Stellungnahme des Europäischen Datenschutzbeauftragten

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

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE -

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,

gestützt auf die Charta der Grundrechte der Europäischen Union, insbesondere auf Artikel 7 und 8,

gestützt auf die 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[1],

gestützt auf die 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 Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr[2], insbesondere auf Artikel 28 Absatz 2,

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. EINLEITUNG

1.1. Konsultation des EDSB

1. Am 27. Juli 2013 nahm die Kommission einen Entwurf 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 („vorgeschlagene Richtlinie“), und einen Entwurf für eine Verordnung des Europäischen Parlaments und des Rates über Interbankenentgelte für kartengebundene Zahlungsvorgänge an.[3] Diese Vorschläge wurden dem EDSB am 28. Juli 2013 zur Konsultation übermittelt.

[1] ABl. L 281 vom 23.11.1995, S. 31.
[2] ABl. L 8 vom 12.1.2001, S. 1.
[3] COM(2013) 547 final und COM(2013) 550 final.

Postanschrift: Rue Wiertz 60 - 1047 Brüssel, Belgien
Dienststelle: Rue Montoyer 30
E-Mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: +32 (0)2 283 19 00 – Fax: +32 (0)2 283 19 50

2. Der EDSB begrüßt die Tatsache, dass er von der Kommission konsultiert wird und ein Verweis auf die vorliegende Stellungnahme in die Präambeln der Rechtsinstrumente aufgenommen wird.

3. Vor der Annahme des Verordnungsvorschlags hatte der EDSB Gelegenheit, der Kommission gegenüber informelle Kommentare abzugeben. Einige dieser Kommentare wurden berücksichtigt. Im Ergebnis wurden die Datenschutzgarantien in dem Verordnungsvorschlag gestärkt.

4. Da die vorgeschlagene Verordnung aus der Perspektive des Datenschutzes keine Probleme aufwirft, konzentriert sich der EDSB in seinen Ausführungen auf die vorgeschlagene Richtlinie.

1.2. Ziele und Anwendungsbereich der vorgeschlagenen Richtlinie

5. Ziel der vorgeschlagenen Richtlinie ist es, die Entwicklung eines EU-weiten Marktes für elektronische Zahlungen weiter voranzubringen, der es Verbrauchern, Einzelhändlern und anderen Marktakteuren ermöglicht, im Einklang mit „Europa 2020“ und der „Digitalen Agenda“ die Vorteile des EU-Binnenmarkts in vollem Umfang zu nutzen. Um die angestrebten Ziele zu erreichen und Wettbewerb, Effizienz und Innovation im elektronischen Zahlungsverkehr zu fördern, sollten nach Auffassung der Kommission Rechtsklarheit und gleiche Wettbewerbsbedingungen gegeben sein, was zu einer Abwärtskonvergenz der Kosten und Preise für Zahlungsdienstnutzer sowie zu einer größeren Auswahl und mehr Transparenz bei Zahlungsdiensten führen, die Erbringung innovativer Zahlungsdienste erleichtern und die Sicherheit von Zahlungsdiensten gewährleisten dürfte.

6. Nach Meinung der Kommission lassen sich diese Ziele durch eine Aktualisierung und Ergänzung des bestehenden Rechtsrahmens für Zahlungsdienste, und zwar durch die Einführung von Vorschriften, die Transparenz, Innovation und Sicherheit bei Massenzahlungen fördern, sowie durch eine Verbesserung der Kohärenz zwischen den nationalen Vorschriften erreichen, wobei vor allem den legitimen Bedürfnissen der Verbraucher Rechnung getragen werden sollte.

2. SPEZIFISCHE ANMERKUNGEN ZUR VORGESCHLAGENEN RICHTLINIE

2.1. Allgemeiner Verweis auf das Datenschutzrecht

7. Der EDSB hält fest, dass die Bereitstellung von Zahlungsdiensten die Verarbeitung personenbezogener Daten durch verschiedene Akteure erforderlich macht: Namen, Kontonummern und Inhalte von Verträgen müssen zwischen Zahlern und Zahlungsempfängern sowie über ihre jeweiligen Zahlungsdienstanbieter ausgetauscht werden, damit die Transfers reibungslos ablaufen können.

