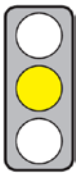
DATENSCHUTZ-GRUNDVERORDNUNG

cep**Analyse** Nr. 36/2012

KERNPUNKTE

Ziel der Verordnung: Die Kommission will das Datenschutzrecht für das Internet-Zeitalter reformieren.

Betroffene: Alle Bürger und Unternehmen, Behörden.



Pro: Die Vereinheitlichung des Datenschutzrechts und die EU-weite Zuständigkeit einer nationalen Behörde verringern die Kosten für die betroffenen Unternehmen und schaffen gleiche Wettbewerbsbedingungen.

Contra: (1) Zuschnitt und Zahl der der Kommission übertragenen Rechtsetzungsbefugnisse sind unter Gewaltenteilungsgesichtspunkten nicht hinnehmbar. Die für ein Rechtsgebiet wesentlichen Entscheidungen hat der europäische Gesetzgeber selbst zu treffen

(2) Die Regelung zur Unwirksamkeit der Einwilligung ist zu unkonkret. Auch sollte hier den Notwendigkeiten bei der Verarbeitung von Gesundheitsdaten Rechnung getragen werden.

(3) Die Regelung zum Beschäftigtendatenschutz ist der Rechtssicherheit nicht dienlich.

INHALT

Titel

Vorschlag KOM(2012) 11 vom 25. Januar 2012 für eine **Verordnung** des Europäischen Parlaments und des Rates zum **Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten** und zum freien Datenverkehr (**Datenschutz-Grundverordnung**)

Kurzdarstellung

Hinweis: Artikel- und Seitenangaben beziehen sich, soweit nicht anders angegeben, auf den Vorschlag KOM(2012) 11.

- **Hintergrund und Ziel**
  - Das EU-Datenschutzrecht datiert im Wesentlichen noch von Mitte der 1990er Jahre (Datenschutz-RL 95/46/EG, zuletzt geändert durch VO (EG) Nr. 1882/2003), also einer Zeit, in der namentlich das Internet noch in den „Kinderschuhen" steckte [KOM(2012) 9, S. 3].
  - Das EU-Datenschutzrecht soll an das Internetzeitalter angepasst werden. Seine Reform zielt im Wesentlichen auf einen „modernen, stabilen, kohärenten und umfassenden Datenschutz-Rechtsrahmen für die Europäische Union" [KOM(2012) 9, S. 13] qua Vollharmonisierung. Deren wichtigster Baustein ist die neue Datenschutz-Grundverordnung (im Folgenden: DS-GVO).
- **Anwendungsbereich**
  - Der sachliche Anwendungsbereich umfasst im Grundsatz jede automatisierte Verarbeitung personenbezogener Daten sowie deren Speicherung in Dateien (Art. 2 Abs. 1; Ausnahmen: Art. 2 Abs. 2).
  - Der persönliche Anwendungsbereich umfasst namentlich
    - den „für die Verarbeitung Verantwortlichen" (im Folgenden: Verarbeiter); Verarbeiter ist, wer allein oder gemeinsam mit anderen über die Verarbeitung personenbezogener Daten entscheidet (Art. 4 Abs. 5),
    - den „Auftragsverarbeiter"; Auftragsverarbeiter ist, wer personenbezogene Daten im Auftrag des Verarbeiters verarbeitet (Art. 4 Abs. 6).
  - Der räumliche Anwendungsbereich umfasst insbesondere
    - Verarbeiter mit Sitz in der EU (Art. 3 Abs. 1), wobei es keine Rolle spielt, ob die Datenverarbeitung als solche in der EU stattfindet oder außerhalb (Erwägungsgrund Nr. 19);
    - Verarbeiter mit Sitz außerhalb der EU (Art. 3 Abs. 2), soweit
      - Daten „in der Union ansässiger Personen" (nicht nur: Unionsbürger, Art. 9 EUV) verarbeitet werden und
      - die Datenverarbeitung dazu „dient", diesen Personen Waren oder Dienstleistungen anzubieten oder das Verhalten dieser Personen zu beobachten, namentlich durch Erstellung von Nutzerprofilen (Erwägungsgrund Nr. 21; sog. Profiling).
  - Die Mitgliedstaaten dürfen unter bestimmten Bedingungen weiterhin nationales Recht setzen für die Verarbeitung u. a.
    - von Gesundheitsdaten (Art. 81 i. V. m. Art. 9 Abs. 2 lit. h);
    - von Arbeitnehmerdaten durch Arbeitgeber „in den Grenzen dieser Verordnung" (Art. 82);
    - durch Behörden oder im Rahmen der Daseinsvorsorge (vgl. Art. 6 Abs. 1 lit. e, Abs. 3 lit. b, Erwägungsgrund Nr. 36)
- **Zulässigkeit der Datenverarbeitung**
  - Die Verarbeitung personenbezogener Daten ist zulässig (Art. 6 Abs. 1 lit. b–f),
    - soweit die Durchführung eines Vertrages, dessen Partei der Betroffene ist, sie erfordert;
    - zur Erfüllung einer rechtlichen Pflicht des Verarbeiters;
    - wenn „lebenswichtige" Interessen des Betroffenen sie erfordern;
    - soweit die Wahrnehmung öffentlicher Aufgaben sie erfordert;
    - wenn sie sonst zur „Wahrung der berechtigten Interessen" des Verarbeiters „erforderlich" ist und Interessen oder Grundrechte und Grundfreiheiten des Betroffenen nicht überwiegen.

