**Stellungnahme des Europäischen Datenschutzbeauftragten**

**zur Gemeinsamen Mitteilung der Kommission und der Hohen Vertreterin der Europäischen Union für Außen- und Sicherheitspolitik zur „Cybersicherheitsstrategie der Europäischen Union“ - ein offener, sicherer und geschützter Cyberraum und zum Vorschlag der Kommission für eine Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union**

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

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

## 1. EINLEITUNG

### 1.1. Konsultation des EDSB

1. Am 7. Februar 2012 nahm die Europäische Kommission und die Hohe Vertreterin der Europäischen Union für Außen- und Sicherheitspolitik eine gemeinsame Mitteilung an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über eine Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum[3] (im Folgenden: „die gemeinsame Mitteilung“ „die Cybersicherheitsstrategie “oder „die Strategie“) an.

2. Zum selben Datum nahm die Kommission einen Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur

[1] ABl. L 281 vom 23.11.1995, S. 31.
[2] ABl. L 8, 12.01.2001, S. 1.
[3] JOIN(2013) 1 final

Postanschrift: rue Wiertz 60 - B-1047 Brüssel
Dienststelle: rue Montoyer 30
E-Mail: edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax: 02-283 19 50

Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union[4] (im Folgenden: „vorgeschlagene Richtlinie“ oder der „Vorschlag“) an. Dieser Vorschlag wurde am 7. Februar 2013 dem EDSB zur Konsultation übermittelt.

3. Vor der Annahme der gemeinsamen Mitteilung hatte der EDSB die Möglichkeit, der Kommission informelle Kommentare zu übermitteln. Er begrüßt es, dass einige seiner Kommentare in der gemeinsamen Mitteilung und im Vorschlag Berücksichtigung gefunden haben.

### 1.2. Ziele der Cybersicherheitsstrategie und der vorgeschlagenen Richtlinie

4. Die gemeinsame Mitteilung richtet die Cybersicherheitsstrategie der Europäischen Union ein und enthält einen umfassenden Überblick über die Vision der EU in Bezug auf die bestmögliche Prävention und Bewältigung von Störungen und Cyberangriffen[5]. Es werden darin fünf strategische Prioritäten und Maßnahmen identifiziert.

   - Widerstandsfähigkeit gegenüber Cyberangriffen[6];
   - drastische Eindämmung der Cyberkriminalität[7];
   - Entwicklung einer Cyberverteidigungspolitik und Aufbau von Kapazitäten im Zusammenhang mit der Gemeinsamen Sicherheits- und Verteidigungspolitik (CSDP)[8];
   - Entwicklung der industriellen und technischen Ressourcen für die Cybersicherheit;
   - Entwicklung einer einheitlichen Cyberraumstrategie der EU auf internationaler Ebene und Förderung der Grundwerte der EU.

5. Abschnitt 1.2 der gemeinsamen Mitteilung sieht vor, dass die in der Cybersicherheitsstrategie identifizierten Maßnahmen auf den Grundwerten der

[4] KOM (2013) 48 endgültig.

[5] Siehe Pressemitteilung IP/13/94 der Europäischen Kommission und des Europäischen Auswärtigen Dienstes vom 7. Februar 2013.

[6] Das Konzept der Widerstandsfähigkeit gegenüber Cyberangriffen wird weder in der gemeinsamen Mitteilung noch in der vorgeschlagenen Richtlinie zur Netz- und Informationssicherheit (NIS) definiert. Er kann jedoch unter Berufung auf das Konzept der Sicherheit gemäß der in der vorgeschlagenen Richtlinie enthaltenen Definition ausgelegt werden, möglichst mit dem ergänzenden Element der Fähigkeit eines Systems, sich von den Auswirkungen eines Sicherheitsvorfalls zu erholen und zur vollen Betriebsfähigkeit zurückzukehren. Die mangelnde Klarheit in Bezug auf diesen zentralen Begriff der Mitteilung ist bedauernswert und stellt einen wichtigen Schwachpunkt der Strategie dar.

[7] Der Begriff „Cyberkriminalität“ wird in Fußnote 5 der gemeinsamen Mitteilung wie folgt definiert „*Unter dem Begriff „Cyberkriminalität“ werden unterschiedlichste kriminelle Tätigkeiten zusammengefasst, bei denen Computer und Informationssysteme entweder Hauptinstrument oder Hauptziel sind. Die Cyberkriminalität umfasst herkömmliche Straftaten (z. B. Betrug, Fälschung, Identitätsdiebstahl), inhaltsbezogene Straftaten (z. B. Verbreitung von kinderpornografischem Material über das Internet, Anstachelung zum Rassismus) und Straftaten, die nur über Computer und Informationssysteme möglich sind (z. B. Angriffe auf Informationssysteme, Überlastungsangriffe, Schadprogramme).*“

[8] Die Gemeinsame Mitteilung enthält keine Definition des Begriffs „Cyberverteidigung“. Die in diesem Bereich vorgesehenen Maßnahmen zielen darauf ab, die Robustheit der Kommunikations- und Informationssysteme zu erhöhen, die dem Schutz der Verteidigungs- und Sicherheitsinteressen der Mitgliedstaaten dienen.

Europäischen Union und dem Schutz der Grundrechte und Grundwerte basieren, die in der Charta der Grundrechte der Europäischen Union garantiert werden, insbesondere in Bezug auf die personenbezogenen Daten und den Schutz der Privatsphäre.

6. Die gemeinsame Mitteilung enthält eine gemeinsame Agenda der Mitgliedstaaten, der Kommission, des Europäischen Parlaments, des Rates, der ENISA sowie von Europol und der Industrie, die zusammenarbeiten, um die Erreichung der Zielsetzungen der Strategie zu garantieren. Es wird vorgeschlagen, alle relevanten Akteure zu einer Konferenz mit hochrangigen Vertretern einzuladen und die Fortschritte nach einem Jahr zu prüfen.

7. Die vorgeschlagene Richtlinie stellt eine der wesentlichen Maßnahmen dar, die dazu beitragen sollen, die Maßnahme Nr. 1 der Cybersicherheitsstrategie umzusetzen, d. h. die „Widerstandsfähigkeit gegenüber Cyberangriffen" zu stärken. Ziel der vorgeschlagenen Richtlinie ist die Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit (NIS) in der EU. Der Vorschlag sieht insbesondere Folgendes vor:

   - verbindliche Maßnahmen der Mitgliedstaaten zur Prävention, dem Umgang und der Reaktion in Bezug auf Sicherheitsrisiken und -vorfälle, die Netze und Informationssysteme beeinträchtigen;
   - Einrichtung eines Kooperationsmechanismus zwischen Mitgliedstaaten und der Kommission, um auf koordinierte und effiziente Weise im Rahmen einer sicheren Infrastruktur Frühwarnungen vor Sicherheitsrisiken und -vorfällen auszutauschen sowie zusammenzuarbeiten und regelmäßige gegenseitige Überprüfungen durchzuführen;
   - Verpflichtung für Marktteilnehmer und öffentliche Verwaltungen, Risikomanagementpraktiken einzuführen und erhebliche Sicherheitsvorfälle bei ihren Kerndiensten zu melden.

### 1.3. Bedeutung des Datenschutzes beim Cybersicherheitspaket und Ziel der Stellungnahme des EDSB

8. Der EDSB begrüßt es, dass die EU eine umfassende Strategie ausgearbeitet hat, um die Sicherheit im Internet zu fördern[9], die durch einen Vorschlag für eine Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit (NIS) in der EU ergänzt wird. Verschiedene Regionen der Welt haben bereits Cybersicherheitsstrategien angenommen oder sind dabei, dies zu tun, um die Risiken und Gefahren des Internets anzugehen. Deshalb war die Annahme einer Strategie der Europäischen Union von entscheidender Bedeutung, um diese Fragen auf eine Weise anzugehen, bei der auch die internationale Dimension der Gefahrenabwehr im Cyberraum berücksichtigt wird.

[9] Der Mangel einer umfassenden EU-Strategie der inneren Sicherheit wurde bereits insbesondere in der Stellungnahme des EDSB zur Mitteilung der Kommission an das Europäische Parlament und den Rat - „EU-Strategie der inneren Sicherheit: Fünf Handlungsschwerpunkte für mehr Sicherheit in Europa", herausgegeben am 17. Dezember 2010, ABl. C 101/6, hervorgehoben.

9. Die Cybersicherheitsstrategie setzt die von der EU im Bereich der Netzwerk- und Informationssicherheit (NIS) entwickelte Politik fort: Im Jahr 2001 gab die Kommission eine Mitteilung zu „Sicherheit der Netze und Informationen: Vorschlag für einen europäischen Politikansatz“[10] und im Jahr 2006 eine Strategie für eine sichere Informationsgesellschaft[11] heraus. Jahre lang lag das Schwergewicht der EU-Politik im Bereich der NIS primär auf der Sicherheit. In diesem Kontext wurden die Rechte auf Schutz der Privatsphäre und Datenschutz lange Zeit als mit der Zielsetzung kollidierend betrachtet (Sicherheit gegen Privatsphäre), weshalb diese bislang im Rahmen der EU-Politik zur NIS nur am Rande angegangen wurden. So gesehen begrüßt der EDSB die explizite Anerkennung des Rechts auf Privatsphäre und des Datenschutzes der Strategie und die Tatsache, dass diese als Grundwerte betrachtet werden, an denen sich die Cybersicherheitspolitik in der EU und auf internationaler Ebene orientieren sollte[12].

