroffenen sein, wie auch der Einsatz bereits vorausgewählter Boxen auf Webseiten. Gerade die letzte Erläuterung spricht dafür, dass der bekannte Opt-out-Mechanismus, zumindest für sich allein betrachtet, nicht ausreicht, um eine wirksame Einwilligung abzugeben. Dies könnte sich eventuell anders darstellen, wenn ein Kästchen etwa bereits ausgewählt ist und er Nutzer dann noch einmal aktiv auf eine Schaltfläche (z.B. „einverstanden“) klicken muss. Denn dann liegt eine aktive Handlung des Betroffenen vor.

Nach Erwägungsgrund 25 muss eine Einwilligung alle Datenverarbeitungsprozesse umfassen, die demselben Zweck oder denselben Zwecken dienen. Es wird also möglich

sein, eine einzige Einwilligung in mehrere Datenverarbeitungen zu erteilen, die für denselben oder dieselben Zwecke durchgeführt werden.

Sollte eine Datenverarbeitung (oder mehrere) unterschiedlichen Zwecken dienen, so muss sich die Einwilligung auf alle Datenverarbeitungen beziehen. Auch diese Vorgabe spricht dafür, dass in Zukunft nicht für jede einzelne Datenverarbeitung eine Einwilligung eingeholt werden muss. Ebenso wenig muss eine Einwilligung für jeden einzelnen Zweck eingeholt werden. Eine Einwilligung kann bzw. soll gerade mehrere (auch unterschiedliche) Zwecke und Datenverarbeitungen umfassen.

Zuletzt noch ein Hinweis auf den recht interessanten Erwägungsgrund 25aa. Dort erkennt der Gesetzgeber ein (gerade im Bereich der Datenanalyse oft vorgebrachtes) Problem, dass häufig bei Datenerhebung nicht genau gesagt werden kann, für welche Zwecke die Daten später auch genutzt werden könnten. Für den Bereich der Wissenschaft und Forschung statuiert dieser Erwägungsgrund daher eine Ausnahme, indem eine Einwilligung auch dann als wirksam angesehen wird, wenn die Zwecke der Datenverarbeitung auf bestimmte Bereiche der Forschung bezogen sind. Dies ist ausreichend.

22. Dezember 2015

Keine Identifizierung Betroffener um jeden Preis?

Nach Art. 10 Abs. 1 DS-GVO soll der für die Verarbeitung Verantwortliche nicht allein aus Gründen der Einhaltung der Vorschriften der DS-GVO verpflichtet sein, zusätzliche Informationen zu erheben und zu verarbeiten, wenn die bei ihm vorhandenen Daten keinen Rückschluss auf einen Betroffenen zulassen.

Die Vorgaben der Vorschrift scheinen etwas verwirrend. Denn zum einen geht sie, wie DS-GVO insgesamt, davon aus, dass personenbezogene Daten verarbeitet werden. Sonst wäre sie überhaupt nicht anwendbar. Auch in Satz 1 heißt es, dass der für die Verarbeitung Verantwortliche „personenbezogene Daten“ verarbeitet. Der Rückschluss auf eine natürliche Person muss also denklogisch möglich sein. Den für die Verarbeitung Verantwortlichen dann nicht verpflichten zu wollen, zusätzliche Informationen zusammen, um den Betroffenen identifizieren zu können, erscheint widersinnig, da diese Möglichkeit ja ohnehin besteht. Sonst würde es sich nicht um personenbezogene Daten handeln.

Die Vorschrift scheint für Fälle zu gelten, in denen bei einem für die Verarbeitung Verantwortlichen vorhandene Informationen noch nicht den Rückschluss auf eine natürliche Person zulassen. In diesem Fall soll er nicht verpflichtet werden, zusätzliche Informationen zu sammeln, damit diese nicht personenbezogenen Daten einen Personenbezug aufweisen. Ein weiterer Zweck der Vorschrift könnte sein, dass früher einmal personenbezogene Daten verarbeitet wurden, dieser Personenbezug mit der Zeit entfallen ist und in dieser Situation es dem für die Verarbeitung Verantwortlichen möglich sein soll, nicht nur um im Anwendungsbereich der Verordnung zu bleiben zusätzliche Informationen zu verarbeiten, um den Personenbezug herzustellen.

Betrachtet man in Ergänzung Erwägungsgrund 45, so spricht einiges dafür, dass Art. 10 sich gar nicht auf vorhandene personenbezogene Daten bezieht (dann stellt sich jedoch überhaupt die Frage nach der Sinnhaftigkeit der Existenz des Artikels, in einer Verordnung, die erst anwendbar ist, wenn personenbezogene Daten verarbeitet werden).

