Beck`sche Kompakt-Kommentare

Datenschutz-Grundverordnung

Bearbeitet von
Prof. Dr. Boris Paal, Dr. Daniel Pauly, Prof. Dr. Stefan Ernst, PD Dr. Eike Michael Frenzel, Barbara Körffer, Prof. Dr. Mario Martini

(Art. 8 Abs. 3 DSRL: ärztliches Personal). Auch andere Personen müssen auf die Geheimhaltung verpflichtet sein; dies umfasst insbes. das nichtfachliche Personal in der **Krankenhausverwaltung**, welches mit der Abrechnung befasst ist. Geregelt werden kann die Geheimhaltungspflicht durch den Mitgliedstaat, aber auch durch andere „zuständige Stellen", etwa durch normativ wirkende Betriebsvereinbarung oder durch die zuständigen Kammern. Einer einzelvertraglichen Regelung fehlt die Eigenschaft einer Vorschrift einer nationalen Stelle, die insoweit die Verantwortung vom Gesetzgeber übernimmt, ein entspr. Regelungsregime zu errichten.

E. Beschränkte Öffnungsklausel (Abs. 4)

Abs. 4 ermächtigt die Mitgliedstaaten, weitere datenschutzrechtliche Bestimmungen zu treffen, dh solche Regelungen, die sich nicht lediglich auf die Rechtgrundlagen für die Verarbeitungen, die angemessenen und spezifischen Maßnahmen, die Garantien sowie die Geheimhaltungspflichten (Abs. 3) beziehen. Diese Regelungen können nur die genetischen, biometrischen und Gesundheitsdaten betreffen. Zum Teil werden sich die „Bedingungen" mit ohnehin vorgesehenen Regelungen überschneiden. „Beschränkungen" können sich indes insbes. auf den Umf. dieser Daten beziehen, die verarbeitet werden dürfen; insoweit ist Abs. 4 nicht redundant. **48**

F. Nationale Bestimmungen

Im BDSG definiert § 3 Abs. 9 bes. Arten personenbezogener Daten (anders als im Falle des Art. 9 werden genetische und biometrische Daten und Daten über die sexuelle Orientierung nicht direkt erfasst) und formuliert gerade in Bezug auf „rassische" und ethnische Herkunft enger („über", nicht „hervorgehen"); § 4a Abs. 3 sieht – der Vorgabe der DSRL entspr. – die ausdr. Einwilligung vor. Nachdem diese Norm auf die DSRL zurückgeht, lassen sich die Überlegungen zu diesem Terminus auf die DS-GVO übertragen, solange die unionsrechtliche Autonomie der Begriffsbildung gewürdigt wird. **49**

Neben der beschr. Öffnungsklausel des Abs. 4 und der Öffnung zu Gunsten der Regelungen zu den Geheimhaltungspflichten nach Abs. 3 sieht auch Abs. 2 mitgliedstaatliche Regelungen vor, in diesem Fall aber alternativ zum Unionsrecht. Schnittstellen ergeben sich insoweit wie folg: aufgrund der Möglichkeit, die Einwilligungsfestigkeit in lit. a gesetzlich zu regeln; aus dem Umstand, dass lit. b auf eine Regelung im Arbeits- oder Sozialrecht angewiesen ist; aus dem Erfordernis geeigneter Garantien bei lit. b, d und h, die durch Unionsrecht oder mitgliedstaatliches Recht festzulegen sind; aus dem Erfordernis einer bestimmten Rechtsgrundlage nach lit. e, h, i und j; sowie angemessenen und spezifischen Maßnahmen nach lit. g, i und j. **50**

