Stellungnahme des Europäischen Datenschutzbeauftragten

zur Verordnung der Kommission zur Festlegung eines Unionsregisters für den am 1. Januar 2013 beginnenden Handelszeitraum des EU-Emissionshandelssystems und die darauffolgenden Handelszeiträume

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 über den 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 die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr[2],

gestützt auf ein Ersuchen um eine Stellungnahme gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 –

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. Einleitung

1.1. Hintergrund

1. Am 18. November 2011 nahm die Kommission die Verordnung (EU) Nr. 1193/2011 der Kommission zur Festlegung eines Unionsregisters für den am 1. Januar 2013 beginnenden Handelszeitraum des EU-Emissionshandelssystems und die darauffolgenden Handelszeiträume gemäß der Richtlinie 2003/87/EG des Europäischen Parlaments und des Rates und der Entscheidung Nr. 280/2004/EG des Europäischen Parlaments und des Rates sowie zur Änderung der Verordnungen

[1] ABl. L 281 vom 23.11.1995, S. 31.
[2] ABl. L 8 vom 12.1.2001, S. 1.

Postanschrift: Rue Wiertz 60 - B-1047 Brüssel
Dienststelle: Rue Montoyer 63
E-Mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

(EG) Nr. 2216/2004 und (EU) 920/2012 („Verordnung“) an.[3] Die Verordnung wurde dem EDSB noch am selben Tag zur Konsultation übermittelt.

2. Bereits vor der Annahme der Verordnung wurde dem EDSB die Möglichkeit zu informellen Kommentaren gegeben. Einige dieser Kommentare wurden in der Verordnung berücksichtigt, und der EDSB hält fest, dass im Ergebnis die Datenschutzgarantien gestärkt wurden.

3. Der EDSB begrüßt diese offizielle Konsultation durch die Kommission sowie die Tatsache, dass die vorliegende Stellungnahme in der Präambel des angenommenen Rechtsinstruments erwähnt wird.

1.2. Ziele und Anwendungsbereich der Verordnung

4. Das EU-Emissionshandelssystem („ETS“) gehört zu den von der Europäischen Union („EU“) eingeführten Maßnahmen, mit denen die Treibhausgasemissionsreduktionsziele des Kyoto-Protokolls erreicht werden sollen. Das ETS führt ein Compliance-System für Betreiber ein und zielt darauf ab, dass Emissionen EU-weit wirksam gedeckelt werden.[4]

5. Die Verordnung ändert und ersetzt ab 1. Januar 2013 ältere Verordnungen der Kommission zu diesem Thema, insbesondere die Verordnungen (EG) Nr. 2216/2004 und (EU) Nr. 920/2010 der Kommission[5], die beide Vorschriften für ein „standardisiertes und sicheres Registrierungssystem“ enthielten.

6. Eine der mit der Verordnung eingeführten Hauptneuerungen ist die Einführung eines zentralen Unionsregisters im Jahr 2012, das an die Stelle des bisherigen Systems einer Kombination nationaler Register tritt.

7. Das Unionsregister und das so genannte Transaktionsprotokoll der Europäischen Union (oder „EUTL“), das auf EU-Ebene bereits besteht, sind zwei Untersysteme, die von der Europäischen Kommission betreut und betrieben werden. Diese beiden Systeme haben unterschiedliche Aufgaben, ergänzen sich jedoch.

8. Im Unionsregister werden die Konten der am ETS beteiligten Akteure (z. B. Anlagenbetreiberkonten, Luftfahrzeugbetreiberkonten, Händlerkonten, Auktionskonten) sowie Aufzeichnungen von zwischen den Konten vorgenommenen Transaktionen geführt. Das Unionsregister ist somit ein zentrales elektronisches Register auf EU-Ebene, das den Emissionshandel von Kontoinhabern innerhalb eines Mitgliedstaats und zwischen Mitgliedstaaten unterstützt.

9. Das EUTL hingegen zeichnet die Zuteilungen, Übertragungen und Löschungen von CO2-Emissionszertifikaten auf und prüft die Schlüssigkeit und Kohärenz bestimmter Vorgänge.

2. Ziele und Aufbau der Stellungnahme des EDSB

10. Zwar ist die Verarbeitung personenbezogener Daten nicht das Hauptziel der Verordnung, doch macht die Verordnung durchaus die Verarbeitung

[3] ABl. L 315 vom 29.11.2011, S. 1.
[4] Zu näheren Informationen über das ETS siehe http://ec.europa.eu/clima/publications/docs/ets_en.pdf.
[5] ABl. L 386 vom 29.12.2004, S. 1, und ABl. L 270 vom 14.10.2010, S. 1.

personenbezogener Daten erforderlich, einschließlich von Informationen aus dem Strafregister und Informationen über mutmaßliche kriminelle Aktivitäten. Diese Daten werden zu dem Zweck verarbeitet, einen Missbrauch der Konten für kriminelle Aktivitäten zu vermeiden.

11. Die personenbezogenen Daten können Personen betreffen, die im Namen von Kontoinhabern als deren „Geschäftsführer“ und Kontobevollmächtigte tätig sind. Außerdem können auch die Kontoinhaber selbst natürliche Personen sein. In diesem Fall können auch ihre personenbezogenen Daten verarbeitet werden. Darüber hinaus werden auch einige Daten über wirtschaftliche Eigentümer der Kontoinhaber erhoben, bei denen es sich ebenfalls um natürliche Personen handeln kann.[6]

12. In Anbetracht der – häufig sensiblen – personenbezogenen Daten, die gemäß der Verordnung verarbeitet werden müssen, empfiehlt der EDSB, in der Verordnung angemessene Datenschutzgarantien vorzusehen.

13. Da die Verordnung bereits angenommen wurde, möchte der EDSB mit dieser Stellungnahme im Wesentlichen helfen zu gewährleisten, dass seine Empfehlungen bei der für Ende 2012 vorgesehenen Änderung der Verordnung berücksichtigt werden.

14. Des Weiteren können die Empfehlungen in dieser Stellungnahme der Kommission und den nationalen Verwaltern bei der Umsetzung der notwendigen Datenschutzgarantien in der Praxis Hilfestellung leisten. Nähere Ausführungen zur praktischen Umsetzung finden sich in den Punkten 41 bis 43, in denen die Ausarbeitung einer umfassenden Datenschutzstrategie gefordert wird, in Punkt 36 zu anderen praktischen Maßnahmen wie Hilfe-Menüs und Warnhinweisen im Unionsregister sowie Schulungsmaterial, und in Punkt 40 über Systemdokumentation und die Veröffentlichung von Informationen auf der Website des Unionsregisters.