Erwägungsgrund 45 spricht nämlich nur von „Daten“ die von dem für die Verarbeitung Verantwortlichen verarbeitet werden. Wenn diese Daten keine Rückschlüsse auf eine natürliche Person zulassen, soll der für die Verarbeitung Verantwortliche nicht verpflichtet

sein, zusätzliche Informationen zu erheben und zu verarbeiten, um die betroffene Person identifizieren und damit den Vorgaben dieser Verordnung entsprechen zu können.

Noch etwas verwirrender wird es, wenn man Art. 10 Abs. 2 DS-GVO betrachtet. Danach soll der für die Verarbeitung Verantwortliche, dem der Nachweis möglich ist, dass er eine betroffene Person nicht identifizieren kann, diese betroffene Person hierüber in Kenntnis setzen.

Man stellt sich freilich unweigerlich die Frage, wie die betroffene Person, die ja für den für die Verarbeitung Verantwortlichen nicht identifizierbar ist, von diesem nun informiert werden soll? Per öffentlichem Hinweis auf einer Internetseite zum Beispiel?

In einem solchen Fall sollen die Rechte der Betroffenen (etwa auf Auskunft und Berichtigung) nicht gelten, es sei denn, wenn der Betroffene gerade für den Zweck der Ausübung dieser Rechte zusätzliche Informationen zur Verfügung stellt, damit er durch den für die Verarbeitung Verantwortlichen identifiziert werden kann.

Meines Erachtens wird diese Vorschrift in der Praxis noch für einige Unstimmigkeiten und Auslegungsschwierigkeiten sorgen.

23. Dezember 2015

Der Rest der Anti FISA-Klausel

Als das Europäische Parlament seinen Entwurf für Datenschutz-Grundverordnung vorlegte, sorgte unter anderem Art. 43a DS-GVO, die sogenannte Anti FISA-Klausel, für Aufmerksamkeit. Nach dem ursprünglichen Entwurf des Parlaments sollte kein Urteil eines ausländischen Gerichts oder keine Entscheidung einer ausländischen Behörde aus einem sogenannten Drittstaat in Europa anerkannt werden oder durchsetzbar sein, welche die Offenlegung bestimmter personenbezogener Daten und deren Übermittlung in Drittstaat verlangte. Erst nach einer Information der zuständigen Datenschutzaufsichtsbehörde und einer Freigabe durch diese sollten entsprechende Daten transferiert werden dürfen. Unbeschadet hiervon sollten jedoch Datentransfers auf der Grundlage internationaler Rechtshilfeabkommen bleiben.

Der Art. 43a DS-GVO, der es in die Endfassung geschafft hat, bildet diese strikten Voraussetzungen nicht mehr ab. Zumindest ist keine Information der Aufsichtsbehörde und eine vorherige Freigabe des Datentransfers durch diese erforderlich. Ein Urteil eines ausländischen Gerichts oder eine Entscheidung einer öffentlichen Behörde des Drittstaates soll nach Art. 43a DS-GVO nur dann anerkannt werden und rechtlich durchsetzbar sein, wenn der verlangte Datentransfer auf einer internationalen Vereinbarung, wie zum Beispiel einem Rechtshilfeabkommen zwischen dem jeweiligen Mitgliedstaat innerhalb der EU und dem Drittstaat, beruht. Diese Voraussetzung soll zudem unbeschadet anderer Rechtsgrundlagen des Datentransfers nach der DS-GVO gelten.

Die Herangehensweise des in Zukunft geltenden Art. 43a DS-GVO ist eine andere, als jene, die der Artikel ursprünglich vorsah. In der alten Fassung wurde dem Grunde nach die Anerkennung derartiger ausländischer Anfragen und darauf fußende Datenübermittlungen untersagt und erst mit der Erlaubnis der zuständigen Aufsichtsbehörde möglich gemacht. Andere Rechtsgrundlagen des Datentransfers in Drittstaaten nach der DS-GVO gelten zudem weiterhin. Im Ergebnis gilt daher, dass Datentransfers auf Anforderung von ausländischen Gerichten oder Behörden selbstverständlich nach der dann geltenden DS-GVO rechtmäßig sein müssen. Die Rechtmäßigkeit kann sich entweder aus den

Bestimmungen zur Datenübermittlung in der DS-GVO selbst ergeben oder aber aus internationalen Rechtshilfeabkommen zwischen den Staaten.

24. Dezember 2015

Allgemeine Gedanken zur Datenschutz-Grundverordnung

Im heutigen letzten Beitrag des EUDataP-Weihnachtskalenders möchte ich nicht einen bestimmten Artikel besprechen, sondern vielmehr etwas allgemeiner die DS-GVO aus meinem persönlichen Blickwinkel betrachten.