Autor: Oliver Sauer | sauer@cep.eu
cep | Kaiser-Joseph-Straße 266 | 79098 Freiburg | Telefon 0761 38693-105 | www.cep.eu

– Grundsätzlich unzulässig ist die Verarbeitung sog. sensibler Daten, etwa zu Religions- oder Glaubenszugehörigkeit, Gesundheit oder strafgerichtlichen Verurteilungen (Art. 9 Abs. 1). Etwas anderes kann z. B. im Arbeitsverhältnis (Art. 9 Abs. 2 lit. b) oder gegenüber Behörden (vgl. Art. 9 Abs. 2 lit. g) gelten.

► **Einwilligung in die Datenverarbeitung**

– Die Verarbeitung personenbezogener Daten ist grundsätzlich auch zulässig bei Einwilligung des Betroffenen (Art. 6 Abs. 1 lit. a).
– Die Einwilligung legalisiert eine Datenverarbeitung ausnahmsweise nicht, wenn
  - zwischen Betroffenem und Verarbeiter ein „erhebliches Ungleichgewicht" besteht (Art. 7 Abs. 4), „vor allem" ein „Abhängigkeitsverhältnis", z. B. Arbeitnehmer zu Arbeitgeber (Erwägungsgrund Nr. 34);
  - die Verarbeitung der Daten grundsätzlich unzulässig ist (vgl. Art. 9 Abs. 1) und (sonstiges) EU-Recht oder nationales Recht eine Einwilligung ausschließt (Art. 9 Abs. 2 lit. a).
– Die Beweislast für die Erteilung der Einwilligung trägt der Verarbeiter (Art. 7 Abs. 1). Bei schriftlicher Erklärung muss die Einwilligung optisch abgesetzt sein (Art. 7 Abs. 2).