15. In Abschnitt 3 dieser Stellungnahme wird kurz dargestellt, welche personenbezogenen Daten im Einklang mit der Verordnung verarbeitet werden müssen, wobei sensible Daten im Mittelpunkt stehen. Diese Darstellung ist notwendig, um die Empfehlungen in den Abschnitten 4 bis 12 dieser Stellungnahme richtig einordnen zu können. In Abschnitt 4 wird eine Klärung der Fragen gefordert, welche personenbezogenen Daten gemäß der Verordnung verarbeitet werden, wer sie verarbeitet und wo die Daten gespeichert werden; auch hier stehen sensible Daten im Mittelpunkt. In den Abschnitten 5 bis 12 finden sich die übrigen Empfehlungen des EDSB, während Abschnitt 13 die Schlussfolgerungen enthält.

3. Personenbezogene Daten, die gemäß der Verordnung verarbeitet werden sollen

Informationen, die von den nationalen Verwaltern im Zusammenhang mit der Eröffnung und Verwaltung von Konten verarbeitet werden

16. Ein Großteil der personenbezogenen Daten, die gemäß der Verordnung zu verarbeiten sind, wird von den nationalen Verwaltern in den EU-Mitgliedstaaten von Antragstellern im Zusammenhang mit dem Antrag auf Eröffnung eines Kontos im Unionsregister erhoben (siehe Artikel 12 bis 24, in denen wiederum auf

[6] Siehe nachstehenden Abschnitt 3 mit näheren Ausführungen zu den Datenkategorien einschließlich besonders schutzwürdiger Daten, die gemäß der Verordnung verarbeitet werden.

verschiedene Anhänge verwiesen wird). Diese „nationalen Verwalter“ sind die Rechtsträger, die dafür zuständig sind, im Namen eines Mitgliedstaats eine Serie von unter die Gerichtsbarkeit eines Mitgliedstaats fallenden Nutzerkonten im Unionsregister zu verwalten.

17. Die Verordnung verlangt von den Antragstellern, zur Eröffnung eines Kontos Informationen einschließlich personenbezogener Daten beim nationalen Verwalter einzureichen. Die geforderten Angaben variieren je nach Kontoart (siehe insbesondere die Anhänge II, III, IV, V und VII).

18. Die Spanne der Daten umfasst: persönliche Identifikationsnummer, Name, Funktion, Anschrift, Telefonnummern (Festnetz und Mobil), Geburtsdatum und Geburtsort und bevorzugte Sprache, Kopien von Personalausweisen und Pässen, Nachweis des ständigen Wohnsitzes und polizeiliches Führungszeugnis.

19. Ferner sind den nationalen Verwaltern einige Angaben zum wirtschaftlichen Eigentümer der juristischen Person mitzuteilen, um einen Missbrauch des Finanzsystems zum Zweck der Geldwäsche und Terrorismusfinanzierung zu verhindern (siehe Anhang III Punkt 5 Buchstabe d).

20. Gemäß Artikel 20 müssen nationale Verwalter unter bestimmten Umständen die Eröffnung eines Kontos ablehnen, u. a. wenn sie berechtigten Grund zu der Annahme haben, dass die Konten möglicherweise für betrügerische Praktiken, die Zertifikate oder Kyoto-Einheiten betreffen, für Geldwäsche, Terrorismusfinanzierung oder andere schwere Straftaten verwendet werden. Nicht näher bestimmt ist, auf welche weiteren Informationen ein nationaler Verwalter zugreifen darf, um zu dem Schluss zu gelangen, dass ein solcher „berechtigter Zweifel“ besteht; dies soll vermutlich im einzelstaatlichen Recht geregelt werden.

21. Neben Artikel 20 erfordert noch eine Reihe anderer Vorschriften über die Kontenverwaltung bei mutmaßlichen kriminellen Aktivitäten die Verarbeitung sensibler personenbezogener Daten durch den nationalen Verwalter. Dazu gehören:

- Artikel 22 über die Ablehnung von Kontobevollmächtigten;
- Artikel 31 über die Sperrung von Konten;
- Artikel 30 über die Schließung von Konten und die Amtsenthebung von Kontobevollmächtigten „auf Initiative des Verwalters“, und
- Artikel 71 über die „Sperrung des Zugangs zu Zertifikaten oder Kyoto-Einheiten bei Verdacht auf betrügerische Transaktionen“.

Informationsaustausch zwischen nationalen Verwaltern, der Kommission und Dritten einschließlich Strafverfolgungsbehörden

22. Der bereits erwähnte Artikel 71 sowie mehrere weitere Artikel der Verordnung (einschließlich Artikel 36 Absatz 4, Artikel 70, 72, 73 und 83) sehen einen Datenaustausch zwischen nationalen Verwaltern, der Kommission und Dritten einschließlich Strafverfolgungsbehörden vor, bei dem auch Informationen über mutmaßliche kriminelle Aktivitäten ausgetauscht werden dürfen.

23. Gemäß Artikel 71 Absatz 3 der Verordnung benachrichtigt der nationale Verwalter (oder die Kommission) „die zuständige Behörde unverzüglich über die Sperre des Zugangs [zu einem Konto]“. Gemäß Artikel 72 arbeiten die nationalen Verwalter

mit den zuständigen Behörden zusammen und informieren, wenn sie wissen oder vermuten, dass Geldwäsche, Terrorismusfinanzierung oder schwere Straftaten vorliegen. Artikel 36 Absatz 4 sieht weitere Mitteilungspflichten vor. Des Weiteren erlaubt Artikel 83 Absatz 8 die Meldung bestimmter Transaktionsmuster an Steuer- und Strafverfolgungsbehörden, auch wenn er dies nicht ausdrücklich fordert.

24. Artikel 70 Absatz 2 und 3 sehen die Meldung von Verstößen gegen die Sicherheitsvorschriften oder von Sicherheitsrisiken an die nationalen Verwalter und die Kommission in Fällen vor, in denen diese Verstöße oder Risiken zur Sperrung des Zugangs zum Unionsregister führen können.

25. Artikel 73 Absatz 1 lautet: „Die Kommission kann den Zentralverwalter anweisen, die Bestätigung einiger oder aller vom Unionsregister ausgehenden Prozesse durch das EUTL vorübergehend auszusetzen, wenn das Register nicht nach den Vorschriften dieser Verordnung geführt und gewartet wird. Sie benachrichtigt umgehend die jeweiligen nationalen Verwalter".