8. Der EDSB begrüßt die Bestimmung in Artikel 84, der zufolge die Verarbeitung personenbezogener Daten für die Zwecke der vorgeschlagenen Richtlinie im Einklang mit den einzelstaatlichen Vorschriften zur Umsetzung der Richtlinie 95/46/EG und der Richtlinie 2002/58/EG sowie der Verordnung (EG) Nr. 45/2001 zu erfolgen hat.

9. Der EDSB erinnert jedoch daran, dass eine eindeutige Benennung der anzuwenden Datenschutzvorschriften zwar wesentlich, aber nicht ausreichend ist. Die Verweise auf das anzuwendende Datenschutzrecht sollten ihren Niederschlag in konkreten Garantien finden, die für alle Situationen gelten, in denen die Verarbeitung personenbezogener Daten vorgesehen ist.

10. In seinem Schreiben im Rahmen der von der Kommission abgehaltenen öffentlichen Konsultation zum Grünbuch „Hin zu einem integrierten europäischen Markt für Karten-, Internet- und mobile Zahlungen“[4], unterstrich der EDSB, dass zur vollständigen Einhaltung der EU-Datenschutzvorschriften die Anwendung konkreter Garantien erforderlich ist. Es unterstrich darin insbesondere, dass beim Austausch und bei der Verarbeitung personenbezogener Daten über Zahler und Zahlungsempfänger bei den verschiedenen Zahlungsdienstanbietern die Grundsätze der Notwendigkeit, Verhältnismäßigkeit und Zweckbindung einzuhalten sind und die Daten nicht länger als erforderlich aufbewahrt werden dürfen. Weiter betonte der EDSB die zentrale Rolle der Transparenz als Mittel, mit dem sich gewährleisten lässt, dass natürliche Personen ihre Datenschutzrechte wirksam wahrnehmen können. Der EDSB empfiehlt daher, in den Wortlaut der vorgeschlagenen Richtlinie ausdrücklich konkrete Garantien aufzunehmen, wie nachstehend näher ausgeführt.

2.2. Rechtsgrundlage für die Verarbeitung personenbezogener Daten

11. Bezüglich der Verarbeitung personenbezogener Daten durch Zahlungssysteme und Zahlungsdienstanbieter sollte in der vorgeschlagenen Richtlinie deutlich zum Ausdruck gebracht werden, dass die Bereitstellung von Zahlungsdiensten die Verarbeitung personenbezogener Daten mit sich bringt. Derzeit sieht der Richtlinienvorschlag gemäß Erwägungsgrund 71 die Verarbeitung personenbezogener Daten lediglich im Zusammenhang mit der Prävention, Untersuchung und Aufdeckung von Betrug im Zahlungsverkehr vor, ohne dabei zu berücksichtigen, dass die Erbringung des Zahlungsdienstes selber schon die Verarbeitung personenbezogener Daten implizieren kann. Mit Blick auf die Rechtsgrundlage einer solchen Verarbeitung sollte in der vorgeschlagenen Richtlinie ausdrücklich

[4] Siehe das Schreiben des EDSB vom 11. April 2012 im Zusammenhang mit der von der GD MARKT durchgeführten öffentlichen Konsultation zum Grünbuch „Ein integrierter europäischer Markt für Karten-, Internet- und mobile Zahlungen“, einsehbar unter: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2012/12-04-11_Mobile_Payments_EN.pdf

klargestellt werden, dass die Verarbeitung personenbezogener Daten erfolgen darf, sofern sie für die Erbringung von Zahlungsdiensten erforderlich ist.

12. Was die Verarbeitung personenbezogener Daten zum Zweck der Prävention, Untersuchung und Aufdeckung von Betrug im Zahlungsverkehr angeht, vertritt der EDSB die Ansicht, dass Artikel 84 des Richtlinienvorschlags nicht präzise genug formuliert ist und daher nicht als gültige Rechtsgrundlage für eine solche Verarbeitung angesehen werden kann. Die Bestimmungen zur Betrugsprävention sollten – zumindest in großen Zügen – genauer den Zweck bzw. die Zwecke der Verarbeitung, die betroffenen personenbezogenen Daten und die Modalitäten der Verarbeitung festlegen. Bei der Festlegung dieser Elemente für die Verarbeitung personenbezogener Daten sollte dem Grundsatz der Verhältnismäßigkeit angemessen Rechnung getragen werden (verarbeitet werden dürfen nur die Daten, die für die Zwecke der Verarbeitung erforderlich sind). Der EDSB empfiehlt daher, in den Richtlinienvorschlag eine genauer gefasste Bestimmung aufzunehmen.

