Zeitschrift für Datenschutz – ZD
www.zd-beck.de

Axel Spies **Neue Europäische Datenschutzverordnung: Kommissionsentwurf gibt tiefen Einblick in EU-Reformpläne**

Seit längerem ist bekannt, dass die grundlegende europäische Datenschutz-RL 95/46/EG überarbeitet werden soll. Einen Entwurf wollte EU-Kommissarin *Reding* eigentlich erst am 25.1.2012 vorstellen. Nun ist ein aktueller Entwurf (http://blog.beck.de/2011/12/08/europaeische-datenschutzverordnung-kommissionsentwurf-gibt-tiefen-einblick-in-eu-reformplaene) einer Verordnung (nicht RL) der geplanten Neuregelung frisch aus der EU-Gesetzesküche aber schon im Internet aufgetaucht.

Der umfangreiche Entwurf enthält viele Neuerungen gegenüber der bisherigen europäischen DS-RL. Allerdings handelt es sich bei dem Dokument um keinen offiziellen Entwurf der Verordnung und ist dementsprechend mit Vorsicht zu interpretieren. Einen solchen Entwurf will EU-Kommissarin *Reding* erst Ende Januar 2012 zum EU-Tag des Datenschutzes vorstellen. Bis dahin kann also noch mit Änderungen gerechnet werden.

Man kann auch noch nicht absehen, wie der Vorschlag am Ende des legislativen Verfahrens, das sich über Jahre hinziehen könnte, aussehen wird. Viele der vorgeschlagenen Regelungen werden wohl unter Beschuss aus verschiedenen Richtungen geraten.

Nachfolgend einige erste Beobachtungen aus internationaler Sicht:

1. Verordnung statt Richtlinie

Zunächst soll es sich nicht mehr um eine Richtlinie, sondern um eine Verordnung handeln. Das bedeutet, dass die neuen Regeln unmittelbar in jedem EU-Mitgliedstaat gelten. Die Staaten hätten dann kaum noch Spielräume bei der Umsetzung, wodurch das Datenschutzrecht europaweit vereinheitlicht und die Umsetzung beschleunigt würde.

2. Das „Recht, vergessen zu werden" („Right to be Forgotten")

Das viel diskutierte „Right to be Forgotten" findet sich in Art. 15 des Entwurfs wieder. Demnach sollen Unternehmen, wie z.B. *Facebook*, explizit dazu verpflichtet werden, veröffentlichte Inhalte auf Wunsch der Nutzer wieder zu löschen, auch wenn diese erst kurz zuvor einer Veröffentlichung ausdrücklich zugestimmt haben.

Ein zumindest vergleichbarer Ansatz besteht bereits im deutschen Datenschutzrecht. So sind nach § 3a BDSG die Erhebung, Verarbeitung und Nutzung personenbezogener Daten an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu speichern. Das „Right to be Forgotten" aus Art. 15 des Entwurfs geht jedoch wesentlich weiter. Nach Abs. 2 sollen Unternehmen, welche veröffentlichte Inhalte auf Wunsch der Nutzer gelöscht haben, auch sicherstellen, dass keine Links oder Kopien der gelöschten Information mehr öffentlich verfügbar sind.

Allerdings ist fraglich, ob das „Right to be Forgotten" in der Praxis umsetzbar ist. So könnte es z.B. zu Problemen im Zusammenhang mit dem US-Beweisermittlungsverfahren im Zivilprozess „Discovery" kommen, für die häufig zwischen den Parteien Tausende von Dokumenten zur Sichtung in den USA angefordert werden. Ein „Right to be Forgotten" könnte die Offenlegung prozessrelevanter Dokumente i.R.d. US-Discovery und für behördliche Verfahren im Inland verhindern, wenn die Daten auf Grund der neuen EU-Datenschutzverordnung gelöscht werden müssen. Für die Prozessparteien bestünde dann die Gefahr empfindlicher Strafen u.a. wegen Beweisvereitelung in den USA. Überdies sind Daten in den meisten Fällen nicht für immer gelöscht, sondern technisch wieder zu rekonstruieren, was die Umsetzung der Vorschrift schwierig machen dürfte.