G. Ausblick

51 Für Art. 9 trifft zu, was schon für Art. 8 DSRL galt, dessen Regelungen „zu den problematischsten Elementen der Richtlinie" gehörten (Dammann/Simitis Art. 9 Erl. 3). Im Vergleich zu Art. 8 DSRL kommt erschwerend hinzu, dass Art. 9 von Anfang an dazu bestimmt ist, unmittelbar zu gelten; das bisweilen Schwächen abmildernde Instrument der Umsetzung in mitgliedstaatliches Recht entfällt daher. Die Regelung hat Schwächen in der Formulierung und Begr. (vgl. die ErwGr), die dem Anspruch des Schutzes der bes. personenbezogenen Daten nicht gerecht wird. Besser wäre es – neben der Änd. der Systematik des Abs. 2 (→ Rn. 40) – insbes. gewesen, die Daten iSd Abs. 1 sämtlich in Art. 4 zu definieren und die Verarbeitung zur Ermittlung der „rassischen" Herkunft von Vornherein auszuschließen sowie die Verarbeitung der bestimmten Daten zu dem jeweils anzuerkennenden Zweck ausnahmsweise zuzulassen. Ein bes. Schutz wäre durchaus möglich gewesen: Die Qualität der Daten des Abs. 1 könnte bei Art. 6 Abs. 1 UAbs. 1 lit. f und Abs. 4 berücksichtigt werden, so dass sie in ihren engen Begriffsbedeutungen absoluten Vorrang genießen und nicht in die Unwägbarkeiten einer Abwägungsentscheidung verstrickt werden.

Art. 10 Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten

[1]Die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln aufgrund von Artikel 6 Absatz 1 darf nur unter behördlicher Aufsicht vorgenommen werden oder wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht, zulässig ist. [2]Ein umfassendes Register der strafrechtlichen Verurteilungen darf nur unter behördlicher Aufsicht geführt werden.

A. Allgemeines

I. Einführung

1 Das Strafrecht ist die **ultima ratio** des Rechtsgüterschutzes. Seine Sanktionen sind die letzten Mittel, die ein Rechtsstaat hat, um die Verletzung bestimmter Rechtsnormen zu bestrafen. Das strafrechtliche Verfahren und die Verurteilung sind für den Beschuldigten bzw. Angeklagten einschneidende Maßnahmen, die für ihn über die Bestrafung hinaus Folgen haben können; schon der Verdacht reicht aus, um den Betroffenen langfristig zu stigmatisieren. Daten über strafrechtliche Verurteilungen und Straftaten sind daher bes. sensible Daten und bleiben es in allen Verarbeitungslagen – anders als politische Meinungen oder Gesundheitsdaten, deren Verarbeitung in bestimmten Kontexten weniger pro-

blematisch ist (vgl. Art. 9 Abs. 2). Deshalb ist Art. 10 eine ggü. Art. 9 selbständige Regelung; dies schlägt sich nun – anders als in der DSRL (vgl. Dammann/Simitis DSRL Art. 8 Erl. 22), im DS-GVO-E(KOM) und im DS-GVO-E(EP) – auch in der Systematik nieder. Unabhängig von Art. 10 gelten die allg. Regelungen, insbes. Art. 5.

II. Entstehungsgeschichte

1. Vergleich mit der DSRL

Art. 10 findet seinen Vorläufer in Art. 8 Abs. 5 DSRL. Die zu verarbeitenden Daten bezogen sich dort auf Straftaten, strafrechtliche Verurteilungen und Sicherungsmaßregeln. Diese Daten durften „nur unter behördlicher Aufsicht oder aufgrund von einzelstaatlichem Recht, das angemessene Garantien vorsieht, erfolgen, wobei ein Mitgliedstaat jedoch Ausnahmen aufgrund innerstaatlicher Rechtsvorschriften, die geeignete bes. Garantien vorsehen, festlegen kann"; die Gegenausnahme war also in der Vorschrift bereits angelegt (vgl. Dammann/Simitis DSRL Art. 8 Erl. 28, die darunter behördliche Einzelentscheidungen auf gesetzlicher Grdl. verstehen). Art. 8 Abs. 5 S. 2 DSRL stellte auf ein „vollständiges Register der strafrechtlichen Verurteilungen" ab. Art. 8 Abs. 5 S. 3 (bzw. UAbs. 2) DSRL eröffnete den Mitgliedstaaten die Möglichkeit, auch Daten über administrative Strafen oder zivilrechtliche Urteile unter behördlicher Aufsicht verarbeiten zu lassen. Dem Wechsel der Handlungsform (Art. 288 AEUV) entspr., aber nicht notwendig erstreckt sich die Öffnungsklausel des S. 1 Hs. 2 nunmehr nicht mehr nur auf mitgliedstaatliches, sondern auch auf Unionsrecht. **2**