10. Angesichts der immer stärkeren Nutzung der Informations- und Kommunikationstechnologien (IKT) vertritt der EDSB die Ansicht, dass Maßnahmen, die auf die Erzielung eines hohen Maßes an Sicherheit in der Online-Umgebung abzielen, dazu beitragen werden, die Sicherheit aller darin verarbeiteten Daten zu gewährleisten, auch der personenbezogenen Daten. Der EDSB unterstreicht, dass die Sicherheit der Datenverarbeitung schon immer ein wesentliches Element des Datenschutzes gewesen ist[13]. In einem derartigen Kontext kann die Annahme einer Cybersicherheitsstrategie und der vorgeschlagenen Richtlinie über eine hohe gemeinsame Netz- und Informationssicherheit einen wesentlichen Beitrag zur Sicherstellung des Schutzes der Rechte natürlicher Personen auf Achtung der Privatsphäre und den Datenschutz in der Online-Umgebung[14] leisten.

11. Auf der anderen Seite unterstreicht der EDSB, dass die Verfolgung der Zielsetzung der Cybersicherheit zum Einsatz von Maßnahmen führen könnte, die einen Eingriff in die Rechte natürlicher Personen auf Schutz der Privatsphäre und ihrer personenbezogenen Daten darstellen können, die in der Europäischen Menschenrechtskonvention, dem Vertrag über die Arbeitsweise der Europäischen Union und der Charta der Grundrechte der EU verankert sind[15]. Der EDSB erinnert darin, dass jeder Eingriff in die Grundrechte natürlicher Personen oder deren Beschränkung mit Artikel 52 Absatz 1 der Charta der Grundrechte der EU vereinbar sein muss. Angesichts der wachsenden Menge personenbezogener Daten, die im Rahmen von Informationssystemen und Netzwerken verarbeitet werden, muss sichergestellt sein, dass alle im Rahmen der Cybersicherheitsstrategie umgesetzten

[10] KOM(2001)298.
[11] KOM(2006)251.
[12] Siehe Abschnitt 1.2, S. 3
[13] Die Sicherheitsanforderungen sind in den Artikeln 22 und 35 der Verordnung (EG) Nr. 45/2001, den Artikeln 16 und 17 der Richtlinie 95/46/EG und den Artikeln 4 und 5 der Richtlinie 2002/58/EG sowie in Artikel 7 des Übereinkommens über den Datenschutz enthalten, das 1981 im Kontext des Europarates angenommen wurde und inzwischen von allen EU-Staaten ratifiziert wurde.
[14] Siehe auch die Rede von Frau Viviane Reding, Vizepräsidentin der Europäischen Kommission „The EU's data protection rules and the Cyber Security Strategy: two sides of the same coin“, 19. Mai 2013, http://europa.eu/rapid/press-release_SPEECH-13-436_en.htm?locale=en
[15] Siehe Artikel 8 EMRK, Artikel 16 AEUV und Artikel 7 und 8 der Charta.

Maßnahmen zur Überwachung und Verbesserung der Sicherheit der Informationssysteme und Netzwerke nicht zu einem unangemessenen Eingriff in das Recht auf Privatsphäre natürlicher Personen führen, zum Beispiel indem ein unbefugter Zugriff auf deren personenbezogene Daten erfolgt.

12. Aus diesem Grund unterstreicht der EDSB, wie wichtig es ist, dass alle betroffenen Grundrechte im Rahmen der Cybersicherheitsstrategie und im Rahmen aller Maßnahmen zu deren Umsetzung gebührlich berücksichtigt werden, was auch für den Schutz natürlicher Personen vor Cybersicherheitsgefahren auf der einen Seite und den Schutz der Privatsphäre und das Recht auf Schutz ihrer personenbezogenen Daten auf der anderen Seite gilt. Der EDSB unterstreicht, dass alle etwaig in der EU umgesetzten Politiken im Bereich der Cybersicherheit und alle diesbezüglichen Maßnahmen sorgfältig abgewogen werden müssen, um mögliche unzulässige Eingriffe in die Rechte natürlicher Personen auf Schutz der Privatsphäre und ihrer personenbezogenen Daten zu vermeiden, insbesondere indem sichergestellt wird, dass sie den Grundsätzen der Notwendigkeit und Verhältnismäßigkeit sowie den anwendbaren Datenschutzvorschriften entsprechen.

13. Der EDSB stellt fest, dass in der Begründung der vorgeschlagenen Richtlinie unter Punkt 1.3 anerkannt wird, dass alle für die Datenverarbeitung Verantwortlichen nach dem Datenschutzrechtsrahmen verpflichtet sind, Sicherheitsvorkehrungen zum Schutz personenbezogener Daten zu treffen und dass diese Verpflichtung im Rahmen der laufenden Reform des Datenschutzrahmens weiterentwickelt wird, einschließlich einer Verpflichtung zur Meldung von Rechtsverletzungen. Die Cybersicherheitsstrategie erkennt ebenfalls in Abschnitt 2.1 an, dass im derzeitigen Datenschutzrahmen die für die Datenverarbeitung Verantwortlichen dafür sorgen, dass Datenschutzvorschriften eingehalten und Schutzmaßnahmen, einschließlich Sicherheitsmaßnahmen, ergriffen werden. Angesichts der Tatsache, dass ein großer Teil aller in der Strategie und der vorgeschlagenen Richtlinie berücksichtigen Netzwerk- und Informationstransaktionen die Verarbeitung personenbezogener Daten betreffen werden, ist die in den Datenschutzvorschriften enthaltene Vorschrift vermutlich die umfassendste im EU-Recht vorgesehene Netzwerk- und Informationssicherheitsvorschrift. Es muss auch festgestellt werden, dass die Grundsätze zur Einrichtung angemessener technischer und organisatorischer Sicherheitsmaßnahmen, basierend auf der Bewertung und dem Management von Risiken und angesichts des Stands der Technik und der Kosten der Maßnahme, die in der vorgeschlagenen Richtlinie enthalten sind, dieselben sind, die bereits in den Datenschutzvorschriften festgelegt werden.

14. Es ist jedoch bedauerlich, dass die Cybersicherheitsstrategie und die vorgeschlagene Richtlinie den Beitrag der bestehenden und erwarteten Datenschutzvorschriften zur Sicherheit nicht hervorheben und nicht umfassend sicherstellen, dass alle etwaigen Verpflichtungen aus der vorgeschlagenen Richtlinie oder anderen Elementen der Strategie die Datenschutzverpflichtungen ergänzen und sich nicht mit diesen überschneiden oder einander widersprechen. Die wichtige Rolle der nationalen

Datenschutzbehörden bei der Umsetzung und Vollstreckung dieser Verpflichtungen wird ebenfalls nicht ausreichend berücksichtigt. Diese Aspekte werden in den Kapiteln 2 und 3 in Bezug auf die EU-Cybersicherheitsstrategie einerseits und die vorgeschlagene Richtlinie andererseits eingehender analysiert.

## 2. ANALYSE DER EU-CYBERSICHERHEITSSTRATEGIE

### 2.1. Allgemeine Anmerkungen zur EU-Cybersicherheitsstrategie

15. Der EDSB stellt fest, dass die vorgeschlagene allgemeine Datenschutzverordnung[16] bei der Cybersicherheitsstrategie nicht berücksichtigt wurde. Auch die laufende Initiative für eine Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt[17] wurde bei der Cybersicherheitsstrategie nicht berücksichtigt. Es wird darauf in der vorgeschlagenen Richtlinie nur indirekt verwiesen, indem die Anbieter von Vertrauensdiensten aus dem Geltungsbereich ausgeschlossen werden. Es ist bedauerlich, dass die Rolle der Vertrauensdienste und der elektronischen Identifizierungsdienste bei der Ausarbeitung der Cybersicherheitsstrategie nicht angemessen analysiert wurde[18].

16. Aufgrund des Mangels einer aufmerksamen Erwägung und vollumfänglichen Berücksichtigung anderer paralleler Initiativen und laufenden Rechtssetzungsverfahren, wie der Datenschutzreform und der vorgeschlagenen Verordnung über die elektronische Identifizierung und Vertrauensdienste, gelingt es der Cybersicherheitsstrategie nicht, einen wirklich umfassenden und ganzheitlichen Überblick über die Cybersicherheit in der EU zu geben und die Risiken der Fortführung eines fragmentierten und bereichsbezogenen Ansatzes aus dem Weg zu räumen.

17. In der gemeinsamen Mitteilung wird eine Reihe von Grundsätzen hervorgehoben, wozu auch die Rechte auf Schutz der Privatsphäre und Datenschutz zählen, auf denen die Cybersicherheitspolitik in der EU und international gründen sollte. Es wird anerkannt, dass die EU einen Beitrag dazu leisten kann, indem sie die Freiheit des Internets unterstützt und die Wahrung der Grundrechte im Internet gewährleistet[19]. Der EDSB begrüßt es, dass der Schutz der Grundrechte auf Achtung der Privatsphäre und Datenschutz explizit als einen der Leitgrundsätze der Cybersicherheitsstrategie erwähnt wurde.

[16] KOM (2012) 11 endgültig
[17] KOM (2012) 238 endgültig
[18] Die in diesem Bereich aufgeworfenen Datenschutzfragen wurden in der Stellungnahme des EDSB vom 27. September 2012 zum Vorschlag der Kommission für eine Verordnung des Europäischen Parlaments und des Rates über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (Verordnung über elektronische Vertrauensdienste) unterstrichen, abrufbar im Bereich Beratung der Website des EDSB unter: www.edps.europa.eu.
[19] Siehe gemeinsame Mitteilung, S. 3

18. Der EDSB stellt ferner mit Zufriedenheit fest, dass explizite Verweise auf die Anforderungen im Hinblick auf den Schutz der Privatsphäre und den Datenschutz in verschiedenen Maßnahmen der Strategie erwähnt werden. Zum Beispiel:
    - In der gemeinsamen Mitteilung wird auf Seite 4 explizit auf Folgendes hingewiesen: „Bei jeder Weitergabe von Informationen im Interesse der Cybersicherheit müssen – soweit es um personenbezogene Daten geht – die EU-Datenschutzvorschriften eingehalten und die Rechte des Einzelnen in diesem Zusammenhang umfassend berücksichtigt werden“;
    - Der Fußnote 7 auf Seite 4 ist zu entnehmen, dass die bei Maßnahmen der Strategie, die in Zusammenhang mit dem Informationsaustausch stehen und bei denen auch personenbezogene Daten betroffen sind, die EU-Datenschutzvorschriften einzuhalten sind;
    - In Abschnitt 2.5 wird explizit auf die Notwendigkeit hingewiesen, angemessene Garantien bei der Übermittlung personenbezogener Daten an Drittstaaten zu garantieren;
    - Die Sicherheitsverpflichtungen aus den anwendbaren Datenschutzvorschriften werden explizit in Abschnitt 2.1 erwähnt;
    - Der eingebaute Schutz der Privatsphäre wird in Abschnitt 2.4 als ein Anreiz betrachtet, der von IKT-Produkthersteller und -Dienstleister gefördert wird.

