DER EUROPÄISCHE
DATENSCHUTZBEAUFTRAGTE

Leitlinien zum Datenschutz bei der Regulierung von Finanzdienstleistungen in der EU

Inhalt

Checkliste mit 10 Punkten zur Analyse von Datenschutz und Privatsphäre

Diese Liste von Fragen, die für politische Entscheidungsträger und Gesetzgeber im Bereich Regulierung von Finanzdienstleistungen erstellt wurde, ist eine Zusammenfassung der 10-Schritte-Methode, die der EDSB in Abschnitt 3 dieser Leitlinien empfiehlt.

1. *Ist es wahrscheinlich, dass personenbezogene Daten, und insbesondere sensible Daten, verarbeitet - also gesammelt, analysiert oder auf irgendeine Weise genutzt werden? Falls ja, um welche Informationen handelt es sich?*

2. *Würde die Verarbeitung von personenbezogenen Daten in das Recht des Einzelnen auf Achtung des Privat- und Familienlebens, der Wohnung und der Kommunikation eingreifen?*

3. *Gibt es einen eindeutigen Zweck der Verarbeitung der personenbezogenen Daten? Werden die Daten zu anderen Zwecken weiter verarbeitet und, falls dem so ist, sind diese mit dem ursprünglichen Zweck vereinbar?*

4. *Gibt es eine Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten?*

5. *Was ist auf der Grundlage der Folgenabschätzung der angemessene Höchstzeitraum, über den personenbezogene Daten gespeichert und aufbewahrt werden dürfen?*

6. *Wer in der EU benötigt zu den angegebenen Zwecken Zugriff auf die Daten?*

7. *Ist es notwendig, personenbezogene Daten an Drittländer weiterzugeben? Wie lautet die Rechtsgrundlage?*

8. *Kann ausreichend garantiert werden, dass betroffene Personen ihr Recht auf Auskunft und Berichtigung sowie weitere maßgebliche Rechte ausüben können?*

9. *Welche technischen und organisatorischen Sicherheitsmaßnahmen sind angemessen, insbesondere dann, wenn große oder komplexe Datenbanken und IT-Systeme ins Auge gefasst werden?*

10. *Können Sie vor einer unabhängigen Kontrollstelle nachweisen, dass die Verarbeitung von personenbezogenen Daten mit dem Datenschutzgesetz übereinstimmt?*

1. Datenschutz und Regulierung von Finanzdienstleistungen

Warum der Datenschutz für die Regulierung von Finanzdienstleistungen maßgeblich ist

1. Das Ziel der Regulierung von Finanzdienstleistungen in der EU ist die Sicherstellung finanzieller Stabilität, eines effizienten Binnenmarkts für Finanzdienstleistungen sowie Marktintegrität und Marktvertrauen.[1] Maßnahmen in diesem Bereich umfassen den Eigenkapitalbedarf von Banken und Regelungen für die Derivatmärkte, Versicherungen, Wertpapier- und Anlagenfonds, Finanzmarktinfrastruktur, Finanzdienstleistungen für Privatkunden und Zahlungssysteme. Seit Beginn der Finanzkrise im Jahr 2008 wurden über 40 neue Gesetze vorgeschlagen, von denen viele aus von den G20 übernommenen Verpflichtungen hervorgingen und von denen die meisten verabschiedet wurden. Diese umfangreichen Vorschriften umfassen die strenge Überwachung der Verhaltensweisen von Börsenmaklern und Investoren in den Finanzmärkten durch mehr Befugnisse für Aufsichtsbehörden, Transparenz für alle Marktteilnehmer, Kontrolle von Risikoverhalten und Schutz von Verbrauchern, Anlegern und Steuerzahlern vor risikoreichen Geschäften. Weitere Maßnahmen wie beispielsweise die Richtlinien zu Geldwäsche und Terrorismusfinanzierung sowie die Haushaltsordnung für den Gesamthaushaltsplan der EU erlegen den Finanzinstitutionen Verpflichtungen auf.

2. Die meisten dieser Maßnahmen betreffen die Tätigkeiten juristischer Personen. Viele von ihnen, wie zum Beispiel diejenigen zu Überwachung, dem Führen von Aufzeichnungen und Berichterstattung, Informationsaustausch, Befugnisse zuständiger Behörden und Sanktionen aufgrund von Verstoß gegen anwendbare Regelungen, erfordern die Verarbeitung personenbezogener Daten, d. h. Daten in Bezug auf direkt oder indirekt bestimmbare natürliche Personen. Einige Maßnahmen greifen außerdem möglicherweise in das Recht auf Privatsphäre ein.

3. Die Achtung der Rechte Einzelner auf Privatsphäre und Datenschutz, die in der Charta der Grundrechte der Europäischen Union („die Charta“) garantiert wird, ist eine wesentliche Bedingung für die Gültigkeit der EU-Rechtsvorschriften.[2] Datenschutzregelungen und –grundsätze stammen insbesondere aus Artikel 8 der Charta und Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) und sollen den freien Datenverkehr innerhalb des Binnenmarkts ermöglichen sowie die Rechte und Interessen von natürlichen Personen schützen. Die richtige Anwendung der Datenschutzregelungen und -grundsätze sollte daher zu Effizienz und Qualität von Politikgestaltung und Gesetzgebung im Bereich Regulierung von Finanzdienstleistungen beitragen.

Zweck dieser Leitlinien

4. Der EDSB möchte sicherstellen, dass die Organe und Einrichtungen der EU die Datenschutzanforderungen kennen und hohe Datenschutzstandards in sämtliche neue Rechtsvorschriften integrieren[3]. Dieses Dokument richtet sich an politische Entscheidungsträger und Gesetzgeber im Bereich Regulierung von

[1] COM(2014) 279 final, Ein reformierter Finanzsektor für Europa.
[2] Siehe verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland Ltd*, Urteil des EuGH vom 8. April 2014.
[3] EDSB-Strategie 2013-2014, „Für Exzellenz im Datenschutz“, 22. Januar 2013.

Finanzdienstleistungen. Es ist Teil des „Policy Toolkit“ für die Organe und Einrichtungen der EU, das der EDSB entwickelt, um eine Politikgestaltung zu ermöglichen, welche die in der Charta verankerten Grundrechte und Grundfreiheiten und insbesondere das Recht auf Privatsphäre und den Schutz personenbezogener Daten achtet.[4] Das Dokument stützt sich auf das Anfang dieses Jahres veröffentlichte Strategiepapier „Der EDSB als Berater von EU-Organen in Fragen der Strategie und Gesetzgebung: ein Rückblick auf die Erfahrungen aus zehn Jahren“, die Empfehlungen des EDSB in den letzten Jahren in ihrer Eigenschaft als Berater der EU-Organe und -Einrichtungen in Fragen der Strategie und Gesetzgebung und als maßgebliche Kontrollinstanz sowie auf die während eines Seminars der GD MARKT im Februar 2014 gewonnenen Erkenntnisse. Es befasst sich mit den Arten von Maßnahmen im Bereich Regulierung von Finanzdienstleistungen, bei denen der Datenschutz am ehesten von Belang ist.

Nutzung dieser Leitlinien

5. Die Leitlinien sind folgendermaßen aufgebaut:

    - Abschnitt 2 fasst die Art der Rechte auf Privatsphäre und den Schutz personenbezogener Daten innerhalb des Rahmens der Grundrechte der EU zusammen;

    - Abschnitt 3 beschreibt die zur Bewertung der Datenschutzaspekte von vorgeschlagenen Maßnahmen erforderlichen analytischen Schritte[5];

    - Abschnitt 4 veranschaulicht die Anwendung von Datenschutzregelungen anhand konkreter Maßnahmen in der aktuellen bzw. vorgeschlagenen Regulierung von Finanzdienstleistungen;

    - Abschnitt 5 legt die Vorschläge des EDSB im Hinblick auf die weitere Arbeit mit politischen Entscheidungsträgern und Gesetzgebern im Bereich Regulierung von Finanzdienstleistungen dar.

6. Diese Leitlinien sollen zusammen mit den Leitlinien der Kommission zur Folgenabschätzung ein praktischer Begleiter im Politikgestaltungsprozess sein. Sie werden laufend überarbeitet, und der EDSB würde Rückmeldungen und Kommentare über ihre Zweckmäßigkeit begrüßen.

7. Der Vorschlag der Kommission für eine Datenschutz-Grundverordnung sieht vor, dass Behörden und öffentliche Stellen „Datenschutz-Folgenabschätzungen“ durchführen („sofern eine solche Folgenabschätzung nicht schon anlässlich des Erlasses des Gesetzes erfolgt ist, auf dessen Grundlage die Behörde oder Einrichtung ihre Aufgaben wahrnimmt und das den fraglichen Verarbeitungsvorgang oder die fraglichen Arten von Verarbeitungsvorgängen regelt“).[6] Der EDSB empfiehlt dementsprechend, dass sich politische Entscheidungsträger auf die neuesten internationalen Standards für Datenschutz-Folgenabschätzungen beziehen, wie z. B.

[4] EDSB-Strategiepapier „Der EDSB als Berater von EU-Organen in Fragen der Strategie und Gesetzgebung: ein Rückblick auf die Erfahrungen aus zehn Jahren“, 4. Juni 2014.
[5] Siehe EDSB-Strategiepapier, Abschnitt 4.3.
[6] Erwägungsgrund 73 und Artikel 33 des Vorschlags für eine Datenschutz-Grundverordnung, KOM(2012) 11 endgültig, 25.1.2012.

ISO-Standard 22307:2008 Finanzdienstleistungen - Datenschutz-Folgenabschätzungen.

2. Übersicht über den Datenschutzrechtsrahmen der EU

Die Charta der Grundrechte der EU

8. Eine EU-Maßnahme ist nur rechtmäßig, wenn sie mit der Charta im Einklang steht.[7] Die Rechte auf Achtung des Privat- und Familienlebens und auf Schutz von personenbezogenen Daten gemäß Artikel 7 und 8 der Charta hängen eng miteinander zusammen und überschneiden sich sogar teilweise.[8] Der Datenschutz als ein Recht hat seine Wurzeln im Recht auf Achtung der Privatsphäre, wie es insbesondere in Artikel 8 der Europäischen Menschenrechtskonvention (EMRK) formuliert ist. Beide Rechte sind jüngste Bekundungen der allgemeinen ethischen Grundsätze von Würde und Autonomie und dem Recht eines jeden Menschen auf die Entwicklung seiner Persönlichkeit und auf ein Mitspracherecht bei Angelegenheiten, die ihn unmittelbar betreffen. Die allgemeine zugrunde liegende Absicht ist es, unzulässige Beeinträchtigung zu verhindern und Personen ausreichend Kontrolle über ihr eigenes Leben zu geben.

9. Nach der Charta, die nach dem Inkrafttreten des Vertrags von Lissabon nun den Wert eines Primärrechts in der EU hat, sind die Rechte auf Privatsphäre und auf Schutz personenbezogener Daten separate Rechte. Es besteht daher in allen Fällen bei der Analyse des Rechts auf Schutz personenbezogener Daten keine Notwendigkeit, auf das frühere Recht auf Privatsphäre zurückzuverweisen. Die maßgebliche Rechtsprechung nennt die Herausforderung für den Gerichtshof der Europäischen Union (EuGH), eine klare und einheitliche Herangehensweise zur Durchsetzung dieser in der Charta festgeschriebenen separaten Rechte und Freiheiten zu entwickeln, deren Unterschiede für den Schutz von natürlichen Personen von erheblicher Bedeutung sind.

Das Recht auf Privatsphäre

10. Das in Artikel 7 der Charta festgelegte Recht des Einzelnen auf Achtung des Privat- und Familienlebens, der Wohnung und der Kommunikation schützt Personen hauptsächlich vor Eingriffen in ihre Privatsphäre.[9] Es handelt sich um ein klassisches „negatives" Recht, das Personen hauptsächlich gegen Eingriffe durch den Staat schützt. Eingriffe müssen gemäß Artikel 52 Absatz 1 der Charta gesetzlich vorgesehen sein, den Wesensgehalt des Rechts achten und „unter Wahrung des Grundsatzes der Verhältnismäßigkeit" gerechtfertigt sein, aus Gründen, dass sie „erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten Anderer tatsächlich entsprechen". Darüber hinaus hat sich das Konzept des Privatlebens in der Rechtsprechung weiterentwickelt und deckt nicht nur private

[7] Verbundene Rechtssachen C-465/00, C-138/01 und C-139/01, *Rechnungshof* und *Österreichischer Rundfunk*, Urteil des EuGH vom 20. Mai 2003.

[8] Verbundene Rechtssachen C-92/09 und C-93/09, *Schecke* und *Eifert*, Urteil des EuGH vom 9. November 2010, Rdnrn. 47-52.

[9] Damit entspricht Artikel 7 der Charta fast genau Artikel 8 der EMRK, wobei der einzige Unterschied der Ersatz des Begriffs „Korrespondenz" durch den Begriff „Kommunikation" in der EMRK ist.