2. Vergleich mit den Entwurfsfassungen

Art. 10 geht auf Art. 9 Abs. 2 lit. j DS-GVO-E(KOM) zurück. Art. 9 Abs. 2 lit. j DS-GVO-E(EP) ersetzte Strafurteile wenig systematisch durch „verwaltungsrechtliche Sanktionen, Urteile, Straftaten, Verurteilungen", was durch den DS-GVO-E(Rat) wieder rückgängig gemacht wurde. In letztgenanntem Entwurf wurde die Regelung aus Art. 9 Abs. 2 ausgegliedert (zunächst Art. 9a DS-GVO-E(Rat)); auch der Verweis auf Art. 6 Abs. 1 und die behördliche Aufsicht wurde dort aufgenommen. Aus der erstmals in DS-GVO-E(EP) Pluralform der Strafregister wurde durch den DS-GVO-E(Rat) „ein vollständiges Strafregister", bevor für die DS-GVO nahezu wieder die Ausgangsformel verwendet wurde. **3**

B. Anforderungen an die Verarbeitung (S. 1)

I. Anwendungsbereich

Art. 10 gilt für auf die **Person des Täters** bzw. des Beschuldigten oder des Angeklagten bezogene Daten; er ist derjenige, der einer Straftat verdächtigt, der verurteilt (oder freigesprochen) oder einer Sicherungsmaßregeln unterworfen wird; diese Daten werden dem bes. Schutz des Art. 10 unterstellt. Personenbezogene **4**

Daten von Opfern oder Zeugen sind auch sensibel, weil sie zT höchstpersönlich betroffen sind, unfreiwillig mit einer Straftat konfrontiert wurden und im Zusammenhang mit dem Verfahren weiteren Gefährdungen ausgesetzt sein können. Allerdings sind ihre Daten nicht Gegenstand des S. 1. Dies ergibt sich aus dem Bezug und aus S. 2, der auch nur für den Täter relevant ist.

5 S. 1 nennt **drei Gegenstände**: strafgerichtliche Verurteilungen, Straftaten und Sicherungsmaßregeln. Diese reichen unterschiedlich weit, weil die strafgerichtliche Verurteilung voraussetzungsvoll ist, soweit – abhängig vom mitgliedstaatlichen Recht, aber doch mit großen Gemeinsamkeiten, vgl. Art. 48, 49 GRCh – der Täter tatbestandsmäßig, rechtswidrig und schuldhaft gehandelt haben muss; die Verurteilung erstreckt sich auf die Art der Strafe und das Strafmaß. „Straftaten" werden auch erfasst, um gerechtfertigtes oder schuldloses Handeln gleichwohl berücksichtigen und die Daten darüber verarbeiten zu können. „Sicherungsmaßregeln" sind Maßnahmen gegen den Straftäter, die keine Strafen darstellen, etwa weil der Täter schuldunfähig gehandelt hat, von ihm aber eine unmittelbare Gefahr ausgeht. Anknüpfungspunkt dafür muss aber auch eine Straftat sein. Damit werden Angaben über Maßnahmen der Gefahrenabwehr gegen bestimmte Personen von Art. 10 S. 1 nicht erfasst.

