zS / Ru 21/2

VII4 - 191 561 - 2 162
Lö 21.2.

Glaser, Anika

Von: Andreas Jaspers [Jaspers@gdd.de]
Gesendet: Montag, 20. Februar 2012 10:40
An: VII4_
Betreff: Stellungnahme GVO
Anlagen: Stellungnahme GVOx.pdf

Sehr geehrte Damen und Herren,

in Anlage eine Stellungnahme der GDD zur den Grundsätzen des Entwurfs einer Datenschutz-Grundverordnung.

Freundliche Grüße

Andreas Jaspers

****

RA Andreas Jaspers

Geschäftsführer der
Gesellschaft für Datenschutz
und Datensicherheit (GDD) e.V.
Pariser Str. 37
53117 Bonn

Fon ++49 228 694313
Fax ++49 228 695638
jaspers@gdd.de
www.gdd.de

****

Stellungnahme

der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD)

zu den Grundsätzen des
Vorschlages der Europäischen Kommission
einer Datenschutz-Grundverordnung - KOM(2012) 11 / 4

1. Ausgestaltung des Datenschutzes durch eine EU-Verordnung - nur für die Privatwirtschaft

Das Instrument der Verordnung ist zur Generierung eines einheitlichen Datenschutzrechts auf europäischer Ebene im privatrechtlichen Bereich ein geeignetes Mittel zur Fortentwicklung eines gemeinsamen europäischen Datenschutzrechts. In einer allgegenwärtig vernetzten Welt unterstützt ein EU-weit einheitlicher Datenschutz die Wirtschaft bei länderübergreifenden Datenverarbeitungen. Gleichzeitig werden in der EU Datenschutzstandards insbesondere für die Online-Welt geschaffen, die insbesondere von weltweit tätigen Anbietern bei der Verarbeitung von Daten der Bürger der EU zu befolgen sind.

Die Argumente für den Erlass des Rechtsinstruments einer Verordnung (VO) - im Wesentlichen die Förderung des gemeinsamen Markts - sprechen in erster Linie für eine Vereinheitlichung des Datenschutzrechts in der Privatwirtschaft. Diese Argumente gelten für die Datenverarbeitung im öffentlichen Bereich nicht in gleicher Weise. Hier ist dem Subsidiaritätsprinzip folgend eine einheitliche Regelung in Form einer VO nicht erforderlich. Sofern weiterhin für den öffentlichen Bereich der Datenschutz durch das Instrument einer Richtlinie geregelt würde, stünde in Deutschland für die Datenverarbeitung des Staates der Weg zum Bundesverfassungsgericht weiterhin offen. Dieses ist insbesondere vor dem Hintergrund bedeutsam, dass das allgemeine Persönlichkeitsrecht in Form der informationellen Selbstbestimmung sowie der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme vom Bundesverfassungsgericht bei der Befassung mit der hoheitlichen Norm ausgestaltet wurde.

2. Modernisierung des Datenschutzes

Mit dem Entwurf der Datenschutz-Grundverordnung (DS-GVO-E) wurden neue Datenschutzinstrumente entworfen, aber das Grundprinzip des Datenschutzrechts beibehalten.

Es ist begrüßenswert, dass der DS-GVO-E am Verbotsprinzip festhält, welches sich unmittelbar dem vom Bundesverfassungsgericht entwickelten Recht auf informationelle Selbstbestimmung ableitet. Das Verbotsprinzip, dessen Anwendung durch jahrelange Rechtsprechung und Literatur gesichert und mit Leben ausgefüllt wurde, schafft mehr Rechtssicherheit, als eine grundsätzliche Erlaubnis der Datenverarbeitung mit Verbotsvorbehalt. „Modernisierung" ist nicht mit Werteaustausch gleichzusetzen. Um einen solchen würde es sich jedoch

in Konsequenz der Abkehrung vom Verbotsprinzip handeln . Insbesondere ein Paradigmenwechsel zum teilweise vertretenen „Sphärenmodell" ist nicht praktikabel, weil bislang keine validen Kriterien existieren, um die nur theoretisch entwickelten Sphären von vermeintlich nicht datenschutzrelevanten öffentlich zugänglichen Informationen bis zur Intimsphäre justiziabel und grundrechtsfest abgrenzen zu können.

