Position zum Vorschlag für eine Datenschutz-Grundverordnung

KOM(2012)11 vom 25.01.2012

Oktober 2012

Die DATEV eG ist das Softwarehaus und der IT-Dienstleister für Steuerberater, Wirtschaftsprüfer und Rechtsanwälte sowie deren Mandanten. 1966 gegründet, zählt die DATEV mit ca. 6.100 Mitarbeitern und rund 200 PC-Programmen heute zu den größten Informationsdienstleistern und Softwarehäusern in Europa.

Tochtergesellschaften in Polen, Italien, Österreich und Spanien sowie Vertriebspartnergesellschaften in Ungarn und Slowakei sprechen für den Erfolg der genossenschaftlichen Idee.

Auftrag der Genossenschaft ist die wirtschaftliche Förderung ihrer mehr als 39.000 Mitglieder durch Unterstützung bei Dienstleistungen, die der Berater für seinen Mandanten übernimmt. Das Leistungsspektrum umfasst vor allem die Bereiche Rechnungswesen, Personalwirtschaft, betriebswirtschaftliche Beratung, Steuern, Enterprise Ressouce Planning (ERP) sowie Organisation und Planung. Die Finanzbuchführungen von rund 2,5 Millionen der meist mittelständischen deutschen Unternehmen und mehr als 10 Millionen Lohn- und Gehaltsabrechnungen werden jeden Monat vom Steuerberater mit DATEV-Software erstellt.

Datensicherung sowie langfristige Archivierung erfolgen im DATEV-Rechenzentrum nach höchsten Qualitätsstandards. Mit DATEVasp und DATEVvsp wird das Datenverarbeitungs- und Telekommunikationsmanagement einer Kanzlei in die sichere DATEV-Cloud verlagert. Das Rechenzentrum schlägt als Datendrehscheibe von Millionen Geschäftsdaten eine virtuelle Brücke zwischen Steuerberatern, Unternehmern, Institutionen und Bürgern.

DATEV begrüßt den Ansatz der Harmonisierung und Modernisierung des Europäischen Datenschutzrechts im Hinblick auf die Herausforderungen der zunehmenden Globalisierung und Digitalisierung der Wirtschaft. Die mit dem Vorschlag für eine Datenschutz-Grundverordnung zum Ausdruck gebrachte Intention, ein hohes Schutzniveau zu gewährleisten und dabei Privatpersonen, Behörden und Unternehmen dauerhaft Rechtssicherheit zu bieten, ist DATEV ein zentrales Anliegen: Für DATEV als berufsständischen IT-Dienstleister für Steuerberater, Wirtschaftsprüfer und Rechtsanwälte sowie deren Mandanten haben Datenschutz und Datensicherheit höchste Priorität und sind von grundlegender Bedeutung. Das Unternehmen steht für außergewöhnlich hohe Standards in diesem Bereich.

Wir möchten Ihre Aufmerksamkeit auf folgende, aus unserer Sicht zentrale, verbesserungswürdige Aspekte lenken:

1. Anwendungsbereich

Der Anwendungsbereich der Verordnung sollte auf solche Daten beschränkt sein, bei denen ein tatsächlicher Personenbezug besteht. Eine zu weite Definition macht viele Geschäftsmodelle unmöglich. Zugleich ist eine zu weitreichende Verwendung von Einwilligungen zu befürchten, mit der Gefahr eines bloßen „Abhakens“ durch den Dateninhaber.

Erleichterungen sollten für pseudonymisierte Daten gelten, sofern der Schlüssel zur Personenzuordnung einen angemessenen Schutz vor der Zuordnung durch Unberechtigte bietet. Die Verarbeitung von Daten, die lediglich unter einer Kundennummer laufen, sollte mit geringeren Sicherheitsmaßnahmen durchgeführt werden können, wenn die Zuordnung über diese Kundennummer nur für einen sehr eingeschränkten Kreis von Mitarbeitern möglich ist. Dies gilt auch für Verarbeitungen unter einer Personalnummer oder sonstigen internen Nummernkreisen.

Der Begriff der Pseudonymisierung sollte explizit in Artikel 4 definiert werden, um die Berücksichtigung einer Pseudonymisierung im Rahmen der Interessenabwägung nach Artikel 6 Absatz 1 Buchstabe f zu ermöglichen. Verschlüsselte Daten sollten als pseudonymisierte Daten gewertet werden.