II. Zulässigkeit der Verarbeitung

6 Die Regelung fordert für die Verarbeitung zunächst **behördliche Aufsicht**; dies schließt eine innerbehördliche Verarbeitung nicht aus, die Art. 10 jedoch voraussetzt. Aufsicht bezieht sich vielmehr auf einen anderen Rechtsträger, der die Daten verarbeitet, insbes. private Unternehmen. Gibt die Behörde die genannten Daten an Dritte weiter (unter Beachtung der allg. Vorschriften), muss sie die Aufsicht darüber und über die weitere Verwendung wirksam ausüben. Insoweit ist die Regelung vollkommen, es bedarf keiner Ausgestaltung durch mitgliedstaatliches Recht. Anders als noch die DSRL besteht nun zu Gunsten der EU eine Kompetenz (Art. 16 Abs. 2 S. 1 AEUV: „im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen"). Für die Regelung der Fragen der Aufbau- und Ablauforganisation der behördlichen Aufsicht sind die Mitgliedstaaten zuständig. Soweit jedoch die Verarbeitung unter behördlicher Aufsicht stattfindet, legitimiert S. 1 die Verarbeitung; demgemäß ist die (wirksame) behördliche Aufsicht auch inzident nachprüfbar. Die Verarbeitung dieser Daten durch staatliche Stellen auf der Grdl. von Art. 6 Abs. 1 UAbs. 1 lit. e iVm mitgliedstaatlichem Recht liegt dem Art. 10 voraus.

7 S. 1 Hs. 2 erlaubt die Verarbeitung, wenn diese nach Unionsrecht (neu) oder mitgliedstaatlichem Recht zulässig ist. Hierin liegt eine weitere **Öffnungsklausel**, wobei die EU eine Kompetenz vorweisen können muss, um entspr. tätig zu werden; in Betracht kommt insoweit insbes. Rechtsetzung im Bereich der justiziellen Zusammenarbeit. Vorbehaltlich der rechtlichen Ausgestaltung können die bes. personenbezogenen Daten damit auf rechtlicher Grdl. auch ohne spezifische behördliche Aufsicht verarbeitet werden, etwa durch Versicherungsunternehmen, Sicherheitsdienste und (auch potentielle) Arbeitgeber. Bsp. sind Nutzung von Auszügen aus dem Bundeszentralregister durch private Unternehmen, die

ua dadurch ermöglicht wird, dass der Betroffene einen Antrag auf Erteilung einer Auskunft stellt. Das Unternehmen, dem der Auszug vorgelegt wird, kann gesetzlich berechtigt (und verpflichtet) werden, diese Daten zu verarbeiten, ohne dass es auf das Einverständnis des Betroffenen ankäme.

Das Unionsrecht und das mitgliedstaatliche Recht müssen geeignete (DSRL: „angemessene") Garantien für die Rechte und Freiheiten der betroffenen Personen vorsehen. Angesichts der bes. Qualität der Daten müssen diese Anforderungen über die ohnehin geltenden Regelungen (ua Art. 5) hinausgehen. In dem Regelungsregime muss zum Ausdruck kommen, dass der Hoheitsträger die Qualität der Daten bei seiner Entscheidung über Maßnahmen berücksichtigt; dazu gehören auch die Bedeutung der Straftat und die seither vergangene Zeitspanne (Dammann/Simitis Art. 8 Erl. 27). Diese Anforderungen werden äußerlich durch eine Aufwertung oder **Aufstufung** des Schutzes verwirklicht. Bei einer Überprüfung einer Maßnahme der Verarbeitung kann die Geeignetheit der Maßnahme streitentscheidend sein, so dass hinsichtlich der Auslegung des Begriffs Geeignetheit eine Vorlage zum EuGH nach Art. 267 AEUV in Betracht kommt. Der Interpretationsspielraum hinsichtlich der Geeignetheit ist zwar kleiner als der hinsichtlich der Angemessenheit (Art. 8 Abs. 5 DSRL); die **Letztentscheidungskompetenz** zur Auslegung dieses Begriffs wird sich der EuGH gleichwohl nicht nehmen lassen. Indem auf den Maßstab der Angemessenheit verzichtet wird, ist der Maßstab nur vermeintlich gelockert: Zum einen fußt die Differenz in der Übersetzung (im Englischen Art. 8 Abs. 5 DSRL: „suitable specific safeguards" gegenüber Art. 10 S. 1: „appropriate safeguards"; in der französischsprachigen Fassung des Art. 8 Abs. 5 DSRL und des Art. 10 jedoch jeweils „garanties appropriées"). Zum anderen gilt im Bereich der Eingriffsverwaltung – und um diese handelt es sich bei der Verarbeitung der Daten – Art. 52 Abs. 1 GRCh. Dass insoweit die Angemessenheit ein wirksamer Maßstab ist, anhand dessen das beschr. Recht und das Recht, auf das die Beschränkung gestützt wird, in ein wechselseitiges Verhältnis gesetzt werden, muss jeweils erstritten werden. Dabei kann es jedoch nicht das Ziel sein, deutsche Grundrechtsdogmatik auf Unionsebene durchzusetzen; Ziel ist vielmehr die Fortführung, Entwicklung und Anwendung der Dogmatik eines unionsrechtlich autonomen Maßstabs der Verhältnismäßigkeit (→ Art. 5 Rn. 4). **8**