19. Der EDSB stellt jedoch fest, dass die Anforderungen an den Schutz der Privatsphäre und den Datenschutz in den Abschnitten bezüglich der Bekämpfung der Cyberkriminalität und der Cyberverteidigungspolitik nicht explizit erwähnt werden. In jedem Fall, wie unten in Abschnitt 2.1.2. näher erläutert wird, müssen die Anforderungen an den Schutz der Privatsphäre und den Datenschutz auch in diesen Aktionsbereichen berücksichtigt werden.

20. Es wird begrüßt, dass auf die Rolle und die Beteiligung der Datenschutzbehörden bei der Bekämpfung der Cyberkriminalität in Abschnitt 2.1 in Bezug auf die Sensibilisierungsmaßnahmen und die vorgeschlagene Richtlinie zur Netz- und Informationssicherheit und in Abschnitt 3.2. in Bezug auf Vorfälle, bei denen unbefugt auf personenbezogene Daten zugegriffen wird, hingewiesen wird. Der EDSB unterstreicht jedoch, dass die Datenschutzbehörden bei allen Maßnahmen der Cybersicherheitsstrategie eine Rolle spielen und nicht nur bei denjenigen, bei denen diese explizit erwähnt werden. Dieser Aspekt wird weiter unten in Teil 2.1.3 näher ausgeführt.

## 2.2. Spezifische Anmerkungen zur EU-Cybersicherheitsstrategie

### *2.2.1. Abgrenzung des Geltungsumfangs der in der Cybersicherheitsstrategie geplanten Maßnahmen*

21. Die Cybersicherheitsstrategie zielt darauf ab, einen ganzheitlichen Ansatz an die „Cybersicherheit“ zu definieren, indem verschiedene Aspekte in unterschiedlichen Bereichen, wie der Widerstandsfähigkeit gegenüber Cyberangriffen, Cyberkriminalität und Cyberverteidigungspolitik angegangen werden. Der EDSB erkennt an, dass viele politische Aspekte, unter anderem

auch technische Sicherheitsaspekte, sorgfältig erwogen werden müssen, um einen angemessenen Schutz der Netzwerk- und Informationssysteme sowie der darin übermittelten Informationen zu gewährleisten. Vom Standpunkt des Datenschutzes aus vertritt der EDSB die Ansicht, dass die Maßnahmen, die zu Zwecken der Stärkung der Widerstandsfähigkeit gegenüber Cyberangriffen und zur Bekämpfung der Cyberkriminalität ergriffen werden, dadurch, dass sie die Sicherheit im digitalen Raum fördern, auch einen wichtigen Beitrag zum Schutz personenbezogener Daten im Cyberraum leisten können.

22. Im Hinblick auf die Taxonomie - und insbesondere die Definition von „Cybersicherheit", „Widerstandsfähigkeit gegenüber Cyberangriffen" und „Cyberverteidigung" stellt der EDSB fest, dass die Kommission Anstrengungen unternommen hat, um einige dieser Konzepte zu Zwecken der gemeinsamen Mitteilung zu definieren (insbesondere in den Fußnoten 4 und 5). Wie den Fußnoten in Abschnitt 1.2 oben zu entnehmen ist, erklären sich die Begriffe „Widerstandsfähigkeit gegenüber Cyberangriffen", „Cyberkriminalität" und „Cyberverteidigung" nicht notwendigerweise von selbst bzw. sind nicht klar definiert. Folglich ist nicht immer klar, was gemeint ist und deshalb ist auch der Geltungsbereich der in der gemeinsamen Mitteilung vorgesehenen Maßnahmen nicht klar. Obgleich die Mitteilung kein verbindliches Strategiedokument ist, wäre es hilfreich gewesen, diesen Begriff näher zu definieren, damit ein eindeutiges, gemeinsames Verständnis dessen, was gemeint ist, und ein klares gemeinsames Verständnis des Geltungsumfangs der in der gemeinsamen Mitteilung vorgesehenen Maßnahmen gewährleistet ist.

23. Vom Standpunkt des Datenschutzes aus betrachtet, ist die Frage der Taxonomie besonders wichtig, da diese Begriffe zur Begründung bestimmter besonderer Maßnahmen verwendet werden, die einen Eingriff in die Grundrechte darstellen, einschließlich der Rechte auf Schutz der Privatsphäre und Datenschutz. Dies ist insbesondere in Bezug auf Maßnahmen im Bereich der Widerstandsfähigkeit gegenüber Cyberangriffen und der „Cyberkriminalität" der Fall.

24. Mit Bezug auf die Maßnahmen, die darauf abzielen, die „Widerstandsfähigkeit gegenüber Cyberangriffen" zu verbessern, begrüßt es der EDSB, dass die gemeinsame Mitteilung auf die anwendbaren und vorgeschlagenen EU-Rechtsvorschriften im Bereich der Netzwerk- und Informationssicherheit Bezug nimmt. Eine der wichtigsten Maßnahmen der gemeinsamen Mitteilung in diesem Bereich besteht in der vorgeschlagenen Richtlinie zur NIS, welche darauf abzielt, einen integrierten EU-Ansatz an die Sicherheit festzulegen. Der EDSB stellt fest, dass die in diesem Bereich geplanten Maßnahmen innerhalb des (aktuellen oder zukünftigen) EU-Rechtsrahmens stattfinden würden und dass ihr Geltungsumfang folglich rechtlich klar umschrieben wäre[20].

[20] Es muss darauf hingewiesen werden, dass die in diesem Bereich vorgeschlagenen Rechtsvorschriften, wie die vorgeschlagene Richtlinie zur NIS, die in Verbindung mit der Strategie vorgelegt wurde, Auswirkungen auf den Datenschutz haben können und deshalb sorgfältig formuliert werden müssen, um etwaige unrechtmäßige Eingriffe in die Rechte auf Privatsphäre und den Datenschutz zu vermeiden.

25. In Bezug auf Maßnahmen, die darauf abzielen, die „Cyberkriminalität“ zu reduzieren, wird in der gemeinsamen Mitteilung versucht, eine Definition des Begriffs „Cyberkriminalität“ in einer Fußnote am Ende der Seite 3 zu geben. Der EDSB begrüßt diesen Versuch, den Begriff aus offensichtlichen Gründen der Rechtssicherheit zu definieren. Nach Ansicht des EDSB ist die zu diesem Zweck in der Strategie enthaltene Definition immer noch recht vage und breitgefasst, da sie generell alle „*kriminelle[n] Tätigkeiten [...], bei denen Computer und Informationssysteme entweder Hauptinstrument oder Hauptziel sind*“ *[umfasst]. (....)*“. In der gemeinsamen Mitteilung wird ferner nicht erschöpfend auf verschiedene EU-Rechtsinstrumente in diesem Bereich verwiesen[21]. Es muss jedoch angemerkt werden, dass die EU-Rechtsvorschriften nur sehr spezifische Aspekte von Straftaten behandeln, die in der Online-Umgebung begangen werden,[22] und dass es noch keine einheitlichen Rechtsvorschriften gibt, die eine umfassende Definition der Straftaten enthalten, die unter den Begriff der „Cyberkriminalität“ fallen. In Ermangelung einer gemeinsamen Definition des Begriffs „Cyberkriminalität“ im Rechtsrahmen der EU sind mehrere der in der Strategie geplanten Maßnahmen zur Bekämpfung der „Cyberkriminalität“ (wie die Maßnahmen zur Stärkung der Zusammenarbeit zwischen Strafverfolgungsbehörden) nicht eindeutig mit genauen, exakt definierten Straftaten verbunden.

26. In der gemeinsamen Mitteilung wird auch auf die Bestimmungen des Budapester Übereinkommens des Europarates über Computerkriminalität verwiesen, das einen wirksamen Rahmen für die Annahme nationaler Rechtsvorschriften zur Behandlung von Cyberkriminalität bietet. Außerdem wird im Budapester Übereinkommen eine Reihe von Straftaten erwähnt, die unter den Begriff der „Cyberkriminalität“ fallen, wie Straftaten gegen die Vertraulichkeit, die Integrität und die Verfügbarkeit von Computerdaten und Computersystemen, computerbezogene Straftaten sowie inhaltsbezogene Straftaten, wie beispielsweise die Verletzung von Urheberrechten und verbundenen Rechten. Zusätzlich zur Tatsache, dass diese Liste sehr breitgefasst ist, wie in der gemeinsamen Mitteilung unterstrichen wird, wurde das Budapester Übereinkommen auch noch nicht von allen Mitgliedstaaten ratifiziert und deshalb sind die Straftaten, die unter den Begriff „Cyberkriminalität“ fallen, im Strafrecht der EU-Mitgliedstaaten nicht harmonisiert. Wenn man ferner berücksichtigt, dass es bei den in diesem Bereich der Strafverfolgung ergriffenen Maßnahmen wahrscheinlicher ist, dass sie zu einem Eingriff in die Rechte natürlicher Personen führen, wäre eine klare und restriktive Definition von „Cyberkriminalität“ einer derart breitgefassten Definition vorzuziehen.

[21] Siehe insbesondere Abschnitt 2.2. „Durchgreifende und wirksame Rechtsvorschriften“, S. 9.