► **Durchführung der Datenverarbeitung**

– Zu den Pflichten im Rahmen der Datenverarbeitung zählen
  - der Einsatz technischer Verfahren, welche die Betroffenen weitestmöglich schonen („Datenschutz durch Technik"), etwa „datenschutzfreundliche Voreinstellungen", z. B. in sozialen Netzwerken (Art. 23);
  - die (mitlaufende) umfängliche Dokumentation (Details: Art. 28), die die grundsätzliche (vorherige) Meldung von Datenverarbeitungen an die Aufsichtsbehörde (Art. 18, 19 der RL 95/46/EG) ablöst; sie gilt nicht für Unternehmen mit weniger als 250 Beschäftigten, die Daten nur als „Nebentätigkeit" verarbeiten (Art. 28 Abs. 4 lit. b);
  - die Einhaltung von Datensicherheitsstandards (Details: Art. 30);
  - die Meldung von Datenschutzverstößen an die Aufsichtsbehörde (Art. 31) und die Betroffenen (Art. 32).
  - „Datenschutz-Folgeabschätzungen" in besonders risikobehafteten Konstellationen (Details: Art. 33);
  - die Bestellung eines Datenschutzbeauftragen (Art. 35) bei Datenverarbeitung
    - durch Betriebe ab 250 Mitarbeiter;
    - in Fällen, in denen die „Kerntätigkeit" des Verarbeiters regelmäßige und systematische „Beobachtung der Betroffenen" erforderlich macht (anders Erläuterung, S. 12 und Erwägungsgrund Nr. 75: in denen „Verarbeitungsvorgänge" einer regelmäßigen und systematischen „Überwachung" bedürfen);
    - durch Behörden oder öffentliche Einrichtungen.
– Zu den Rechten der Betroffenen zählen:
  - Das „Recht auf Vergessenwerden und auf Löschung": Der Betroffene kann unter bestimmten Bedingungen die Löschung seiner Daten und Unterlassen weiterer Verbreitung verlangen (Art. 17 Abs. 1) sowie „alle vertretbaren Schritte", um Dritte davon in Kenntnis zu setzen (Art. 17 Abs. 2).
  - Das „Recht auf Datenübertragbarkeit": Der Betroffene hat einen Anspruch auf Kopie der eigenen Daten in einem „gängigen elektronischen Format", etwa um sie auf einen anderen Anbieter, z. B. von Internet-Dienstleistungen, zu übertragen (Details: Art. 18).
  - Ein Widerspruchsrecht, das Rechtfertigungslasten für den Verarbeiter auslösen kann (Details: Art. 19).
– Adressat der Pflichten ist regelmäßig der Verarbeiter, je nach Pflicht auch der Auftragsverarbeiter.

► **Nationale Datenschutzbehörden**

– Jeder Mitgliedstaat verpflichtet sich zur Einrichtung einer effektiven Datenschutzaufsicht (Art. 46 Abs. 1).
– Die Aufsichtsbehörde handelt bei der Erfüllung der ihr übertragenen Aufgaben (Art. 52) und der Wahrnehmung ihrer Befugnisse (Art. 53) „völlig" unabhängig (Art. 47 Abs. 1). Insbesondere ist sie in keiner Form weisungsgebunden (vgl. Art. 47 Abs. 2).
– Grundsätzlich ist jede Aufsichtsbehörde (nur) im Hoheitsgebiet ihres Staates zuständig (Art. 51 Abs. 1). Hat ein Verarbeiter oder Auftragsverarbeiter Niederlassungen in mehr als einem Mitgliedstaat, so ist die Behörde im Mitgliedstaat der „Hauptniederlassung" (Art. 4 Abs. 13, Erwägungsgrund Nr. 27) auch in den anderen Mitgliedstaaten zuständig (Art. 51 Abs. 2; sog. Prinzip der zentralen Anlaufstelle).

► **Rechtsschutz**

– Das Recht auf Beschwerde bei einer Aufsichtsbehörde haben
  - jede betroffene natürliche Person (Art. 73 Abs. 1);
  - Einrichtungen, Organisationen oder Verbände, deren Zielsetzung der Datenschutz ist, im Namen betroffener natürlicher Personen (Art. 73 Abs. 2) sowie im eigenen Namen (Art. 73 Abs. 3).
– Das Recht auf gerichtlichen Rechtsschutz gegen eine Aufsichtsbehörde haben
  - grundsätzlich jede betroffene natürliche oder juristische Person (vgl. Art. 74 Abs. 1, 2);
  - Einrichtungen, Organisationen oder Verbände, deren Zielsetzung der Datenschutz ist, im Namen betroffener natürlicher Personen (Art. 76 Abs. 1, 73 Abs. 2 i. V. m. Art. 74).
– Das Recht auf gerichtlichen Rechtsschutz gegen Verarbeiter und Auftragsverarbeiter haben
  - jede betroffene natürliche Person (Art. 75 Abs. 1);
  - Einrichtungen, Organisationen oder Verbände, deren Zielsetzung der Datenschutz ist, im Namen betroffener natürlicher Personen (Art. 76 Abs. 1, 73 Abs. 2 i. V. m. Art. 75).

► **Haftung und Sanktionen**

– Verarbeiter und Auftragsverarbeiter haften gesamtschuldnerisch mit Entlastungsmöglichkeit (Art. 77).
– Die Mitgliedstaaten sehen zur Ahndung von Verstößen strafrechtliche Sanktionen vor (Art. 78 Abs. 1).