Positiv ist sicherlich zu bewerten, dass zu einem Großteil (wenn auch nicht, wie häufig in der Öffentlichkeit dargestellt, in Gänze) eine europaweite Vereinheitlichung des Datenschutzrechts erfolgen wird. Der Wunsch nach Vereinheitlichung ist im Rahmen der Verhandlung im Prinzip auch von allen Beteiligten geäußert und als Ziel ausgegeben worden. Andererseits muss man feststellen, dass die DS-GVO in einigen Bereichen Öffnungsklauseln enthält und die Mitgliedstaaten teilweise verpflichtet bzw. es ihnen gestattet, nationale Regelungen vorzusehen. Dies gilt etwa für den betrieblichen Datenschutzbeauftragten, für die Altersgrenze bei der Einwilligung von Minderjährigen bei der Nutzung von Informationsdiensten, für den Schutz personenbezogener Daten von Verstorbenen oder die Datenverarbeitung von Gesundheitsdaten und anderen besonderen Arten personenbezogener Daten. In diesen Bereichen wird es in Zukunft nationale Vorgaben geben, die im Detail in den Mitgliedstaaten unterschiedlich ausfallen können. Völlig ausgeklammert aus der DS-GVO ist jedoch die Frage, wann welches nationale Recht in Zukunft gelten wird. Die DS-GVO erklärt in ihrem Art. 3 allein, wann sie selbst Anwendung findet, nicht jedoch wann nationales Datenschutzrecht anwendbar ist, welches Mitgliedstaaten im Rahmen der Öffnungsklauseln erlassen haben. Wenn diese Entscheidung den Mitgliedstaaten überlassen bleibt, kann dies in der Praxis zu unterschiedlichen Standards führen.

Ebenfalls nicht einheitlich werden in Zukunft die Regelungen zur Datenverarbeitung über Cookies sein. Dies hat in der Vergangenheit bereits zu Rechtsunsicherheiten geführt. Die sogenannte ePrivacy-Richtlinie und ihre Regelungen zur Einwilligung beim Einsatz von Cookies stellen nach Auffassung der Kommission eine Spezialregelung gegenüber der DS-GVO dar und gehen daher dieser vor. Aus diesem Grund ist auch eine Reform dieser Richtlinie in naher Zukunft angedacht.

Daneben ist eine Tendenz in der DS-GVO zu erkennen, dass sowohl auf für die Verarbeitung Verantwortliche als auch Auftragsverarbeiter erhöhte Dokumentationspflichten zukommen werden. Um es salopp auszudrücken: es wird also mehr Papier produziert werden müssen, um rechtmäßiges Handeln darlegen zu können. Das ist nicht unbedingt negativ, da auf diese Weise die jeweils Verantwortlichen in gewisser Weise gezwungen werden, sich mit dem Thema "Datenschutz" auseinanderzusetzen. Dennoch kann dies einiges an kontinuierlichem Mehraufwand bedeuten.

Viele Prinzipien und Regelungen der DS-GVO kennen wir bereits aus dem geltenden Recht, so etwa den Grundsatz, dass personenbezogene Daten verarbeitet werden dürfen, wenn eine Einwilligung oder eine andere Rechtsgrundlage vorliegt. Auch wenn bekannte Prinzipien fortgeführt werden, so garniert die DS-GVO diese häufig doch mit einigen (wenn auch kleineren) Anpassungen. Der Teufel mag in der Zukunft bzw. bei der Umsetzung der DS GVO also häufig im Detail stecken.

Andererseits wird es jedoch auch komplette Neuerungen geben. Bei der Anwendung der DS-GVO wird sich für diese Neuerungen zeigen, inwieweit die Verordnung ausreichend präzise und für die Praxis anwendbare Regelung geschaffen hat oder eventuell doch zu allgemein oder unklare Formulierung verwendet. Auslegungshilfen für neue Regelungsbereiche gibt es hierbei zunächst einmal kaum, wenn man von den Erwägungsgründen der Verordnung absieht.

Gerade was Neuerscheinungen, wie das Recht auf Datenportabilität, die Einrichtung des Datenschutzausschusses, den one-stop-shop-Mechanismus oder das sogenannte „Recht auf Vergessenwerden“ betrifft, darf man gespannt sein, wie diese Regelungen in der Praxis angewendet werden. Eventuell werden hier auch erst gerichtliche Entscheidungen für Klarheit sorgen.

In jedem Fall lässt sich sagen, dass die nächsten Jahre aus datenschutzrechtlicher Sicht in Europa sicherlich spannend werden. Man muss jedoch hoffen, dass die Datenschutz-Grundverordnung in der Praxis in einer Form anwendbar ist, die für die Adressaten (also datenverarbeitende Stellen als auch Betroffene) verständlich und vorhersehbar bleibt. Ansonsten läuft man eventuell Gefahr, dass hier ein neues Gesetz geschaffen wurde, das in der Praxis nicht eingehalten wird.