Situationen ab, sondern auch Personen, die mit rein persönlichen, familiären oder sozialen Tätigkeiten befasst sind.[10]

11. In der Praxis erfordert dies, dass in das Recht auf Privatsphäre eingreifende Maßnahmen auf einer ordnungsgemäßen empirischen Beurteilung anderer, weniger in die Privatsphäre eingreifender Mittel gegründet werden.[11] Der EuGH hat für Recht erkannt, dass es einen unverhältnismäßigen Eingriff in das Privatleben darstellen würde, Informationen über Gehälter von leitenden Angestellten von halbstaatlichen Unternehmen zu veröffentlichen.[12] In einem anderen Urteil hat das Gericht eine EU-Maßnahme annulliert, welche die Veröffentlichung von Informationen über Begünstigte von Agrarsubventionen auf einer Website erforderte, da es keine Beweise dafür gab, dass der Gesetzgeber weniger eingreifende Alternativen in Erwägung gezogen hatte.[13]

Das Recht auf den Schutz personenbezogener Daten

12. Personenbezogene Daten umfassen sämtliche Informationen in Bezug auf bestimmte oder bestimmbare Personen. In der EMRK ist der Datenschutz nicht Gegenstand eines separaten Rechts, sondern ist von Artikel 8 EMRK über das Recht auf Privatsphäre abgeleitet, was sich in der maßgeblichen Rechtsprechung widerspiegelt. Dies ist in der EU in Bezug auf die Charta der Grundrechte nicht der Fall. Artikel 8 der Charta formuliert den Schutz personenbezogener Daten als ein separates, proaktives Recht, das Personen zu der Erwartung berechtigt, dass ihre Informationen durch *jeden*, nicht nur den Staat, nur dann verarbeitet werden, wenn die in Artikel 8 Absätze 2 und 3 festgelegten wesentlichen Anforderungen erfüllt sind. Die Verarbeitung muss nach Treu und Glauben erfolgen, für den Menschen (die „betroffene Person" im EU-Recht) transparent sein und zu besonderen Zwecken erfolgen. Die Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken, und die Einhaltung ihrer Rechte muss von einer unabhängigen Stelle überwacht werden. Diese Bedingungen, die auf einigen, wenn auch nicht allen, der Grundsätze in Richtlinie 95/46/EG (im Folgenden „die Datenschutzrichtlinie") basieren, können als der „Wesensgehalt" des Rechts betrachtet werden.[14] Das Recht auf den Schutz personenbezogener Daten dient auch dem Schutz anderer Grundrechte und Freiheiten, insbesondere – aber nicht ausschließlich – dem Recht auf Privatsphäre, indem es den Ausgleich anderer Interessen und Ziele der EU verlangt.[15]

13. Artikel 16 AEUV bietet die Rechtsgrundlage für die Annahme von Regelungen in Bezug auf Datenschutz und den freien Datenverkehr innerhalb der EU. Diese Regelungen (unten zusammengefasst) sehen ein System von Kontrollen und Ausgleichen sowie konkrete Rechte und Pflichten, Verfahren und Überwachungsmechanismen vor. Sie gelten für sämtliche Verarbeitung personenbezogener Daten, nämlich die ganz oder teilweise automatisierte oder

[10] Siehe auch die Arbeitsunterlage der Artikel-29-Datenschutzgruppe über die Überwachung elektronischer Kommunikation am Arbeitsplatz, WP55, 2002.
[11] *Schecke*, Rdnrn. 81-85.
[12] *Rundfunk*, Rdnr. 74.
[13] *Schecke*, Rdnrn. 81-86.
[14] Wie durch den EuGH durch Bezugnahme auf einen unabhängigen Datenschutzbeauftragten als einen „wesentlichen Bestandteil" von Artikel 8 bestätigt wird; Rechtssache C-14/10 *Kommission gegen Österreich*, Urteil des EuGH vom 16. Oktober 2012; C-288/12 *Kommission gegen Ungarn*, Urteil des EuGH vom 8. April 2014.
[15] Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", WP 136, 2007, S. 7.

sonstige Verarbeitung personenbezogener Daten, die in einer Datei gespeichert werden sollen, mit Ausnahme der Verarbeitung, die für die Ausübung von Tätigkeiten erfolgt, die nicht in den Anwendungsbereich des EU-Rechts fallen, oder die zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird.[16] Jeder Mitgliedstaat muss nationale Vorschriften auf alle Verarbeitungen anwenden, „die im Rahmen der Tätigkeiten einer Niederlassung ausgeführt werden, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet dieses Mitgliedstaats besitzt", auch wenn sich die Niederlassung selbst in einem anderen Mitgliedstaat oder in einem Drittland befindet.[17] Eines oder mehrere dieser Instrumente könnten daher für Maßnahmen bei der Regulierung von Finanzdienstleistungen gelten.

14. Das heißt, der EU-Rahmen verbietet nicht die Verarbeitung personenbezogener Daten; im Gegenteil, die EU fördert die Verarbeitung, wobei die „Spielregeln" für Bürger, Unternehmen und Behörden klargestellt werden müssen.

Datenschutz und Privatsphäre als eigenständige Rechte

15. Datenschutz und Privatsphäre sind daher sowohl in ihrer Art als auch in ihrer Umsetzung eigenständige Rechte und erfordern eine separate Analyse und Anwendung. Der Anwendungsbereich von Datenschutz ist weitläufig. Während die Bestimmung des Eingriffs in die Privatsphäre vom Zusammenhang abhängt, gelten Datenschutzregelungen für sämtliche Verarbeitung vorbehaltlich bestimmter Ausnahmen.[18] Ebenso, in einem anderen Sinne, ist das Recht auf Privatsphäre breiter angelegt als das Recht auf Datenschutz, da es sich auf Haus und Familie bezieht und zusätzlich zu personenbezogenen Angaben noch viele andere Dimensionen umfasst.[19] Demnach sind nicht alle Situationen, die in den Anwendungsbereich des Datenschutzrechts fallen, durch das Recht auf Privatsphäre abgedeckt, und nicht alle Situationen, die das Recht auf Privatsphäre betreffen, beinhalten die Verarbeitung personenbezogener Daten.

16. Einige Maßnahmen beinhalten die Verarbeitung personenbezogener Daten und müssen als solche mit den Datenschutzregelungen übereinstimmen, obwohl sie das Recht auf Privatsphäre nicht berühren. Der EuGH hat beispielsweise für Recht befunden, dass es nicht als Eingriff in das Privatleben ausgelegt werden kann, wenn ein Arbeitgeber Aufzeichnungen der Namen und Gehaltsangaben seiner Mitarbeiter führt (obwohl dies natürlich als Datenverarbeitung die Einhaltung der EU-Datenschutzregelungen erfordern würde).[20]

17. In anderen Fällen betrifft die Verarbeitung personenbezogener Daten das Recht auf Privatsphäre. Im oben zitierten *Rundfunk*-Urteil hat der EuGH für Recht befunden, dass die Kommunikation von Informationen durch den Arbeitnehmer - ob „sensibel" oder nicht - über Arbeitnehmer an einen Dritten (z. B. im fraglichen Fall eine Behörde) das Recht auf Privatsphäre der betroffenen Personen tatsächlich verletzt.[21] Diese Wirkung wird wahrscheinlich, wenn die jeweiligen Informationen sensibel sind (z. B. medizinische Daten), die Informationen zu Überwachungszwecken oder zum

[16] Artikel 3 der Richtlinie 95/46/EG.
[17] Artikel 4 Absatz 1 Buchstabe a der Richtlinie 95/46/EG. Siehe auch Rechtssache C-131/12, *Google Spain gegen Agencia Española de Protección de Datos*, Urteil des EuGH vom 13. Mai 2014, Rdnr. 52.
[18] Siehe obige Ziffer 13.
[19] Siehe z. B. das Urteil des U.S. Supreme Court in der Rechtssache *Griswold gegen Connecticut* (1965).
[20] *Rundfunk*, Rdnr. 74.
[21] *Rundfunk*, Rdnrn. 74- 75.

Strafvollzug verwendet werden oder die Verarbeitung etwas Permanentes oder Systematisches hat, z. B. wenn die Informationen aufbewahrt und nicht nur erhoben und verwendet werden.

18. Die Unterscheidung dieser beiden Rechte spiegelte sich in gewissem Maße im Urteil in der Rechtssache *Digital Rights Ireland* betreffend die verpflichtende Aufbewahrung von Kommunikationsdaten wider. In diesem Fall hat der EuGH für Recht befunden, das es nicht ausreichend war, Artikel 7 auf das Recht auf Privatsphäre anzuwenden (obwohl dies der Fokus der nationalen Gerichte war, die die jeweiligen verbundenen Rechtssachen an den EuGH verwiesen haben). Vorratsdatenspeicherung stellte die Verarbeitung personenbezogener Daten im Sinne von Artikel 8 dar und musste daher auch den konkreten Anforderungen des Artikels entsprechen.[22]

19. Wie diese Leitlinien erläutern sollen, hilft das Verständnis von Umfang, Zweck und Rechtsgrundlage der Verarbeitung personenbezogener Daten bei der Beurteilung, ob die vorgeschlagene Maßnahme in das Recht auf Privatsphäre nach Artikel 7 der Charta eingreift.

Übersicht über den Datenschutzrahmen

20. Der Rechtsrahmen für die Verarbeitung personenbezogener Daten in der EU besteht derzeit aus vier wesentlichen Instrumenten:

    - Die **Richtlinie 95/46/EG**[23] bzw. Datenschutzrichtlinie ist das Kernstück des Datenschutzrechts in Europa. In ihr werden allgemeine Regelungen über die Rechtmäßigkeit der Verarbeitung personenbezogener Daten und über die Rechte von Personen festgelegt, deren Daten verarbeitet werden (betroffene Personen). Sie verlangt von jedem Mitgliedstaat, dafür zu sorgen, dass eine für die Überwachung der Umsetzung der Richtlinie verantwortliche unabhängige Aufsichtsbehörde vorhanden ist.

    - Die **Verordnung (EG) Nr. 45/2001**[24] deckt die Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der EU ab und legt den EDSB als unabhängige Kontrollbehörde fest.

    - Die **Richtlinie 2002/58/EG**[25] betrifft die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation und legt Regelungen von besonderer Relevanz fest, einschließlich zu Vertraulichkeit, Abrechnungs- und Verkehrsdaten und Regelungen zu unerbetenen Werbenachrichten.

---

[22] *Digital Rights*, Rdnr. 29.

[23] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23.11.1995, S. 31-50**.** Die Richtlinie wird gerade überarbeitet und durch die vorgeschlagene Datenschutz-Grundverordnung (Fußnote 6) ersetzt, die, sobald sie in Kraft tritt, die Überarbeitung von Richtlinie 2002/58/EG und Verordnung (EG) Nr. 45/2001 erfordert, um die Abstimmung der Regelungen sicherzustellen.

[24] Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr (ABl. L 008 vom 12.1.2001, S. 1-22).

[25] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) ABl. L 201 vom 31.7.2002, S. 37-47).

- Der **Rahmenbeschluss 2008/977/JI des Rates**[26] betrifft die polizeiliche und justizielle Zusammenarbeit in Strafsachen sowie auf den Austausch personenbezogener Daten anwendbare Regeln, einschließlich nationaler und EU-Datenbanken sowie Übermittlungen an zuständige Behörden und an Privatpersonen zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder Vollstreckung strafrechtlicher Sanktionen.

3. Zehn analytische Schritte

21. Wie im vorstehenden Abschnitt angedeutet, ist der EU-Rechtsrahmen komplex. Der EDSB hat daher für die Regulierung von Finanzdienstleistungen eine 10-Schritte-Methode entwickelt, die politische Entscheidungsträger bei potenziellen Schwierigkeiten unterstützen kann.

1) Identifizierung der zu verarbeitenden personenbezogenen Daten

Definition von personenbezogenen Daten

22. Jede Maßnahme, die die Verarbeitung personenbezogener Daten vorsieht, sollte die Arten der personenbezogenen Daten klar festlegen, insbesondere zu verarbeitende sensible Daten.

23. Personenbezogene Daten sind als Informationen bezüglich einer bestimmten oder bestimmbaren natürlichen Person („betroffene Person“) definiert[27]. Eine bestimmbare Person ist eine Person, die direkt oder indirekt insbesondere durch eine Identifikationsnummer oder einen oder mehrere Faktoren bestimmt werden kann, die für ihre physische, physiologische, mentale, wirtschaftliche, kulturelle oder soziale Identität spezifisch ist. Dies ist ein breit angelegtes Konzept, das viel mehr als nur Informationen umfasst, die eine Person unmittelbar identifizieren, z. B. einen Namen, eine nationale Registrierung oder eine Steueridentifikationsnummer. Es würde z. B. auch Informationen in Bezug auf Vergütung, Einkommen und Vermögen und die Beträge von Personen zugewiesenen staatlichen Beihilfen, biometrische Informationen, IP-Adressen, Verkehrs- und Standortdaten, tägliche Arbeits- und Ruhezeiträume und entsprechende Pausen und Intervalle beinhalten.[28]

Sensible Daten

24. Regulierungsmaßnahmen im Finanzsektor erfordern häufig die Verarbeitung von Daten in Bezug auf Straftaten und Verurteilungen in Strafverfahren einschließlich Verdacht auf Straftaten. Sie werden als „*sensible Daten*“ bezeichnet.[29] Die anderen

[26] Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl. L 350 vom 30.12.2008, S. 60-71. Der Rahmenbeschluss wird ebenfalls gerade überarbeitet und ersetzt durch einen Vorschlag für eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständige Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgungen von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr; KOM(2012) 10 endgültig, 25.1.2012.