3. Datenzugriff durch ausländische Behörden und Gerichte

Abs. 1 des Art. 42 stellt klar, dass Datenanforderungen durch Gerichtsurteile oder richterliche Beschlüsse und Entscheidungen von Behörden außerhalb der EU nicht in der EU anerkannt und nicht durchgesetzt werden, es sei denn, es bestehen internationale Abkommen oder Verträge zwischen dem Drittstaat und dem Mitgliedstaat.

Diese Vorschrift hat möglicherweise nur klarstellenden Charakter. Eine direkte Datenanforderung bei Auftragnehmer

oder bei der Verantwortlichen Stelle, d.h. beim Auftraggeber („data processor or data controller") ohne Zwischenschaltung eines zuständigen nationalen Gerichts oder Behörde wäre schon aus völkerrechtlicher Hinsicht ausgeschlossen (so argumentiert jedenfalls *Junker*, Electronic Discovery gegen deutsche Unternehmen, 2008, Rdnr. 111 – der *US-Supreme Court* sieht das anders).
Ob sich die Vorschrift sogar auf Schiedssprüche im Ausland bezieht, ist unklar, aber nach dem Wortlaut dieses Abs. 1 durchaus denkbar („tribunal"). Aus US-Sicht besteht die Gefahr, dass eine solche Vorschrift von den US-Gerichten als unbeachtliches „Blocking Statute" eingestuft wird (s. hierzu *Spies/Schröder* MMR 2008, 275 ff.).
Womöglich handelt es sich bei den Vorschriften des Art. 42 um eine Reaktion auf den Streit mit den USA, der sich um die Nutzung von Daten europäischer Bürger zu Terrorismusabwehr und anderen Zwecken nach US-Recht dreht. *Microsoft* hatte diesen Sommer i.R.e. Anhörung zugegeben, Daten aus der Cloud in Europa an US-Behörden nach dem US Patriot Act zu übermitteln. EU-Kommissarin *Reding* hatte sich in der Vergangenheit bereits mehrfach kritisch gegenüber dem Datenzugriff von US-Behörden auf Grundlage des US-Patriot Act positioniert – ebenso *Abgeordnete des EU-Parlaments*.
Trotz dieses generellen Vollsteckungsverbots enthält der nachfolgende Abs. 2 dann doch eine Vorschrift mit Anforderungen für den Fall, dass die Justiz- und Strafverfolgungsbehörden in Drittstaaten doch auf in der EU belegene Daten zugreifen möchten. Nach dem Wortlaut dieses Abs. 2 ist ein solcher Zugriff nur mit Zustimmung der zuständigen Datenschutzbehörde zulässig. Dieses Erfordernis ist nicht ganz nachvollziehbar, da nach dem HaagBewÜK eigentlich keine Mitwirkung der Datenschutzbehörde bei der Beweisübermittlung ins Ausland vorgesehen ist; zuständig sind vielmehr (und das wohl ausschließlich) die „Zentralen Behörden" (die Landesjustizministerien oder das zuständige OLG). Sinn und Zweck der Zwischenschaltung einer zuständigen Datenschutzbehörde werden sicherlich noch zu erörtern sein – ebenso die Vereinbarkeit der Norm mit dem Prozedere in internationalen Verträgen und Abkommen, wie dem genannten HaagBewÜK oder den Abkommen, welche die internationale Zusammenarbeit in Strafsachen regeln (MLATs). Der Abstimmungsprozess der Betroffenen mit diesen Behörden nach diesem Abs. 2 dürfte kompliziert und aus Mangel an Kapazitäten zeitraubend sein.
Auf die Beweisermittlung i.R.d. US-Discovery wird die Neuregulierung aber wohl keinen Einfluss haben. In dem Entwurf heißt es in Art. 41 Abs. 1 (e) weiterhin: „A set of transfers of personal data to a third country or an international organisation may take place on condition that the transfer is necessary for the establishment, exercise or defence of legal claims." Diese bereits in der EU-DS-RL enthaltene Norm wurde im deutschen Recht in § 4c Abs. 1 Nr. 4 BDSG umgesetzt. Einer Dokumentenanforderung im Zivilprozess aus den USA (Discovery), die meistens direkt von der gegnerischen Partei ausgeht, dürfte demnach Art. 42 des Entwurfs nicht den Weg nach Europa abschneiden.