Der DS-GVO-E enthält zahlreiche und wesentliche Vorschläge zur Fortentwicklung des bisherigen europäischen und deutschen Datenschutzrechts. Er normiert dabei viele Überlegungen zur Modernisierung, die bisher nur als Zielvorstellungen oder Ideen vorlagen. Zu nennen sind die Instrumente „privacy by default", „privacy by design", „Recht auf Vergessen werden" und „Datenportabilität". Insbesondere die rechtlichen Forderungen nach Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen sind zwar wenig konkretisiert, in Anbetracht der dynamischen Entwicklung der Informationstechnik sind diese Prinzipien auch im Wege einer Datenschutzgrundverordnung aber nicht weiter konkretisierbar. Hier bedarf es dynamischer delegierter Rechtsakte, die jedoch ihrerseits wegen der Bußgeldbewährung eine rechtsstaatliche Durchformung erforderlich machen.

3. *Öffnungsklauseln für den nationalen Gesetzgeber*

Art 80 ff. DS-GVO-E sehen Rechtsbereiche vor, in denen eine mitgliedstaatliche Regelung eröffnet wird. Insbesondere der Umstand, dass der Umgang mit den Beschäftigtendaten weitgehend durch das jeweilige nationale Arbeitsrecht bestimmt wird, macht eine diesbezügliche Öffnungsklausel erforderlich. Insofern muss kritisch hinterfragt werden, inwieweit überhaupt durch delegierte Rechtsakte diese Öffnungsklausel wieder konterkariert werden kann.

4. *Vorbehalt wesentlicher Regelungsinhalte*

In 46 delegierten Rechtsakten und Durchführungsbestimmungen, die sämtliche Bereiche des Datenschutzes von der Zulässigkeit über Transparenz-, Sicherheits- und Organisationsanforderungen erfassen, können die Bestimmungen der DS-GVO auf Initiative der EU-Kommission konkretisiert werden. Problematisch ist, dass auch wesentliche Aspekte des Datenschutzes delegierten Rechtsakten überantwortet sind und damit Unsicherheit über evidente Themen verbleiben. Exemplarisch kann die Interessenabwägung im Rahmen der Zulässigkeit der Datenverarbeitung gem. Art. 6 Abs. 1 f) i.V.m Abs. 5 DS-GVO-E genannt werden. Hier ist zu prüfen, ob entweder der Vorbehalt des delegierten Rechtsakts gestrichen wird, was z.B. für die Interessenabwägung zu fordern ist, oder aber Leitlinien für die delegierten Rechtsakte in die DS-GVO aufgenommen werden.

5. *Bürokratieabbau*

Es ist begrüßenswert, dass von der Notifikation von Verfahren personenbezogener Datenverarbeitung bei staatlichen Meldestellen, wie sie bisher im Grundsatz in der EG-DS-Richtlinie (95/46/EG) geregelt sind, abgesehen wird.

Nach dem DS-GVO-E bedarf die Datenschutz-Folgenabschätzung jedoch immer der Konsultation der Aufsichtsbehörde. Dabei werden deren Voraussetzungen nicht nur durch delegierte Rechtsakte bestimmt, sondern auch durch Festlegung der jeweiligen nationalen Aufsichtsbehörden (Art. 34 Nr. 2 b). Dies macht die Fälle der Einschaltung der staatlichen Fremdkontrolle in die Geschäftsprozesse der Datenverarbeitung von Unternehmen unab-

sehbar. Hier enthält der DS-GVO-E Potenziale zum Bürokratieabbau. So könnte die Datenschutz-Folgenabschätzung auf den betrieblichen Datenschutzbeauftragten übertragen werden, der sich in Zweifelfällen mit der Aufsichtsbehörde ins Benehmen setzt. Durch die Stärkung der betrieblichen Selbstkontrolle könnten zeitaufwendige Konsultationen begrenzt und zugleich die Stellung des Datenschutzbeauftragten und damit seine Akzeptanz im Unternehmen gestärkt werden.

Bei der Entwicklung von „Standardvorlagen" der EU-Kommission zur Dokumentation der Verarbeitungsprozesse (Art. 28 Abs. 6) bzw. „Standartvorlagen und Verwaltungsvorschriften" für das Verfahren der Genehmigung und Zurateziehung der Aufsichtsbehörden bei der Technikfolgenabschätzung sollte auch die fachliche Expertise der Vertreter der Datenschutzpraxis insbesondere der betrieblichen Datenschutzbeauftragten eingeholt werden, um Bürokratie auf der operativen Ebene der Datenschutzorganisation zu verhindern.