[27] Artikel 2 Buchstabe a der Richtlinie 95/46/EG.

[28] Die Artikel-29-Datenschutzgruppe analysiert in ihrer Stellungnahme 4/2007 die vier Elemente des Konzepts, d. h. „alle Informationen“, „betreffend“, „bestimmte oder bestimmbare“ und „natürliche Person“, von denen jedes bewertet werden muss, um zu bestimmen, ob „personenbezogene Daten“ in einer gegebenen Situation zur Debatte stehen. Siehe auch Ziffer 4.1 des EDSB-Strategiepapiers.

[29] Artikel 8 der Richtlinie 95/46/EG beschreibt „besondere Kategorien“ personenbezogener Daten. Artikel 10 der Richtlinie 45/2001 behandelt die Verarbeitung dieser Kategorien durch die Organe oder Einrichtungen der EU; Artikel 6 des Rahmenbeschlusses 2008/977/JI behandelt die Verarbeitung durch Strafvollzugsbehörden.

Arten von sensiblen Daten nach EU-Recht umfassen Daten, die Rassen- oder ethnische Zugehörigkeit, politische, religiöse oder philosophische Ansichten, die Mitgliedschaft in einer Gewerkschaft und Angaben über den Gesundheitszustand oder über das Sexualleben offenlegen. In der EU ist die Verarbeitung sensibler Daten grundsätzlich verboten, es sei denn, sie erfüllt strenge Auflagen und wendet angemessene Vertraulichkeit und Garantien an, wie sie nach nationalem Recht vorgeschrieben sind.[30]

Anonymisierung

25. Personenbezogene Daten, die anonymisiert wurden, d. h. Daten, die so verändert wurden, dass die betroffene Person nicht länger bestimmbar ist, fallen nicht unter die EU-Datenschutzregelungen.[31] Die Technik macht es jedoch immer besser möglich, eine Person unter Nutzung anonymisierter Daten erneut zu identifizieren, zum Beispiel in Kombination mit anderen verfügbaren, möglicherweise sogar öffentlich verfügbaren Informationsquellen. Das beste Mittel, um sicherzustellen, dass die Person geschützt ist, besteht daher nicht in der Anonymisierung, sondern darin, die Verarbeitung personenbezogener Daten so gering wie möglich zu halten.

Definition von Verarbeitung und des für die Verarbeitung Verantwortlichen

26. „Verarbeitung" ist definiert als jeder „mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten".[32] Maßnahmen, die die Verarbeitung personenbezogener Daten beinhalten (unabhängig davon, ob befunden wurde, dass diese in die Privatsphäre eingreift oder nicht), müssen mit den geltenden Datenschutzbestimmungen übereinstimmen.

27. Der „für die Verarbeitung Verantwortliche" ist die juristische oder natürliche Person, die die „Zwecke und Mittel" der Verarbeitung festlegt und der in der EU die meisten gesetzlichen Verantwortlichkeiten und Verpflichtungen zum Datenschutz zufallen, wie z. B. Sicherstellung der Datenqualität, Anwendung angemessener Sicherheitsmaßnahmen und Reaktion auf die Ausübung der Rechte der betroffenen Person. Bei Maßnahmen, die die Verarbeitung personenbezogener Daten beinhalten, sollte die Identität des für die Verarbeitung Verantwortlichen eindeutig sein.

Empfehlung

28. Sämtliche Maßnahmen, die die Verarbeitung personenbezogener Daten beinhalten, sollten eine materiell-rechtliche Bestimmung enthalten, die verlangt, dass die Verarbeitung in Übereinstimmung mit den EU- und den nationalen Datenschutzbestimmungen stattfindet. Dies sollte im Basisrechtsakt selbst enthalten sein und nicht in delegierten Rechtsakten oder Durchführungsrechtsakten der

[30] Artikel 8 Absatz 5 der Richtlinie 95/46/EG. Siehe nachstehend die Ziffern 59-61 zu Datensicherheitsmaßnahmen.
[31] Erwägungsgrund 26 der Richtlinie 95/46/EG.
[32] Artikel 2 Buchstabe b der Richtlinie 95/46/EG.

Kommission oder in Umsetzungsmaßnahmen von Mitgliedstaaten.[33] Die Bestimmung sollte so präzise wie möglich Folgendes abdecken:

a) die Art der zu verarbeitenden Daten und insbesondere sensiblen Daten;

b) wie lange die Daten gespeichert werden;

c) wer auf die Daten zugreifen kann; und

d) angemessene Garantien zum Schutz der Rechte von Personen.

2) Beurteilung, ob die Datenverarbeitung in das Recht auf Privatsphäre eingreift

29. Zur Feststellung, ob eine vorgeschlagenen Maßnahme mit dem Recht auf Privatsphäre und dem Recht auf Datenschutz im Einklang steht, sind separate Analysen erforderlich. Falls ein Eingriff in das Recht auf Privatsphäre offenbar wird, wird Artikel 52 Buchstabe 1 der Charta relevant.[34]

Befugnis zum Betreten privater Räumlichkeiten in der Marktmissbrauchsverordnung

Eine Befugnis zum Betreten privater Räumlichkeiten zur Beschlagnahme von Dokumenten in jedweder Form ist hochgradig eingreifend. Unter normalen Umständen sollten Inspektionen vor Ort durch zuständige Behörden auf die Geschäftsräume des fraglichen Unternehmens beschränkt sein und die Inspektion privater Räumlichkeiten von Mitarbeitern ausschließen, es sei denn, dies ist zwingend erforderlich.

Der EDSB argumentierte in seiner Stellungnahme zum Vorschlag der Kommission, dass eine solche Befugnis grundsätzlich einer vorherigen gerichtlichen Genehmigung bedürfen sollte. Die angenommene Verordnung sieht, wie im nationalen Recht gefordert, eine Bestimmung betreffend die vorherige Genehmigung durch eine Justizbehörde vor.

Empfehlung

30. Politische Entscheidungsträger sollten als Teil der Folgenabschätzung in Erwägung ziehen, ob ein Eingriff im Verhältnis zum Zweck der Maßnahme steht und ob das gewünschte Ergebnis mit anderen Maßnahmen und einem geringeren Eingriff in das gefährdete Grundrecht erzielt werden könnte.[35] Falls kein alternatives Mittel zur Verfügung steht, sollten politische Entscheidungsträger versuchen, den Eingriff auf das zu beschränken, was zum Erreichen der angegebenen Zwecke unbedingt erforderlich ist.[36] Dies könnte durch die Reduzierung der zu verarbeitenden

[33] Siehe z. B. die Stellungnahme des EDSB zum Europäischen Beschluss zur vorläufigen Kontenpfändung, 13. Oktober 2011, S. 4.
[34] Siehe obenstehende Ziffern 10-11.
[35] In den verbundenen Rechtssachen C-92/09 und C-93/09 *Schecke* hat der EuGH in Randnummer 81 festgehalten, dass die EU-Gesetzgeber beim Erlass von Maßnahmen, die die verpflichtende Veröffentlichung bestimmter Informationen über Empfänger von EU-Geldern auferlegen, Methoden der Veröffentlichung dieser Informationen hätten erwägen sollen, die im Einklang mit dem Zweck einer solchen Veröffentlichung gestanden hätten, zugleich aber auch in das Recht dieser Empfänger auf Achtung ihres Privatlebens im Allgemeinen und auf Schutz ihrer personenbezogenen Daten im Besonderen weniger stark eingegriffen hätten.
[36] Der EuGH hat für Recht befunden, dass der Gestaltungsspielraum des Gesetzgebers aufgrund des Ausmaßes und der Schwere des Eingriffs in die Grundrechte von Personen notwendigerweise eingeschränkt wurde; *Digital Rights Ireland*, Rdnr. 48.

Datenmenge oder durch Festlegung von Garantien zum Schutz der Rechte von Personen im Dokument selbst erreicht werden.[37]

3) Definition des Zwecks für die Verarbeitung personenbezogener Daten

31. Personenbezogene Daten dürfen nur für „festgelegte eindeutige und rechtmäßige" Zwecke erhoben und „nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden".[38] Dabei handelt es sich um den Grundsatz der *„Zweckbindung"*. Bei der Regulierung von Finanzdienstleistungen beinhalten legitime öffentliche Interessen unter anderem die Stabilität des Finanzsystems, Transparenz, die Verhinderung von Marktmissbrauch, die Erhöhung der Marktintegrität und des Anlegerschutzes sowie die Bekämpfung von Geldwäsche. Vollstreckungsbehörden können Informationen von Dritten wie z. B. über Bevölkerung, soziale Sicherheit, Steuerregister oder Telecom-Betreiber verlangen, welche ursprünglich zu anderen Zwecken erhobene personenbezogene Daten umfassen. Maßnahmen, die dies vorsehen, sollten ausdrücklich die in Artikel 13 der Datenschutzrichtlinie festgelegten Ausnahmen anwenden, nach dem Mitgliedstaaten gesetzgeberische Maßnahmen ergreifen dürfen, die erforderlich sind, um Überwachung, Inspektion oder Regulierungsfunktionen in Verbindung mit einem wirtschaftlichen oder finanziellen Interesse eines Mitgliedstaats oder der EU zu gewährleisten.

32. Im Rahmen dieser Maßnahmen erhobene Daten sollten nicht für andere unvereinbare Zwecke weiterverwendet werden. Die Artikel-29-Datenschutzgruppe hat zu den Kriterien für die Bewertung der Vereinbarkeit von Zwecken eine Anleitung zur Verfügung gestellt.[39] Die Weiterverarbeitung zu anderen Zwecken, die die Rechte der Person beeinträchtigen könnten, ist wahrscheinlich unvereinbar. Zum Beispiel sollten Daten, die ursprünglich zum Zweck der Bekämpfung von Terrorismus und Geldwäsche erhoben wurden, nicht zum Zweck der Bekämpfung von Betrug und Steuerhinterziehung weiterverwendet werden, es sei denn, das anwendbare Instrument gibt diese Zwecke konkret an.[40]

33. Die EU-Datenschutzbestimmungen enthalten außerdem den Grundsatz der *Datenminimierung*, nach dem nur Daten erhoben und verwendet werden, die den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen.[41] Politische Entscheidungsträger sollten für jede Art von personenbezogenen Daten die Verhältnismäßigkeit der Verarbeitung mit den „verfolgten legitimen Zwecken" vergleichen und bewerten, ob der Zweck der Maßnahme ohne die Verarbeitung der Daten erfüllt werden könnte.[42]

---

[37] Siehe folgende Ziffern 50-58. Stellungnahme des EDSB zu Vorschlägen für Märkte für Finanzinstrumente, 10. Februar 2012, Ziffern 40-2, 47.

[38] Artikel 6 Absatz 1 Buchstabe b der Richtlinie 95/46/EG, Artikel 4 Absatz 1 Buchstabe b der Richtlinie 45/2001 und Artikel 3 des Rahmenbeschlusses 2008/977/JI.

[39] Siehe Stellungnahme der Artikel-29-Datenschutzgruppe 3/2013 über Zweckbindung, 2013.

[40] Siehe Stellungnahme des EDSB zu Geldwäsche, 4. Juli 2013, S. 8-9.

[41] Artikel 6 Absatz 1 Buchstabe c der Richtlinie 95/46/EG und Artikel 4 Absatz 1 Buchstabe c der Richtlinie 45/2001.

[42] *Schecke* Rdnr. 74.

Insiderlisten

„Insiderinformationen“ beziehen sich auf nicht öffentliche Fakten über Emittenten von Finanzinstrumenten, die, wenn sie veröffentlicht würden, die Preise dieser Finanzinstrumente oder damit verbundener derivativer Instrumente erheblich beeinträchtigen würden („Insider-Geschäfte“). Nach Artikel 18 der Marktmissbrauchsverordnung müssen Emittenten von Finanzinstrumenten (oder eine in deren Namen oder auf deren Rechnung handelnde Person) eine Liste aller Personen vorlegen, die Zugriff auf Insiderinformationen haben und die gemäß einem Arbeitsvertrag für den Emittenten arbeiten oder die Aufgaben ausführen, durch die sie Zugriff auf Insiderinformationen haben, wie z. B. Berater, Buchhalter oder Ratingagenturen. Diese Insiderlisten ermöglichen den zuständigen Behörden die Untersuchung möglicher Insidergeschäfte oder möglichen Marktmissbrauchs.

Nach der Empfehlung des EDSB enthält die Marktmissbrauchsverordnung eine ausdrückliche Bezugnahme auf den Zweck der Listen, die Hauptelemente der Liste, den Grund, warum Personen eingebunden sind und eine Bezugnahme auf das Erfordernis, den EDSB zu Entwürfen technischer Durchführungsstandards zu konsultieren, die durch die ESMA zu erstellen sind, zum genauen Format von Insiderlisten und zum Format zu deren Aktualisierung.