2.3. Verhältnismäßigkeit der Verarbeitung

13. Es ist dafür zu sorgen, dass die verschiedenen Beteiligten nur Zugriff auf Daten erhalten, die für die Erbringung ihrer Dienste erforderlich sind, und dass sie nur diese verarbeiten (siehe beispielsweise Erwägungsgrund 26). So sollten beispielsweise Mobilfunkunternehmen, die für die Übertragung des Überweisungsauftrags verantwortlich sind, keinen Zugriff auf Informationen über die Zahlungsmodalitäten erhalten. Dies sollte ausdrücklich in einer Bestimmung des verfügenden Teils der vorgeschlagenen Richtlinie festgelegt werden.

14. Desgleichen sollten die Bestimmungen über den Zugang Dritter (siehe weiter unten Punkt 2.7) in Artikel 58 und 59 der vorgeschlagenen Richtlinie deutlich zum Ausdruck bringen, dass Informationen über die „Verfügbarkeit ausreichender Geldbeträge“ aus einem einfachen „Ja“ oder „Nein“ auf die Frage bestehen sollten, ob ausreichende Geldbeträge verfügbar sind, und nicht beispielsweise aus einem Kontoauszug.
15. Der EDSB unterstreicht die Bedeutung der Anwendung der Grundsätze „Datenschutz durch Technik“ und „Datenschutz durch datenschutzfreundliche Voreinstellungen“ in allen gemäß der vorgeschlagenen Richtlinie entwickelten und eingesetzten Datenverarbeitungssystemen. Diese beiden Konzepte gehen auf die derzeitige Datenschutzrichtlinie 95/46/EG zurück und werden vermutlich im Rahmen der vorgeschlagenen Allgemeinen Datenschutzverordnung rechtlich anerkannt werden (siehe Artikel 23)[5]. Unter „Datenschutz durch Technik“ versteht man die Einbeziehung des Datenschutzes und des Schutzes der Privatsphäre schon in den Entwurf neuer Produkte, Dienstleistungen und Verfahren, die die Verarbeitung personenbezogener Daten implizieren, während „Datenschutz durch datenschutzfreundliche

[5] COM(2012) 11 final.

Voreinstellungen“ bedeutet, dass standardmäßig die datenschutzfreundlichsten Voreinstellungen vorgenommen werden.

16. Beim „Datenschutz durch Technik“ ist unter anderem dafür zu sorgen, dass Datenverarbeitungssysteme so ausgelegt sind, dass möglichst wenige Daten verarbeitet werden (Datenminimierung), dass standardmäßig datenschutzfreundliche Voreinstellungen vorgenommen werden, dass der Zugriff auf Daten einer Person auf das für die Erbringung des Dienstes unbedingt Erforderliche beschränkt wird, und dass Instrumente zum Einsatz kommen, mit denen Nutzer ihre personenbezogenen Daten besser schützen (z. B. Zugriffskontrollen, Verschlüsselung usw.) und ihre Rechte besser ausüben können.

17. Der EDSB hat wiederholt unterstrichen, wie wichtig es ist, schon vor der Annahme der vorgeschlagenen Allgemeinen Datenschutzverordnung diese Konzepte bei der Umsetzung der Digitalen Agenda angemessen zu berücksichtigen[6]. Er empfiehlt daher, in den verfügenden Teil des Richtlinienvorschlags die Verpflichtung aufzunehmen, „Datenschutz durch Technik / Datenschutz durch datenschutzfreundliche Voreinstellungen“ in alle Datenverarbeitungssysteme einzubauen, die im Rahmen der vorgeschlagenen Richtlinie entwickelt und eingesetzt werden.

