Basis der Anmerkungen sind die Ratsdokumente 12312/1/14 vom 17.9.2014 bzw. 11028/14 vom 30.06.2014

Art. 4 Abs. 3 / Definitionen

Die Definition von „processing" unterscheidet nicht zwischen Verarbeiten als Haupt- oder-Nebenleistung. Dies wirkt sich spätestens bei den Regelungen zu den Informationspflichten und zu den Processors aus.

Empfehlung:
Es sollte in der EU-DSGVO differenziert werden, ob die Kenntnisnahme von personenbeziehbaren Daten durch Dienstleister als Haupt- oder als Nebenleistung der Beauftragung erfolgt.

Art. 10 / Identifizierung

Art. 10 bestimmt, dass der Controller, der anhand der von ihm verarbeiteten Daten eine natürliche Person nicht bestimmen kann, nicht verpflichtet ist, zur bloßen Einhaltung einer Vorschrift dieser Verordnung zusätzliche Daten einzuholen, um die betroffene Person zu bestimmen.

Empfehlung:
Der Processor sollte durchgängig mitgenannt werden. Das EP hat dies in seiner Entschließung auch bereits angelegt.

Art 15. / Auskunft und Berufsgeheimnis

Das Berufsrecht untersagt Berufsträgern die Weitergabe von Daten ohne Einwilligung des Mandanten/Patienten. Im deutschen Recht geht diese berufliche Verschwiegenheitspflicht dem Auskunftsrecht des BDSG vor (vgl. KG Berlin, 20.08.2010 zu § 1 Abs. 3 BDSG).

Berufsgeheimnisträger, deren Aufgabe in der umfassenden Beratung ihrer Mandanten bzw. Patienten liegt, verarbeiten oft auch Daten Dritter, die sie von ihren Mandanten erhalten haben. Der Berufsgeheimnisträger sichert seinem Mandanten bzw. Patienten die vertrauliche Behandlung aller ihm zur Verfügung gestellten Daten und seine Verschwiegenheit auch für Sachverhalte zu, die er lediglich beiläufig erfährt. Wenn der Berufsgeheimnisträger gegenüber Dritten informations- und auskunftspflichtig werden würde, verlöre die berufliche Schweigepflicht ihre Substanz, sie würde ausgehöhlt und eine uneingeschränkte Berufsausübung durch einen vertrauensvollen Informationsaustausch würde unmöglich.

Dieses wird vom EP sowie in den Ratsdokumenten 11028/14 v. 30.6.2014 und 12312/1/14 v. 17.9.2014 auch grundsätzlich anerkannt. Allerdings ist in den aktuellen Ratsdokumenten der Schutz des Berufsgeheimnisses in **Art. 15** – anders als vom EP (Art. 15 II c) – nicht vorgesehen.

Empfehlung:

Erweiterung des Art. 15 – im Einklang mit dem u.a. in Art. 14a IV e, Art. 28 IV c sowie Erw. 71 – um Ausnahmen für Daten, die einem Berufsgeheimnis unterliegen.

Art. 22 / Controller-Processor

Die in den aktuellen Ratsdokumenten vorgesehene schärfere Trennung zwischen den Pflichten von Controller und Processor ist zu begrüßen. Insbesondere erfreulich ist die

klare Verantwortlichkeit des Controllers für die Überprüfung der Wirksamkeit der Datenschutz-Maßnahmen bei der Verarbeitung (Art. 26 I).

Art. 26 Abs. 1a / Processor (Subunternehmer-Problematik)

Die fehlende Unterscheidung zwischen der Kenntnisnahme der Daten durch den Dienstleister als Hauptleistung oder als Nebenleistung droht zu nicht durchführbaren Anforderungen zu führen:
Die Formulierung in Art. 26 Abs. 1a würde dazu führen, dass für die Kenntnisnahme von personenbezogenen Daten im Rahmen der Wartung von Datenverarbeitungsanlage die Regelungen zur Auftragsdatenverarbeitung entsprechend anzuwenden ist (vgl. § 11 Abs. 5 BDSG). Bei der Beauftragung eines Callcenters mit der Durchführung einer Kundenbefragung führt dies dazu, dass auch der Wartungspartner der Telefonanlage des Callcenters in die Beauftragungskette nach Art. 26 Abs. 1a einbezogen werden müsste. Eine weitere Folge wäre die Information nach Art. 14 Abs. 1a lit. c über die Empfänger der Daten; eine Forderung, die in den Zeiten der arbeitsteiligen Wirtschaft nicht jeden Wartungspartner der eingesetzten Maschinen, Hard- und Software umfassen kann.

Empfehlung:
Art 26 Abs. 1a nur bei Einbeziehung eines weiteren Processors für die Hauptleistung und keine Geltung, wenn die Kenntnisnahme von personenbezogenen Daten durch den Dienstleister des Processors bei der Wartung der Anlage des Dienstleisters nicht auszuschließen ist.