Empfehlung

34. Die Maßnahme sollte stets die Zwecke angeben, für die personenbezogene Daten verarbeitet werden und so weit wie möglich die Weiterverarbeitung, die als vereinbar oder nicht vereinbar angesehen wird.

4) Festlegung einer Rechtsgrundlage für die Datenverarbeitung

Mögliche Rechtsgründe

35. Nach Artikel 8 Absatz 2 der Charta dürfen Daten nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Diese Gründe sind in der Datenschutzrichtlinie und in der Verordnung (EG) Nr. 45/2001 näher erläutert.[43] In der Richtlinie werden mehrere mögliche Gründe für die legitime Verarbeitung genannt:

    a) die betroffene Person hat ohne jeden Zweifel ihre Einwilligung gegeben;

    oder die Verarbeitung ist erforderlich:

    b) für die Erfüllung eines Vertrags mit der betroffenen Person;

    c) für die Erfüllung einer rechtlichen Verpflichtung, der der für die Verarbeitung Verantwortliche unterliegt;

    d) für die Wahrung lebenswichtiger Interessen der betroffenen Person;

    e) für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt; oder

    f) zur Verwirklichung des berechtigten Interesses, das von den dem für die Verarbeitung Verantwortlichen wahrgenommen wird, vorbehaltlich einer

[43] Artikel 7 der Richtlinie 95/46/EG und Artikel 5 der Verordnung Nr. 45/2001.

zusätzlichen Abwägungsprüfung zum Schutz der Rechte und Interessen der betroffenen Person[44].

36. Verordnung Nr. 45/2001 betreffend die Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der EU enthält eine ähnliche Formulierung, lässt jedoch den Grund des „berechtigten Interesses" aus. Eine gemeinsame angewendete Rechtsgrundlage ist die Notwendigkeit der Datenverarbeitung für die Durchführung einer Aufgabe, die im öffentlichen Interesse auf der Grundlage des EU-Rechts ausgeführt wird.[45]

Einwilligung als Rechtsgrundlage

37. Die Einwilligung der betroffenen Person kann eine offensichtliche Rechtsgrundlage darstellen, ist jedoch aufgrund der Bedingungen, die für eine gültige Einwilligung erfüllt werden müssen, nicht immer eine angemessene Rechtsgrundlage.[46] In Bezug auf die Transparenz des Schuldnervermögens sollte die rechtmäßige Verarbeitung von Daten zu dem Schuldnervermögen zum Beispiel nicht auf Einwilligung basieren, sondern auf der Übereinstimmung mit einer gesetzlichen Verpflichtung oder der Wahrnehmung eines öffentlichen Interesses.[47] Für Maßnahmen zur Bekämpfung von Geldwäsche hat der EDSB die „Notwendigkeit zur Übereinstimmung mit einer gesetzlichen Verpflichtung" als eine angemessene Rechtsgrundlage vorgeschlagen.[48] Zur Erhöhung der Transparenz an Finanzmärkten vorgesehene Maßnahmen sollten die Durchführung einer im öffentlichen Interesse stehenden Aufgabe anstatt Einwilligung erwägen. Eine Einwilligung kann jedoch in einmaligen, kurzfristigen Situationen angemessen sein, in denen es keine Möglichkeit für ungebührlichen Druck auf die betroffene Person gibt oder als zusätzliche Schutzebene für besonders vertrauliche Informationen.

Sensible Daten

38. Sensible Daten (d. h. Daten über Straftaten usw. - siehe Definition in obigem Punkt 24) dürfen nur dann verarbeitet werden, wenn eine von mehreren Ausnahmen gilt:[49]

    a) die betroffene Person hat ausdrücklich in die Verarbeitung dieser Daten eingewilligt, es sei denn, die Gesetze des Mitgliedstaats sehen etwas anderes vor;

    b) die Verarbeitung ist erforderlich, um den Rechten und Pflichten des für die Verarbeitung Verantwortlichen auf dem Gebiet des Arbeitsrechts Rechnung zu tragen, sofern dies aufgrund von einzelstaatlichem Recht, das angemessene Garantien vorsieht, zulässig ist;

[44] Siehe Stellungnahme der Artikel-29-Datenschutzgruppe 06/2014 zum Begriff des legitimen Interesses des für die Verarbeitung Verantwortlichen nach Artikel 7 der Richtlinie 95/46/EG.
[45] Artikel 5 Buchstabe a der Verordnung Nr. 45/2001.
[46] Artikel 2 Buchstabe h der Richtlinie 95/46/EG und Artikel 2 Buchstabe h der Verordnung Nr. 45/2001.
[47] Siehe Stellungnahme des EDSB zum Grünbuch der Kommission „Effiziente Vollstreckung gerichtlicher Entscheidungen in der Europäischen Union: Transparenz des Schuldnervermögens", 22. September 2008, Ziffern 9-12.
[48] Siehe Stellungnahme des EDSB zu Geldwäsche, Ziffer 33.
[49] Artikel 8 Absatz 2 der Richtlinie 95/46/EG.

c) die Verarbeitung ist zum Schutz der lebenswichtigen Interessen der betroffenen Person oder eines Dritten erforderlich, sofern die Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben;

d) die Verarbeitung erfolgt auf der Grundlage angemessener Garantien durch eine politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation, die keinen Erwerbszweck verfolgt, im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung nur auf die Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die Daten nicht ohne Einwilligung der betroffenen Personen an Dritte weitergegeben werden; oder

e) die Verarbeitung bezieht sich auf Daten, die die betroffene Person offenkundig öffentlich gemacht hat, oder ist zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche vor Gericht erforderlich.

Empfehlung

39. Maßnahmen, die personenbezogene Daten beinhalten, sollten auf einer ordnungsgemäßen Analyse der Rechtsgrundlage für diese Verarbeitung basieren und gegebenenfalls die Rechtsgrundlage für die Verarbeitung im Dokument selbst angeben. Maßnahmen, die die Verarbeitung sensibler Daten (wie in der Datenschutzrichtlinie definiert) vorsehen, müssen deutlich machen, welche der fünf Ausnahmen zum allgemeinen Verbot anwendbar ist.

5) Beurteilung und Rechtfertigung einer angemessenen Aufbewahrungsfrist für die Daten

40. Für die angegebenen Zwecke als erforderlich erachtete personenbezogene Daten sollten gelöscht werden, sobald die Daten für diese Zwecke nicht länger erforderlich sind, es sei denn, es sind besondere EU- oder nationale Bestimmungen anwendbar, wie zum Beispiel diejenigen, die die Aufbewahrung dieser Daten für einen gegebenen Zeitraum, z. B. für Steuerzwecke, vorschreiben.[50]

[50] Artikel 6 Absatz 1 Buchstabe e der Richtlinie 95/46/EG und Artikel 4 Absatz 1 Buchstabe e der Verordnung Nr. 45/2001. Siehe Stellungnahme des EDSB zu Vorschlägen über Märkte für Finanzinstrumente, Ziffer 16.

Vorratsdatenspeicherung bezüglich Überwachung von Wertpapierfirmen und möglicher Geldwäsche

Jüngste Maßnahmen haben abweichende Methoden für die Speicherung personenbezogener Daten angewandt, die als Bestandteil der Überwachung der Einhaltung von EU-Regelungen erhoben worden sind.

Die Marktmissbrauchsverordnung fordert, dass personenbezogene Daten, die als Bestandteil von Überwachungstätigkeiten verarbeitet werden, für höchstens fünf Jahre gespeichert werden.

Die überarbeitete Richtlinie über Märkte für Finanzinstrumente verlangt von Wertpapierfirmen die Aufbewahrung von Aufzeichnungen von sämtlichen erbrachten bzw. durchgeführten Dienstleistungen, Tätigkeiten und Transaktionen für fünf Jahre oder „bis zu sieben Jahren", wenn die Daten durch eine zuständige Behörde angefordert werden.

Der Vorschlag der Kommission für eine neue Geldwäsche-Richtlinie schlägt eine Aufbewahrungsfrist von fünf Jahren nach Leistung der Zahlung vor, die bis auf 10 Jahre erweitert werden könnte – eine Bestimmung, die der EDSB als willkürlich und empirisch ungerechtfertigt infrage gestellt hat.

41. Die Festlegung der Vorratsdatenspeicherungsfrist in einem Rechtsakt erhöht die Rechtssicherheit und entspricht eher den bewährten Verfahren. Die Frist sollte nicht willkürlich festgelegt werden, sondern auf der Grundlage von objektiven Kriterien und einer Analyse von Fall zu Fall.

Empfehlung

42. Die Gesetzgeber sollten sorgfältig auswerten, welche Aufbewahrungsfrist für die zu verarbeitenden personenbezogenen Daten für den angegebenen Zweck ausreichend und verhältnismäßig wäre. Die Folgenabschätzung sollte eine Analyse der maßgeblichen Optionen beinhalten. Politische Entscheidungsträger sollten auch die Möglichkeit einer Revisionsklausel in Erwägung ziehen, die die Überprüfung und Überarbeitung der anfänglichen Aufbewahrungsfrist vorsieht oder anordnet. In Ermangelung einer ausdrücklichen Frist sollte der vorgeschlagene Rechtsakt zumindest verlangen, dass Daten gelöscht werden, sobald sie nicht mehr erforderlich sind.

6) Feststellung, welche Parteien innerhalb der EU Zugriff auf die personenbezogenen Daten haben

43. Der Austausch personenbezogener Daten zwischen in der EU ansässigen Privatorganisationen bzw. Behörden zählen auch als Datenverarbeitung innerhalb des Anwendungsbereichs der Datenschutzbestimmungen. Separate Bestimmungen gelten für den Austausch von Daten, je nachdem, ob es sich bei der beteiligten Behörde:[51]

    - um eine Strafvollzugs- oder Justizbehörde handelt, die dem Rahmenbeschluss 2008/977/JI unterliegen könnte; oder

[51] Siehe Stellungnahme des EDSB zu Geldwäsche, S. 7-8.

- um eine Verwaltungsbehörde, die Kredit- oder Finanzinstitute beaufsichtigt und auf nationaler Ebene wahrscheinlich der Datenschutzrichtlinie oder auf EU-Ebene der Verordnung Nr. 45/2001 unterliegt.[52]

Empfehlung

44. Vorschläge sollten in Bezug auf die jeweiligen zuständigen Behörden so präzise wie möglich sein und unter anderem Folgendes beinhalten:

    - die Arten der auszutauschenden Daten;
    - die Zwecke, für die die Daten übermittelt und weiterverarbeitet werden könnten[53]; und
    - Garantien gegen den Zugriff auf Daten durch andere externe Behörden oder Dritte, die ein Interesse an dem verfolgten Zweck haben.[54]

7) Festlegung einer korrekten Rechtsgrundlage für die Übermittlung personenbezogener Daten außerhalb der EU

45. Die Übermittlung personenbezogener Daten an Drittländer birgt besondere Risiken für den Einzelnen und das Erfordernis einer solchen Offenlegung muss mit den Rechten des Einzelnen in Einklang gebracht werden.[55] Gemäß Artikel 25 und 26 der Datenschutzrichtlinie und Artikel 9 der Verordnung Nr. 45/2001 dürfen personenbezogene Daten grundsätzlich nur an ein Drittland übermittelt werden, wenn die Kommission, unbeschadet der Einhaltung anderer anwendbarer Vorschriften, der Ansicht ist, dass das Empfängerland ein ausreichendes Schutzniveau gewährleistet.[56] In Ermangelung eines Angemessenheitsbeschlusses dürfen personenbezogene Daten nur übermittelt werden, wenn die Übermittlung in eine begrenzte Anzahl von Ausnahmen fällt, unter anderem:

    a) die betroffene Person hat ohne jeden Zweifel ihre Einwilligung gegeben;

    b) die Übermittlung ist für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich;

---

[52] Artikel 7 und 8 der Verordnung Nr. 45/2001 regulieren die Übermittlung personenbezogener Daten innerhalb oder zwischen Organen und Einrichtungen der EU und an sonstige Empfänger.

[53] Stellungnahme des EDSB zu der Haushaltsordnung für den Gesamthaushaltsplan der Europäischen Gemeinschaften, 12. Dezember 2006, S. 12-18, Ziffer 22.

[54] Siehe z. B. die Stellungnahme des EDSB zu der Bekämpfung von Geldwäsche, S. 21-22.

[55] Eine detaillierte Anleitung siehe Arbeitsunterlage der Artikel-29-Datenschutzgruppe 1/2009 über Offenlegungspflichten im Rahmen der vorprozessualen Beweiserhebung bei grenzüberschreitenden zivilrechtlichen Verfahren (pre-trial discovery).