[22] Zum Beispiel: Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme; Richtlinie 2011/92/EU zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornografie; Beschluss 2001/413/JI des Rates zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln.

### *2.2.2. Anwendbarkeit der Datenschutzvorschriften auf alle Maßnahmenbereiche der EU-Cybersicherheitsstrategie*

27. Jedes Mal, wenn EU-Politiken und Rechtsvorschriften die Funktionsweise und die Nutzung von Netzwerken und Informationssystemen berühren, über welche eine ständig steigende Menge personenbezogener Daten verarbeitet werden, muss anerkannt werden, dass die Anforderungen an den Schutz der Privatsphäre und den Datenschutz eine wesentliche Rolle spielen und dass sie notwendigerweise angemessen berücksichtigt werden müssen.

28. Wie unter Punkt 18 oben erwähnt, begrüßt es der EDSB, dass in verschiedenen Punkten der gemeinsamen Mitteilung auf die Rechtsvorschriften zum Schutz der Privatsphäre und zum Datenschutz verwiesen wird: Sie werden zu Beginn der Strategie als Leitgrundsätze der Cybersicherheitsstrategie erwähnt, aber auch in den spezifischen Maßnahmen, wie denjenigen bezüglich der Widerstandsfähigkeit gegenüber Cyberangriffen, der Entwicklung der industriellen und technischen Ressourcen für die Cybersicherheit und der Entwicklung einer einheitlichen Cyberraumstrategie der EU auf internationaler Ebene sowie der Förderung der Grundwerte der EU.

29. Der EDSB stellt jedoch mit Bedauern fest, dass in den Abschnitten bezüglich der Bekämpfung der Cyberkriminalität (Abschnitt 2.2)[23] und der Entwicklung einer Cyberverteidigungspolitik (Abschnitt 2.3) kein spezifischer Verweis auf die Datenschutzbestimmungen enthalten ist. Obgleich dies in der Strategie nicht explizit angegeben wird, stellt der EDSB fest, dass zahlreiche der in diesen Bereichen geplanten Maßnahmen die Verarbeitung und den Austausch personenbezogener Daten umfassen.

30. Was den Kampf gegen die Cyberkriminalität angeht, unterstreicht der EDSB, dass die in der Strategie geplanten Maßnahmen häufig das Erfassen, den Austausch und die Bewertung von personenbezogenen Daten natürlicher Personen erforderlich machen (wie Namen und IP-Adressen), einschließlich derjenigen von Opfern von Straftaten und mutmaßlichen Straftaten, deren Verarbeitung mit spezifischen Gefahren für den Schutz der Privatsphäre und den Datenschutz dieser natürlichen Personen verbunden ist. Dies ist zum Beispiel vermutlich bei Maßnahmen der Fall, die darauf abzielen, die operativen Kapazitäten und die Koordinierung zwischen Strafverfolgungsbehörden zu verbessern. Die Verarbeitung personenbezogener Daten im Bereich der polizeilichen und justiziellen Zusammenarbeit im strafrechtlichen Bereich macht - aufgrund der eingreifenden Natur und der wesentlichen Auswirkungen, die diese Verarbeitung auf das Leben der natürlichen Personen haben kann - eine hohes Maß des Datenschutzes erforderlich.

[23] Mit Ausnahme des spezifischen Falls der Zentralstelle für die Vergabe von Internet-Namen und -Adressen (ICANN), wobei die Maßnahmen zur Zuweisung einer größeren Verantwortung an Registrierstellen für Domänennamen und zur Sicherstellung der Korrektheit der Informationen über die Eigentümer von Websites den EU-Vorschriften entsprechen müssen, einschließlich den Bestimmungen zum Datenschutz, siehe Seite 10.

31. Der Austausch personenbezogener Daten zwischen Strafverfolgungsbehörden in der EU im Kontext von Ermittlungen und der Strafverfolgung unterliegt derzeit den Datenschutzanforderungen gemäß Beschluss des Rates 2008/977/JI[24]. Ein Vorschlag für eine Richtlinie zur Regelung der Verarbeitung personenbezogener Daten im Bereich der polizeilichen und justiziellen Zusammenarbeit im strafrechtlichen Bereich wird derzeit vom Europäischen Parlament und vom Rat[25] geprüft und sollte den Rahmenbeschluss des Rates ersetzen. Dieses Instrument wird die Datenschutznorm werden, die bei der Verarbeitung von Daten durch die Strafverfolgungsbehörden in der EU angewandt werden muss, und wird sowohl die Verarbeitung personenbezogener Daten durch diese Behörden als auch den Austausch personenbezogener Daten mit anderen Empfängern regeln.

32. Wie in früheren Stellungnahmen bereits unterstrichen[26], ist der EDSB davon überzeugt, dass die Maßnahmen zur Bekämpfung der Cyberkriminalität mit sorgfältig ausgearbeiteten Datenschutzsicherungen eingesetzt werden müssen, um sicherzustellen, dass die Überwachung und die Verarbeitung personenbezogener Daten durch die Strafverfolgungsbehörden nur streng zielgerichtet sowie auf verhältnismäßige Weise und unter angemessener Berücksichtigung der Rechte der betroffenen Personen erfolgen. So sollten beispielsweise Maßnahmen, die darauf abzielen, die operativen Kapazitäten der Strafverfolgungsbehörden zu fördern, einschließlich des Europäischen Zentrums zur Bekämpfung der Cyberkriminalität, nur in Übereinstimmung mit einer klaren Rechtsgrundlage durchgeführt werden, in welcher das Ausmaß der einzusetzenden operativen Kapazitäten ausreichend präzise definiert wird (wie die Arten der bekämpften Straftaten, die Arten der operativen Instrumente, ob diese die Verarbeitung personenbezogener Daten umfassen und die Modalitäten einer solchen Verarbeitung)[27]. Eine derartige Maßnahme sollte nur dann durchgeführt werden, wenn die Bedingungen der Notwendigkeit und der Verhältnismäßigkeit erfüllt sind.

33. Mit Bezug auf den Bereich der Verteidigungspolitik, stellt der EDSB fest, dass mehrere Maßnahmen vermutlich in gewissem Maß die Verarbeitung personenbezogener Daten umfassen werden. Dies gilt beispielsweise für Maßnahmen wie die Verbesserung des Informationsaustausches und den Austausch von Informationen über Frühwarnungen oder Antworten auf Sicherheitsvorfälle zwischen zivilen und militärischen Akteuren der EU,

---

[24] 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, 30.12.2008, S. 60-71.

[25] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates um Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, KOM (2010) 010 endgültig.

[26] Siehe insbesondere die Stellungnahme des EDSB zur Mitteilung der Europäischen Kommission an den Rat und das Europäische Parlament zur Errichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität, 29. Juni 2012, abrufbar im Bereich Beratung der Website des EDSB unter: www.edps.europa.eu.

[27] Siehe auch die Stellungnahme des EDSB zum Europäischen Zentrum zur Bekämpfung der Cyberkriminalität, ebd.

welche den Austausch personenbezogener Daten zulassen können (wie IP-Adressen und Namen von Kontaktpersonen innerhalb der betroffenen Organisationen). Die Verarbeitung personenbezogener Daten in diesem Rahmen fällt in den Geltungsbereich der Verordnung (EG) Nr. 95/46. Spezifische Ausnahmen zur Beschränkung des Geltungsbereichs der Pflichten und Rechte können in diesem Fall, sofern erforderlich, gemäß Artikel 13 der genannten Richtlinie angewandt werden.

34. Abschließend und grundsätzlich unterstreicht der EDSB die Bedeutung der Definition angemessener Datenschutzsicherungen bei der Umsetzung von Maßnahmen, die auf eine verbesserte Koordinierung der verschiedenen Akteure abzielen. Die Stärkung der Koordinierung der Akteure wird in vielen Bereichen der Strategie angestrebt, wie in Bezug auf die Cyberkriminalität, die Cyberverteidigung und die Außenbeziehungen der EU. Insbesondere muss geklärt werden, ob oder ob nicht, und falls ja, mit welchen Modalitäten, eine solche Koordinierung den Austausch von personenbezogenen Daten natürlicher Personen erforderlich macht (z. B. ausschließlich zwischen zuständigen Behörden oder mit dem privaten Sektor; mit Sitz in der EU oder außerhalb der EU). Es muss sichergestellt werden, dass jede Verarbeitung personenbezogener Daten im Kontext des Koordinierungsmechanismus unter Achtung der Rechte natürlicher Personen auf Schutz der Privatsphäre und Datenschutz erfolgt. In der Strategie wurde dem Bedarf eines hohen Datenschutzniveaus bei der Übermittlung personenbezogener Daten an Drittstaaten (Abschnitt 2.5) eine gewisse Bedeutung eingeräumt, was begrüßt wird. Es sind jedoch größere Anstrengungen bei der Einrichtung der Koordinierungmechanismen erforderlich, die in der Strategie vorgesehen sind, damit angemessene Datenschutzsicherungen in Bezug auf die Modalitäten des Austausches personenbezogener Daten definiert werden.

### *2.2.3. Rolle der Datenschutzbehörden beim Schutz der Cybersicherheit*

35. Die Datenschutzbehörden spielen eine wichtige Rolle im Kontext der Cybersicherheit. Als Hüter des Rechts auf Schutz der Privatsphäre und Datenschutz von natürlichen Personen setzen sich die Datenschutzbehörden aktiv für den Schutz personenbezogener Daten sowohl offline als auch online ein. Als Teil ihres Mandats führen sie Ermittlungen durch, behandeln Beschwerden, führen Vorabkontrollen durch und geben Stellungnahmen zu Datenverarbeitungsvorgängen heraus, auch zu solchen die online und über elektronische Kommunikationsnetzwerke erfolgen[28]. Diesbezüglich muss unterstrichen werden, dass die Sicherheit personenbezogener Daten ein wichtiger Bestandteil ihrer Aufgaben ist (zum Beispiel die Überwachung der Einhaltung von Artikel 17 der Richtlinie 95/46/EG). Sie spielen weiterhin eine wichtige Rolle bei der Überwachung der Verarbeitung personenbezogener Daten, die von den Akteuren durchgeführt werden, die an der Umsetzung der Cybersicherheitsstrategie beteiligt sind.