6. *Prinzip der betrieblichen Selbstkontrolle durch Datenschutzbeauftragte*

Die GDD begrüßt, dass das Prinzip der betrieblichen Selbstkontrolle durch Datenschutzbeauftragte auf dem Gebiet des Datenschutzes in den DS-GVO-E Einzug gefunden hat. Jedoch ist dieses Prinzip geschwächt. Zu dieser Schwächung führt zum einen die in Art. 35 DS-GVO-E geregelte grundsätzliche Bestellpflicht für einen betrieblichen Datenschutzbeauftragten bei einer Unternehmensgröße von mehr als 250 Mitarbeitern. Nach der VO kann die Bestellung zudem auf 2 Jahre begrenzt werden. Damit würden insbesondere im Mittelstand eine unabhängige interne Compliance-Instanz und ein Anwalt der Betroffenen zum Datenschutz fehlen. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit geht davon aus, dass nur noch 0,3% der deutschen und 0,2% der europäischen Unternehmen zur Bestellung eines Datenschutzbeauftragten verpflichtet würden.

Aus Sicht der GDD ist der geplante hohe Schwellenwert von 250 Mitarbeitern für die Grundrechtsposition des Datenschutzes äußerst kontraproduktiv. Zum einen ist zu befürchten, dass viele Unternehmen unterhalb dieses Schwellenwertes in Ermangelung einer internen Complianceinstanz zum Thema "Datenschutz" nur unzureichend die datenschutzrechtlichen Anforderungen bei der Verarbeitung von Kunden- und Mitarbeiterdaten beachten. Zum anderen ist der Wegfall des betrieblichen Datenschutzbeauftragten auch unter Wirtschaftlichkeitsgesichtspunkten wenig sinnvoll. So müssten sich zur Befolgung der geplanten EU-Verordnung die Fachabteilungen im Unternehmen die notwendigen datenschutzrechtlichen Kenntnisse selber aneignen, die bisher beim Datenschutzbeauftragten gebündelt waren mit der Folge, dass erhebliche Synergieeffekte verloren gingen. Zum anderen wären die Betroffenen, vor allen Dingen Kunden und Mitarbeiter, gehalten, sich mit ihren Datenschutzfragen und -beschwerden unmittelbar an die staatliche Datenschutzaufsichtsbehörde zu wenden, die ihrerseits Ermittlungen im Unternehmen anstellen müssten. Diese Aufgabe wird zurzeit weitgehend von den betrieblichen Datenschutzbeauftragten wahrgenommen, die die in Rede stehenden Sachverhalte sach- und zeitnah aufklären können. Aber auch im Verhältnis der Unternehmensleitung zur Mitarbeitervertretung fehlt die Kompetenz des betrieblichen Datenschutzbeauftragten bei der Beurteilung datenschutzrelevanter Prozesse der Mitarbeiterdatenverarbeitung mit der Folge, dass die jeweiligen Interessen ohne mögliche Moderation durch den Datenschutzbeauftragten aufeinander prallen.

Von der GDD ebenfalls sehr kritisch gesehen wird die geplante zeitliche Befristung der Bestellung Datenschutzbeauftragter im Unternehmen auf zwei Jahre. Diese zeitliche Befristung steht einer unabhängigen Aufgabenwahrnehmung entgegen. Nicht zuletzt auf Grund der Datenschutzskandale im Umgang mit Mitarbeiter- und Kundendaten in den letzten Jahren ist mit der Novellierung des Bundesdatenschutzgesetzes im Jahr 2009 dem betrieblichen Da-

tenschutzbeauftragten ein Kündigungsschutz eingeräumt worden. Dieser soll ihm die notwendige Unabhängigkeit bei der Prüfung und Behandlung von datenschutzrelevanten Sachverhalten ermöglichen. Dieser datenschutzrechtliche Schutz würde mit Inkrafttreten der Verordnung wegfallen.

Die GDD tritt dafür ein, dass die Regelungen zum betrieblichen Datenschutzbeauftragten überarbeitet und der Schwellenwert für die Bestellung von Datenschutzbeauftragten deutlich nach unten korrigiert, zumindest aber eine nationale Öffnungsklausel vorgesehen wird.