[56] Sollen die Daten an eine internationale Organisation übermittelt werden, muss ein angemessenes Schutzniveau gewährleistet sein. Siehe die Beschlüsse der Europäischen Kommission in Bezug auf die aktuelle Angemessenheit http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm (Abruf vom 16.11.2014). Gemäß Artikel 9 der Verordnung Nr. 45/2001 hat der für die Verarbeitung Verantwortliche – d. h. das Organ oder die Einrichtung der EU, das bzw. die die Übermittlung veranlasst hat - ebenfalls die Möglichkeit, die Angemessenheit des von dem betreffenden Drittland oder der betreffenden internationalen Organisation gebotenen Schutzniveaus zu beurteilen. Siehe EDSB, „Die Übermittlung personenbezogener Daten an Drittländer und internationale Organisationen durch Organe und Einrichtungen der EU: Positionspapier“, 14. Juli 2014.

c) die Übermittlung ist für den Abschluss oder zur Erfüllung eines Vertrags erforderlich, der im Interesse der betroffenen Person vom für die Verarbeitung Verantwortlichen mit einem Dritten geschlossen werden soll;

d) die Übermittlung ist entweder zur Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich oder gesetzlich vorgeschrieben.

46. Diese Arten von Ausnahmen müssen sorgfältig, restriktiv und von Fall zu Fall ausgelegt werden.[57] Die Gründe des „wichtigen öffentlichen Interesses" implizieren insbesondere Interessen, die durch die auf in der EU niedergelassene für die Verarbeitung Verantwortliche anwendbare nationale Gesetzgebung als solche identifiziert werden; die Interessen von Drittländern oder selbst die von Drittländern festgelegten rechtlichen Anforderungen sind in sich selbst nicht gültig oder ausreichend.[58] Bestimmte Maßnahmen im Bereich der Regulierung von Finanzdienstleistungen sehen vor, dass für die Verarbeitung Verantwortliche bei der Hilfe für Strafvollzugsbehörden oder private Interessenverbände, die illegale Aktivitäten wie Geldwäsche oder Betrug bekämpfen, über ihre konkreten gesetzlichen Verpflichtungen hinausgehen. Falls gemäß innerstaatlichem Recht, dem der für die Verarbeitung Verantwortliche unterliegt, in dem Mitgliedstaat ein wichtiges öffentliches Interesse vorliegt, könnte diese Ausnahme auf Übermittlungen von personenbezogenen Daten an zuständige Behörden von Drittländern anwendbar sein, wenn dies für die Überwachung von in deren Gebieten ansässigen Mutterunternehmen erforderlich ist, die in einem oder mehreren Mitgliedstaaten ein Tochterunternehmen haben. Das „öffentliche Interesse" kann jedoch nicht zur Rechtfertigung wiederholter, massiver oder struktureller Übermittlungen von Daten herangezogen werden, wie der EDSB in Bezug auf die vorgeschlagene Massenübermittlung personenbezogener und sensibler Daten an das Ausland zum Zwecke der Bekämpfung von Geldwäsche argumentiert hat.[59]

47. Falls keine der Ausnahmen anwendbar ist, muss der Absender der Daten angemessene Garantien erbringen, um sicherzustellen, dass die betroffenen Personen im Rahmen eines durchsetzbaren, rechtsverbindlichen Instruments angemessen geschützt sind[60]. Für private Rechtsträger nimmt dies normalerweise die Form einer Vereinbarung mittels standardmäßiger Vertragsklauseln, verbindlicher unternehmensinterner Vorschriften oder *Ad-hoc*-Vereinbarungen zwischen dem Absender und dem Empfänger der Daten an. Für den öffentlichen Sektor können diese Garantien durch Verbindlichkeiten abgedeckt sein, die in Absichtserklärungen oder rechtsverbindlichen internationalen Vereinbarungen enthalten sind. Wenn

[57] Artikel-29-Datenschutzgruppe, Arbeitsunterlage zu einer gemeinsamen Auslegung von Artikel 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995, S. 7.

[58] Artikel-29-Datenschutzgruppe, Arbeitsunterlage zu Artikel 26 Absatz 1, S. 14-15. Die Datenschutzgruppe weist darauf hin, dass Erwägungsgrund 58 der Richtlinie 95/46/EG in Bezug auf den internationalen Austausch von Daten festlegt, dass dieser „zwischen Steuer- oder Zollverwaltungen in verschiedenen Ländern" oder „zwischen Diensten, die für Angelegenheiten der sozialen Sicherheit zuständig sind" erforderlich sein könnte, was auf das Interesse von Behörden eines EU-Mitgliedstaats und nicht nur auf Interessen von Behörden im Drittland hindeutet.

[59] Siehe Stellungnahme des EDSB zu Geldwäsche, S. 11-12.

[60] Die Garantien müssen ausreichenden Schutz der Daten durch den Empfänger aufweisen, und zwar durch Bereitstellung detaillierter Verpflichtungen zu Aspekten wie z. B. dem Recht von betroffenen Personen zur Durchsetzung von Ansprüchen aufgrund der Verletzung der vertraglichen Verpflichtungen des Importeurs oder Exporteurs, der Verpflichtungen des Exporteurs und des Importeurs, Einzelheiten zu Haftung, Schlichtung und Gerichtsbarkeit, geltendem Recht, Überwachung usw.

angemessene Garantien erbracht werden, könnte das anwendbare Recht vom Absender der Daten zusätzlich verlangen, die zuständigen Datenschutzbehörden zu benachrichtigen oder eine vorherige Genehmigung von diesen einzuholen.[61]

48. Artikel 13 des Rahmenbeschlusses 2008/977/JI sieht eine separate spezifische Regelung für internationale Übermittlungen vor, die zur Verhütung, Ermittlung, Feststellung von Straftaten oder zur Vollstreckung strafrechtlicher Sanktionen erforderlich sind.

Empfehlung

49. Maßnahmen, die die Übermittlung personenbezogener Daten an Drittländer vorsehen, müssen eindeutig auf der Rechtsgrundlage für die Übermittlung erfolgen und sollten fallweise Entscheidungen vorsehen, die den Grundsatz der Datenminimierung achten (siehe obigen Punkt 33). Es könnte angemessen sein, ausdrücklich Garantien vorzusehen, die Qualität, Relevanz und Vertraulichkeit der Daten sicherstellen, sowie die vorherige ausdrückliche Genehmigung der zuständigen Behörde für die weitere Übermittlung von Daten an oder durch ein Drittland.

8) Bereitstellung angemessener Garantien für die Datenschutzrechte von Personen

a) Auskunftsrecht

50. Personen haben das Recht, über die Verarbeitung ihrer personenbezogenen Daten und über ihre Rechte ausreichend informiert zu werden, ungeachtet dessen, ob die Daten direkt von ihnen oder aus anderen Quellen erhoben wurden.[62] Sie sollten zumindest über die Identität des für die Verarbeitung Verantwortlichen, den Zweck der Verarbeitung und über weitere möglicherweise relevante Angaben informiert werden.

51. Maßnahmen sollten angemessene Garantien dafür vorsehen, dass dieses Recht gewahrt wird. Zum Beispiel sollte die im Zusammenhang mit Whistleblowing[63] beschuldigte Person über die Art der Beschuldigung informiert werden. Im Fall von EU-weiten Datenbanken, die personenbezogene Daten enthalten, sollte die Kommission oder die sonstige für ihre Verwaltung zuständige Stelle dafür sorgen, dass die Datenschutzrichtlinie auf ihrer Website öffentlich abrufbar ist.

[61] Gemäß der Verordnung Nr. 45/2001 hat der EDSB die Möglichkeit, eine Genehmigung für die Übermittlung personenbezogener Daten auszustellen.

[62] Artikel 10 und 11 der Richtlinie 95/46/EG, Artikel 11 und 12 der Verordnung Nr. 45/2001 und Artikel 16 des Rahmenbeschlusses 2008/977/JI.

[63] Verfahren zur Meldung mutmaßlicher Missstände ermutigen typischerweise die Mitglieder einer Organisation mit dem Versprechen von Straffreiheit, Verstöße gegen bestehende Regeln durch einen früheren oder aktuellen Partner/Kollegen zu melden, der sich nach anwendbarem Recht schuldig gemacht haben könnte.

Das Auskunftsrecht im Kontext von Verfahren zur Meldung mutmaßlicher Missstände

Die Marktmissbrauchsverordnung sieht vor, dass zuständige Behörden und Arbeitgeber Verfahren für die Meldung tatsächlicher oder potenzieller Verstöße gegen die Verordnung haben.

Die Person, gegen die im Bericht des Informanten Anschuldigungen erhoben werden, sollte durch die für das Verfahren zur Meldung mutmaßlicher Missstände verantwortliche Person so schnell wie möglich informiert werden, nachdem die Informationen zuerst gemeldet worden sind.

Der Beschuldigte sollte über Folgendes informiert werden:

1) die für das Verfahren zur Meldung mutmaßlicher Missstände verantwortliche Instanz,

2) die Fakten der Beschuldigung,

3) die Abteilungen oder Dienste innerhalb seines eigenen Unternehmens oder in anderen Körperschaften oder Unternehmen der Gruppe, von der das Unternehmen ein Teil ist, die den Bericht erhalten könnten und

4) darüber, wie er seine Rechte auf Zugriff und Korrektur ausüben kann.

Wenn es jedoch ein erhebliches Risiko dafür gibt und weiterhin geben wird, dass diese Benachrichtigung die Fähigkeit des Unternehmens oder der zuständigen Behörde zur wirksamen Untersuchung des Vorwurfs oder zur Erhebung der erforderlichen Beweise beeinträchtigen würde, darf die für das Verfahren zur Meldung mutmaßlicher Missstände verantwortliche Person die Benachrichtigung des Beschuldigten verzögern.

Stellungnahme der Artikel-29-Datenschutzgruppe 1/2006 zur Anwendung der EU-Datenschutzvorschriften auf interne Verfahren zur Meldung mutmaßlicher Missstände in den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität, S. 13.

b) Recht auf Auskunft, Berichtigung und Löschung

52. Nach Beginn der Verarbeitung haben Personen das Recht, vom für die Verarbeitung Verantwortlichen ohne Einschränkung in angemessenen Abständen und ohne übermäßige Verzögerungen oder Kosten Informationen über die verarbeiteten Datenkategorien, über den Zweck der Verarbeitung, über den Empfänger und über die „Logik“ im Zusammenhang mit der automatischen Verarbeitung ihrer personenbezogenen Daten einzuholen. Personen können Auskunft auf die in einer verständlichen Form verarbeiteten personenbezogenen Daten erhalten. Dieses Auskunftsrecht, das insbesondere für Personen relevant ist, die von Informanten des Fehlverhaltens beschuldigt werden, steht in enger Verbindung mit dem Recht auf eine gute Verwaltung einschließlich des Rechts, vor einer Entscheidung gehört zu werden,

des Rechts auf wirksamen Rechtsbehelf und des Rechts der Verteidigung von jedem, der unter Anklage steht.[64]

53. Falls die Verarbeitung nicht mit den Datenschutzbestimmungen übereinstimmt, weil z. B. Daten unvollständig oder inkorrekt sind, können Personen die Berichtigung, Löschung oder Sperrung der Daten erlangen.[65] Dies gilt auch, wenn die personenbezogenen Daten „nicht den Zwecken der Verarbeitung entsprechen, dafür nicht erheblich sind oder darüber hinausgehen, (...) nicht auf dem neuesten Stand sind oder (...) länger als erforderlich aufbewahrt werden, es sei denn, ihre Aufbewahrung ist für historische, statistische oder wissenschaftliche Zwecke erforderlich".[66] Schließlich muss der für die Verarbeitung Verantwortliche möglicherweise Dritte, denen die Daten offengelegt wurden, über durchgeführte Berichtigungen oder Löschungen benachrichtigen, sofern kein unverhältnismäßig hoher Aufwand damit verbunden ist.[67]

c) Widerspruchsrecht

54. Personen haben das Recht, gegen die Verarbeitung von sie betreffenden Daten jederzeit aus überwiegenden, schutzwürdigen, sich aus ihrer besonderen Situation ergebenden Gründen Widerspruch einzulegen.[68] Falls der Widerspruch gerechtfertigt ist, ist die Verarbeitung dieser Daten zu beenden.

55. Personen haben auch das Recht, „nicht einer Entscheidung unterworfen zu werden, die für sie rechtliche Folgen nach sich zieht oder sie erheblich beeinträchtigt und die ausschließlich aufgrund einer automatisierten Verarbeitung von Daten zum Zwecke der Bewertung einzelner Aspekte ihrer Person ergeht, wie beispielsweise ihrer beruflichen Leistungsfähigkeit, ihrer Kreditwürdigkeit, ihrer Zuverlässigkeit usw."[69]

---

[64] Artikel 41, 47 und 48 der Charta der Grundrechte. Das Recht einer Person („betroffene Person") auf Zugang zu den sie betreffenden erhobenen Daten ist in Artikel 8 Absatz 2 der Charta festgelegt. Dieses Recht wird in Artikel 12 Buchstabe a der Richtlinie 95/46/EG, in Artikel 13 der Verordnung Nr. 45/2001 und in Artikel 17 des Rahmenbeschlusses 2008/977JI weiter dargelegt. Artikel 13 der Verordnung Nr. 45/2001 legt Folgendes fest: „Die betroffene Person hat das Recht, jederzeit frei und ungehindert innerhalb von drei Monaten nach Eingang eines entsprechenden Antrags unentgeltlich von dem für die Verarbeitung Verantwortlichen folgende Auskünfte zu erhalten: (…)". Der EuGH hat für Recht erkannt, dass das Auskunftsrecht „zwingend für die Vergangenheit gelten muss. Denn andernfalls wäre die betroffene Person weder in der Lage, wirksam ihr Recht auf Veranlassung der Berichtigung, Löschung oder Sperrung von Daten wahrzunehmen, die ihrer Ansicht nach unbefugt verarbeitet wurden oder falsch sind, noch, einen gerichtlichen Rechtsbehelf einzulegen und Schadensersatz zu erlangen." Rechtssache C-553/07, *College van burgemeester en wethouders van Rotterdam gegen M.E.E. Rijkeboer*, Urteil des EuGH vom 7. Mai 2009, Rdnr. 54.