2.4. Aufsicht durch zuständige Behörden

18. Der EDSB begrüßt, dass gemäß Erwägungsgrund 32 der vorgeschlagenen Richtlinie zuständige Behörden bei der Aufsicht über die Einhaltung der Vorschriften durch die Zahlungsinstitute gehalten sind, ihre Befugnisse „unter Achtung der Grundrechte einschließlich des Rechts auf Privatsphäre“ auszuüben. Der Erwägungsgrund besagt ferner, dass für die Ausübung dieser Befugnisse, die auf schwerwiegende Eingriffe in das Recht auf Achtung des Privat- und Familienlebens, der Wohnung sowie der Kommunikation hinauslaufen können, die Mitgliedstaaten adäquate und wirksame Absicherungen gegen Missbrauch oder Willkür eingerichtet haben sollten, beispielsweise in Fällen der vorherigen Genehmigung der zuständigen Justizbehörde des betreffenden Mitgliedstaats. Der EDSB erinnert daran, dass diese Anforderungen unbeschadet der Kontrolle durch eine unabhängige Behörde (nationale Datenschutzbehörde) gemäß Artikel 8 Absatz 3 der Charta der Grundrechte der Europäischen Union bestehen.

19. Dem EDSB wäre es jedoch lieber, wenn derartige Anforderungen in einer Bestimmung im verfügenden Teil der vorgeschlagenen Richtlinie konkretisiert würden. Er empfiehlt daher, in Artikel 22 zu den Anforderungen an zuständige Behörden hinzuzufügen, dass sie mit

[6] Siehe Stellungnahme des EDSB vom 18. März 2010 zu „Stärkung des Vertrauens in die Informationsgesellschaft durch die Förderung des Schutzes von Daten und Privatsphäre“ und Stellungnahme des EDSB vom 10. April 2013 zur Mitteilung der Kommission „Die Digitale Agenda für Europa – digitale Impulse für das Wachstum in Europa“, abrufbar im Abschnitt Beratung auf der Website des EDSB: www.edps.europa.eu

offiziellem Beschluss Dokumente und Informationen anfordern können, und zwar unter Angabe der Rechtsgrundlage und des Zwecks des Ersuchens sowie der angeforderten Informationen und der Frist, innerhalb derer die Informationen bereitzustellen sind.

2.5. Informationsaustausch

20. Gemäß Artikel 25 der vorgeschlagenen Richtlinie tauschen die zuständigen Behörden Informationen untereinander, mit der Europäischen Zentralbank und den nationalen Zentralbanken der Mitgliedstaaten, der EBA und anderen zuständigen Behörden aus, die nach den auf Zahlungsdienstleister anwendbaren Rechtsvorschriften der Union oder der Mitgliedstaaten benannt worden sind.

21. Gemäß Artikel 26 Absatz 3 stellen die zuständigen Behörden einander alle wesentlichen und/oder zweckdienlichen Informationen zur Verfügung, insbesondere bei Zuwiderhandlungen oder mutmaßlichen Zuwiderhandlungen eines Agenten, einer Zweigniederlassung oder einer Stelle, in die Tätigkeiten ausgelagert werden. Gelegentlich wird es bei diesem Informationsaustausch mit Sicherheit um bestimmte oder bestimmbare natürliche Personen gehen, wie einen Agenten, einen Zahlungsdienstnutzer oder einen Verbraucher.

22. Nach Auffassung des EDSB sind beide Bestimmungen zu vage und bieten daher keine angemessene Rechtsgrundlage für die verlangte Verarbeitung personenbezogener Daten. Mit Blick auf die Zweckbindung fehlt es in der vorgeschlagenen Richtlinie an näheren Angaben zu den Zwecken des Informationsaustauschs und zu der Art der auszutauschenden Daten, einschließlich personenbezogener Daten. Der EDSB hält weiter fest, dass in der vorgeschlagenen Richtlinie keinerlei konkrete Frist für die Aufbewahrung der verarbeiteten personenbezogenen Daten festgelegt ist. Dies dürfte Unsicherheit und unerwünschte Vielfalt in der Umsetzung und/oder Praxis in den Mitgliedstaaten mit sich bringen.

23. In Anbetracht dessen empfiehlt der EDSB, i) die Zwecke zu erwähnen, zu denen personenbezogene Daten von nationalen zuständigen Behörden, der Europäischen Zentralbank, den nationalen Zentralbanken und den anderen in Artikel 25 genannten Behörden verarbeitet werden dürfen; ii) die Art personenbezogener Daten anzugeben, die gemäß der vorgeschlagenen Richtlinie verarbeitet werden dürfen, und iii) einen angemessenen Aufbewahrungszeitraum für die Daten im Rahmen der genannten Verarbeitung (oder zumindest genaue Kriterien für dessen Festsetzung auf nationaler Ebene) festzulegen.