26. Artikel 83 Absatz 7 besagt: „Die nationalen Verwalter stellen allen anderen nationalen Verwaltern und dem Zentralverwalter[7] nach einem sicheren Verfahren die Namen und Identitätsangaben der Personen zur Verfügung, deren Kontoeröffnung sie abgelehnt haben oder deren Ernennung zum Kontobevollmächtigten sie abgelehnt haben, ebenso wie die Namen und Identitätsangaben des Kontoinhabers sowie der Bevollmächtigten von Konten, deren Zugang gesperrt wurde, oder von Konten, die (unter anderem) wegen bestimmter bekannter oder vermuteter krimineller Aktivitäten geschlossen wurden". Auch wenn es in der Verordnung ausdrücklich so nicht steht, soll nach den Erläuterungen der Kommission mit dieser Bestimmung das Risiko verringert werden, dass Kontoinhaber und deren Kontobevollmächtigte, denen die Eröffnung eines Kontos verweigert wurde, oder deren Konten wegen Verdachts auf kriminelle Aktivitäten gesperrt oder geschlossen wurden, in der Folge in einem anderen Mitgliedstaat erfolgreich die Eröffnung eines Kontos beantragen. Ein erneuter Antrag in einem anderen Mitgliedstaat nach einer Ablehnung oder Sperrung ist an sich nach der Verordnung nicht verboten. Auch schließt eine nicht erfolgreiche Antragstellung in einem Mitgliedstaat die Möglichkeit einer späteren erfolgreichen Antragstellung in einem anderen Mitgliedstaat nicht aus. Um jedoch das so genannte „Forum Shopping" nicht zu fördern und eine wirksame Zusammenarbeit zu unterstützen, sieht die Verordnung eine Regelung für den Informationsaustausch vor, die eigentlich wie eine Schwarze Liste funktioniert und nationale Verwalter darauf hinweist, unter Umständen Neuanträge der betreffenden Personen oder Organisationen verschärft zu prüfen.[8]

27. Gemäß Artikel 83 Absatz 2 bis 6 hat Europol unmittelbaren Zugriff auf das Unionsregister und das EUTL und haben bestimmte Dritte einschließlich Strafverfolgungs- und Steuerbehörden auf Antrag Zugang (weitere Einzelheiten hierzu in Abschnitt 7).

4. Bedarf an weiteren Klarstellungen bezüglich der gemäß der Verordnung verarbeiteten personenbezogenen Daten

[7] Zum Zentralverwalter siehe nachfolgenden Abschnitt 5.
[8] Siehe Abschnitt 10 mit konkreten Empfehlungen zu dieser Schwarzen Liste.

Werden personenbezogene Daten innerhalb oder außerhalb des Unionsregisters gespeichert und ausgetauscht?

28. Die Verordnung enthält keine Aussage dazu, ob irgendwelche im Zusammenhang mit der Kontenverwaltung verarbeiteten personenbezogenen Daten im Unionsregister auch gespeichert werden. Der Verordnung ist auch nicht zu entnehmen, ob der Informationsaustausch zwischen den nationalen Verwaltern und der Kommission innerhalb oder außerhalb des Unionsregisters und des EUTL erfolgt. Aus dem Wortlaut der Verordnung geht also nicht hervor, ob irgendwelche sensiblen Daten im Unionsregister und im EUTL erfasst und gespeichert werden.

29. Eine solche Angabe wäre allerdings von großer Bedeutung, da gemäß Artikel 81 Absatz 1 der Verordnung die im Unionsregister gespeicherten Daten für 15 Jahre aufzubewahren sind. Dies ist ein langer Aufbewahrungszeitraum, der im Hinblick auf die Speicherung vieler Kategorien sensibler Daten kaum angemessen sein dürfte.[9]

30. Laut Auskunft der Kommission wird wohl ein Großteil der bei der Eröffnung eines Kontos erhobenen Daten wie die Kopien des polizeilichen Führungszeugnisses oder Kopien von Pässen, Personalausweisen und Nachweisen des Wohnsitzes nicht in das Unionsregister hochgeladen, sondern vielmehr vor Ort von den nationalen Verwaltern nach den nationalen Datenschutzvorschriften verarbeitet und gespeichert.

31. Daten aus dem polizeilichen Führungszeugnis werden anscheinend nicht systematisch in das Unionsregister eingegeben. Es kann jedoch nicht ausgeschlossen werden, dass ein nationaler Verwalter beispielsweise in das Kommentarfeld in der Datenbank Gründe für die Ablehnung der Eröffnung eines Kontos eingibt. Bei Personaldokumenten werden Gültigkeitsdauer und Ausweis- bzw. Passnummer in das Unionsregister eingegeben, nicht jedoch Kopien der jeweiligen Dokumente.

32. Anscheinend kann auch die Tatsache, dass eine Kontoeröffnung abgelehnt oder ein Konto gesperrt wurde, im Unionsregister vermerkt werden[10].

Klärung der Frage, ob Unionsregister und EUTL sensible Daten enthalten dürfen

33. In Anbetracht dessen empfiehlt der EDSB, den Wortlaut der Verordnung zu ändern und dabei klarzustellen, welche Daten inner- bzw. außerhalb des Unionsregisters und des EUTL verarbeitet werden. In diesem Zusammenhang würde der EDSB insbesondere eine allgemeine Bestimmung in der Verordnung begrüßen, der zufolge keine besonderen Datenkategorien[11] und hier vor allem keine polizeilichen Führungszeugnisse oder Informationen über begangenen oder mutmaßlichen Betrug oder andere kriminelle Aktivitäten im EUTL oder im Unionsregister gespeichert werden.[12]

34. Etwaige Ausnahmen von dieser Regel sollten gesondert geregelt werden und müssen notwendig und verhältnismäßig sein. Wie bereits unter Punkt 27 festgestellt,

[9] Siehe Abschnitt 9 zu den Aufbewahrungsfristen.
[10] Die Kommission erläuterte hierzu, dass diese Informationen auf keinen Fall „international übermittelt“ werden (siehe nachstehenden Abschnitt 11 über internationale Übermittlungen).
[11] Siehe Artikel 8 der Richtlinie 95/46/EG.
[12] Dies sollte auch in der in den Punkten 41 bis 43 erwähnten Datenschutzstrategie deutlich gemacht werden.

kann anscheinend auch die Tatsache, dass eine Kontoeröffnung abgelehnt oder ein Konto gesperrt wurde, im Unionsregister vermerkt werden. In Kombination mit dem Namen des Kontoinhabers, der eine natürliche Person sein kann, oder mit den Namen der Kontobevollmächtigten (z. B. der Geschäftsführer) können diese Informationen als sensible Daten gelten. Diese und ähnliche Ausnahmen sind angemessen zu begründen und in der Verordnung gesondert zu regeln.