[65] Artikel 12 Buchstabe b der Richtlinie 95/46/EG, Artikel 14 bis 16 der Verordnung Nr. 45/2001 und Artikel 17 des Rahmenbeschlusses 2008/977JI.

[66] Rechtssache C-131/12, *Google Spain*, Rdnr. 92. Artikel 6 Absatz 1 Buchstabe c bis e der Richtlinie 95/46/EG und Artikel 4 Absatz 1 Buchstabe c bis e verlangen, dass der für die Verarbeitung der Daten Verantwortliche die Qualität der verarbeiteten Daten ungeachtet der Handlungen der betroffenen Personen sicherstellt.

[67] Artikel 12 Buchstabe c der Richtlinie 95/46/EG,

[68] Artikel 14 der Richtlinie 95/46/EG und Artikel 18 der Verordnung Nr. 45/2001.

[69] Artikel 15 der Richtlinie 95/46/EG, Artikel 19 der Verordnung Nr. 45/2001 und Artikel 7 des Rahmenbeschlusses 2008/977/JI. Eine Ausnahme zu diesem Recht liegt vor, wenn die Entscheidung a) im Rahmen des Abschlusses oder der Erfüllung eines Vertrags getroffen und dem Ersuchen der betroffenen Person auf Abschluss oder Erfüllung des Vertrags stattgegeben wurde oder die Wahrung ihrer berechtigten Interessen durch geeignete Maßnahmen wie beispielsweise die Möglichkeit, ihren Standpunkt geltend zu machen, garantiert wird oder b) durch ein Gesetz zugelassen ist, das Garantien zur Wahrung der berechtigten Interessen der betroffenen Personen festlegt.

d) Einschränkungen der Rechte betroffener Personen

56. Eine Einschränkung der Rechte betroffener Personen kann durch Ziele allgemeinen Interesses gerechtfertigt sein, einschließlich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen, eines wichtigen wirtschaftlichen oder finanziellen Interesse eines Mitgliedstaats oder der EU einschließlich Währungs-, Haushalts- und Steuerangelegenheiten sowie Kontroll-, Überwachungs- und Ordnungsaufgaben, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt verbunden sind.[70] Falls die Rechte eingeschränkt sind, muss die Maßnahme möglicherweise zusätzliche Garantien vorsehen, z. B. die Zeiträume und Umstände, in denen die Einschränkung anwendbar wäre.[71]

57. Derartige Einschränkungen müssen Ausnahmen bleiben und die in Artikel 52 Absatz 1 der Charta festgelegten Bedingungen erfüllen. Sobald sie nicht mehr notwendig ist, darf die die Rechte einschränkende Maßnahme nicht mehr angewandt werden. In Bezug auf die vorgeschlagene Änderung der Geldwäscherichtlinie hat der EDSB empfohlen, dass die Maßnahme eine Frist festlegt, nach deren Ablauf die Einschränkung des Auskunftsrechts nicht länger anwendbar wäre, und dass diese Einschränkung nicht auf die Fälle anwendbar sein sollte, die in der Folge als unbegründet oder irrelevant betrachtet werden.[72]

Empfehlung

58. Maßnahmen, die angesichts dieser analytischen Schritte als besonders eingreifend erscheinen, sollten bei der Bereitstellung von Garantien, dass Personen, deren personenbezogene Daten verarbeitet werden, ihre Rechte ausüben können, so explizit wie möglich sein. Jede Einschränkung dieser Rechte sind in der Maßnahme ausdrücklich vorzusehen und zu rechtfertigen und in Übereinstimmung mit Artikel 52 Absatz 1 der Charta zeitlich befristet sein.

9) Erwägung angemessener Datensicherheitsmaßnahmen

59. Die Regulierung von Finanzdienstleistungen stützt sich auf große Datenbanken und komplexe IT-Systeme, die von Finanzinstituten oder Aufsichtsbehörden betrieben werden. Die EU-Datenschutzbestimmungen verlangen von den für die Verarbeitung Verantwortlichen die Umsetzung angemessener technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten vor versehentlicher oder unrechtmäßiger Beschädigung oder zufälligem Verlust, Änderung, unbefugter Offenlegung oder unbefugtem Zugriff, insbesondere dann, wenn die Verarbeitung die Übermittlung von Daten über ein Netzwerk beinhaltet, und vor allen anderen unrechtmäßigen Formen der Verarbeitung. Dies bedeutet, dass der für die Verarbeitung Verantwortliche Sicherheitsrisiken erkennen, auswerten, priorisieren

[70] Artikel 13 der Richtlinie 95/46/EG und Artikel 20 der Verordnung Nr. 45/2001.

[71] Gemäß Artikel 20 der Verordnung Nr. 45/2001 ist die betroffene Person über die wesentlichen Gründe für diese Einschränkung und darüber zu unterrichten, dass sie das Recht hat, sich an den EDSB zu wenden. Die betroffene Person hat ebenfalls das Recht auf indirekten Zugang zu ihren Daten über Vermittlung des EDSB, der sie darüber informiert, ob die Daten richtig verarbeitet wurden und, falls dies nicht der Fall ist, ob alle erforderlichen Berichtigungen vorgenommen wurden. Siehe EDSB-Leitlinien zu den Rechten betroffener Personen im Hinblick auf die Verarbeitung personenbezogener Daten, 25. Februar 2014, S. 26-34. Beispiel siehe Stellungnahme des EDSB zu Geldwäsche, S.15-16.

[72] Siehe Stellungnahme des EDSB zu Geldwäsche, S.15-16.

und wie für die konkrete Verarbeitung angemessen behandeln muss. Insbesondere die Verarbeitung sensibler Daten erfordert ein höheres Sicherheitsniveau.

60. Angemessene technische und organisatorische Maßnahmen für die Bewältigung der erkannten Risiken können zu Funktionen führen, die die Gesamtübereinstimmung der Maßnahme mit den Datenschutzbestimmungen unterstützen. Sie könnten das Recht auf Auskunft, Überprüfung und Sicherung der Datenqualität erleichtern und für Protokollaufzeichnungen für die Datenauskunft, Übertragungen und Änderung und Eliminierung von Daten nach der Aufbewahrungsfrist sorgen. Die konkreten Maßnahmen könnten Folgendes umfassen:

    - Verschlüsselung, für Vertraulichkeit und Integrität der Daten;
    - sichere Verbindungen und Maßnahmen zur Festlegung und zum Schutz logischer Sicherheitsbereiche wie Firewalls, Systeme zur Verhinderung und Erkennung von unberechtigten Zugriffen;
    - Verhinderung des unbefugten physischen Zugangs zur IT-Infrastruktur und zu gesicherten Räumlichkeiten;
    - Autorisierungs- und Authentifizierungsverfahren für IT-Systeme;
    - Mitarbeiter-Screening und Aufgabenabgrenzung; und
    - organisatorische Maßnahmen zur Sicherstellung angemessener Reaktionen auf Sicherheitszwischenfälle, insbesondere die Verletzung in Bezug auf personenbezogene Daten.[73]

61. Die vorgeschlagene Datenschutz-Grundverordnung der Kommission fördert die Konzepte *Privacy by design*, wobei Datenschutz und Privatsphäre ab der Konzeptionsphase und während ihrer gesamten Nutzungsdauer in neue Produkte, Dienstleistungen und Verfahren integriert sind, und *Privacy by default*, wobei die Standardeinstellungen eines Systems die Privatsphäre schützen. Der EDSB kann praktische Beratung zur Verfügung stellen, wie diese Konzepte in entsprechende „Stufe 2"-Standards[74] für Datenverarbeitung in Datenbanken, Frühwarnsystemen und anderen IT-Systemen zu integrieren sind.

Empfehlung

62. Maßnahmen, die eine Datenverarbeitung durch große IT-Systeme beinhalten, sollten auf einer sorgfältigen Beurteilung ihrer Notwendigkeit basieren. Sie sollten angemessene technische und organisatorische Garantien zum Schutz personenbezogener und häufig sensibler Daten und die Rücksprache mit dem EDSB

[73] Gemäß Artikel 4 Absatz 3 der ePrivacy-Richtlinie 2002/58/EG müssen Betreiber von öffentlich zugänglichen elektronischen Kommunikationsdiensten spezifische Vertraulichkeits- und Sicherheitsanforderungen einführen Sie müssen außerdem Datenschutzverletzungen melden, und in der Datenschutz-Grundverordnung ist eine derartige Pflicht für alle für die Verarbeitung Verantwortlichen vorgesehen. Diese Anforderungen können auch im Rahmen von bestimmten sektoralen Instrumenten oder des allgemeinem Zivilrechts in Bezug auf Haftung erforderlich sein und gelten allgemein als bewährt.

[74] Stufe 2 des vierstufigen „Lamfalussy-Verfahrens" für den EU-Gesetzgebungsprozess in Bezug auf Finanzdienstleitungen bezieht sich Durchführungsrechtsakte, die von der Kommission auf der Grundlage von Entwürfen bzw. Empfehlungen der europäischen Finanzaufsichtsbehörden verabschiedet wurden. Siehe http://ec.europa.eu/internal_market/securities/lamfalussy/index_en.htm (Abruf vom 16.11.2014).

in Bezug auf die Entwicklung technischer Standards durch delegierte Rechtsakte und Durchführungsrechtsakte vorsehen.

10) Einführung besonderer Verfahren für die Beaufsichtigung der Datenverarbeitung

63. Die Verarbeitung personenbezogener Daten wird von nationalen Datenschutzbehörden beaufsichtigt und in Bezug auf die Organe und Einrichtungen der EU wie z. B. die europäischen Finanzaufsichtsbehörden, vom EDSB.[75] Gemäß Verordnung (EG) Nr. 1060/2009 über Ratingagenturen z.B. wird, wenn zuständige Behörden Informationen mit der Europäischen Wertpapier- und Marktaufsichtsbehörde (ESMA) austauschen, die Verarbeitung durch nationale zuständige Behörden auf nationaler Ebene von den Datenschutzbehörden beaufsichtigt, wohingegen die Verarbeitung durch die ESMA der Aufsicht des EDSB unterliegt. Die für die Verarbeitung Verantwortlichen müssen die zuständige Datenschutzbehörde über jede Verarbeitung informieren, die besondere Risiken für die Rechte und Freiheiten von betroffenen Personen beinhalten kann, bevor mit der Verarbeitung begonnen wird.[76] Risikobehaftete Verarbeitungen, die wahrscheinlich eine solche „Vorabkontrolle" durch den EDSB erfordern[77], sind unter anderem:

    a) Verarbeitungen von Daten, die Verdächtigungen, Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßregeln betreffen, wie z. B. in Verfahren zur Meldung mutmaßlicher Missstände;

    b) Verarbeitungen, die dazu bestimmt sind, die Persönlichkeit der betroffenen Person zu bewerten, einschließlich ihrer Kompetenz, ihrer Leistung und ihres Verhaltens; und

    c) Verarbeitungen, die darauf abzielen, Personen von einem Recht, einer Leistung oder einem Vertrag auszuschließen, zum Beispiel bei der Bewertung der Kreditwürdigkeit von Verbrauchern.[78]

Empfehlung

64. Maßnahmen, die Tätigkeiten vorsehen, die besondere Risiken für die Rechte von Personen beinhalten, sollten die Verfahren für die Benachrichtigung der zuständigen Datenschutzbehörden angeben und Vorabkontrollen der Verarbeitung personenbezogener Daten anstreben.

4. Anwendung der Methode auf Maßnahmen im Bereich der Regulierung von Finanzdienstleistungen

Dieser Abschnitt wendet zur Veranschaulichung die oben beschriebene 10-Schritte-Methode auf drei typische Bestimmungen mit Folgen für das Recht auf Privatsphäre und auf den Schutz personenbezogener Daten an, die in vor Kurzem verabschiedeten Instrumenten im Bereich der Regulierung von Finanzdienstleistungen enthalten sind:

a. Transparenz und Veröffentlichung von Sanktionen;

b. Verfahren zur Meldung mutmaßlicher Missstände; und

[75] Artikel 28 der Richtlinie 95/46/EG und Artikel 41 der Verordnung Nr. 45/2001.
[76] Artikel 20 der Richtlinie 95/46/EG und Artikel 27 der Verordnung Nr. 45/2001.
[77] Artikel 27 Absatz 2 der Verordnung Nr. 45/2001.
[78] Siehe Stellungnahme des EDSB zu Wohnimmobilienkreditverträgen vom 25. Juli 2011.

c. Aufzeichnung von Telekommunikation und Befugnisse zur Anforderung von Telefon- und Verkehrsdaten.