4. Datenschutzbeauftragte

Für Unternehmen mit mehr als 250 Mitarbeitern soll es zudem verpflichtend sein, Datenschutzbeauftragte einzusetzen, wenn die Haupttätigkeit nicht mit personenbezogenen Daten direkt in Verbindung steht. Datenschutzbeauftragte sollen für mindestens zwei Jahre ernannt werden und einen hohen Kündigungsschutz genießen.
In Deutschland ist nach § 4g BDSG ein solcher Datenschutzbeauftragter einzusetzen, wenn mindestens 20 Personen mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt sind. In manchen anderen EU-Mitgliedstaaten gibt es solche Regelungen allerdings noch nicht, sodass die Zahl der Datenschutzbeauftragten in der EU wohl steigen wird.

5. Benachrichtigungspflicht bei Bruch der Datensicherheit

Dies ist ebenfalls ein international wichtiges Thema (z.B. bei der Speicherung der Daten über die Grenze in einer Cloud). Nach Art. 28 soll eine generelle Benachrichtigungspflicht bei Bruch der Datensicherheit EU-weit eingeführt werden. Die Unternehmen sollen danach 24 Stunden Zeit bekommen, nach einem unbefugten Datenzugriff die zuständige Datenschutzbehörde zu benachrichtigen. Handelt es sich um Daten, bei denen ein unberechtigter Zugriff für die Betroffenen Folgen haben könnte, sollen die Unternehmen binnen 24 Stunden auch diese Betroffenen benachrichtigen müssen (Art. 29).
Nach dem 2009 eingeführten § 42a BDSG sind unbefugte Datenzugriffe, bei denen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen, unverzüglich der zuständigen Aufsichtsbehörde sowie den Betroffenen mitzuteilen. Die Benachrichtigung des Betroffenen muss danach unverzüglich erfolgen.
Die Meldepflicht wird nach dem Verordnungsentwurf im Vergleich zur deutschen Vorschrift ausgeweitet. So sind unbefugte Datenzugriffe durch Dritte generell binnen 24 Stunden der zuständigen Datenschutzbehörde zu melden, unabhängig von der Intensität der möglichen Folgen für den Betroffenen. Hiervon sind nicht nur die Verantwortliche Stelle (data controller), sondern auch Auftragnehmer (data processors) betroffen. Der deutsche Datenschutz sieht eine solche Meldepflicht der Verantwortlichen Stelle nur im Falle schwerwiegender Beeinträchtigungen für den Betroffenen vor.

6. Einwilligung

Ebenso werden die Anforderungen für eine Einwilligung des Betroffenen zur Datenverarbeitung erhöht. Nach Art. 7 des Verordnungsentwurfs muss die Daten verarbeitende Stelle nachweisen, dass der Betroffene in die Datenverarbeitung selbst sowie in den bestimmten Zweck der Verarbeitung eingewilligt hat. Die Einwilligung muss zudem freiwillig, eindeutig und ausdrücklich sowie nach vorheriger Aufklärung erfolgen. Art. 1 Abs. 3 spricht von „any freely given specific, informed and explicit indication of his or her wishes by which the data subject signifies agreement to personal data relating to them being processed."

7. Länderübergreifende Datenverarbeitung

Neu scheint auch die Regelung zur grenzüberschreitenden Datenverarbeitung innerhalb der Union zu sein. So soll in einem solchen Fall nur eine einzelne Datenschutzbehörde zur Überwachung der Datenverarbeitung befugt sein. Dabei sollte es sich um die Datenschutzbehörde des Mitgliedstaats handeln, in welchem die Daten verarbeitende Stelle ihren

Hauptsitz hat (Erwägung 83 des Entwurfs).

8. Sanktionen

Zudem könnten Unternehmen, die sich nicht an die Datenschutzregeln der EU halten, künftig mit hohen Strafen, je nach Schwere des Verstoßes, von bis zu fünf Prozent ihres weltweiten Umsatzes belangt werden.