– Jede Aufsichtsbehörde kann, unmittelbar auf die Verordnung gestützt, Geldbußen verhängen (Art. 79 Abs. 1). Deren Höhe kann in Abhängigkeit von der Schwere des Verstoßes bis zu 1.000.000 Euro oder bei Unternehmen 2% des weltweiten Jahresumsatzes erreichen (Details: Art. 79 Abs. 3–6).

- **Rechtsetzungsbefugnisse der Kommission** (s. cepÜbersicht)
  Die Verordnung enthält 26 Ermächtigungen zum Erlass delegierter Rechtsakte (Art. 290 AEUV; s. cepStudie) und 25 Ermächtigungen zum Erlass von Durchführungsrechtsakten (Art. 291 AEUV; s. cepAnalyse).

Subsidiaritätsbegründung der Kommission

Ein EU-weit einheitlicher Datenschutz ist laut Kommission erforderlich, um den grenzüberschreitenden Verkehr personenbezogener Daten zu ermöglichen (S. 6). Zugleich wird so allen Betroffenen EU-weit ein wirksamer Datenschutz garantiert (S. 7).

Politischer Kontext

Das Datenschutzpaket vom Januar 2012 umfasst eine Mitteilung [KOM(2012) 9], die vorliegende Verordnung, die namentlich die bisherige Datenschutz-Richtlinie 95/46/EG ersetzt (Art. 88) und den „allgemeinen EU-Datenschutzrahmen“ [s. KOM(2012) 9, S. 4] absteckt, sowie eine Richtlinie [KOM(2012) 10] für die Polizeiliche und Justizielle Zusammenarbeit in Strafsachen (PJZS), die den bisherigen Rahmenbeschluss 2008/977/JI ersetzt.

Stand der Gesetzgebung

25.01.12	Annahme durch Kommission
16.02.12	Überweisung an die Ausschüsse seitdem: Subsidiaritätsrügen des französischen Senats (06.03.12), der belgischen Abgeordnetenkammer (27.03.12), des deutschen Bundesrates (30.03.12; s. Bundesrats-Drucksache 52/12), des schwedischen Reichstags (30.03.12) und des italienischen Abgeordnetenhauses (04.04.12).
23.05.12	Stellungnahme Europäischer Wirtschafts- und Sozialausschuss (EWSA)
15.01.13	1. Lesung im Plenum des Europäischen Parlaments (EP)
Offen	Annahme durch EP und Rat, Veröffentlichung im Amtsblatt, Inkrafttreten

Politische Einflussmöglichkeiten

Federführende Generaldirektion:	GD Justiz
Ausschüsse des Europäischen Parlaments:	Bürgerliche Freiheiten, Justiz und Inneres (federführend), Berichterstatter Jan Philipp Albrecht (Fraktion Grüne/EFA, D)
Ausschüsse des Deutschen Bundestags:	Innenausschuss (federführend)
Entscheidungsmodus im Rat:	Qualifizierte Mehrheit (Annahme durch Mehrheit der Mitgliedstaaten und mit 255 von 345 Stimmen; Deutschland: 29 Stimmen)

Formalien

Kompetenznorm:	Art. 16 Abs. 2 AEUV (Datenschutz), Art. 114 AEUV (Binnenmarkt)
Art der Gesetzgebungszuständigkeit:	Geteilte Zuständigkeit (Art. 4 Abs. 1, 2 AEUV)
Verfahrensart:	Art. 294 AEUV (ordentliches Gesetzgebungsverfahren)

BEWERTUNG

Ökonomische Folgenabschätzung

Die Vereinheitlichung des Datenschutzrechts und die EU-weite Zuständigkeit einer nationalen Behörde verringern tendenziell **Aufwand und Kosten für die** betroffenen **Unternehmen und schaffen** tendenziell **gleiche Wettbewerbsbedingungen**.

Juristische Bewertung

Kompetenz

Unproblematisch. Rechtsgrundlage ist vornehmlich die neue EU-Datenschutzkompetenz (Art. 16 Abs. 2 AEUV).

Subsidiarität

Eine Regulierung auf EU-Ebene ist für grenzüberschreitende Sachverhalte sinnvoll. Insbesondere kann die Regulierung des „ortlosen“ Mediums Internet nur in transnationalem Rahmen gelingen. Soweit ausschließlich innerstaatliche Sachverhalte betroffen sind, ist eine EU-einheitliche Regelung hinterfragbar. Zugunsten einer EU-Regelung lässt sich jedoch ins Feld führen, dass ansonsten für teils sehr vergleichbare Vorgänge zweierlei Datenschutzrecht Anwendung fände. Namentlich durch das Internet, dessen Regulierung Hauptziel der Reform ist, wird die Bedeutung des Grenzübertritts nivelliert; er ist dort für Anbieter wie Nutzer virtuell.