Transparenzmaßnahmen und Veröffentlichung von Sanktionen

Schritt 1: Identifizierung der zu verarbeitenden personenbezogenen Daten

Eine Reihe von Maßnahmen, wie zum Beispiel die Richtlinie 2014/65/EU über Märkte für Finanzinstrumente und die Richtlinie 2013/36/EU über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen, sehen die Veröffentlichung von Sanktionen aufgrund von Verstößen gegen die Finanzdienstleistungsbestimmungen einschließlich der Identifikation der für den Verstoß verantwortlichen Person vor. Die Überwachung der Tätigkeiten von Unternehmen zur Sicherstellung der Integrität des Marktes setzt wahrscheinlich auch Berichtspflichten voraus. Unternehmen müssen möglicherweise personenbezogene Daten über deren Mitarbeiter bzw. über deren Kunden offenlegen.

Schritt 2: Beurteilung, ob die Datenverarbeitung in das Recht auf Privatsphäre eingreift

Die Veröffentlichung von Namen von Personen, die verurteilt wurden, weil sie gegen Bestimmungen verstoßen haben, stellt einen Eingriff in ihr Recht auf Privatsphäre dar. Es gibt mehrere Möglichkeiten, diesen Eingriff zu minimieren:

a) Die Veröffentlichung sollte nicht automatisch erfolgen und vermieden werden, falls der Zweck durch weniger eingreifende Mittel erfüllt werden kann. Die Behörde sollte in der Lage sein, ihr Ermessen von Fall zu Fall anzuwenden und weniger ernsthafte Verstöße nicht zu veröffentlichen, wenn der Verstoß nicht zu erheblichem Schaden geführt hat oder wenn sich die Partei kooperativ zeigt. Eine Veröffentlichung sollte durch die Schwere des Verstoßes und des durch Dritte erlittenen Schadens, den Grad der persönlichen Verantwortung und Rückfälligkeit sowie weitere besondere Umstände gerechtfertigt sein.[79]

b) Eine Veröffentlichung sollte verschoben werden, bis die letzte Instanz eines Gerichtsverfahrens durchlaufen worden ist, und niemals in Situationen erfolgen, in denen die Entscheidung angefochten werden kann und in denen er letztendlich durch ein Gericht aufgehoben wird.[80]

c) Vor der Veröffentlichung der Entscheidung sollte das betreffende Unternehmen aufgefordert werden, anzugeben, welche Daten als vertraulich angesehen und daher nicht veröffentlicht werden sollten.

d) Die Namen natürlicher Personen (Mitarbeiter oder sonstige Personen) sollten aus den veröffentlichten Beschlüssen gelöscht werden und die Funktionen von Personen, auf die in diesen Beschlüssen oder sonstigen Dokumenten Bezug genommen wird, sollten geprüft und durch allgemeinere Angaben (z. B. „Geschäftsführer“) ersetzt werden.

[79] Stellungnahme des EDSB zu Insider-Geschäften und Marktmanipulation vom 10. Februar 2012, Ziffer 45; Stellungnahme des EDSB zur Tätigkeit von Kreditinstituten und Beaufsichtigung vom 10. Februar 2012, Ziffer 21; Stellungnahme des EDSB zu Ratingagenturen vom 10. Februar 2012, Ziffer 47.
[80] Stellungnahme des EDSB zu Vorschlägen über Märkte für Finanzinstrumente, Ziffer 61.

Schritt 3: Festlegung des Zwecks für die Datenverarbeitung

Transparenz soll dabei helfen, zukünftige Verstöße zu verhindern und Marktbetreiber über bestimmte Verstöße zu informieren. Obwohl Transparenz das Recht auf Privatsphäre beeinträchtigt und die vom EuGH festgelegten Anforderungen erfüllen muss,[81] kann sie ein legitimes Ziel darstellen, unter der Bedingung, dass Vertraulichkeitsanforderungen erfüllt werden.

Schritt 4: Festlegung einer Rechtsgrundlage für die Datenverarbeitung

Eine angemessene Rechtsgrundlage für die Veröffentlichung wäre die Durchführung einer Aufgabe im öffentlichen Interesse oder die Einhaltung einer dem für die Verarbeitung Verantwortlichen auferlegten gesetzlichen Verpflichtung anstelle der Einwilligung der betroffenen Person.

Schritt 5: Beurteilung und Rechtfertigung einer angemessenen Aufbewahrungsfrist

Personenbezogene Daten sollten von dem Unternehmen bzw. der Aufsichtsbehörde nur so lange wie nötig aufbewahrt werden und anonymisiert werden, sobald personenbezogene Daten für die Anwendung der jeweiligen EU-Verordnung nicht mehr relevant sind. Da die Veröffentlichung in den meisten Fällen im Internet erfolgt, sollte von den Mitgliedstaaten verlangt werden, dafür zu sorgen, dass personenbezogene Daten nur über einen angemessenen Zeitraum online aufbewahrt und dann systematisch gelöscht werden.[82]

Schritt 6: Feststellung, welche Parteien innerhalb der EU Zugriff auf die personenbezogenen Daten haben

Personen sollten nur dann auf personenbezogene Daten zugreifen können, wenn sie diese notwendigerweise kennen müssen, und dürfen diese Daten nur auf Anweisung des für die Verarbeitung Verantwortlichen verarbeiten.

Es müssen angemessene technische und organisatorische Maßnahmen eingeführt werden, um Daten gegen versehentliche oder unrechtmäßige Beschädigung, zufälligen Verlust, Änderung und unrechtmäßige Offenlegung zu schützen, zum Beispiel durch Aufklärung der Mitarbeiter. Wenn ein Zugriff auf Anforderung durch Dritte wie zum Beispiel Strafvollzugsbehörden vorgesehen ist, muss klar sein, von welchen Behörden und zu welchen Zwecken die personenbezogenen Daten weiterverarbeitet werden dürfen.

Schritt 7: Festlegung einer korrekten Rechtsgrundlage für die Übermittlung personenbezogener Daten außerhalb der EU

Die Zusammenarbeit zwischen zuständigen Behörden in der EU und Behörden in Drittländern beinhaltet typischerweise den Austausch von Informationen über grenzüberschreitenden Handel und über Mutterunternehmen in einem Staat, die ein Tochterunternehmen in einem anderen Staat haben.

Falls dieser Austausch eine Übermittlung personenbezogener Daten in ein Drittland bedeutet, dass nach Ansicht der Kommission kein angemessenes Schutzniveau aufweist, so könnte ein im nationalen Recht festgeschriebener wichtiger Grund des öffentlichen Interesses

[81] Stellungnahme des EDSB zu Vorschlägen über Märkte für Finanzinstrumente**,** Ziffer 51; Verbundene Rechtssachen C-92/09 und C-93/09, *Schecke*, Rdnrn. 56-64.

[82] Stellungnahme des EDSB zu Insider-Geschäften und Marktmanipulation, Ziffern 49-50*;* Stellungnahme des EDSB zu Vorschlägen über Märkte für Finanzinstrumente, Ziffer 64.

angemessen sein. Übermittlungen sollten nicht automatisch erfolgen, sondern auf einer fallweisen Einschätzung ihrer Notwendigkeit und Verhältnismäßigkeit basieren. Auf jede weitere Übermittlung an ein anderes Drittland sind Bedingungen anzuwenden, wie beispielsweise das Verlangen der ausdrücklichen schriftlichen Genehmigung der Behörde des Mitgliedstaats.[83]

Schritt 8: Bereitstellung angemessener Garantien für die Datenschutzrechte von Personen

Zuständige Behörden sollten bei der Information von betroffenen Personen vor der Veröffentlichung von Entscheidungen über Sanktionen proaktiv vorgehen und deren Recht auf Widerspruch aus überzeugenden rechtmäßigen Gründen wahren.[84]

Schritt 9: Erwägung angemessener Datensicherheitsmaßnahmen

Maßnahmen, die auf die Erhöhung der Transparenz abzielen, sollten vorsehen, dass die Mitarbeiter zuständiger Behörden die berufliche Schweigepflicht einhalten, und sollten die Offenlegung vertraulicher Informationen verbieten.[85]

Verfahren zur Meldung mutmaßlicher Missstände

Schritt 1: Identifizierung der zu verarbeitenden personenbezogenen Daten

Verfahren für die Meldung von Verstößen oder mutmaßlichen Missständen haben Auswirkungen auf den Schutz der personenbezogenen Daten des Informanten und der des Fehlverhaltens beschuldigten Person.[86] Für Verfahren zur Meldung mutmaßlicher Missstände verantwortliche Personen sollten sorgfältig beurteilen, ob es verhältnismäßig und angemessen ist, die Anzahl der zur Meldung von mutmaßlichem Fehlverfahren berechtigten Personen, die Kategorien von Personen, die beschuldigt werden können und die Verstöße, denen sie beschuldigt werden können, zu begrenzen.

Schritt 2: Beurteilung, ob die Datenverarbeitung in das Recht auf Privatsphäre eingreift

Die Geheimhaltung der Identität von Informanten sollte in allen Stufen des Verfahrens gewahrt werden, es sei denn, deren Offenlegung wird durch nationales Recht im Zusammenhang mit weiteren Ermittlungen oder anschließenden Gerichtsverfahren verlangt.[87]

---

[83] Stellungnahme des EDSB zu den Vorschlägen für eine Richtlinie über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen, Ziffern 14-16. Ein Beispiel dieser Bestimmung findet sich in Artikel 29 der Marktmissbrauchsverordnung.

[84] Artikel 14 der Richtlinie 95/46/EG. Stellungnahme des EDSB zu Vorschlägen über Märkte für Finanzinstrumente, Ziffer 62*;* Stellungnahme des EDSB zu Insider-Geschäften und Marktmanipulation, Ziffer 48.

[85] Stellungnahme des EDSB zu den Vorschlägen für eine Richtlinie über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen, Ziffern 17 und 18.

[86] Stellungnahme der Artikel-29-Datenschutzgruppe 1/2006 zur Anwendung der EU-Datenschutzvorschriften auf interne Verfahren zur Meldung mutmaßlicher Missstände in den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität.

[87] Stellungnahme des EDSB zu Vorschlägen über Märkte für Finanzinstrumente**,** Ziffer 67**;** Stellungnahme des EDSB zu Vorschlägen der Kommission über Insider-Geschäfte und Marktmanipulation**,** Ziffer 54.; EDSB-Leitlinien zu den Rechten betroffener Personen im Hinblick auf die Verarbeitung personenbezogener Daten, S. 32

Schritt 5: Beurteilung und Rechtfertigung einer angemessenen Aufbewahrungsfrist

Aufbewahrungsfristen für personenbezogene Daten, die im Rahmen der Ermittlung in einem Bericht zusammengestellt werden, sind auf ein Minimum zu reduzieren. Es sollte im Grunde nicht nötig sein, Daten länger als zwei Monate nach Abschluss der Ermittlung aufzubewahren, es sei denn, es werden ein Gerichtsverfahren oder Disziplinarmaßnahmen gegen die beschuldigte Person oder, im Fall falscher oder verleumderischer Erklärungen, gegen den Informanten eingeleitet.

Schritt 8: Bereitstellung angemessener Garantien für die Datenschutzrechte von Personen

Des Fehlverhaltens beschuldigte Personen müssen ihr Recht auf Verteidigung, das Recht, vor einer sie betreffenden Entscheidung angehört zu werden, und das Recht auf wirksamen Rechtsbehelf gegen eine sie betreffende Entscheidung oder eine sie betreffende Maßnahme ausüben können.[88] Informanten sollten ermutigt werden, gekennzeichnete und vertrauliche Berichte anstelle von anonymen Berichten einzureichen, und die für das Verfahren verantwortlichen Personen sollten die Identität von Informanten offenlegen, wenn sich die Anschuldigung als böswillig herausgestellt hat.[89]

Schritt 10: Einführung besonderer Verfahren für die Beaufsichtigung der Datenverarbeitung

Jedes Verfahren zur Meldung mutmaßlicher Missstände bedeutet die Verarbeitung personenbezogener Daten in Bezug auf mutmaßliche Straftaten und birgt als solches bestimmte Risiken sowohl für die Personen, die das mutmaßliche Fehlverhalten melden, als auch für die Beschuldigten. Das Verfahren sollte daher der zuständigen Datenschutzbehörde zur Vorabkontrolle vorgelegt werden.