2. Besondere Betroffenheit von Berufsgeheimnisträgern

a) 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. Diesem sollte durch eine Aufnahme einer entsprechenden Ausnahme in Artikel 14 und Artikel 15, dass die Verschwiegenheitspflicht über der Auskunftspflicht steht, Rechnung getragen werden.

b) Auch die Informationspflicht auf elektronischem Weg muss die Anforderungen an Datenschutz und –sicherheit wahren. Besonders gilt dies bei Informationen, die einem Berufsgeheimnis unterliegen. Dies kann nur dann erfüllt werden, wenn der für die Verarbeitung Verantwortliche sich bei seinem Gegenüber zweifelsfrei sicher ist, dass dieser der berechtigte Empfänger ist. Die Aufsichtsbehörden akzeptieren die Auskunft an die Postanschrift des Auskunftsbegehrenden, wenn diese mit der in den Systemen übereinstimmt; i.Ü. empfehlen sie eine Identifizierung anhand einer Ausweiskopie. Bei einer angegebenen Emailadresse ist diese Identifikation durch den Auskunftspflichtigen nicht ohne weiteres möglich. Zudem sollten berufsrechtlich geschützte Daten nicht unverschlüsselt versendet werden, dies wird bei den meisten Auskunftsbegehrenden aber nicht umsetzbar sein. Die Informationspflicht auf elektronischem Weg nach Artikel 12 sollte daher nur bestehen, wenn der Antragsteller seine Identität zweifelsfrei nachweist und ein angemessenes Verschlüsselungsverfahren zwischen Absender und Empfänger eingesetzt werden kann.

c) Im Rahmen einer Beratung, die einer berufsrechtlichen Verschwiegenheit unterliegt, werden oftmals auch Daten von Beteiligten erfasst, die nicht von dem Fall der betroffenen Person getrennt werden können und ebenfalls von der berufsrechtlichen Verschwiegenheit umfasst werden. Dies beträfe beispielweise die Daten von Streitgegnern und Zeugen bei Rechtsanwälten, aber auch die Daten von Kreditoren und Debitoren bei Steuerberatern. Jedenfalls diese sollten von der in Artikel 18 geregelten der Datenportabilität ausgeschlossen werden (vgl. dazu i.Ü. auch „4. Datenportabilität“).

3. Informationspflichten

Die Informationspflicht nach Erwägungsgrund 48 und Artikel 14 sowie das Auskunftsrecht nach Erwägungsgrund 51 und Artikel 15 umfassen auch die Aufbewahrungsdauer. Diese ist zu Beginn der Datenverarbeitung noch nicht mit Sicherheit bestimmbar, da sie in Abhängigkeit von Vorfällen in der Zukunft ist. So kann sich der Beginn der Aufbewahrungsfrist eines Geschäftsvorfalls „Kauf“ nach hinten verschieben, wenn z.B. ein Gewährleistungsfall an der gekauften Sache eintritt. Weil dies bei Begründung des Rechtsgeschäfts nicht voraussehbar ist, sollten die Informationspflicht in Erwägungsgrund 48 und in Artikel 14 Absatz 1 Buchstabe c sowie das Auskunftsrecht in Erwägungsgrund 51 und Artikel 15 Absatz 1 Buchstabe d insoweit neutral gehalten werden.

4. Datenportabilität

Artikel 18 gibt der betroffenen Person das Recht, vom für die Verarbeitung Verantwortlichen die Herausgabe einer Kopie der verarbeiteten Daten zu verlangen, wenn die Daten in einem strukturierten elektronischen Format verarbeiten werden. Jedoch birgt es im Rahmen eines einfachen Kundenverhältnisses für die betroffene Person keine Vorteile, wenn sie über einen Herausgabeanspruch z.B. alle Verkaufsvorgänge in einer Kundenbeziehung eines Online- oder eines Offline-Händlers erhält. Sie kann diese Daten nicht bei einem anderen Online-/Offline-Händler einsetzen. Im Gegenteil: Das Risiko eines Datenverlustes steigt mit jeder Übergabe eines kompletten Datensatzes.

Zudem sind die Unternehmen bislang gehalten, die unterschiedlichen Verfahren nach Zuständigkeiten und Prozessen zu trennen, um einen Zugriff durch Unberechtigte auszuschließen. Die Datenportabilität würde dieses Gebot der Zweckbindung aufbrechen, um möglicherweise nie gestellte Herausgabeforderungen befriedigen zu können. Das Recht auf Datenübertragbarkeit erhöht die Wahrscheinlichkeit zum Einsatz von Maßnahmen zum Profiling, wenn Daten auf einer gemeinsamen Plattform gehalten werden, unabhängig davon, ob die betroffene Person damit einverstanden ist oder nicht.

Wenn die Zielsetzung die Portierung zwischen Netzwerken ist, sollte dies in Artikel 18 ausdrücklich zum Ausdruck gebracht werden. Das Informationsbedürfnis der betroffenen Person über die über ihn gespeicherten Daten kann über das Auskunftsrecht Artikel 15 erfüllt werden.