Dass die Gegenausnahme des Art. 8 Abs. 5 S. 1 DSRL nicht mehr im Wortlaut des S. 1 enthalten ist, schließt nicht aus, dass einzelne Garantien im Einzelfall ausgesetzt werden. Gelöst werden kann dies – nur auf gesetzlicher Grdl. – über den **Maßstab der Angemessenheit**: In Fällen, in denen Rechtsgüter, zu deren Schutz die besagten Daten verarbeitet werden sollen, hochrangig und unmittelbar gefährdet sind, kann das Schutzniveau daher abgesenkt werden. Ein Bsp. ist die erweiterte Auskunft aus dem Bundeszentralregister für bestimmte Berufe. **9**

C. Register (S. 2)

S. 2 schließt die Auslagerung eines umfassenden Registers der strafrechtlichen Verurteilungen aus dem staatlichen Bereich ohne spezifische behördliche Aufsicht aus. Er bezieht sich nur auf S. 1 Hs. 2, nachdem S. 1 Hs. 1 die spezifische **10**

behördliche Aufsicht voraussetzt. Damit erscheinen die nach S. 1 aE vorzusehenden Garantien ein Stück weit als Kompensation für den Verzicht auf diese Form der Aufsicht. Der Anwendungsbereich dieser Ausnahme ist damit sachlich beschr. Hintergrund ist das Risikopotential, welches von vollständigen Strafregistern ausgeht, die außerhalb des Hoheitsträgers oder auch nur ohne eine bes. Kontrolle geführt werden. In Deutschland sind allerdings Art. 33 Abs. 4 GG und das Art. 2 Abs. 1 iVm 1 Abs. 1 GG insoweit maßstabsbildend, als eine Auslagerung des umfassenden Strafregisters auch unter bes. behördlicher Aufsicht kaum vorstellbar ist.

D. Nationale Bestimmungen

11 S. 1 Hs. 2 erfordert ein hohes Maß mitgliedstaatlicher Rechtsetzung. Wegen der Vorgängerregelung in Art. 8 Abs. 5 DSRL und der geringfügigen Änd. ist jedoch ein wesentlicher Teil der Regelungsaufgaben bereits erledigt, was eine Nachführung zur Anpassung an die geltenden Regelungen und die Optimierung des Datenschutzes nicht ausschließt.