Vorschlag als Art. 26 Abs. 3a

> *„Keine Verarbeitung von Daten im Auftrag nach Absatz 1 liegt vor, wenn fremd in Anspruch genommene Tätigkeiten nicht den Zweck der Verarbeitung personenbezogener Daten haben, sondern in denen andere Dienstleistungsschwerpunkte im Vordergrund stehen und der damit verbundene Umgang mit personenbezogenen Daten nur unvermeidlich oder eine Kenntnisnahme personenbezogener Daten bei der Leistungserbringung nicht ausgeschlossen ist. In diesem Fall ist eine Geheimhaltungsverpflichtung des Dienstleisters sowie eine Beschränkung der Kenntnisnahme auf die Zweckbindung der Dienstleistung erforderlich.“*

(so auch das Bayerische Landesamt für Datenschutzaufsicht, Erläuterungen zu § 11 BDSB, abrufbar unter www.lda.bayern.de)

Art. 26 Abs. 1a /Processor (Formerfordernisse)

Die strenge Schriftformklausel in § 11 Abs. 1 BDSG zeigt, dass diese Vorgabe digitalisierte Geschäftsmodelle sehr erschwert, wenn nicht gar einschränkt. In der EU-DSGVO sollte beachtet werden, dass nicht durch zu hohe formelle Anforderungen oder unzureichende Übersetzungen das Ziel der Erleichterung der Datenverarbeitung in Europa erschwert wird.

Empfehlung:
Hinsichtlich der Anforderung des „written consent“ in Art. 26 Abs. 1a ist in der deutschen Fassung darauf zu achten, dass Textform ausreicht, da dem gesetzlichen Schriftformerfordernis nach den Regelungen des BGB durch eine Zustimmung in elektronischer Form allein durch eine qualifiziert elektronische Signatur genüge getan werden kann.
Bei der Formulierung des Art. 26 Abs. 2 ist zu beachten, dass keine Formvorschriften für die Beauftragung vorgebeben werden, die ein gesetzliches Schriftformerfordernis darstellen.

Art. 26 / Processor (Rechenzentrumstourismus)

Problematisch ist, dass dem Controller die Überprüfung der Wirksamkeit der Datenschutz-Maßnahmen bei der Verarbeitung beim Processorin der Regel aufgrund seiner Kenntnisse nicht wirksam möglich ist. Die Überprüfung für den Controller durch Prüfer in jedem Einzelfall kann zu einem regelrechten „Rechenzentrumstourismus" führen (vorgesehen in Art. 26 II (h)). Dieser Prüfungsakt selbst stellt nicht nur ein potentielles Sicherheitsrisiko dar (Betreten der Sicherheitsbereiche durch betriebsfremde Personen), sondern erschwert auch effektive Arbeitsabläufe. Im Rahmen einer Auslagerung von weisungsgebundenen Datenverarbeitungsprozessen in eine Cloud müsste der Cloud-Nutzer sogar die Wirksamkeit der Maßnahmen an sämtlichen Orten prüfen, an denen die vom ihm bereit gestellten Daten (potentiell) verarbeitet werden (könnten).

Ein verlässlicher Nachweis in Form einer Verhaltensregel nach Artikel 38 oder von Zertifikaten nach Artikel 39 kann hier eine Entlastung für alle Beteiligte sein, ohne das Datenschutzniveau zu gefährden. Gleichzeitig wird hiermit ein Anreiz für die Selbstregulierung zur Konkretisierung rechtlicher und technischer Vorgaben sowie die Sicherung von Compliance geschaffen. Die Durchführung eines Audits durch den Processor sowie die Veröffentlichung der Ergebnisse im Internet gibt dem für die Verarbeitung Verantwortlichen die Möglichkeit, auch ohne eigene technische Sachkenntnis seinen Auswahl- und Kontrollaufgaben nachzukommen. Dabei ist zu beachten, dass der Schutzbedarf unterschiedlich ausgeprägt sein kann, abhängig davon, welche Art von Daten verarbeitet werden. Ein guter Ansatz, dieser Vielfalt gerecht zu werden, sind branchen- und unternehmensspezifische Code of Conducts.
Dabei muss es möglich sein, durch bestimmte nachgewiesene Zertifizierungen Kontrollen vor Ort ablehnen zu können, sofern der Anscheinsbeweis des konformen Verarbeitens nicht erschüttert wird.

Empfehlung:
Ausweitung des in Art. 28 IIaa angelegte Anscheinsbeweis auf Art. 28 II (h) und Regelung, in welchen Fällen eine Vor Ort-Kontrolle nicht verlangt werden kann.

Art. 31 / Meldepflicht

Es ist zu begrüßen, dass im Ratsdokument 12312/1/14 v. 17.9.2014 in Art. 31 I die Meldepflicht des Controllers auf Fälle, die ein besonderes Risiko für das Datensubjekt bergen, begrenzt wird. Diese Einschränkung der Meldepflicht ist demgegenüber in Art. 31 II nicht vorgesehen: Der Processor muss danach bei jeder Datenschutzverletzung den Controller informieren. Danach müsste er u.a. auch dann den Controller informieren, wenn z.B. ein Post-Zusteller ein Schreiben in den falschen Briefkasten wirft und der sich redlich verhaltende Fehlempfänger das Schreiben zurückgibt. Eine Meldung ist in diesen Fällen unnötige Bürokratie und führt zudem zur Überflutung des Controllers mit Informationen.