2.6. Transparenz und Auskunftspflicht gegenüber betroffenen Personen

24. Der EDSB nimmt zur Kenntnis, dass mehrere Bestimmungen[7] eine Reihe von Anforderungen für mehr Transparenz gegenüber den Nutzern enthalten. Seiner Auffassung nach sollte das Erfordernis der Transparenz bei Zahlungsdiensten auch die Transparenzpflicht bezüglich der Verarbeitung personenbezogener Daten natürlicher Personen beinhalten. Betroffenen Personen sollte mitgeteilt werden, wer welche Daten zu welchem Zweck verarbeitet, und wie lange und auf welche Weise sie ihre Rechte, einschließlich des Rechts auf Auskunft über ihre Daten und deren Berichtigung oder Löschung, ausüben können.

25. Der EDSB empfiehlt daher, in einer Bestimmung im verfügenden Teil der vorgeschlagenen Richtlinie konkret die Verpflichtung festzuhalten, natürliche Personen im Einklang mit nationalen Vorschriften zur Umsetzung der Artikel 10 und 11 der Richtlinie 95/46/EG und mit Artikel 11 der Verordnung (EG) Nr. 45/2001 angemessen über die Verarbeitung personenbezogener Daten zu informieren.

26. Auch Erwägungsgrund 35 sollte geändert werden und die Bereitstellung aller in der Richtlinie „*sowie in der Richtlinie 95/46/EG und in der Verordnung (EG) Nr. 45/2001*" verlangten Informationen fordern (außerdem sollte das Wort „*nur*" gestrichen werden, da die Informationsanforderungen in der Richtlinie nicht die einzigen sind).

27. Der rechtzeitigen Unterrichtung über die Verarbeitung personenbezogener Daten vor der Anforderung des Zahlungsdienstes kommt umso größere Bedeutung zu, als die Einwilligung des Nutzers eine zentrale Rolle spielen soll und die Autorisierung eines Zahlungsvorgangs nur als erfolgt gilt, wenn der Zahler seine Einwilligung erteilt hat. Bevor der Zahler einer Transaktion zustimmt, sollte er nicht nur über die Berechnungen von Preisen und Entgelten, sondern auch über die Modalitäten der Verarbeitung seiner personenbezogenen Daten informiert sein, damit er eine Entscheidung über die Zahlung in voller Sachkenntnis und in Kenntnis der Folgen für die Verarbeitung seiner personenbezogenen Daten treffen kann.

28. Der EDSB begrüßt, dass die Bestimmungen zur Transparenz klare Vorgaben über die Mittel zur Unterrichtung der Nutzer und zur Tatsache vorsehen, dass diese Informationen jederzeit verfügbar zu sein haben. Er empfiehlt, in den Bestimmungen bezüglich der Transparenz ausdrücklich zu besagen, dass die Modalitäten für die Unterrichtung der Nutzer auch für die Angaben zur Verarbeitung personenbezogener Daten gemäß Artikel 10 und 11 der Richtlinie 95/46/EG gelten.

[7] So z. B. Artikel 37 bis 42, Artikel 44 bis 46, Artikel 49 bis 51 und die Erwägungsgründe 32, 35, 39 bis 42.

2.7. Zugang Dritter

29. Artikel 58 und 59 der vorgeschlagenen Richtlinie enthalten Vorschriften über den Zugang zu Informationen über Zahlungskonten und die Nutzung dieser Informationen durch dritte Zahlungsdienstleister und Drittemittenten von Zahlungsinstrumenten.

30. Der EDSB stellt fest, dass die Kommission bei der Abfassung dieser Artikel dem Datenschutz und hier vor allem dem Grundsatz der Datenminimierung Aufmerksamkeit geschenkt hat. Nach Auffassung des EDSB lassen die einschlägigen Bestimmungen allerdings einen zu großen Auslegungsspielraum. So werden beispielsweise die Begriffe „Verfügbarkeit ausreichender Geldbeträge“ und „sensible Zahlungsdaten“ nirgendwo im Wortlaut der vorgeschlagenen Richtlinie definiert. Dies könnte zu Diskrepanzen bei der Umsetzung in den Mitgliedstaaten führen und möglicherweise Datenschutzprobleme beim Zugang Dritter mit sich bringen, sollten diese undefinierten Begriffe in den einzelstaatlichen Rechtsvorschriften zu großzügig ausgelegt werden.