36. Der EDSB bedauert es deshalb, dass die Datenschutzbehörden in Abschnitt 3 der Strategie sowie in der Darstellung der wichtigsten Akteure auf Seite 17

[28] Ihre Aufgaben und Befugnisse sind in Artikel 28 der Richtlinie 95/46/EG definiert.

nicht als beteiligte Akteure im Bereich der Cybersicherheit erwähnt werden. In Abschnitt 3 werden unter anderem NIS-Behörden/CERTs, Strafverfolgungsbehörden und die Verteidigungsbehörden aufgeführt, wobei der ENISA eine besondere Rolle und Verantwortung sowohl national als auch auf europäischer und internationaler Ebene zukommt. Wie oben jedoch unterstrichen, spielen die Datenschutzbehörden eine wichtige Rolle bei der Förderung der Cybersicherheit. Dies macht es erforderlich, dass die Datenschutzbehörden von den oben genannten Akteuren, aber auch unabhängig von diesen, unter Berücksichtigung ihres Mandats angemessen eingebunden werden.

37. Dies bedeutet auf der einen Seite, dass die Datenschutzbehörden bei der Umsetzung von Maßnahmen, welche die Verarbeitung personenbezogener Daten umfassen, angemessen in ihrer Eigenschaft als Aufsichtsbehörden einbezogen werden sollten. Zu den Maßnahmen, die gemäß Abschnitt 2.1 „Widerstandsfähigkeit gegenüber Cyberangriffen" ergriffen werden sollen, zählt beispielsweise auch die Durchführung eines EU-Pilotprojekts zur Bekämpfung von Botnets und Schadprogrammen**.** Angesichts der Tatsache, dass Maßnahmen in diesem Kontext den Schutz auf Privatsphäre und von personenbezogenen Daten natürlicher Personen beeinflussen könnten, empfiehlt der EDSB, dass die Umsetzung des Pilotprojekts unter Aufsicht der zuständigen Datenschutzaufsichtsbehörden erfolgt.

38. Auf der anderen Seite sollten die Datenschutzbehörden als relevante Akteure im Bereich der Cybersicherheit anerkannt werden, so dass sich die in Abschnitt 3 der Strategie angesprochene Kooperation auch auf diese erstreckt. Die Strategie erkennt in gewissem Maß den Bedarf einer solchen Kooperation mit den Datenschutzbehörden an, wenn bei Sicherheitsvorfällen vermutlich unbefugt auf personenbezogene Daten zugegriffen wurde[29]. Eine derartige Zusammenarbeit sollte jedoch nicht auf das Mandat der Datenschutzbehörden im Bereich der Ermittlung und Überwachung von Verletzungen personenbezogener Daten beschränkt sein. Die für die NIS zuständigen Behörden, CERTs, ENISA und Strafverfolgungsbehörden sollten grundsätzlich mit den Datenschutzbehörden beim Austausch bewährter Verfahren sowie bei Sensibilisierungsmaßnahmen im Bereich der Cybersicherheit zusammenarbeiten. Ebenso sollten der EDSB und die nationalen Behörden angemessen an der Konferenz mit hochrangigen Vertretern beteiligt werden, die für 2014 einberufen werden wird, um den Fortschritt bei der Umsetzung der Strategie zu bewerten, da diese in diesem Bereich beteiligte Akteure sind.

[29] Siehe S. 19.

## 3. ANALYSE DER VORGESCHLAGENEN RICHTLINIE

### 3.1. Allgemeine Empfehlungen zur vorgeschlagenen Richtlinie

#### *3.1.1. Sicherstellen, dass beim Einsatz der NIS die Datenschutzbestimmungen vollumfänglich gewährleistet sind*

39. Der EDSB begrüßt den in Artikel 1 Absatz 5 des Vorschlags enthaltenen expliziten Verweis auf den derzeit anwendbaren Datenschutzrechtsrahmen in der EU, insbesondere die Richtlinie 95/46/EG und die Richtlinie 2002/58/EG[30]. Er begrüßt ferner die Tatsache, dass der Erwägungsgrund 41 der vorgeschlagenen Richtlinie vorsieht, dass die Umsetzung der vorgeschlagenen Richtlinie im Einklang mit der Charta der Grundrechte der Europäischen Union und insbesondere den Rechten auf Achtung des Privatlebens und der Kommunikation und dem Recht auf Schutz personenbezogener Daten erfolgt. Er stellt jedoch fest, dass, obgleich der Erwägungsgrund 39 die Einhaltung der Verordnung (EG) Nr. 45/2001 in Bezug auf die Verarbeitung personenbezogener Daten durch Organe und Einrichtungen der Union erwähnt, ein derartiger Verweis in Artikel 1 Absatz 5 fehlt. Der EDSB empfiehlt den Gesetzgebern, einen derartigen Verweis auf die Verordnung (EG) Nr. 45/2001 in Artikel 1 Absatz 5 des Vorschlags einzufügen.

40. Der EDSB begrüßt es ebenso, dass im Vorschlag[31] die vorgeschlagene Datenschutzverordnung[32] zur Kenntnis genommen wird, welche die Richtlinie 95/46/EG im Hinblick auf allgemeine Bestimmungen ersetzen wird, die für die Datenverarbeitungsvorgänge durch den privaten Sektor und öffentliche Verwaltungen anwendbar sind. Artikel 1 Absatz 1 des Vorschlags unterstreicht, dass die Einhaltung dieser Bestimmung sichergestellt werden muss, wenn die vorgeschlagene Datenschutzverordnung in Kraft tritt. Artikel 17 schreibt es den Mitgliedstaaten vor, dass sichergestellt werden muss, dass die bei Sicherheitsvorfällen mit Folgen für den Schutz personenbezogener Daten vorgesehenen Sanktionen mit den Sanktionen im Einklang stehen, die in der dann rechtsverbindlichen Datenschutzverordnung vorgesehen sind.

41. Es ist jedoch zu bedauern, dass die Interaktion des gegenwärtigen und des zukünftigen Datenschutzrechtsrahmens mit der vorgeschlagenen Richtlinie zur NIS nicht eingehender analysiert wurde und dass im Vorschlag nicht genauer festgelegt wird, wie diese Interaktion funktionieren würde. Wie in den nachfolgenden Abschnitten noch näher ausgeführt wird, lässt der Vorschlag viele Fragen offen, wie:

    - das Verhältnis zwischen den darin enthaltenen Pflichten in Bezug auf die Sicherheit und andere Sicherheitsvorschriften, die in anderen

[30] 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“).
[31] Siehe Artikel 1 Absatz 5 und Artikel 17 der vorgeschlagenen Richtlinie.
[32] KOM (2012) 11 endgültig

Rechtsinstrumenten vorgesehen sind (wie der aktuelle und zukünftige Datenschutzrahmen, die Telekommunikationsrechtsvorschriften und der Vorschlag einer Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen), und das Sicherheitsniveau, das von den betroffenen Akteuren anzuwenden ist;

- die Pflichten der für NIS zuständigen Behörden im Hinblick auf das Niveau der Vertraulichkeit und Sicherheit, das diese in Bezug auf die im Rahmen des neuen Verfahrens zur Meldung von Vorfällen eingehenden Daten gewährleisten müssen;
- der Inhalt der Meldung eines Vorfalls und ob diese Meldung personenbezogene Daten bzw. welche personenbezogene Daten sie umfassen kann (im Rahmen von delegierten Rechtsakten zu entscheiden);
- die Modalitäten der Interaktion der für NIS zuständigen Behörden mit Datenschutzbehörden und mit der ENISA, falls der Vorfall Persönliches umfasst.

42. Außerdem unterstreicht der EDSB die auf die aktuellen Datenschutzvorschriften sowie die vorgeschlagene Datenschutzverordnung zurückgehende Notwendigkeit, den eingebauten Schutz der Privatsphäre und den eingebauten Datenschutz[33] bei der Gestaltung und dem Betrieb von Mechanismen zu gewährleisten, die in der vorgeschlagenen Richtlinie vorgesehen sind[34]. Der EDSB empfiehlt deshalb, dass eine Bestimmung in den Vorschlag aufgenommen wird, die vorschreibt, dass der Datenschutz schon in einer frühen Phase der Ausarbeitung der Mechanismen, die im Rahmen des Vorschlags eingerichtet werden, und im gesamten Zyklus der Prozesse, Verfahren, Organisationen, Techniken und Infrastrukturen berücksichtigt werden muss. Es sollte ein Erwägungsgrund hinzugefügt werden, um diese Anforderung auch in der vorgeschlagenen Datenschutzverordnung zu erläutern.

### *3.1.2. Der Geltungsbereich des Vorschlags*

43. Die vorgeschlagene Richtlinie schreibt den Mitgliedstaaten unter anderem vor, öffentlichen Verwaltungen und den in Artikel 3 Absatz 8 definierten „Marktteilnehmern“ Sicherheitspflichten aufzuerlegen. Die Definition von „Marktteilnehmer“ umfasst wichtige Anbieter von Diensten der Informationsgesellschaft und Betreiber kritischer Infrastrukturen in den Bereichen Energie, Verkehr, Banken, Börsen und Gesundheit. Eine nicht erschöpfende Liste der Marktteilnehmer, die in den Anwendungsbereich des Vorschlags fallen, ist in Anhang II enthalten, in dem insbesondere folgende wichtige Anbieter von Diensten der Informationsgesellschaft aufgeführt werden: Plattformen des elektronischen Geschäftsverkehrs, Internet-Zahlungs-Gateways, soziale Netze, Suchmaschinen, Cloud-Computing-Dienste und Application Stores.