Verwendung von Freitextfeldern

35. Wie bereits unter Punkt 30 festgestellt, werden Daten aus dem polizeilichen Führungszeugnis anscheinend nicht systematisch in die Datenbank eingegeben. Wie jedoch unter Punkt 31 erläutert, kann nicht ausgeschlossen werden, dass ein nationaler Verwalter beispielsweise in das Kommentarfeld der Datenbank Gründe für die Ablehnung der Eröffnung eines Kontos eingibt. Für derartige Fälle empfiehlt der EDSB, in der Verordnung die Eingabe sensibler Daten in die Freitextfelder ausdrücklich zu untersagen, sofern dies für die Verwaltung des Unionsregisters nicht notwendig ist, hierzu in einem angemessenen Verhältnis steht und gemäß der Verordnung eindeutig zulässig ist (siehe Punkt 34).

36. Für die Praxis empfiehlt der EDSB, den Nutzern des Unionsregisters klare Weisungen (in Form eines Hilfe-Menüs, von Warnhinweisen, Schulungsmaterial oder in anderer Form) dahingehend zu geben, dass derartige Informationen nicht in die Kommentarfelder eingegeben werden dürfen.

Daten über wirtschaftliche Eigentümer

37. Ferner empfiehlt der EDSB, in der Verordnung klar zu regeln, welche Daten über wirtschaftliche Eigentümer verarbeitet werden sollen (siehe Punkt 19).

5. Der Zentralverwalter

38. Gemäß Artikel 4 und 5 (zusammen zu lesen mit Artikel 3 Absatz 2 der Verordnung sowie mit Artikel 20 der Richtlinie 2003/87/EG) führt und wartet ein von der Kommission benannter Zentralverwalter das Unionsregister sowie das EUTL.

39. Aus der Verordnung geht jedoch nicht hervor, ob der Zentralverwalter ein Beamter der Europäischen Kommission, ein Bediensteter eines anderen Organs, einer Agentur oder Einrichtung der EU oder einer nach dem Recht eines der Mitgliedstaaten eingerichteten Stelle sein soll. Ebenso wenig wird klar, welche Pflichten die Kommission bzw. der von ihr benannte Zentralverwalter, sofern er nicht Beamter der Kommission ist, hat. Diese Aspekte bedürfen der Klarstellung. Sollte vor allem die Kommission die Absicht haben, wie sie es dem EDSB gegenüber erläuterte, selbst als Zentralverwalter zu fungieren, sollte dies im Wortlaut der Verordnung klar zum Ausdruck gebracht werden.

40. Des Weiteren empfiehlt der EDSB, dies auch auf praktischer Ebene deutlich zu machen, also in der Systemdokumentation einschließlich der in den Punkten 41 bis 43 erwähnten Datenschutzstrategie, sowie in dem der Öffentlichkeit zugänglichen Teil der Website des Unionsregisters.

6. Zuweisung von Aufgaben und Zuständigkeiten: Annahme einer Datenschutzstrategie

41. Begrüßen würden wir ferner eine Klarstellung der Verteilung von Aufgaben und Zuständigkeiten im Bereich des Datenschutzes auf nationale Verwalter und Zentralverwalter.

42. Der EDSB empfiehlt, in einer umfassenden Datenschutzstrategie für das ETS oder in einem ähnlichen Dokument, das gemeinsam von der Kommission und nationalen Verwaltern erarbeitet wird, genau festzulegen, welche Stelle wofür zuständig sein soll, und dabei anzugeben, welche Datenschutzvorschriften jeweils gelten. In diesem Dokument könnte beispielsweise festgelegt werden, wer die betroffenen Personen informiert, wer tätig wird, wenn betroffene Personen Auskunft über ihre Daten oder deren Berichtigung, Sperrung oder Löschung beantragen, wer für die Sicherheit des Unionsregisters und des EUTL zuständig ist, und wer die Entscheidungen bezüglich ihrer Gestaltung trifft.

43. In der Verordnung könnte die Annahme eines solchen Dokuments ausdrücklich verlangt werden. Dort sollten auch seine wesentlichen Elemente festgelegt werden.

7. Zugriff auf Daten durch Europol und andere Dritte

44. Gegenstand von Artikel 83 ist die Vertraulichkeit der im EUTL und im Unionsregister gespeicherten Daten. In diesem Artikel ist geregelt, wem und unter welchen Umständen die Daten zur Verfügung gestellt werden dürfen. Gemäß Absatz 1 gilt grundsätzlich, dass alle im EUTL und im Unionsregister enthaltenen Informationen als vertraulich zu behandeln sind, soweit „in Rechtsvorschriften der EU oder in nationalen Rechtsvorschriften, die ein berechtigtes und mit dieser Verordnung vereinbares Ziel verfolgen und verhältnismäßig sind“ nicht anders geregelt.

45. Im weiteren Verlauf des Artikels wird eine Reihe von Rechtsträgern (einschließlich Strafverfolgungs- und Steuerbehörden von Mitgliedstaaten, Europäisches Amt für Betrugsbekämpfung, Europäischer Rechnungshof, Eurojust und andere) aufgeführt, die auf Antrag im Unionsregister und im EUTL gespeicherte Daten beziehen können, wenn derartige Anträge für die Wahrnehmung ihrer Aufgaben unerlässlich sind. In Artikel 83 Absatz 5 heißt es ausdrücklich, dass dies auch „anonymisierte Transaktionsdaten zur Aufdeckung verdächtiger Transaktionsmuster“ umfassen kann. Weiter sieht Artikel 83 Absatz 5 vor, dass diese Rechtsträger wiederum „anderen Rechtsträgern verdächtige Transaktionsmuster melden können“.

46. Darüber hinaus wird gemäß dem Beschluss 2009/371/JI des Rates zur Errichtung des Europäischen Polizeiamtes Europol zur Durchführung seiner Aufgaben ständiger Lesezugriff auf Daten im Unionsregister und im EUTL gewährt. Europol unterrichtet die Kommission regelmäßig über die Verwendung dieser Daten.