31. Im Fall der „Verfügbarkeit ausreichender Geldbeträge“ empfiehlt der EDSB eine Klarstellung dahingehend, dass die an den Dritten übermittelte Information aus einem einfachen „Ja“ oder „Nein“ auf die Frage besteht, ob ausreichende Geldbeträge verfügbar sind, und nicht beispielsweise aus einem Kontoauszug.

32. Den Begriff „sensible Zahlungsdaten“ kennt das Datenschutzrecht nicht. In Artikel 8 der Richtlinie 95/46/EG sind die Sonderkategorien sensibler Daten aufgelistet, für die ein höheres Schutzniveau besteht. Zahlungsdaten gehören nicht zu den dort aufgeführten Kategorien. Das bedeutet nicht, dass personenbezogene Daten im Zusammenhang mit Zahlungen datenschutzrechtlich nicht geschützt sind, aber sie zählen nicht zu den „sensiblen“ Daten. Der EDSB empfiehlt daher, das Wort „sensibel“ zu streichen und stattdessen den Ausdruck „Zahlungsdaten“ zu verwenden.

2.8. Sicherheitsanforderungen

33. Der EDSB begrüßt die in Artikel 5 Buchstabe j vorgesehene Verpflichtung für Zahlungsinstitute, den zuständigen Behörden ein Dokument zur Sicherheitspolitik, eine detaillierte Risikobewertung in Bezug auf die erbrachten Zahlungsdienste und eine Beschreibung von Sicherheits- und Risikominderungsmaßnahmen zur Gewährleistung eines angemessenen Schutzes der Zahlungsdienstnutzer vor den festgestellten Risiken, einschließlich Betrug und illegaler Verwendung sensibler und personenbezogener Daten vorzulegen.

34. Da Sicherheit im Bereich der Zahlungsdienste von zentraler Bedeutung ist, ist zu gewährleisten, dass bei der Verarbeitung personenbezogener Daten und ihrer Weitergabe an die diversen Zwischenstellen die Grundsätze der Vertraulichkeit und Sicherheit gemäß Artikel 16 und 17

der Richtlinie 95/46/EG eingehalten werden. Der EDSB empfiehlt, in Erwägungsgrund 6 und Artikel 85 hinzuzufügen, dass bei der Verarbeitung personenbezogener Daten die in Artikel 16 und 17 der Richtlinie 95/46/EG niedergelegten Sicherheitsanforderungen einzuhalten sind.

35. Erwägungsgrund 6 und Artikel 85 sehen die Verpflichtung vor, sicherheitsrelevante Vorfälle unverzüglich der Europäischen Bankenaufsichtsbehörde zu melden. Der EDSB weist nachdrücklich darauf hin, dass es ähnliche Meldeanforderungen auch gemäß der Richtlinie 2002/58/EG, geändert durch die Richtlinie 2009/136/EG, gibt, und zwar für den Telekommunikationssektor; sobald sich dort personenbezogene Daten natürlicher Personen in Gefahr befunden haben, muss die verantwortliche Stelle dies der zuständigen Behörde (also der Datenschutzbehörde oder der Telekom-Regulierungsbehörde) sowie gegebenenfalls den betroffenen Personen mitteilen.