[33] Siehe Artikel 23 der vorgeschlagenen Allgemeinen Datenschutzverordnung.
[34] Siehe auch die Stellungnahme des EDSB zur Mitteilung der Kommission „Die Digitale Agenda für Europa – digitale Impulse für das Wachstum in Europa“, 10. April 2013, abrufbar im Abschnitt Beratung der Website des EDSB unter: www.edps.europa.eu.

44. Obgleich die im Vorschlag enthaltene Verpflichtung zur Einhaltung von Mindestsicherheitsvorgaben durch den privaten Sektor und die öffentliche Verwaltung begrüßt wird, stellt der EDSB jedoch fest, dass mehrere Sicherheitsverpflichtungen den Anbietern elektronischer Kommunikationsnetzwerke und -dienste bereits im anwendbaren EU-Rechtsrahmen gemäß Rahmenrichtlinie 2002/21/EG und den für die Verarbeitung Verantwortlichen gemäß den Datenschutzvorschriften auferlegt wurden[35]. Der EDSB glaubt, dass ein integrierter Ansatz an die Sicherheit erforderlich ist, um die Risiken in Bezug auf die NIS zu dämpfen, was wiederum dazu beitragen könnte, die Risiken für den Schutz der Privatsphäre und den Datenschutz zu verringern. Dies ist in einer immer stärker vernetzten digitalen Umgebung, wo unbeabsichtigte und beabsichtigte Störungen leicht von einem System auf das andere übergreifen können, wichtiger denn je. Der EDSB ist der Ansicht, dass - wie in Punkt 13 oben unterstrichen - die Sicherheitsverpflichtung, die in den Datenschutzvorschriften vorgesehen ist, wahrscheinlich die umfassendste Netzwerk- und Informationssicherheitsverpflichtung des EU-Rechts ist. Diesbezüglich bietet die Richtlinie, wie weiter unten nachgewiesen wird, keinen voll integrierten Ansatz.

45. Es wird erstens im Vorschlag nicht klar und erschöpfend definiert, welche Marktteilnehmer in den Geltungsbereich des Vorschlags fallen. Der Vorschlag enthält eine nicht erschöpfende Liste der betreffenden Marktteilnehmer, die auf nicht harmonisierte Weise von den Mitgliedstaaten auf weitere Akteure erweitert werden kann. Es könnte auch die Frage aufgeworfen werden, warum bestimmte Sektoren, die eine wichtige Rolle bei der Netzwerks- und Informationssicherheit spielen, nicht in die Liste aufgenommen wurden, wie die Hersteller von Hard- und Software oder die Anbieter von Sicherheitssoftware und -diensten. Dem derzeitigen Wortlaut des Vorschlags ist ferner nicht klar zu entnehmen, ob Organe und Einrichtungen der EU in den Geltungsbereich des Vorschlags fallen. Dem Erwägungsgrund 38 gemäß scheint dies der Fall zu sein, dies sollte jedoch in Artikel 1 des Vorschlags eindeutiger ausgeführt werden. Der EDSB empfiehlt deshalb den Gesetzgebern, für mehr Klarheit und Gewissheit in Artikel 3 Absatz 8 bezüglich der Definition der Marktteilnehmer zu sorgen, die in den Geltungsbereich des Vorschlags fallen und eine erschöpfende Liste vorzusehen, die alle relevanten Akteure umfasst, um so einen vollständig harmonisierten und integrierten Ansatz an die Sicherheit in der EU zu gewährleisten. Der EDSB empfiehlt weiterhin, in Artikel 1 Absatz 2 Buchstabe c zu klären, dass der Vorschlag auch für Organe und Einrichtungen der EU anwendbar ist.

46. Zweitens wird die Annahme eines integrierten Ansatzes an die Sicherheit auch dadurch gefährdet, dass mehrere Marktteilnehmer ausdrücklich aus dem Geltungsbereich des Vorschlags ausgeschlossen werden. Artikel 1 Absatz 1[36] berücksichtigt die derzeitigen rechtlichen Anforderungen, die bereits für öffentliche Kommunikationsnetze oder öffentlich zugängliche elektronische

[35] Siehe Fußnote 13.
[36] Siehe auch Erwägungsgrund 5.

Kommunikationsdienste in der Definition gemäß Richtlinie 2002/21/EG vorgesehen sind. Artikel 1 Absatz 3 schließt diese deshalb aus dem Geltungsbereich des Vorschlags aus. Artikel 1 Absatz 3 schließt ferner Vertrauensdiensteanbieter aus dem Geltungsbereich des Vorschlags aus, da diese Gegenstand der Anforderungen der vorgeschlagenen Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt sein werden[37]. Derartige Ausschlüsse können für Verwirrung sorgen, da auf diese Weise unterschiedliche Rechtsvorschriften nebeneinander bestehen, ohne dass geklärt wird, wie diese miteinander interagieren. Insbesondere sollte geklärt werden, ob das in Richtlinie 2002/21/EG vorgesehene Sicherheitsniveau auch für diejenigen Akteure anwendbar ist, die in den Geltungsbereich der vorgeschlagenen Richtlinie fallen. Der EDSB empfiehlt, dass eine horizontalere Rolle dieses Vorschlags im Hinblick auf Sicherheitsanforderungen anerkannt wird, indem in Artikel 1 explizit ausgeführt wird, dass diese unbeschadet bestehender oder zukünftiger detaillierter Vorschriften in spezifischen Bereichen gelten (wie diejenigen für Anbieter von Vertrauensdiensten in der vorgeschlagenen Verordnung zur elektronischen Identifizierung).

## 3.2. Spezifische Anmerkungen zur vorgeschlagenen Richtlinie

### *3.2.1. Zu den in der vorgeschlagenen Richtlinie enthaltenen Definitionen*

47. Es sollte geklärt werden, ob die Definition von „Netz und Informationssystem“ gemäß Artikel 3 Absatz 1 auch private lokale Netze umfassen soll, die nicht mit dem Internet verbunden sind. Da die Kommission keine Begründung für die Auferlegung von Verpflichtungen für isolierte private Netze gibt, scheinen private Netzwerke nicht in den Geltungsbereich des Vorschlags zu fallen. Dies sollte in Artikel 3 Absatz 1 geklärt werden.

48. Die in Artikel 3 Absatz 4 enthaltene Definition von „Sicherheitsvorfall“ sollte weiter geklärt werden, auch in Bezug auf die Definition von Sicherheit in Artikel 3 Absatz 2 und die Definition von Sicherheitsrisiko gemäß Artikel 3 Absatz 3. Es ist zum Beispiel nicht klar, ob ein Angriff auf ein Informationssystem als Vorfall zu betrachten ist, wenn es dem Angreifer nicht gelingt, die Sicherheit zu beeinträchtigen. Diesbezüglich könnte auf die in Artikel 2 Buchstabe h der Datenschutzrichtlinie für elektronische Kommunikation[38] enthaltene Definition der Verletzung des Schutzes personenbezogener Daten zurückgegriffen werden, wobei die Verletzung eine Folge haben muss (Veränderung, Verlust usw.).

[37] Vgl. ebd.

[38] Artikel 2 Buchstabe h der Richtlinie 2002/58/EG in der Fassung der Richtlinie 2009/136/EG sieht vor, dass eine Verletzung des Schutzes personenbezogener Daten zu „eine[r] Verletzung der Sicherheit, die auf unbeabsichtigte oder unrechtmäßige Weise zur Vernichtung, zum Verlust, zur Veränderung und zur unbefugten Weitergabe von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übertragen, gespeichert oder auf andere Weise im Zusammenhang mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in der Gemeinschaft verarbeitet werden“.

*3.2.2. Zu den Verpflichtungen der Mitgliedstaaten hinsichtlich der Prävention, des Umgangs und der Reaktion in Bezug auf Sicherheitsrisiken und -vorfälle*

49. Artikel 5 Absätze 1 und 2 schreiben den Mitgliedstaaten vor, eine nationale NIS-Strategie und einen nationalen NIS-Kooperationsplan anzunehmen. Artikel 5 Absatz 2 enthält die Anforderungen an die nationalen NIS-Kooperationspläne. Darin ist insbesondere die Einrichtung eines Risikobewertungsplans zur Bestimmung der Risiken und zur Bewertung der Auswirkungen potenzieller Sicherheitsvorfälle vorgesehen. Der EDSB glaubt, dass die Verpflichtung, einen „Risikobewertungsplan" einzurichten, zu eng gefasst ist, da dieser Begriff andere Aktivitäten ausschließt, die zum Management der Informationssicherheitsrisiken[39] erforderlich sind, wie, um nur die wichtigsten zu nennen, die Erstellung risikobasierter Prioritätenlisten und die Risikobehandlung (Übertragung, Vermeidung, Abschwächung usw.), einschließlich der Kriterien für die Auswahl möglicher Gegenmaßnahmen und die Akzeptanz von Restrisiken. Anstatt auf eine Formulierung zurückzugreifen, die alle erforderlichen Aktionen umfasst, empfiehlt der EDSB, dass eine solche Anforderung in der „Einrichtung und Beibehaltung eines Risikomanagementrahmens" bestehen sollte (was natürlich auch eine Risikobewertungsphase umfasst).

50. Artikel 6 Absatz 1 des Vorschlags sieht die Einrichtung einer für die Netz- und Informationssicherheit zuständigen nationalen Behörde vor (im Folgenden „für die NIS zuständige Behörde"). Der EDSB begrüßt die in Artikel 6 Absatz 5 und in Artikel 15 Absatz 5 vorgesehene Verpflichtung für die für die NIS zuständige nationale Behörde, sofern angemessen, die nationale Datenschutzbehörde zu konsultieren und mit dieser zusammenzuarbeiten. Der EDSB glaubt, dass die Zusammenarbeit entscheidend ist, um einerseits sicherzustellen, dass ein hohes Sicherheitsniveau erzielt wird, und andererseits dass dem Schutz der Privatsphäre und dem Datenschutz bei den Maßnahmen zum Schutz der Sicherheit der Netzwerke und Informationssysteme gebührlich Rechnung getragen wird. Er fordert außerdem die Einbeziehung der Datenschutzbehörden in der Praxis und gegebenenfalls in die Definition und Umsetzung nationaler NIS-Strategien und -Kooperationspläne.