47. Der EDSB empfiehlt erstens, die Zwecke genauer zu definieren, zu denen die aufgeführten Rechtsträger einschließlich Europol Zugriff auf die Daten haben. Eine einfache Auflistung der Namen der Rechtsträger, an die Daten übermittelt werden dürfen, ist datenschutzrechtlich gesehen keine ausreichende „Zweckbestimmung“. Anstelle einer einfachen Auflistung der Rechtsträger sollte bestimmt werden, dass ein Zugriff gemäß Artikel 83 auf Fälle beschränkt ist, in denen dieser für Zwecke,

die in der Verordnung genau benannt und aufgeführt sind, erforderlich ist und in einem angemessenen Verhältnis dazu steht.

48. Der EDSB erinnert daran, dass grundsätzlich alle denkbaren Zwecke von Übermittlungen personenbezogener Daten angegeben werden und jeweils mit dem Zweck vereinbar sein sollten, für den sie ursprünglich erhoben wurden. Jegliche Ausdehnung auf Fragen, die nicht in den Tätigkeitsbereich des Unionsregisters fallen (z. B. Geldwäsche, Terrorismusfinanzierung oder andere schwere Straftaten) sollte sorgfältig begründet und eindeutig eingegrenzt werden.

49. In diesem Zusammenhang hält der EDSB fest, dass die Verordnung (EU) Nr. 920/2010 der Kommission, nunmehr durch die Verordnung geändert, eine präzisere Beschreibung der Zwecke bot, denn in ihrem Artikel 75 Absatz 3 heißt es, dass Daten zur Verfügung gestellt werden können, „wenn die Anträge gerechtfertigt und für Ermittlungen, zur Aufdeckung und Verfolgung von Betrugsfällen, zu Zwecken der Steuerverwaltung oder des Steuervollzugs oder zur Bekämpfung von Geldwäsche, Terrorismusfinanzierung oder schweren Straftaten unerlässlich sind". Eine ähnliche, allerdings restriktivere Formulierung wäre auf jeden Fall einer einfachen Auflistung der Rechtsträger vorzuziehen, an die Daten übermittelt werden dürfen, wie sie in der derzeitigen Verordnung zu finden ist. So könnte beispielsweise die in der Verordnung verwendete Formulierung bezüglich der Ablehnung von Kontoneröffnungen auch hier angebracht sein, wobei sie noch ausreichend Spielraum für Strafverfolgungs- und Steuerbehörden lässt. Übermittlungen könnten so auf Fälle beschränkt werden, in denen sie für Ermittlungen, zur Aufdeckung und Verfolgung von „betrügerischen Praktiken, die Zertifikate oder Kyoto-Einheiten betreffen, von Geldwäsche, Terrorismusfinanzierung oder anderen schweren Straftaten, bei denen das Konto möglicherweise eine instrumentelle Rolle spielt" unerlässlich sind.

50. Im Hinblick auf den Zugang zu „anonymisierten Transaktionsdaten zur Aufdeckung verdächtiger Transaktionsmuster" ist zu unterstreichen, dass die Daten auch weiterhin als „personenbezogene Daten" zu betrachten sind und damit so lange den Datenschutzvorschriften unterliegen, wie die betreffenden Personen indirekt bestimmbar sind. Die Tatsache, dass einige „Anonymisierungstechniken" angewandt wurden, heißt noch nicht, dass die Daten zwangsläufig als „anonymisiert" im Sinne von Erwägungsgrund 26 der Richtlinie 95/46/EG gelten können.[13] Ein Datensatz kann personenbezogene Daten enthalten und möglicherweise zur Bestimmung einer natürlichen Person führen, auch wenn direkte Kennzeichen entfernt und mehrere zusätzliche Anonymisierungstechniken angewandt wurden.[14] In Anbetracht der Tatsache, dass Daten von Kontoinhabern erfasst und für 15 Jahre im Unionsregister und im EUTL gespeichert werden, ist es eher unwahrscheinlich, dass in diesem Aufbewahrungszeitraum Daten über Transaktionen wirklich als anonymisiert in dem Sinne betrachtet werden können, dass sie nicht bis zu den natürlichen Personen zurückverfolgt werden können, die diese Transaktionen durchgeführt haben. Sollte das Ziel dieser Bestimmung

[13] Erwägungsgrund 26, siehe vor allem die Passage: „Bei der Entscheidung, ob eine Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem für die Verarbeitung Verantwortlichen oder einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen".

[14] Siehe S. 17 bis 22 der Stellungnahme der Artikel 29-Datenschutzgruppe zum Begriff „personenbezogene Daten" (WP 136). Siehe ferner die einschlägigen Ausführungen in einer Reihe von Stellungnahmen des EDSB, beispielsweise Abschnitt 3.1 der Stellungnahme des EDSB zur Vorabkontrolle des Europäischen Überwachungssystems (TESSy) vom 3. September 2010.

weiterhin darin bestehen, den Strafverfolgungsbehörden die Möglichkeit zu geben, nach Entdecken „eines verdächtigen Transaktionsmusters“ zu bestimmen, welche Kontoinhaber sich an dieses Muster gehalten haben, um Ermittlungen durchzuführen und diese Kontoinhaber oder die natürlichen Personen, die in ihrem Namen tätig geworden sind, strafrechtlich zu verfolgen, dann bedeutet dieses Ziel an sich schon, dass eine Bestimmung der betreffenden Personen erforderlich ist.

51. Um jegliches Missverständnis in diesem Punkt zu vermeiden, empfiehlt der EDSB eine Klarstellung in der Verordnung. Es sollten ferner in der Verordnung wie auf praktischer Ebene Garantien eingefügt werden, mit denen die Anwendung angemessener Anonymisierungstechniken gewährleistet wird, bevor in großem Umfang Transaktionsdaten zu einem Zweck übermittelt werden, der im Wesentlichen „Data Mining“ ist. Neben der Pseudonymisierung (beispielsweise durch die Verschlüsselung von Kontoinhabern) können weitere Anonymisierungstechniken erforderlich sein, wenn die Pseudonymisierung allein nicht wirksam genug ist, weil beispielsweise die Wahrscheinlichkeit besteht, dass trotz Pseudonymisierung die Transaktionen mit denselben Personen verknüpft werden können.[15]

52. Der EDSB hält fest, dass im Zusammenhang mit dem direkten Zugang auf das Unionsregister und das EUTL für Europol bezüglich der Anonymisierung in spezifischen Bestimmungen gewährleistet werden sollte, dass Europol personenbezogene Daten erst nach Anwendung angemessener Anonymisierungstechniken abfragen kann.