E. Ausblick

12 Die Veränderungen, die durch die Umstellung von der Handlungsform der Richtlinie auf die Handlungsform der VO bewirkt werden, sind materiell **vergleichsweise geringfügig**. Der Regelungsmechanismus – unmittelbare Geltung der kompletten Vorschriften der VO, Ausfüllung durch das mitgliedstaatliche Recht iÜ – muss auch hier angenommen und in der behördlichen und in der gerichtlichen Praxis in Gang gesetzt werden. Nicht ausgeschlossen erscheint es, dass im Falle zögerlicher oder unvollständiger Regelungstätigkeit des mitgliedstaatlichen Gesetzgebers die Situation auftritt, dass der EuGH – von der Unionsrechtswidrigkeit des mitgliedstaatlichen Verhaltens abgesehen – zur Tat schreiten und die Lücken füllt, entspr. seiner Vorgehensweise bei nicht umgesetzten Richtlinien. Dies betrifft zwar alle Schnittstellen der DS-GVO, die Unions- und mitgliedstaatliches Recht miteinander verbinden. Bei der Freigabe der Verarbeitung der Daten des Art. 10 S. 1 ist das Risikopotential jedoch nochmals erhöht.

Art. 11 Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist

(1) Ist für die Zwecke, für die ein Verantwortlicher personenbezogene Daten verarbeitet, die Identifizierung der betroffenen Person durch den Verantwortlichen nicht oder nicht mehr erforderlich, so ist dieser nicht verpflichtet, zur bloßen Einhaltung dieser Verordnung zusätzliche Informationen aufzubewahren, einzuholen oder zu verarbeiten, um die betroffene Person zu identifizieren.

(2) [1]Kann der Verantwortliche in Fällen gemäß Absatz 1 des vorliegenden Artikels nachweisen, dass er nicht in der Lage ist, die betroffene Person zu identifizieren, so unterrichtet er die betroffene Person hierüber, sofern möglich. [2]In diesen Fällen finden die Artikel 15 bis 20 keine Anwendung, es sei denn, die betroffene Person stellt zur Ausübung ihrer in diesen Artikeln niedergelegten Rechte zusätzliche Informationen bereit, die ihre Identifizierung ermöglichen.

A. Allgemeines

I. Einführung

Art. 11 ist eine Konsequenz der **Speicherbegrenzung** nach Art. 5 Abs. 1 lit. e und der Zweckbindung einerseits und des Rechts des Betroffenen, Auskunft über die Verarbeitung der erhobenen Daten zu erhalten, andererseits, vgl. Art. 15 ff. Die Vorschrift ist auch **Ausdruck des Misstrauens**, welches der Verordnungsgeber den Verantwortlichen und die Verantwortlichen den ASB entgegenbringen: Wenn die Speicherbegrenzung, die Zweckbindung und die Erforderlichkeit zentrale Anforderungen an die Verarbeitung sind, so ist die Behauptung abwegig, dass die Identifizierung, die Verbindung zwischen Daten und Person gerade deswegen nicht aufgeh. werden könne, weil man im Anschluss dieser Person ggü. noch zu Auskünften etc. verpflichtet sein könnte. Es würde ein – ohne weitere Regelung – rechtswidriges und tatsächlich unmögliches Verhalten eingefordert. Zugleich kann der Verantwortliche nicht für sich in Anspruch nehmen, Daten entgegen der Speicherbegrenzung, der Zweckbindung und der Erforderlichkeit weiter zu speichern, um Pflichten einzuhalten, die im Falle der Beachtung der Maßstäbe nicht gelten können; ErwGr 52 S. 2 DS-GVO-E(KOM) führte hierzu aus: „Ein für die Verarbeitung Verantwortlicher sollte personenbezogene Daten nicht nur deshalb speichern, um auf mögliche Ansuchen reagieren zu können." **1**

Die Regelung ist damit nicht zwecklos: Sie stellt klar, dass der Wegfall der Erforderlichkeit Rückwirkung entfaltet. Der Verantwortliche hat nicht mehr nachzuweisen, wessen Daten er wann verarbeitet hat (vgl. Begr. in DS-GVO-E(KOM), S. 9, zum damaligen Art. 10). **2**