51. Artikel 7 sieht die Einrichtung eines IT-Notfallteams durch jeden Mitgliedstaat vor, das innerhalb der zuständigen Behörde eingerichtet werden könnte. Der EDSB empfiehlt, in Anhang I klarzustellen, dass die Datenschutzanforderungen auch Teil der wesentlichen Anforderungen sind, die von CERTs eingehalten werden müssen. Der EDSB stellt weiterhin mit Zufriedenheit fest, dass die CERTS über die nationale zuständige Behörde, die sie überwachen, sofern erforderlich, zur Ausführung ihrer Aufgaben die spezifische Zusammenarbeit der Datenschutzbehörden in Bezug auf den Schutz personenbezogener Daten anfordern können.

[39] Siehe z. B. ISO/IEC 27005:2008 Informationstechnik - IT-Sicherheitsverfahren - Leitfaden für das Informationssicherheits-Management

### *3.2.3. Zur Festlegung von Sicherheitsvorschriften für Marktteilnehmer und öffentliche Verwaltungen*

52. Der EDSB begrüßt es, dass den Marktteilnehmern und öffentlichen Verwaltungen in Artikel 14 Sicherheits- und Meldungsverpflichtungen auferlegt werden, die darauf abzielen, eine Risikomanagementkultur zu schaffen und sicherzustellen, dass die gravierendsten Sicherheitsvorfälle gemeldet werden.

53. Artikel 14 Absatz 2 sieht vor, dass öffentliche Verwaltungen und Marktteilnehmer den für die NIS zuständigen Behörden Sicherheitsvorfälle melden, die erhebliche Auswirkungen auf die Sicherheit der von ihnen bereitgestellten Kerndienste haben. Die Umstände, wann eine Meldung erforderlich ist, sowie der Inhalt und das Format der Meldung sind im Vorschlag selbst nicht definiert, werden aber im Rahmen von delegierten Rechtsakten und Durchführungsrechtsakten definiert werden. Der EDSB unterstreicht, dass es dem Text durch die Auslassung materiellrechtlicher Bestimmungen zu diesen Aspekten an ausreichender Rechtssicherheit für die Marktteilnehmer und öffentlichen Verwaltungen mangelt, die in den Geltungsbereich einer solchen Meldung fallen. Ferner sollte im Vorschlag geklärt werden, welche Arten personenbezogener Daten erfasst werden können (wie der Name von Mitarbeitern, die für die Sicherheit zuständig sind) und ob die Meldung und die diesbezüglichen Nachweise auch Einzelheiten der personenbezogenen Daten umfassen, die von einem spezifischen Sicherheitsvorfall betroffen sind, und wenn ja, in welchem Ausmaß. Der EDSB erinnert daran, dass personenbezogene Daten nur dann übermittelt werden sollten, wenn dies für die Handhabung des Sicherheitsvorfalls unbedingt erforderlich ist. Der EDSB empfiehlt, dass diese Aspekte der Meldung im Text des Vorschlags selbst im Detail dargelegt werden (siehe eine detaillierte Analyse in Abschnitt 3.2.4.) und dass angemessene Sicherungen vorgesehen werden, um einen ausreichenden Schutz der Daten sicherzustellen, die von den NIS-Behörden verarbeitet werden (ungeachtet der Tatsache, ob es sich hierbei um personenbezogene, sensible oder vertrauliche Daten handelt).

54. Der EDSB begrüßt es, dass Artikel 15 Absatz 5 ausdrücklich die enge Zusammenarbeit zwischen NIS-Behörden und Datenschutzbehörden bei der Bearbeitung von Sicherheitsvorfällen vorsieht, die zu Verletzungen des Schutzes personenbezogener Daten führen. Der EDSB empfiehlt, dass in Artikel 14 geklärt wird, dass Meldungen von Sicherheitsvorfällen gemäß Artikel 14 Absatz 2 unbeschadet der Verpflichtung zur Meldung der Verletzung des Schutzes personenbezogener Daten gemäß den anwendbaren Datenschutzvorschriften (d. h. gemäß Datenschutzrichtlinie für elektronische Kommunikation und der vorgeschlagenen Allgemeinen Datenschutzverordnung) Anwendung finden. Eine ähnliche Bestimmung ist in Artikel 15 Absatz 2 der vorgeschlagenen Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt[40] enthalten. Zusätzlich empfiehlt der EDSB, dass die wichtigsten Meldeverfahren von Sicherheitsvorfällen, die Verstöße gegen den Schutz

[40] KOM (2012) 238 endgültig, op.cit.

personenbezogener Daten umfassen, an die für NIS zuständigen Behörden ausdrücklich in einer Bestimmung des Vorschlags dargelegt werden (siehe weitere Anmerkungen in Abschnitt 3.2.4). Es muss sichergestellt sein, dass das Verfahren unter Achtung der Zuständigkeit der Datenschutzbehörden (oder anderer nationaler Regulierungsstellen gemäß Datenschutzrichtlinie für elektronische Kommunikation) durchgeführt wird.

55. In dem Vorschlag wird außerdem die Bekanntmachung der Informationen über den Sicherheitsvorfall festgelegt. Artikel 14 Absatz 4 sieht Folgendes vor: „*Die zuständige Behörde kann die Öffentlichkeit unterrichten oder die öffentliche Verwaltung und die Marktteilnehmer zur Unterrichtung verpflichten, wenn sie zu dem Schluss gelangt, dass die Bekanntmachung des Sicherheitsvorfalls im öffentlichen Interesse liegt*." Der EDSB vertritt die Auffassung, dass diese Informationen grundsätzlich keine personenbezogenen Daten von natürlichen Personen enthalten sollten, die am Sicherheitsvorfall beteiligt sind. Zum Zwecke von Artikel 14 Absatz 4 wird das öffentliche Interesse in den meisten Fällen verfolgt, indem nur anonyme oder wirkungsvoll anonymisierte Daten offengelegt werden. Falls jedoch diese Informationen auch personenbezogene Daten umfassen, weist der EDSB darauf hin, dass bei der Entscheidung der Offenlegung personenbezogener Daten ein ausgeglichenes Gleichgewicht der unterschiedlichen betroffenen Interessen gewährleistet werden muss. Diesbezüglich unterstrich der Gerichtshof im Urteil in der Rechtssache *Schecke*[41], dass die Offenlegung personenbezogener Daten (wie beispielsweise des Namens und der genauen Beträge, welche die Empfänger von EU-Mitteln erhalten haben) zu Eingriffen in die Rechte auf Schutz der Privatsphäre und Datenschutz der betroffenen natürlichen Personen führen und nur bei Bestehen der Prüfung der Notwendigkeit und der Verhältnismäßigkeit unter Berücksichtigung des verfolgten Zwecks erfolgen kann.

56. Abschließend stellt der EDSB fest, dass Artikel 14 Absatz 8 Kleinstunternehmen von den Sicherheitsverpflichtungen und der Pflicht der Meldung von Sicherheitsvorfällen gemäß Artikel 14 Absätze 1 und 2 befreit. Der EDSB unterstreicht, dass einige der in Anhang II der vorgeschlagenen Richtlinie aufgeführten Marktteilnehmer neu gegründete Unternehmen sein könnten, die ihr Geschäft als Dienstleister der Informationsgesellschaft rasch ausbauen (z. B. neue soziale Netzwerke) und bereits eine wesentliche Rolle in ihrem Marktsektor spielen. Die aktuelle Definition von Kleinstunternehmen[42] trifft auf diese unter Umständen nicht zu. Der EDSB empfiehlt den Gesetzgebern eine Änderung von Artikel 14 Absatz 8, damit der Ausschluss von Kleinstunternehmen nicht auf diejenigen Wirtschaftsteilnehmer zutrifft, die eine wesentliche Rolle bei der Erbringung von Diensten der Informationsgesellschaft spielen, z. B. aufgrund der Art der von ihnen bearbeiteten Informationen (z. B. biometrische oder sensible Daten).

[41] Verbundene Rechtssachen C-92/09 und C-93/09, *Schecke*, Randnummern 56-64.

[42] Empfehlung der Kommission 2003/361/EG vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, in welcher ein Kleinstunternehmen definiert wird als: „*ein Unternehmen [...], das weniger als 10 Personen beschäftigt und dessen Jahresumsatz bzw. Jahresbilanz 2 Mio. EUR nicht überschreitet*."

3.2.4. *Zum Austausch von Informationen über NIS-Vorfälle und Bedrohungen mit der für die NIS zuständigen Behörde und innerhalb des Kooperationsnetzwerks.*

57. Gemäß der in Artikel 14 enthaltenen Meldepflicht sind die Marktteilnehmer und öffentlichen Verwaltungen verpflichtet, Informationen über NIS-Vorfälle mit der zuständigen NIS-Behörde auszutauschen. Obgleich der Inhalt einer solchen Meldung und die Arten von Daten, die den für die NIS zuständigen Behörden mitgeteilt werden müssen, im Vorschlag nicht aufgeführt sind, kann davon ausgegangen werden, dass die Meldungen Informationen, die als vertraulich zu betrachten sind, sowie auch personenbezogene Daten sensibler Art enthalten würden.