Dieser Strafmechanismus erinnert an die Sanktionen nach dem EU-Kartellrecht (z.B. die Paradefälle gegen *Microsoft*) – z.B., wenn gegen die Bedingungen zur Verarbeitung besonders sensibler Daten verstoßen wird, den Benachrichtigungspflichten bei Datenzugriff durch Dritte nicht nachgekommen wird oder unzulässigerweise Daten außerhalb der EU übertragen werden. Die in Art. 79 vorgeschlagenen Strafen sollen auf jeden Fall den finanziellen Vorteil des Verstoßes übersteigen. Damit wird eine Form des Strafschadensersatzes in diesem Sektor in der EU eingeführt.

9. Erstes Fazit

Es ist nicht klar, wer den öffentlich bekannt gewordenen Entwurf verfasst hat und wer was zu den einzelnen Artikeln beigetragen hat. Es scheint, dass die *Kommission* versucht, im Entwurf möglichst umfangreiche Vorschläge in den weiteren Beratungsprozess zur Diskussion zu stellen, um später Kompromisse mit den anderen beteiligten Gremien eingehen zu können. Praktische Bedenken könnten sich u.a. aus der Umsetzung der Vorschriften zu Rechten der Individuen beim Erstellen von Nutzerprofilen (Art. 18: Measures based on profiling) ergeben. Denkbar ist auch, dass der o.g. Art. 42 zum US Patriot Act in eine separate Gesetzesmaßnahme der EU ausgegliedert wird, um eine zügige Umsetzung der Vorschrift sicherzustellen. Aus US-Sicht ist ziemlich wahrscheinlich, dass die *US-Regierung* und zahlreiche von den neuen Vorschriften betroffenen US-Unternehmen gegen die neuen Vorschriften im Entwurf Stellung beziehen werden. Dafür bedarf es allerdings erst noch einer ausführlichen Analyse des mehr als 100 Seiten langen Textes in einer offiziellen Fassung.

Dr. Axel Spies
ist Rechtsanwalt in der Kanzlei Bingham McCutchen LLP in Washington DC und Mitherausgeber der Zeitschrift ZD.

Paul Voigt **Facebook plant Verbesserungen im Umgang mit dem Datenschutz**

ZD-Aktuell 2011, 89

Das Betreiben eines sozialen Netzwerks führt zwangsläufig zu einer Sammlung von personenbezogenen Daten in erheblichem Umfang. Mit der Anzahl der Nutzer des sozialen Netzwerks steigen auch die datenschutzrechtlichen (Missbrauchs-)Risiken. *Facebook* steht daher in besonderer Art und Weise unter der Beobachtung der Datenschutzbehörden. Schließlich zählt das weltweit größte soziale Netzwerk inzwischen ca. 800 Mio. Nutzer.

Die datenschutzrechtlichen Bedenken führten in letzter Zeit zu einer erheblichen Aktivität deutscher Datenschutzaufsichtsbehörden, die sich jedoch verstärkt auf kleinere „Nebenprodukte" des Facebook-Dienstes konzentrierten.

So drohte der Schleswig-Holsteinische Datenschutzbeauftragte *Weichert* an, gegen private und öffentliche Webseitenbetreiber mit Sitz in Schleswig-Holstein vorzugehen, wenn diese den sog. Facebook-„Like"-Button auf ihrer Webseite integriert haben (vgl. Gutachten des *ULD Schleswig-Holstein*, abrufbar unter: https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf).

Auch der *Hamburgische Datenschutzbeauftragte* beschäftigt sich intensiv mit der Datenverarbeitung bei *Facebook* (vgl. http://www.datenschutz-hamburg.de/ihr-recht-auf-datenschutz/internet/facebook.html). Auf diese Weise wird insbesondere aus norddeutschen Bundesländern versucht, das in den USA ansässige *Facebook* auf dem Umweg über die deutschen Webseitenbetreiber anzugreifen (vgl. zur Frage der Verantwortlichkeit deutscher Webseitenbetreiber für etwaige Datenschutzverstöße von *Facebook* *Voigt/Alich*, NJW 2011, 3541 ff.).