II. Entstehungsgeschichte

1. Vergleich mit der DSRL

Eine unmittelbare Vorgängervorschrift in der DSRL gab es nicht. Dies ist damit zu erklären, dass die Widerspruchsfreiheit der Umsetzung der Richtlinie durch mitgliedstaatliche Regelungen gemeinschafts- bzw. unionsrechtlich vorausgesetzt wurde. **3**

2. Vergleich mit den Entwurfsfassungen

4 Art. 10 DS-GVO-E(KOM) regelte lediglich, dass der Verantwortliche für den Fall, dass er eine natürliche Person anhand der von ihm verarbeiteten Daten nicht bestimmen kann, nicht verpflichtet sein sollte, zur Einhaltung der DS-GVO zusätzliche Daten einzuholen, um die Person zu bestimmen.

5 Art. 10 DS-GVO-E(EP) erstreckte diese Regelung auf den Verarbeiter eines Auftrags, ergänzte hinsichtlich des Bestimmens „direkt" und „indirekt" und ersetzte die Rechtsfolge, dass der Verantwortliche nicht verpflichtet sei, Daten einzuholen, dadurch, dass ihm dies nicht gestattet sein solle. Abs. 2 S. 1 stellte den Verantwortlichen von der Verpflichtung frei, eine Vorschrift der DS-GVO einzuhalten, wenn er diese nicht einhalten könne. Abs. 2 S. 2 sah eine Verpflichtung des Verantwortlichen vor, die betroffene Person zu informieren, wenn er dem Verlangen dieser Person nicht nachkommen könne.

6 Art. 11 DS-GVO-E(Rat) enthielt – der geänd. Zählung entspr. – die nochmals abgeänderte Regelung, die letztlich auch in Kraft trat.

B. Keine Verpflichtung zur erneuten Identifizierung (Abs. 1)

7 Art. 11 Abs. 1 verweist zunächst auf das Fehlen oder den Wegfall der Erforderlichkeit der Identifizierung für den vorgesehenen Zweck. So mag iRd Ausgestaltung eines Kundenbindungsprogrammes – mit Einwilligung des Betroffenen – die Verarbeitung personenbezogener Daten noch erforderlich sein, um diesem individuell konfektionierte Angebote zukommen zu lassen. Sobald dieser Zweck erfüllt ist und die Daten entpersonalisiert wurden, um sie für das Controlling oder die Lagerhaltungsplanung zu berücksichtigen, fehlt es an der Erforderlichkeit.

8 Nach ErwGr 57 S. 2 soll sich der Verantwortliche nicht weigern, zusätzliche Inf. entgegenzunehmen, die von der betroffenen Person beigebracht werden, um – hierin ist die Zweckbestimmung zu sehen – ihre Rechte geltend zu machen. Dies ist insoweit unproblematisch, als sich dieses Beibringen als aktives, wenngleich konkludentes Tun ggü. dem Verantwortlichen darstellt und dieses Verhalten als – auf die Nachführung bzw. Rekonstruktion beschränkt – Einwilligung gewertet werden kann; ohne weitere Erkl. können diese Daten einer Weitergabe (etwa nach Art. 6 Abs. 4) nicht zugänglich sein. Die erneute oder rekonstruierte Identifizierung soll – wegen des Anspruchs der Technologieneutralität wenig überraschend auch für Online-Dienste gelten (ErwGr 57 S. 3).

9 Dass die Regelung vorsieht, dass der Verantwortliche nicht verpflichtet ist, Inf. aufzubewahren, einzuholen oder zu verarbeiten, ist jedenfalls für die Aufbewahrung (welche trotz ihrer Statik auch eine Verarbeitung darstellt, vgl. Art. 4 Nr. 2) fragwürdig, soweit damit angedeutet wird, dass er gleichwohl dazu berechtigt sein könnte. De lege lata ist es dem Verantwortlichen ohne weiteres nicht gestattet, die Inf. aufzubewahren. Letztlich berücksichtigt der Wortlaut damit insbes. die Möglichkeiten des Art. 6 Abs. 1 UAbs. 1 lit. f und Art. 6 Abs. 4.