36. Es ist daher für Kohärenz mit den Anforderungen bei Verletzungen des Schutzes personenbezogener Daten zu sorgen, wie sie bereits für Telekomanbieter gemäß der Richtlinie 2002/58/EG, geändert durch die Richtlinie 2009/136/EG, gelten, und mit den diesbezüglichen Bestimmungen in der vorgeschlagenen Allgemeinen Datenschutzverordnung, die für alle für die Verarbeitung Verantwortlichen gelten würden (Artikel 31 und 32). In einem Erwägungsgrund der vorgeschlagenen Richtlinie sollte klargestellt werden, dass die Verpflichtungen zur Meldung von Sicherheitszwischenfällen unbeschadet anderer Verpflichtungen zur Meldung von Zwischenfällen bestehen, die in anderen Rechtsakten geregelt sind, insbesondere der im Datenschutzrecht formulierten Anforderungen bezüglich der Meldung von Verstößen gegen den Schutz personenbezogener Daten (in der Richtlinie 2002/58/EG und in der vorgeschlagenen Allgemeinen Datenschutzverordnung) und der in der vorgeschlagenen Richtlinie über Netzwerk- und Informationssicherheit[8], vorgesehenen Meldeanforderungen bei Sicherheitszwischenfällen, einem Vorschlag, zu dem der EDSB am 14. Juni 2013 eine Stellungnahme herausgegeben hat[9]. Der EDSB weist ferner darauf hin, dass die Tatsache, dass in Artikel 85 der vorgeschlagenen Richtlinie der noch in Verhandlung stehende Richtlinienvorschlag über Netz- und Informationssicherheit erwähnt wird, eine unklare Situation hervorruft, die den Klarstellungsbedarf noch weiter unterstreicht.

37. Artikel 87 der vorgeschlagenen Richtlinie besagt, dass die Mitgliedstaaten dafür sorgen, dass ein Zahlungsdienstleister die Authentifizierung durch Dritte anwendet. Weiter besagt der Artikel, dass die Europäische Bankenaufsichtsbehörde (EBA) in Zusammenarbeit mit

[8] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union, COM(2013) 48 final.

[9] Stellungnahme des EDSB vom 14. Juni 2013 zur „Cybersicherheitsstrategie der Europäischen Union“, abrufbar im Abschnitt Beratung auf der Website des EDSB: www.edps.europa.eu

der Europäischen Zentralbank (EZB) für Zahlungsdienstleister Leitlinien über den neuesten Stand der Kundenauthentifizierung und jegliche Ausnahmen von der verstärkten Kundenauthentifizierung erstellt. Der EDSB empfiehlt, in dem Richtlinienvorschlag darauf zu verweisen, dass der EDSB zu konsultieren ist, sobald es in den Leitlinien um die Verarbeitung personenbezogener Daten geht.

2.9. Normen und Interoperabilität

38. Die vorgeschlagene Richtlinie unterstreicht die Notwendigkeit der Entwicklung und Stärkung von Normen und Interoperabilität. Wie bereits in unserem Beitrag zur öffentlichen Konsultation ausgeführt, sind wir der Auffassung, dass der Entwicklung dieser Normen Datenschutzfolgenabschätzungen vorausgehen sollten, in denen die Auswirkungen verfügbarer neuer Technologien auf den Schutz der Privatsphäre und der Daten natürlicher Personen untersucht werden sollten. Im Verlauf dieses Prozesses sollte ermittelt werden, welche Risiken mit den einzelnen verfügbaren technischen Optionen einhergehen und welche Vorkehrungen ergriffen werden müssten, um Bedrohungen des Datenschutzes möglichst gering zu halten. Wir schlagen daher vor, in einer Bestimmung des verfügenden Teils der vorgeschlagenen Richtlinie verpflichtend vorzusehen, dass diese Normen nach Durchführung von Datenschutzfolgenabschätzungen und auf deren Grundlage entwickelt werden.

3. SCHLUSSFOLGERUNGEN

Der EDSB begrüßt die Bestimmung in Artikel 84, der zufolge die Verarbeitung personenbezogener Daten für die Zwecke der vorgeschlagenen Richtlinie im Einklang mit den einzelstaatlichen Vorschriften zur Umsetzung der Richtlinie 95/46/EG und der Richtlinie 2002/58/EG sowie der Verordnung (EG) Nr. 45/2001 zu erfolgen hat.

Der EDSB empfiehlt Folgendes:

- Die Verweise auf das anzuwendende Datenschutzrecht sollten in konkreten Garantien ihren Niederschlag finden, die für alle Situationen gelten, in denen die Verarbeitung personenbezogener Daten vorgesehen ist.

- Im Richtlinienentwurf sollte deutlich gemacht werden, dass die Bereitstellung von Zahlungsdiensten die Verarbeitung personenbezogener Daten zur Folge haben kann.