53. Schließlich weist der EDSB noch darauf hin, dass die in Artikel 83 Absatz 1 geregelte Vertraulichkeit nicht nur für Daten gilt, die im Unionsregister und im EUTL erfasst sind, sondern auch für alle außerhalb dieser Datenbanken gespeicherten personenbezogenen Daten, die gemäß der Verordnung verarbeitet werden sollen. Vertraulichkeit ist wichtig für die vor Ort von den nationalen Verwaltern verarbeiteten personenbezogenen Daten, aber auch im Hinblick auf die zwischen nationalen Verwaltern und der Kommission ausgetauschten Daten, hauptsächlich, wenn auch nicht ausschließlich, mit Blick auf die unter Punkt 26 bereits erwähnte und nachstehend in Abschnitt 10 näher erörterte Schwarze Liste.

8. Veröffentlichung personenbezogener Daten im Internet

54. Aus Gründen der Transparenz werden im öffentlich zugänglichen Teil der Website des Unionsregisters bestimmte Informationen einschließlich einer begrenzten Menge personenbezogener Daten (z. B. Kontaktdaten) von Kontoinhabern und ihren Bevollmächtigten angezeigt. Einige dieser Angaben sind vorgeschrieben, andere fakultativ. Gemäß Artikel 83 Absatz 9 und 10 können sich Kontoinhaber für oder gegen die Veröffentlichung bestimmter personenbezogener Daten über sie oder ihre Bevollmächtigten entscheiden ("Opt-in"/"Opt-out").

55. In den Anhängen II, IV, VII und XII ist nämlich Punkt für Punkt geregelt, i) welche Informationen ins Internet gestellt werden, ii) welche nicht dort eingestellt werden, iii) welche Angaben auf besonderen Antrag angezeigt werden ("Opt-in"), und iv) welche Angaben angezeigt werden, sofern nichts anderes beantragt wurde ("Opt-out").

[15] Siehe S. 21 der bereits in Fußnote 14 genannten Stellungnahme der Artikel 29-Datenschutzgruppe.

56. Der EDSB begrüßt diese Klarstellungen und hat keine weiteren Anmerkungen dazu, welche Datenkategorien veröffentlicht bzw. nicht veröffentlicht werden sollten und welche Einwilligung jeweils erforderlich ist.

57. Der EDSB würde jedoch eine allgemeine Bestimmung in der Verordnung dahingehend begrüßen, dass abgesehen von den in der Verordnung konkret genannten Daten keine anderen personenbezogenen Daten auf der Website der Öffentlichkeit zugänglich gemacht werden.

9. Aufbewahrungsfrist

Einführung und allgemeine Anmerkungen

58. Artikel 81 Absatz 1 der Verordnung besagt: „Das Unionsregister und jedes andere [Kyoto-Protokoll]-Register bewahren Aufzeichnungen über alle Vorgänge, Protokollierdaten und Kontoinhaber 15 Jahre lang bzw. so lange auf, bis etwaige Fragen im Zusammenhang mit ihrer Durchführung geklärt sind, je nachdem, welcher Zeitpunkt später eintritt".

59. Der EDSB hat zur Kenntnis genommen, dass die Anforderungen bezüglich der Datenaufbewahrung im Einklang mit den „Data Exchange Standards of the United Nations Framework Convention on Climate Change" festgelegt wurden, die von allen Parteien des Kyoto-Protokolls einschließlich der EU und aller EU-Mitgliedstaaten vereinbart wurden.[16]

60. Dessen ungeachtet empfiehlt der EDSB, Artikel 81 Absatz 1 klarer zu formulieren und darauf hinzuweisen, dass die Datenaufbewahrungsanforderungen den EU-Datenschutzvorschriften entsprechen müssen, denen zufolge personenbezogene Daten „nicht länger, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden", aufbewahrt werden dürfen.[17]

61. In Anbetracht der Datenschutzanforderungen, aber auch unter Berücksichtigung der internationalen Verpflichtungen nach dem Kyoto-Protokoll empfiehlt der EDSB, in der Verordnung klarer zu regeln, welche Kategorien personenbezogener Daten 15 Jahre lang aufbewahrt werden müssen und für welche Kategorien personenbezogener Daten diese Aufbewahrungsfrist nicht gilt.

62. Außerdem sollten für die Kategorien personenbezogener Daten, für die diese Aufbewahrungsfrist nicht gilt (weil sie beispielsweise außerhalb des Unionsregisters verarbeitet werden), angemessene eigene Aufbewahrungsfristen festgelegt werden oder sollte, sofern ausreichend, die Verordnung zumindest die Festlegung angemessener Aufbewahrungsfristen nach einzelstaatlichem Recht im Einklang mit den nationalen Rechtsvorschriften zur Umsetzung der Richtlinie 95/46/EG fordern.

[16] Siehe „Data Exchange Standards for Registry Systems under the Kyoto Protocol, Technical Specifications (Version 1.1.8)", insbesondere Abschnitt 7 „Data Logging Specifications" auf S. 66, abrufbar unter http://unfccc.int/files/kyoto_mechanisms/registry_systems/application/pdf/des_full_ver_1.1.8.pdf.
[17] Artikel 6 Absatz 1 Buchstabe e der Richtlinie 95/46/EG.

Hauptbedenken im Zusammenhang mit der Datenaufbewahrung: sensible Daten einschließlich polizeilicher Führungszeugnisse und Daten über Verdächtigungen

63. In seiner Analyse empfiehlt der EDSB der Kommission insbesondere, sich mit dem Thema Daten aus polizeilichen Führungszeugnissen zu befassen (einschließlich aller Informationen oder „Anmerkungen“ in der Datenbank zum Inhalt dieser Führungszeugnisse, z. B. anlässlich der Ablehnung einer Kontoeröffnung oder der Sperrung eines Kontos). Nach nationalem Recht werden Einträge in das Strafregister nach Ablauf bestimmter Fristen aus den entsprechenden Datenbanken durch die Mitgliedstaaten gelöscht. Eine Pauschalregelung, der zufolge Angaben zum polizeilichen Führungszeugnis eines Kontoinhabers oder Geschäftsführers 15 Jahre lang gespeichert werden müssen, also unter Umständen noch lange nach der Löschung dieser Daten aus dem Strafregister des betreffenden Mitgliedstaats, wäre übertrieben.