5. Auftragsverarbeitung

a) Der für die Verarbeitung Verantwortliche ist nach Artikel 22 zur Überprüfung der Wirksamkeit der Datenschutz-Maßnahmen bei der Verarbeitung verantwortlich. In der Regel ist es ihm aber aufgrund seiner Kenntnisse nicht möglich, diese Überprüfung beim Auftragsverarbeiter wirksam vorzunehmen. Die Überprüfung durch Prüfer in jedem Einzelfall kann zu einem regelrechten „Rechenzentrumstourismus“ führen. Dieser stellt nicht nur selbst ein potentielles Sicherheitsrisiko dar, 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.

   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 Selbstre-

gulierung zur Konkretisierung rechtlicher und technischer Vorgaben sowie die Sicherung von Compliance geschaffen.

Die Durchführung eines Audits durch den Auftragsverarbeiter 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.

b) Nach Artikel 26 Absatz 2 Buchstabe a und Absatz 3 ist der Auftragsverarbeiter strikt weisungsgebunden. Ihm stehen keine eigenständigen Entscheidungsbefugnisse zu. Die Begründung von Pflichten des Auftragsverarbeiters neben dem Auftraggeber ist daher unnötig. Das in Artikel 24 normierte Konstrukt des „joint controllers“ kann entfallen, da dies aus Betroffenensicht die Verantwortlichkeiten eher verschleiert als konkretisiert. Die bisherige Gestaltung zwischen verantwortlicher Stelle und weisungsgebundenem Dienstleister klärt die Verantwortlichkeiten umfassend.

c) Der Mehrwert, der sich aus Artikel 26 und 28 ergebenen doppelten Dokumentation bei der Auftragsverarbeitung in Vertrag bzw. Rechtsakt und einer weiteren Dokumentation, ist nicht ersichtlich. Redundante Dokumentationspflichten sollten verhindert und die damit einhergehenden Verwaltungslasten auf ein Mindestmaß reduziert werden.

d) Name und Kontaktdaten eines Datenschutzbeauftragten können durch einen Verweis auf eine öffentliche Seite, die stets aktuelle Informationen zur Person des Datenschutzbeauftragten enthält, konstant aktuell gehalten werden. Damit wird die in Artikel 28 Absatz 2 vorgesehene, mit Verwaltungsaufwand verbundene Aktualisierung in jedem einzelnen Vertragsverhältnis über eine Auftragsdatenverarbeitung entbehrlich.

e) Die Angabe von Fristen begegnet zu Beginn der Datenverarbeitung dem Problem, dass sie noch nicht mit Sicherheit bestimmbar sind, da sie in Abhängigkeit von Vorfällen in der Zukunft liegen. Artikel 28 Absatz 2 Buchstabe g sollte insoweit neutral gehalten werden.

6. Meldepflichten bei Datenschutzverletzungen

a) Bei der durch Artikel 31 eingeführten Meldepflicht bei Datenschutzverletzungen ist zu bedenken, dass eine Weitergabe von personenbezogenen Daten, die unberechtigt an eine vertrauenswürdige Umgebung gelangen, für die betroffene Person keinerlei Relevanz hat: Nach dem Verordnungsvorschlag müsste ein Unternehmen den Betroffenen auch dann informieren, wenn z.B. ein Post-Zusteller ein Schreiben in den falschen Briefkasten wirft und der sich redlich verhaltende Fehlempfänger das Schreiben an den Absender zurückgibt. Eine Meldung ist in diesen Fällen unnötige Bürokratie. Von Artikel 31 sollten nur Fälle erfasst werden, bei denen besonders schutzwürdige Interessen der betroffenen Person verletzt werden oder ihre schwerwiegende Beeinträchtigung droht.

b) Eine Meldefrist von 24 Stunden kann unrealistisch kurz sein. Es sollte die Schadensabwendung im Vordergrund stehen, nicht eine bürokratische Pflicht.