Verhältnismäßigkeit

Die Rechtsform der Verordnung verhindert, dass das EU-Datenschutzrecht in den Mitgliedstaaten unterschiedlich umgesetzt wird. Für eine effektive Regulierung des Internets dürfte dies unerlässlich sein, weil sonst eine Abwanderung von Unternehmen in Länder mit dem niedrigsten Standard droht. Eine Vollharmonisierung auch

für innerstaatliche Sachverhalte ist hingegen nicht erforderlich und damit unverhältnismäßig. Allerdings bewirkt bereits die jetzige Datenschutz-Richtlinie in der Auslegung durch den EuGH ein hohes Maß an Harmonisierung, sodass die Veränderung zum Status quo auf den ersten Blick dramatischer aussieht, als sie praktisch ist.

Vereinbarkeit mit EU-Recht

Zuschnitt und Zahl der der Kommission übertragenen Rechtsetzungsbefugnisse sind unter Gewaltenteilungsgesichtspunkten **nicht hinnehmbar**. **Die** für ein Rechtsgebiet **wesentlichen Entscheidungen hat der** europäische **Gesetzgeber** von Rechts wegen selbst **zu treffen** (vgl. Art. 290 Abs. 1 AEUV). Die genauen Auswirkungen der Reform sind überdies angesichts der zahlreichen „Leerstellen" des Verordnungstextes für die Praxis nur schwer vorhersagbar.

Die Erstreckung der Verordnung auf Verarbeiter mit Sitz außerhalb der EU ist rechtlich unbedenklich. Staaten – und auch die EU – dürfen einen Sachverhalt regeln, wenn er eine hinreichend enge sachliche Verbindung zu ihrem Hoheitsgebiet aufweist. Völkerrechtspraxis und -doktrin im Allgemeinen sowie die Rechtsprechung des EuGH im Besonderen sind hierbei großzügig (s. zuletzt EuGH, Rs. C-366/10, Air Transport Association of America u. a., Tz. 110, 121 ff.). Die vorgesehene Anknüpfung an den Wohnort des Betroffenen in der EU für diese Verarbeiter, relevant vor allem bei Internet-Nutzung, wird danach nicht problematisch sein. Erst recht nicht problematisch ist die Erstreckung der Verordnung auf Verarbeiter in der EU auch für den Fall, dass die Daten außerhalb der EU verarbeitet werden. Eine andere Frage ist die tatsächliche Durchsetzbarkeit der EU-Datenschutzstandards in diesen Fällen.

Klarstellungsbedürftig ist, wann die Datenverarbeitung eines Verarbeiters außerhalb der EU, namentlich bei Internet-Sachverhalten, dazu „dient", dem in der EU ansässigen Nutzer Waren oder Dienstleistungen anzubieten. Ähnliche Abgrenzungsschwierigkeiten sind für den Gerichtsstand bei Verbraucherverträgen geläufig (vgl. EuGH, Rs. C- 585/08 u. a., Pammer).

Das „Recht auf Datenübertragbarkeit" ist seiner Idee nach wesentlich auf Internet-Sachverhalte zugeschnitten (z. B. soziale Netzwerke), geht in seinem Anwendungsbereich unnötigerweise aber weit darüber hinaus.

Vereinbarkeit mit deutschem Recht

Das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG)**, wie es das BVerfG in jahrzehntelanger Rechtsprechung,** beginnend mit dem Volkszählungsurteil (BVerfG, 1 BvR 209/83 u. a.), **entfaltet hat, wird** von der unmittelbar anwendbaren DS-GVO weitgehend **verdrängt** (Art. 288 Abs. 2 AEUV; vgl. auch Art. 91). **Ob und inwieweit der EuGH willens und in der Lage ist, einen gleichwertigen EU-Grundrechtsschutz** auf Grundlage namentlich der Art. 16 Abs. 1 AEUV, Art. 8 Abs. 1, 2 GRCh **zu entwickeln, muss sich zeigen** (etwa EuGH, Rs. C-92/09 u. a., Schecke und Eifert).