Aufzeichnung von Telekommunikation und Befugnisse zur Anforderung von Telefon- und Verkehrsdaten

Schritt 1: Identifizierung der zu verarbeitenden personenbezogenen Daten

Die Datenkategorien in Bezug auf zu verarbeitende Kommunikationen sind klar festzulegen.[90] „Verkehrsdaten“ werden im EU-Recht definiert als „Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein elektronisches Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden“.[91] Diese Daten umfassen typischerweise personenbezogene Daten einschließlich der Identität von Personen, die den Anruf tätigen und empfangen, Zeitpunkt und Dauer des Anrufs, das benutzte Netz und, im Fall tragbarer Geräte, den geografischen Standort des Nutzers. Einige auf die Nutzung von Internet und E-Mail bezogene Verkehrsdaten, wie beispielsweise die Liste besuchter Websites, können darüber hinaus wichtige Einzelheiten über den Inhalt der Kommunikation offenlegen.[92] Bei der Bezugnahme auf Kommunikationsdaten sollte deutlich zwischen „Verkehrsdaten“ und Informationen über den Inhalt der Kommunikation (das „Gespräch“) unterschieden werden.

[88] Stellungnahme des EDSB zu Vorschlägen über Märkte für Finanzinstrumente**,** Ziffer 68.
[89] Siehe EDSB-Leitlinien zu den Rechten betroffener Personen im Hinblick auf die Verarbeitung personenbezogener Daten, S. 32
[90] Stellungnahme des EDSB zu Vorschlägen über Märkte für Finanzinstrumente**,** Ziffer 34.
[91] Richtlinie 2002/58/EG, Artikel 2.
[92] Stellungnahme des EDSB zu Insider-Geschäften und Marktmanipulation, Ziffer 24**.** Stellungnahme des EDSB zu Vorschlägen über Märkte für Finanzinstrumente**,** Ziffer 44**.**

Schritt 2: Beurteilung, ob die Datenverarbeitung in das Recht auf Privatsphäre eingreift

Unternehmen im Finanzdienstleistungssektor zeichnen häufig den Inhalt der die Transaktionen betreffenden Gespräche auf.[93] Selbst dann, wenn die jeweiligen Gespräche sich ganz oder hauptsächlich auf finanzielle Transaktionen oder professionelle Tätigkeiten beziehen, umfassen die Aufzeichnungen dieser Kommunikationen personenbezogene Daten, und der Zugriff auf diese Daten durch zuständige Behörden stellt einen erheblichen Eingriff in das Recht auf Privatsphäre dar. Die Maßnahme sollte den Zugriff auf den Inhalt der Kommunikationen durch die zuständigen Behörden ausdrücklich ausschließen, es sei denn, der Zugriff ist unbedingt erforderlich.[94] Der Zugriff auf Kommunikationsdaten durch die zuständige Behörde sollte eine richterliche Genehmigung im Interesse der harmonisierten Anwendung der EU-Gesetzgebung in allen Mitgliedstaaten erfordern.[95]

Schritt 3: Festlegung des Zwecks für die Datenverarbeitung

Informationen zu telefonischer und elektronischer Kommunikation unter Einbindung von Mitarbeitern eines Unternehmens können bei der Untersuchung von Fehlverhalten oder Verletzungen der Verpflichtungen eines Unternehmens wertvoll sein. Maßnahmen, die den Zugriff auf diese Informationen ermöglichen, sollten den Zweck für diese Verarbeitung in Übereinstimmung mit Artikel 6 Absatz 1 der Datenschutzrichtlinie genau festlegen.[96] Befugnisse zur Anforderung von Verkehrsdaten sollten klar definiert sein und auf Fälle beschränkt werden, in denen es einen begründeten Verdacht gibt, dass diese Aufzeichnungen geeignet sein könnten, einen Nachweis für die Verletzung der Verpflichtungen des Unternehmens zu erbringen.

Schritt 5: Beurteilung und Rechtfertigung einer angemessenen Aufbewahrungsfrist

Die Maßnahme sollte einen angemessenen Höchstzeitraum für die Aufbewahrung von Daten festlegen, der sowohl für Unternehmen als auch für zuständige Behörden gilt, die für die Beaufsichtigung des jeweiligen Finanzmarkts/der jeweiligen Finanztätigkeit verantwortlich sind.[97]

Schritt 8: Bereitstellung angemessener Garantien für die Datenschutzrechte von Personen

Die Maßnahme sollte das Recht des Empfängers vorsehen, die Entscheidung betreffend die Auskunft über Kommunikationsdaten, der durch die zuständige Behörde ergangen ist, gerichtlich prüfen zu lassen.[98] Die Maßnahme sollte sicherstellen, dass die betroffene Person über das Recht zur Berichtigung von die Person betreffenden Daten sowie über das Recht, sich an den EDSB zu wenden, informiert wird.[99]

---

[93] Stellungnahme des EDSB zu Vorschlägen über Märkte für Finanzinstrumente, Ziffer 20.
[94] Stellungnahme des EDSB zu Insider-Geschäften und Marktmanipulation, Ziffern 25, 32 und 34. Stellungnahme des EDSB zu Vorschlägen über Märkte für Finanzinstrumente, Ziffer 32.
[95] Stellungnahme des EDSB zu Insider-Geschäften und Marktmanipulation, Ziffer 27; Stellungnahme des EDSB zu Ratingagenturen, Ziffer 18.
[96] Stellungnahme des EDSB zu Vorschlägen über Märkte für Finanzinstrumente, Ziffer 28.
[97] Stellungnahme des EDSB zu Vorschlägen über Märkte für Finanzinstrumente, Ziffer 38.
[98] Stellungnahme des EDSB zu Insider-Geschäften und Marktmanipulation, Ziffer 28.
[99] Stellungnahme des EDSB zu einer Meldung für eine Vorabkontrolle in Bezug auf die Aufzeichnung, die Speicherung und das Abhören von Telefongesprächen in den Generaldirektionen M und P, Brüssel, 5. Mai 2006 (Fall 2005-376), S.11-13.

5. Zusammenarbeit mit dem EDSB

65. Gemäß Artikel 28 Absatz 2 der Verordnung Nr. 45/2001 muss die Kommission den EDSB konsultieren, wenn sie einen Vorschlag für Rechtsvorschriften bezüglich des Schutzes der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten annimmt.

66. In der Praxis hat der EDSB beim Anbieten von Beratung in allen Phasen der Politikgestaltung und des Gesetzgebungsverfahrens eine proaktive Rolle eingenommen, nicht nur für die Kommission, sondern auch für das Parlament und den Rat.[100] Darüber hinaus wurde nach Gesprächen mit der Kommission vereinbart und in einer Notiz vom Generalsekretär im Dezember 2006 festgelegt, dass die Dienststellen der Kommission vor der Annahme eines Vorschlags mit Bezug auf Datenschutz den EDSB informell konsultieren sollten und dass, wenn die Kommission selbst der Gesetzgeber ist (Richtlinien oder Verordnungen der Kommission, „Komitologie" oder sonstige Beschlüsse, Verhandlungsmandat) oder für nichtlegislative Dokumente, die formelle Rücksprache vor der Annahme des Rechtsaktes durch das Kollegium stattfinden sollte, und zwar unbeschadet einer informellen Rücksprache während der Vorbereitungsphase. Der EDSB wünscht die Fortsetzung und Vertiefung dieser Arbeitsvereinbarungen.

67. Es geschieht immer häufiger, dass Durchführungsrechtsakte und delegierte Rechtsakte von den EU-Finanzaufsichtsbehörden vorbereitet, üblicherweise nach einer öffentlichen Konsultation, und der Kommission vorgelegt werden, die diese Entwürfe dann praktisch nur in einem sehr eingeschränkten Umfang ändern kann. Der EDSB behält sich das Recht vor, diese Entwürfe mittels einer öffentlichen Stellungnahme zu kommentieren; es wäre jedoch in den meisten Fällen angemessener, der Kommission die Anmerkungen direkt vorzulegen, und zwar sowohl formell nach als auch informell vor der Annahme des Dokuments. Die Kommission muss dem EDSB ausreichend Zeit zur Prüfung der Dokumente zur Verfügung stellen, damit dieser eine wertvolle Empfehlungen abgeben kann.

68. Der EDSB würde Rückmeldungen zu diesen Leitlinien begrüßen und beabsichtigt, deren Wirksamkeit und Relevanz spätestens im Jahr 2019 zu überprüfen.

Brüssel, den 26. November 2014

[100] Siehe Ziffer 3.2 des EDSB-Strategiepapiers.

Anhang: Stellungnahmen des EDSB im Zusammenhang der EU-Regulierung von Finanzdienstleistungen

(Über die Erstellung einer Frühwarnsystem-Datenbank) Stellungnahme des EDSB zu dem geänderten Vorschlag für eine Verordnung des Rates zur Änderung der Verordnung (EG, Euratom) Nr. 1605/2002 über die Haushaltsordnung für den Gesamthaushaltsplan der Europäischen Gemeinschaften (KOM(2006)213 endg.); Vorschlag für eine Verordnung (EG, Euratom) der Kommission zur Änderung der Verordnung (EG, Euratom) Nr. 2342/2002 mit Durchführungsbestimmungen zur Verordnung (EG, Euratom) Nr. 1605/2002 des Rates über die Haushaltsordnung für den Gesamthaushaltsplan der Europäischen Gemeinschaften, angenommen am 12. Dezember 2006, ABl. C 94 vom 28.4.2007.

Stellungnahme des EDSB zum Grünbuch der Kommission „Effiziente Vollstreckung gerichtlicher Entscheidungen in der Europäischen Union: Transparenz des Schuldnervermögens“, angenommen am 22. September 2008, ABl. C 20 vom 27.1.2009.

Stellungnahme des EDSB zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Einlagensicherungssysteme (Neufassung), angenommen am 9. September 2010, ABl. C 323 vom 30.11.2010.

Stellungnahme des EDSB zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister, angenommen am 19. April 2011, ABl. C 216/04 vom 22.7.2011.

Stellungnahme des EDSB zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung der technischen Vorschriften für Überweisungen und Lastschriften in Euro und zur Änderung der Verordnung (EG) Nr. 924/2009, angenommen am 23. Juni 2011, ABl. C 284/01 vom 28.9.2011.

(Zu Beratung über nationale Kreditdatenbanken zur Bewertung der Kreditwürdigkeit von Verbrauchern) Stellungnahme des EDSB zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Wohnimmobilienkreditverträge, angenommen am 25. Juli 2011, ABl. C 377/02 vom 23.12.2011.

Stellungnahme des EDSB zu einem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Einführung eines Europäischen Beschlusses zur vorläufigen Kontenpfändung im Hinblick auf die Erleichterung der grenzüberschreitenden Eintreibung von Forderungen in Zivil- und Handelssachen, angenommen am 13. Oktober 2011, ABl. C 373/03 vom 21.12.2011.

Stellungnahme des EDSB zu den Vorschlägen der Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über Märkte für Finanzinstrumente zur Aufhebung der Richtlinie 2004/39/EG des Europäischen Parlaments und des Rates und für eine Verordnung des Europäischen Parlaments und des Rates über Märkte für Finanzinstrumente und zur Änderung der Verordnung über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister, angenommen am 10. Februar 2012, ABl. C 147 vom 25.5.2012.

Stellungnahme des EDSB zu den Vorschlägen der Kommission für eine Verordnung des Europäischen Parlaments und des Rates über Insider-Geschäfte und Marktmanipulation und für eine Richtlinie des Europäischen Parlaments und des Rates über strafrechtliche Sanktionen für Insider-Geschäfte und Marktmanipulation, angenommen am 10. Februar 2012, ABl. C 177 vom 20.6.2012.

Stellungnahme des EDSB zu den Vorschlägen der Kommission für eine Richtlinie über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen sowie für eine Verordnung über Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen, angenommen am 10. Februar 2012, ABl. C 175 vom 19.6.2012.

Stellungnahme des EDSB zum Vorschlag der Kommission für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EG) Nr. 1060/2009 über Ratingagenturen, angenommen am 10. Februar 2012, ABl. C 139/02 vom 15.5.2012.

Stellungnahme des EDSB zu den Vorschlägen für eine Verordnung über Europäische Risikokapitalfonds und für eine Verordnung über Europäische Fonds für soziales Unternehmertum, angenommen am 14. Juni 2012, ABl. C 335 vom 1.11.2012.

Stellungnahme des EDSB über einen Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und Finanzierung des Terrorismus, und über einen Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Übermittlung von Angaben zum Auftraggeber bei Geldtransfers, angenommen am 4. Juli 2013, ABl. C 32 vom 4.2.2014.

Stellungnahme des EDSB zum Vorschlag der Kommission für eine Verordnung des Europäischen Parlaments und des Rates zur Verbesserung der Wertpapierabrechnungen in der Europäischen Union und über Zentralverwahrer (CSDs) sowie zur Änderung der Richtlinie 98/26/EG, angenommen am 9. Juli 2012, ABl. C 336 vom 6.11.2012.

Stellungnahme des EDSB zu einem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2006/48/EG und 2009/110/EG sowie zur Aufhebung der Richtlinie 2007/64/EG, und für eine Verordnung des Europäischen Parlaments und des Rates über Interbankenentgelte für kartengebundene Zahlungsvorgänge, angenommen am 5. Dezember 2013, ABl. C 38 vom 8.2.2014.