7. Betrieblicher Datenschutzbeauftragter

a) 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 der Abstimmungsaufwand mit der Aufsichtsbehörde entfällt. Die Abstimmung in komplexen Zweifelsfällen durch den Datenschutzbeauftragten mit der Aufsichtsbehörde bleibt davon unbenommen.

b) Die Einrichtung eines Datenschutzbeauftragten sollte branchenabhängig sein und sich maßgeblich nach der Sensibilität der betroffenen Daten richten. Insbesondere sollte das Gefährdungspotential für die Persönlichkeitsrechte der Betroffenen in Artikel 35 berücksichtigt werden. In Abhängigkeit vom Gefährdungspotential steigt der Beratungs- und Unterstützungsbedarf durch einen Datenschutzbeauftragten. Denn mit zunehmender Technologisierung der Datenverarbeitung steigen auch die Anforderungen an das Verständnis technischer Prozesse und die Berücksichtigung rechtlicher Vorga-

ben. Auch wenn das Unternehmen in einer Branche tätig ist, bei der das Risiko sich u.U. nur hinsichtlich der Mitarbeiter-Daten realisieren kann, ist der Aufwand für das Unternehmen überschaubar, da es sich auch durch eine externe Dienstleistung das erforderliche Fachwissen zukaufen kann.

8. Verhaltensregeln und Zertifikate

Für Datenverarbeitungsdienstleister gehören Datenschutz und Datensicherheit zum Geschäftsmodell und sind von existenzieller Bedeutung. Dies gilt in besonderer Weise für DATEV als Dienstleister für Berufsgeheimnisträger. Für die Akzeptanz neuer Dienstleistungen, die über das Internet und über mobile Kommunikationsplattformen möglich werden, ist das Vertrauen der Beteiligten unabdingbar. Dabei ist zu beachten, dass der Schutzbedarf unterschiedlich ausgeprägt sein kann, abhängig davon, welche Art von Daten verarbeitet werden.

a) Ein guter Ansatz, dieser Vielfalt gerecht zu werden, sind branchen- und unternehmensspezifische Selbstverpflichtungen. Die freiwilligen Verhaltenskodizes dienen auch dem Zweck, den Nutzer bei der Entscheidung für einen im Wettbewerb stehenden Dienst zu unterstützen. Zum Beispiel braucht der Anwender die Information über die zugesicherten Datenschutzmaßnahmen, um zu entscheiden, welche Daten er in einem Cloud-Computing-Dienst verarbeiten kann. Für Anwendungen ohne personenbezogene Daten liegt dies im Ermessen des Anwenders, für die Verarbeitung personenbezogener Daten dagegen müssen sich verantwortliche Stellen und insbesondere Berufsgeheimnisträger aufgrund ihrer gesetzlichen Verantwortung von den Schutzmaßnahmen überzeugen können.

   Um die Hürden für das sinnvolle Instrument der Selbstverpflichtung nicht zu hoch zu legen, sollte es nicht Voraussetzung sein, dass die Selbstverpflichtung über die gesetzlichen Vorgaben hinausgehen muss. Einen Mehrwert bringt bereits eine Selbstverpflichtung, die den gesetzlichen Rahmen konkretisiert und auch für die Betroffenen einsehbar ist. Hierfür sollte in Artikel 38 ein Anspruch auf Anerkennung durch die Aufsichtsbehörde verankert werden. Sowohl bei dieser Anerkennung als auch bei der Stellungnahme muss die Aufsichtsbehörde zu einer zeitnahen Reaktion verpflichtet sein. Es müssen gerichtliche Mittel bei Ablehnung der Genehmigung oder Untätigkeit der Aufsicht zur Verfügung stehen. Die Selbstverpflichtung ist dann ein robustes Instrument, wenn sie mit periodischen, externen neutralen Kontrollen kombiniert wird.

b) Zertifikate können dazu beitragen, Transparenz für den Nutzer von Diensten zu schaffen. Dieses Ziel wird jedoch nur dann erreicht, wenn die Nutzer nicht vor die Schwierigkeit eines Vergleichs von ähnlichen Zertifikaten und Prüfzeichen gestellt wird. Zudem muss der Aufwand für die Unternehmen, die an Zertifikaten und Prüfzeichen interessiert sind, vertretbar bleiben. Dies ist nur der Fall, wenn nicht zu einer unüberschaubaren Flut von parallel existierenden Zertifikaten und Prüfzeichen kommt. Dieses sollte sich in Erwägungsgrund 77 widerspiegeln.

9. Sanktionsrahmen

Sanktionen sollten verhältnismäßig bleiben. Der Umsatz eines Unternehmens eignet sich anders als in Artikel 79 vorgesehen nicht als Maßstab, da dieser aufgrund unterschiedlicher Margen in den Branchen in vergleichbaren Fällen keine Gleichwertigkeit der Sanktion gewährleistet. Ein Datenschutzverstoß sollte nicht durch das Bußgeld zu einer existenzvernichtenden Bedrohung werden.

10. Weitere Aspekte

Ergänzend möchten wir Sie auf die Stellungnahme unseres Dachverbands BITKOM hinweisen, die hier abrufbar ist:

http://www.bitkom.org/files/documents/BITKOM_Stellungnahme_EU-VO_20120518_.pdf