64. Der EDSB unterstreicht ferner seine Bedenken bezüglich der Aufbewahrung von Daten über Konteninhaber, Bevollmächtigte oder Geschäftsführer, gegen die Ermittlungen eingeleitet wurden, vor allem, wenn in der Folge ihre Unschuld festgestellt wird. Dies kann beispielsweise der Fall sein, wenn der Antrag eines Rechtsträgers auf Eröffnung eines Kontos abgelehnt wurde, während gegen ihn wegen betrügerischer Praktiken, die Zertifikate oder Kyoto-Einheiten betreffen, ermittelt wurde. Ein Beispiel: Gemäß Artikel 20 Absatz 2 Buchstabe b kann ein nationaler Verwalter eine Kontoeröffnung ablehnen, „wenn gegen den angehenden Kontoinhaber oder – im Falle einer juristischen Person – gegen einen der Geschäftsführer ermittelt wird oder in den vorangegangenen fünf Jahren wegen betrügerischer Praktiken, die Zertifikate oder Kyoto-Einheiten betreffen, wegen Geldwäsche, Terrorismusfinanzierung oder anderer schwerer Straftaten, bei denen das Konto möglicherweise eine instrumentelle Rolle spielt, ein rechtskräftiges Urteil ergangen ist“. Ergänzt wird diese Bestimmung durch Artikel 83 Absatz 7, der besagt: „Die nationalen Verwalter stellen allen anderen nationalen Verwaltern und dem Zentralverwalter nach einem sicheren Verfahren die Namen und Identitätsangaben der Personen zur Verfügung, denen sie eine Kontoeröffnung gemäß Artikel 20 Absatz 2 abgelehnt haben […]“.

65. Es ist unerlässlich, für solche Daten angemessene und nicht übertrieben lange Aufbewahrungsfristen festzulegen, gleichgültig, ob die personenbezogenen Daten inner- oder außerhalb des Unionsregisters verarbeitet werden.

66. Um diesen Bedenken Rechnung zu tragen, empfiehlt der EDSB, in der Verordnung eindeutig festzulegen, welche Aufbewahrungsfristen für sensible Daten über Kontoinhaber und ihre Bevollmächtigten, einschließlich Daten aus polizeilichen Führungszeugnissen oder Daten über Ermittlungen oder Verdachtsfälle, gelten sollen. Folgende Bestimmungen könnten beispielsweise angemessen sein:

- Für Daten, die außerhalb des EUTL und des Unionsregisters erhoben und verarbeitet werden, könnte die Verordnung vorsehen, dass sie verhältnismäßigen Aufbewahrungsfristen unterliegen, die im Einklang mit den nationalen Rechtsvorschriften zur Umsetzung der Richtlinie 95/46/EG festgelegt werden;
- für den Fall, dass sensible Daten innerhalb des Unionsregisters oder des EUTL verarbeitet werden, oder dass sensible Daten über eine andere formalisierte Datenaustauschregelung mit den nationalen Verwaltern und dem Zentralverwalter ausgetauscht werden, sollte die Verordnung nach Anhörung der Mitgliedstaaten angemessene, nicht übertrieben lange Aufbewahrungsfristen vorgeben. Die

Festlegung eines umfassenden und kohärenten Rahmens für die Datenaufbewahrung ist besonders wichtig für die in Artikel 83 Absatz 7 vorgesehenen, regelmäßig aktualisierten Schwarzen Listen über Kontoinhaber oder Bevollmächtigte, die krimineller Aktivitäten verdächtigt werden.

Zweitrangige Bedenken

67. Es ist zweifelhaft, ob längst überholte Adressen, Telefonnummern, Passnummern oder Geburtsdaten von Geschäftsführern, die schon lange nicht mehr diese Position in den betreffenden Unternehmen bekleiden, wirklich 15 Jahre lang aufbewahrt werden müssen. Für diese und ähnliche Datenkategorien könnten vermutlich kürzere Aufbewahrungsfristen festgelegt werden.

Beginn der Aufbewahrungsfrist

68. Der EDSB empfiehlt der Kommission eine klare Aussage dazu, ab wann die Aufbewahrungsfrist läuft; dies könnte beispielsweise das Datum sein, an dem die Informationen in die elektronische Datenbank hochgeladen werden.

10. Weitere Garantien für den Datenaustausch gemäß Artikel 83 Absatz 7: Schwarze Listen von Kontoinhabern und Bevollmächtigten, die nachweislich oder vermutlich kriminellen Aktivitäten nachgehen

69. Die in Artikel 83 Absatz 7 vorgesehenen Schwarzen Listen[18] machen angemessene Datenschutzgarantien auf der praktischen Ebene erforderlich. Weiter sollte in der Verordnung zumindest Folgendes bestimmt werden:
- Die betroffenen Personen sollten in angemessener Form darüber in Kenntnis gesetzt werden, dass sie auf die Schwarze Liste gesetzt wurden;
- es sollte eine Regelung vorgesehen werden, nach der Anträge betroffener Personen auf Auskunft, Berichtigung, Sperrung oder Löschung bearbeitet werden;
- es sollte eine Regelung vorgesehen werden, die gewährleistet, dass die Informationen auf der Schwarzen Liste richtig und auf dem neuesten Stand sind;
- alle personenbezogenen Daten sollten gelöscht werden, sobald ihre Aufbewahrung nicht länger erforderlich ist (siehe hierzu auch vorstehenden Punkt 66);
- der Zugang zur Schwarzen Liste sollte klar auf nationale Verwalter und den Zentralverwalter und auf bestimmte Zwecke im Zusammenhang mit der Kontoverwaltung wie die Vermeidung des „Forum Shopping“ beschränkt werden (sofern zulässig, sollten etwaige Ausnahmen in der Verordnung eindeutig geregelt sein und angemessen begründet werden).

11. Datenübermittlungen an die „International Transaction Log“ (internationale Transaktionsprotokolliereinrichtung)

70. Zur Kommunikation von Transaktionen, mit denen Kyoto-Einheiten übertragen werden, unterhält das Unionsregister gemäß Artikel 6 Absatz 1 eine Kommunikationsverbindung mit der „International Transaction Log“ (ITL) des Rahmenübereinkommens der Vereinten Nationen über Klimaänderungen (UNFCC).

[18] Siehe vorstehenden Punkt 26.

71. Artikel Absatz 2 wiederum sieht vor, dass auch das EUTL zur Aufzeichnung und Prüfung der Übertragungen gemäß Absatz 1 eine Kommunikationsverbindung mit dem ITL unterhält.