- Es sollte in der vorgeschlagenen Richtlinie ausdrücklich klargestellt werden, dass die Verarbeitung personenbezogener Daten erfolgen darf, sofern sie für die Erbringung von Zahlungsdiensten erforderlich ist.

- Im verfügenden Teil sollte eine Bestimmung mit der Verpflichtung hinzugefügt werden, dass „Datenschutz durch Technik / Datenschutz durch datenschutzfreundliche Voreinstellungen“ in alle Datenverarbeitungssysteme eingebettet wird, die im Zusammenhang mit der vorgeschlagenen Richtlinie entwickelt und verwendet werden.

- Bezüglich des Informationsaustauschs sollten i) die Zwecke erwähnt werden, zu denen personenbezogene Daten von nationalen zuständigen Behörden, der Europäischen Zentralbank, den nationalen Zentralbanken und den anderen in Artikel 25 genannten Behörden verarbeitet werden dürfen; sollte ii) die Art personenbezogener Daten angegeben werden, die gemäß der vorgeschlagenen Richtlinie verarbeitet werden dürfen, und sollte iii) ein angemessener Aufbewahrungszeitraum für die Daten im Rahmen der genannten Verarbeitung (oder zumindest genaue Kriterien für dessen Festsetzung) festgelegt werden.

- In Artikel 22 sollte den Anforderungen an zuständige Behörden hinzugefügt werden, dass sie mit offiziellem Beschluss Dokumente und Informationen anfordern können, und zwar unter Angabe der Rechtsgrundlage und des Zwecks des Ersuchens sowie der angeforderten Informationen und der Frist, innerhalb derer die Informationen bereitzustellen sind.

- In Artikel 31 sollte aufgenommen werden, dass die Modalitäten für die Unterrichtung der Nutzer auch für die Angaben zur Verarbeitung personenbezogener Daten gemäß Artikel 10 und 11 der Richtlinie 95/46/EG gelten.

- Im Fall der „Verfügbarkeit ausreichender Geldbeträge“ in Artikel 58 und 59 sollte eine Klarstellung dahingehend erfolgen, dass die an den Dritten übermittelte Information aus einem einfachen „Ja“ oder „Nein“ auf die Frage besteht, ob ausreichende Geldbeträge verfügbar sind, und nicht beispielsweise aus einem Kontoauszug.

- Im Begriff „sensible Zahlungsdaten“ in Artikel 58 sollte das Wort „sensibel“ gestrichen und stattdessen nur der Ausdruck „Zahlungsdaten“ verwendet werden.

- In einem Erwägungsgrund sollte klargestellt werden, dass die Verpflichtungen zur Meldung von Sicherheitszwischenfällen unbeschadet anderer Verpflichtungen zur Meldung von Zwischenfällen bestehen, die in anderen Rechtsakten geregelt sind, insbesondere der im Datenschutzrecht formulierten Anforderungen bezüglich der Meldung von Verstößen gegen den Schutz personenbezogener Daten (in der Richtlinie 2002/58/EG und in der vorgeschlagenen Allgemeinen Datenschutzverordnung) und der in der vorgeschlagenen Richtlinie über Netzwerk- und Informationssicherheit vorgesehenen Meldeanforderungen bei Sicherheitszwischenfällen.

- Es ist zu gewährleisten, dass bei der Verarbeitung personenbezogener Daten und ihrer Weitergabe an die verschiedenen Zwischenstellen die Grundsätze der Vertraulichkeit und der Sicherheit der Verarbeitung gemäß Artikel 16 und 17 der Richtlinie 96/46/EG eingehalten werden.

- Dem verfügenden Teil der vorgeschlagenen Richtlinie sollte eine Bestimmung mit der Verpflichtung hinzugefügt werden, dass Normen nach der Durchführung von Datenschutzfolgenabschätzungen und auf deren Grundlage entwickelt werden.

- In der vorgeschlagenen Richtlinie sollte erwähnt werden, dass der EDSB zu konsultieren ist, sobald es in den EBA-Leitlinien über den neuesten Stand der Kundenauthentifizierung und jegliche Ausnahmen von der verstärkten Kundenauthentifizierung um die Verarbeitung personenbezogener Daten geht.

Brüssel, den 5. Dezember 2013

(unterzeichnet)

Giovanni BUTTARELLI
Stellvertretender Europäischer Datenschutzbeauftragter