Die Regelung, dass Datenverarbeitung aufgrund Einwilligung nicht in Betracht kommt, wenn zwischen Betroffenem und Verarbeiter ein „erhebliches Ungleichgewicht" besteht, **ist wenig konkret und damit fragwürdig. Unklar ist die Situation z. B. im Verhältnis zwischen Verbraucher und Versicherung. Dort kommt hinzu, dass eine belastbare Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten**, die für verschiedene Versicherungen praxiswichtig ist, **abseits der Einwilligung oftmals nicht bestehen wird** (vgl. Art. 81, Art. 9 Abs. 2 lit. h). Die Regelung sollte daher überdacht und mindestens um Fallgruppen ergänzt werden. Zumal gilt dies deshalb, weil an eine Missachtung der fehlenden Einwilligung ggf. hohe Bußen geknüpft sind (Art. 79 Abs. 6 lit. a); insoweit bestünde auch rechtlich ein Bestimmtheitsproblem (vgl. Art. 103 Abs. 2 GG). Entsprechendes gilt für die wenig konkret und zudem selbstwidersprüchlich geregelte Pflicht zur Bestellung eines Datenschutzbeauftragten unterhalb der Schwelle von 250 Mitarbeitern (Art. 79 Abs. 6 lit. j); hier gäbe es zumindest die Option konkretisierender Rechtsetzung durch die Kommission (Art. 35 Abs. 11 i. V. m. Art. 86).

Der Beschäftigtendatenschutz erfährt eine kryptische Regelung: Während die Kommission nicht müde wird, ihr Harmonisierungsziel zu betonen, wird just in diesem ungemein praxiswichtigen Bereich die nach jetziger Rechtslage bestehende umfassende Harmonisierung (vgl. zuletzt EuGH, Rs. C-468/10 u. a., ASNEF) zugunsten der Mitgliedstaaten gelockert – indes dann doch wieder nur „in den Grenzen dieser Verordnung" (Art. 82 Abs. 1) – und schließlich mit der Option delegierter Rechtsakte versehen (Art. 82 Abs. 3). **Nationale Rechtsetzung in diesem Bereich wird** daher **bis auf weiteres mit erheblicher Rechtsunsicherheit belastet sein**.

Die „völlige", also auch institutionelle, nicht nur funktionale, Unabhängigkeit der Datenschutzbehörden (Art. 47 Abs. 1, 2; so bereits EuGH, Rs. C-518/07 für Art. 28 Abs. 1 der RL 95/46/EG) ist mit dem aus dem Demokratieprinzip (Art. 20 Abs. 1 GG) traditionell abgeleiteten grundsätzlichen Verbot sog. ministerialfreier Räume nur schwer vereinbar. Das Beschwerde- und Klagerecht gegen behördliche Aufsichtsmaßnahmen (Art. 73, 74) kann diesen Umstand nicht vollständig kompensieren.

Die Einführung eines Verbandsklagerechts begegnet Bedenken. Insbesondere ist für die klageberechtigten Vereinigungen unionsrechtlich kein Anerkennungsverfahren vorgesehen. Ein solches Verfahren sollte daher der nationale Gesetzgeber normieren, wie z. B. im Umweltrecht (§ 3 Umwelt-Rechtsbehelfsgesetz; vgl. auch §§ 63, 64 Bundesnaturschutzgesetz).

Zusammenfassung der Bewertung

Die Vereinheitlichung des Datenschutzrechts und die EU-weite Zuständigkeit einer nationalen Behörde verringern die Kosten für die betroffenen Unternehmen und schaffen gleiche Wettbewerbsbedingungen. Zuschnitt und Zahl der der Kommission übertragenen Rechtsetzungsbefugnisse sind unter Gewaltenteilungsgesichtspunkten nicht hinnehmbar. Die für ein Rechtsgebiet wesentlichen Entscheidungen hat der europäische Gesetzgeber selbst zu treffen. Die Regelung zur Unwirksamkeit der Einwilligung ist zu unkonkret. Auch sollte hier den Notwendigkeiten bei der Verarbeitung von Gesundheitsdaten Rechnung getragen werden. Die Regelung zum Beschäftigtendatenschutz ist der Rechtssicherheit nicht dienlich.