72. In Anbetracht dieser Kommunikationsverbindungen und damit auch des Datenaustauschs im Rahmen dieser Vereinbarungen empfiehlt der EDSB, in der Verordnung klarzustellen, ob und wenn ja, welche personenbezogenen Daten an das ITL übermittelt werden. Auf jeden Fall empfiehlt der EDSB, in der Verordnung ausdrücklich zu bestimmen, dass keine besonderen Datenkategorien an das ITL übermittelt werden dürfen.

73. Wie bereits unter Punkt 32 festgestellt, kann anscheinend beispielsweise die Tatsache, dass eine Kontoeröffnung abgelehnt oder ein Konto gesperrt wurde, im Unionsregister vermerkt werden. In Kombination mit dem Namen des Kontoinhabers, der eine natürliche Person sein kann, oder mit den Namen der Kontobevollmächtigten (z. B. der Geschäftsführer) können diese Informationen als sensible personenbezogene Daten gelten. Das Übermittlungsverbot könnte für diese und ähnliche Situationen gelten.

12. Datensicherheit

74. Zum Thema Sicherheit besagt Artikel 4 Absatz 4 der Verordnung Folgendes: „Das Unionsregister erfüllt die funktionalen und technischen Spezifikationen der Datenaustauschnormen für Registrierungssysteme im Rahmen des Kyoto-Protokolls gemäß dem Beschluss 12/CMP.1 sowie die in den Datenaustausch- und technischen Spezifikationen gemäß Artikel 79 festgelegten Hardware-, Netz-, Software- und Sicherheitsauflagen“.

    Artikel 79 Absatz 2 wiederum lautet: „Die Datenaustausch- und technischen Spezifikationen werden nach Anhörung der Arbeitsgruppe der Verwalter des Ausschusses für Klimaänderung festgelegt und müssen den funktionalen und technischen Spezifikationen der Datenaustauschnormen für Registrierungssysteme im Rahmen des Kyoto-Protokolls, die gemäß dem Beschluss 12/CMP.1 festgelegt wurden, genügen“.

75. Sollte der Zentralverwalter jetzt oder in Zukunft Bediensteter der Kommission oder eines anderen Organs, einer Agentur oder Einrichtung der EU sein, empfiehlt der EDSB, auch auf die einschlägigen Bestimmungen der Verordnung (EG) Nr. 45/2001 zu verweisen (Artikel 22 und 23).

76. Darüber hinaus empfiehlt der EDSB, in die Verordnung selbst bereits ein Mindestmaß an Sicherheitsgarantien aufzunehmen. Sie könnten beispielsweise Folgendes umfassen:

- Das Unionsregister und das EUTL werden im Einklang mit einem systemspezifischen Sicherheitsplan betrieben, der nach einer umfassenden Risikobewertung und unter Berücksichtigung internationaler Standards sowie bewährter Vorgehensweisen in Mitgliedstaaten aufgestellt wurde, und
- der Sicherheitsplan sowie seine Durchführung werden regelmäßig von einem unabhängigen Dritten geprüft.

13. Schlussfolgerungen

77. Der EDSB empfiehlt, bei einer Änderung der Verordnung im weiteren Verlauf des Jahres 2012 Folgendes zu tun:

- Es sollte deutlicher gemacht werden, welche personenbezogenen Daten gemäß der Verordnung verarbeitet werden sollen und welche personenbezogenen Daten im Unionsregister und im EUTL gespeichert und verarbeitet werden. Der EDSB würde insbesondere eine allgemeine Bestimmung in der Verordnung begrüßen, der zufolge im EUTL und im Unionsregister keine besonderen Kategorien personenbezogener Daten erfasst werden (Abschnitt 4).
- Es sollte klar bestimmt werden, ob der Zentralverwalter ein Beamter der Europäischen Kommission, ein Bediensteter eines anderen Organs, einer Agentur oder Einrichtung der EU oder einer nach dem Recht eines der Mitgliedstaaten eingerichteten Stelle sein soll (Abschnitt 5).
- Für die Verteilung von Aufgaben und Zuständigkeiten sollte die Annahme einer Datenschutzstrategie gefordert werden (Abschnitt 6).
- Es sollten die Zwecke genauer bestimmt werden, für die Dritte einschließlich Europol Daten abfragen dürfen, und es sollten angemessene Garantien für die Anonymisierung bei „Data Mining“ gegeben werden (Abschnitt 7).
- Die Veröffentlichung sensibler Daten sollte untersagt werden (Abschnitt 8).
- Es sollten Änderungen bei den Aufbewahrungsfristen vorgenommen werden, um zu gewährleisten, dass die Datenaufbewahrungsanforderungen im Einklang mit den EU-Datenschutzvorschriften stehen (Abschnitt 9).
- Es sollte sichergestellt werden, dass betroffene Personen angemessen über die Tatsache in Kenntnis gesetzt werden, dass sie auf die Schwarze Liste gesetzt wurden, dass eine Regelung vorliegt, mit der das Recht betroffener Personen auf Auskunft gewahrt wird, und dass die Angaben auf der Schwarzen Liste richtig und auf dem neuesten Stand sind; es sollte für angemessene Aufbewahrungsfristen, Beschränkungen beim Zugang und bei den Zwecken, zu denen die Schwarze Liste verwendet werden darf, gesorgt werden (Abschnitt 10).
- Die Übermittlung sensibler personenbezogener Daten aus der Europäischen Union heraus, insbesondere an die internationale Transaktionsprotokolliereinrichtung, sollte untersagt werden (Abschnitt 11).
- Und es sollten nähere Angaben zu Sicherheit und Rechenschaftspflicht (Audits) gemacht werden (Abschnitt 12).

78. Des Weiteren empfiehlt der EDSB der Kommission und den Mitgliedstaaten, seine Anmerkungen bei der Umsetzung der erforderlichen Datenschutzgarantien auf der praktischen Ebene zu berücksichtigen. In diesem Zusammenhang könnte eine Datenschutzstrategie angenommen werden und könnten Informationen auf die Website des Unionsregisters gestellt, andere praxisbezogene Maßnahmen wie Hilfe-Menüs und Warnhinweise im Unionsregister erstellt und Schulungsmaterial bereitgestellt werden.

Brüssel, den 11. Mai 2012

(**unterzeichnet**)

Giovanni BUTTARELLI
Stellvertretender Europäischer Datenschutzbeauftragter