Empfehlung:
Deshalb sollte in Art. 31 II hinsichtlich des Risikos ein Verweis auf Art. 31 I vorgesehen werden.

Art. 33 / data protection impact assessment (PIA) / Voraussetzungen

Es besteht ein Widerspruch zwischen Erwägungsgrund 71 (bei Berufsgeheimnissen ist eine Folgenabschätzung nicht zwingend) während in Art. 33 Abs. 1 das Berufsgeheimnis als Beispiel für eine PIA aufgeführt wird. Berufsgeheimnisse werden idR über die berufsrechtlichen Regelungen geschützt. Offen ist hier auch, wie z.B. in diesem Zusammenhang mit branchenüblichen Verschwiegenheitsvorgaben umzugehen ist, wie dem Bankgeheimnis.

Empfehlung:

Streichung des Berufsgeheimnisses als Voraussetzung für eine PIA in Art. 31 Abs. 1.

Art. 33 / data protection impact assessment (PIA)/ Erleichterungen

Die PIA hat sich bislang in Form der Vorabkontrolle bewährt: Bestimmte Verarbeitungen mit einem gewissen Risikograd unterlagen einer vorherigen Betrachtung nach Risikogesichtspunkten (vgl. § 4d Abs. 5 BDSG).
Es fehlt in den Ratsdokumenten die Möglichkeit der Erleichterung durch die Bestellung eines DPOs. Auch wenn der Rat nicht davon ausgeht, dass die Einbeziehung und Meldung an Aufsichtsbehörden vorgesehen sein wird, ist doch eine höhere Akzeptanz und ein gesteigertes Vertrauen durch Kunden, Beschäftigte und Bürger in die Datenverarbeitung zu erwarten, wenn Folgeabschätzungen durch eine fachkundige, weisungsunabhängige Person durchgeführt werden.

Empfehlung:
Die – auch freiwillige – Einrichtung eines Datenschutzbeauftragten sollte zur Bürokratieentlastung des Unternehmens beitragen. Dies kann erreicht werden, wenn der unabhängige Datenschutzbeauftragte die Folgenabschätzung selbst vornimmt und damit ein denkbarer Abstimmungsaufwand mit der Aufsichtsbehörde entfällt. Die Abstimmung in komplexen Zweifelsfällen durch den Datenschutzbeauftragten mit der Aufsichtsbehörde bleibt davon unbenommen.

Art. 34 / prior consultation

Die vorherige Konsultation der Aufsichtsbehörde in bestimmten Fällen kann sich zu einer verstärkten Bürokratisierung entwickeln, wenn bestimmte Datenverarbeitungsvorgänge mit Aufsichtsbehörden abgestimmt werden müssen. Hier hat sich auch die Regelung zur Selbstregulierung aus dem BDSG bewährt, welche beispielsweise die Meldepflicht gegenüber der Aufsichtsbehörde oder Vorabkontrolle bei der Bestellung eines DSB entfallen ließ.

Empfehlung:
Aufnahme eines Artikel 34 Absatz 6 a (neu):
„Die in Absätzen 1 – 6 genannten Pflichten entfallen, sofern der Controller oder der Processor einen unabhängigen Datenschutzbeauftragten eingesetzt hat und dieser die Datenschutz-Folgenabschätzung nach Artikel 33 durchgeführt hat."

Art. 35 / Datenschutzbeauftragter (DSB)

Der Wegfall der Bestellpflicht auf EU-Ebene ist ein Rückschritt hinsichtlich der qualitativen Beratungskompetenz innerhalb der Unternehmen und behördlichen Einrichtungen. Ein Großteil des Vertrauens der Bürger, Kunden und Beschäftigten beruht auf der Existenz und Pflicht zur Einbeziehung dieser Einrichtung. Es ist zu befürchten, dass durch den faktischen Wegfall das Vertrauen in die Datenverarbeitung leidet und mittelbar dadurch digitale Märkte nicht genutzt werden können. Die Aufgaben des DSB hinsichtlich der Sensibilisierung der Mitarbeiter des Controllers und des Processors (Art. 37 Abs. 1 lit. a) bleiben ohne ihn offensichtlich ungeregelt.

Empfehlung:
Die Bestellpflicht zu einem DSB auf Europaebene regeln.

Art 77 / Haftung

Die Regelung in Art. 77 Abs. 1 regelt eine gesamtschuldnerische Haftung des Controllers mit dem Processor gegenüber dem Geschädigten. Dies ist nicht interessensgerecht und seitens des Processors nicht kalkulierbar. Dieser hat keine Möglichkeit beispielsweise die Einhaltung der Zulässigkeitsvoraussetzungen durch den Controller zu prüfen.
Eine Haftung des Controller reicht aus, dieser kann im Innenverhältnis nach den allgemeinen Verschuldenstatbeständen den Processor in Anspruch nehmen.

Empfehlung:
Streichung des Processors in Art. 77 Abs. 1.