58. Die mit den für die NIS zuständigen Behörden ausgetauschten personenbezogenen Daten können zum Beispiel Namen und Kontaktdaten des Sicherheitspersonals bei den meldenden Organisationen sowie die IP-Adressen umfassen, die als Teil der technischen Daten in Bezug auf den Sicherheitsvorfall zur Verfügung gestellt werden. Diese IP-Adressen können sich auf die natürlichen Personen beziehen, die vom Vorfall betroffen sind, sowie auf die natürlichen Personen, die zu einem gewissen Zeitpunkt in den Verdacht geraten, für den Vorfall verantwortlich zu sein. Obgleich die meldende Organisation und die für die NIS zuständige Behörde nicht notwendigerweise in der Lage wäre, die IP-Adresse direkt mit einer identifizierten Person in Verbindung zu treffen, stellen diese IP-Adressen dennoch personenbezogene Daten dar, da sie eine indirekte Identifizierung der dahinter stehenden Person erlauben (über den Anbieter von Internetdiensten oder auf anderem Wege). Eine derartige Identifizierung könnte außerdem während der Untersuchung entweder von der für die NIS zuständigen Behörde oder von den Strafverfolgungsbehörden beantragt werden, an welche diese Daten gemäß Artikel 10 Absatz 4 und Artikel 15 Absatz 4 weiter übermittelt werden können. Der EDSB unterstreicht, dass die Verarbeitung personenbezogener Daten durch die für die NIS zuständigen Behörden nur dann für rechtmäßig betrachtet werden kann, wenn sie auf einer angemessenen Rechtsgrundlage gemäß Artikel 7 der Richtlinie 95/46/EG basiert und zur Erreichung des Zweckes angemessen ist (Grundsatz der Verhältnismäßigkeit). Dies wird nachfolgend näher erörtert werden.

59. Der EDSB stellt weiterhin fest, dass alle etwaig von den für die NIS zuständigen Behörden erhobenen Informationen mit anderen Empfängern geteilt werden können. Artikel 15 Absatz 4 sieht vor, dass die für die NIS zuständigen Behörden den Strafverfolgungsbehörden Sicherheitsvorfälle melden, bei denen ein schwerwiegender krimineller Hintergrund vermutet wird. Die Informationen, die von den für die NIS zuständigen Behörden erhoben werden, können auch innerhalb eines Kooperationsnetzwerkes ausgetauscht werden, das aus den in der EU für die NIS zuständigen Behörden sowie der Kommission besteht. Ziel dieses Kooperationsnetzwerks ist es, einen strukturierten und koordinierten Informationsaustausch sowie eine koordinierte Aufdeckung (über ein Frühwarnungsverfahren gemäß Artikel 10) und eine koordinierte Reaktion (über ein Verfahren zur koordinierten Antwort gemäß Artikel 11) bezüglich der NIS zu ermöglichen. Andere betroffene EU-

Einrichtungen, einschließlich der ENISA (Artikel 8 Absatz 2), das bei Europol angesiedelte Europäische Zentrum zur Bekämpfung der Cyberkriminalität und die Datenschutzbehörden (Artikel 8 Absatz 3 Buchstabe f), können das Kooperationsnetzwerk auf Anfrage unterstützen und die Informationen können mit diesen ausgetauscht werden. Nachstehend folgt eine Bewertung der Frage, ob eine ausreichende Rechtsgrundlage für den Austausch personenbezogener Daten mit diesen weiteren Empfängern gegeben ist und welche Sicherungen vorgesehen werden sollten, um die Rechte natürlicher Personen im Kontext eines derartigen Informationsaustausches zu schützen.

*Die Rechtsgrundlage für die Verarbeitung und den Austausch personenbezogener Daten im Rahmen der vorgeschlagenen Richtlinie*

60. In Artikel 1 Absatz 6 der vorgeschlagenen Richtlinie wird anerkannt, dass die Meldung von NIS-Vorfällen und der Austausch von Informationen im Kooperationsnetzwerk die Verarbeitung personenbezogener Daten erforderlich machen kann. Gemäß diesen Bestimmungen ist die Verarbeitung personenbezogener Daten zu diesen Zwecken nach Artikel 7 der Richtlinie 95/46/EG notwendig, „*um die mit dieser Richtlinie verfolgten Ziele des öffentlichen Interesses zu erreichen* (...)". In Erwägungsgrund 39 der vorgeschlagenen Richtlinie wird hinzugefügt, dass die Verarbeitung „*[i]m Hinblick auf diesen legitimen Zweck […] weder unverhältnismäßig [ist ]noch handelt es sich um einen nicht tragbaren Eingriff, der das [...] verbriefte Recht auf den Schutz personenbezogener Daten in ihrem Wesensgehalt antastet*." Aus diesem Grund sieht Artikel 1 Absatz 6 vor, dass eine derartige Verarbeitung „*von den Mitgliedstaaten nach Artikel 7 der Richtlinie 95/46/EG und der Richtlinie 2002/58/EG in ihrer in einzelstaatliches Recht umgesetzten Form genehmigt*" wird.

61. In Artikel 7 der Richtlinie 95/46/EG sind sechs spezifische und ausschließliche Rechtsgrundlagen aufgeführt, welche die Verarbeitung personenbezogener Daten rechtfertigen können. Es ist jedoch dem Erwägungsgrund 39 und dem Artikel 1 Absatz 6 des Vorschlags nicht zu entnehmen, welche dieser Rechtsgrundlagen die Verarbeitung personenbezogener Daten seitens der zuständigen Behörde zu Zwecken des Umgangs mit NIS-Sicherheitsvorfällen und zu Zwecken des Austausches von Informationen mit anderen zuständigen Behörden rechtfertigen würde. Nach Ansicht des EDSB kann eine derartige Verarbeitung gemäß Artikel 7 Buchstabe e der Richtlinie 95/46/EG gerechtfertigt sein, da diese „*für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt und dem für die Verarbeitung Verantwortlichen oder dem Dritten, dem die Daten übermittelt werden, übertragen wurde*". Deshalb empfiehlt er, dass in Artikel 1 Absatz 6 des Vorschlags angegeben wird, dass die Verarbeitung gemäß Artikel 7 Buchstabe e der Richtlinie 95/46/EG gerechtfertigt wäre, da sie notwendig ist, um die mit der vorgeschlagenen Richtlinie verfolgten Ziele des öffentlichen Interesses zu erreichen.

62. Der EDSB unterstreicht jedoch, dass den Grundsätzen der Notwendigkeit und der Verhältnismäßigkeit gebührend Rechnung getragen werden muss, so dass

nur Daten, die zur Erreichung des verfolgten Ziels unbedingt erforderlich sind, verarbeitet werden. Dies muss nicht nur seitens der öffentlichen Verwaltungen und der Marktteilnehmer sichergestellt werden, die vom Sicherheitsvorfall betroffen sind und die diesbezügliche Daten verarbeiten, sondern auch (i) bei Erfassung der personenbezogenen Daten durch die für die NIS zuständigen Behörden (d. h. im Vorfallmeldungsformular), (ii) bei der Gestaltung des strukturierten Informationsaustausches durch das Kooperationsnetzwerk und (iii) bei der weiteren Übermittlung personenbezogener Daten an andere Empfänger (insbesondere zuständige Behörden auf nationaler und EU-Ebene).

*Sicherstellung der Verhältnismäßigkeit bei der Verarbeitung und dem Austausch personenbezogener Daten*

63. Bei der Erfassung der Daten sollte im Meldungsformular angegeben werden, dass die personenbezogenen Daten strukturell erfasst werden (zum Beispiel der Name der innerhalb der Organisation für die Sicherheit zuständigen Person). Es sollte auch eindeutig angegeben werden, ob und unter welchen Bedingungen die Organisation Einzelheiten der IP-Adressen aufführen sollte, die aus den technischen Berichten hervorgehen, in denen beschrieben wird, was in den IT-Systemen und Netzwerken zum Zeitpunkt des Sicherheitsvorfalls vorgegangen ist. Ferner sollten Angaben dazu gemacht werden, ob unbefugt auf personenbezogene Daten zugegriffen wurde.

64. Falls dies der Fall ist, sollten spezifische Verfahren für den Umgang mit diesen Fällen seitens der für die NIS zuständigen Behörden zusammen mit den Datenschutzbehörden vorgesehen sein. Nach Ansicht des EDSB muss sichergestellt sein, dass das Ausmaß der Verarbeitung personenbezogener Daten durch die für die NIS zuständigen Behörden deren Mandat entspricht und es zu keiner Überschneidung mit den Aufgaben der Datenschutzbehörden kommt. Während die Datenschutzbehörden als Teil ihres Mandats befugt sind, bei Bedarf Zugang zu personenbezogenen Daten zu erhalten[43], um einen unbefugten Zugang zu personenbezogenen Daten einzuschätzen und Abhilfe zu schaffen, können es die Aufgaben der für die NIS zuständigen Behörden eventuell nicht notwendigerweise erforderlich machen, dass diese alle Einzelheiten der personenbezogenen Daten kennen, auf die unbefugt zugegriffen wurde. Angesichts der Tatsache, dass die Verarbeitung personenbezogener Daten durch die Datenschutzbehörden im Kontext von Untersuchungen bei Verletzungen der Datensicherheit nur bei Bedarf erfolgt, sollten die für die NIS zuständigen Behörden, deren Mandat die Ermittlung von Verletzungen der Datensicherheit nicht umfasst, umso mehr nur dann befugt sein, personenbezogene Daten zu erheben und zu verarbeiten, wenn dies im Rahmen eines Sicherheitsvorfalls unbedingt erforderlich ist.

65. Der EDSB empfiehlt, dass alle oben genannten Aspekte im Vorschlag geklärt werden, zumindest die Hauptelemente. Derzeit sieht Artikel 14 Absatz 7 vor, dass die Kommission ermächtigt ist, mittels Durchführungsrechtsakten die für

[43] Wie insbesondere in Artikel 28 Absatz 3 der Richtlinie 95/46/EG, in dem die Befugnisse der Datenschutzbehörden definiert sind, und in Artikel 15 Buchstabe a Absatz 3 der Datenschutzrichtlinie im Bereich der elektronischen Kommunikation Richtlinie 2002/58/EG, zuletzt geändert durch die Richtlinie 2009/136/EG, vorgesehen.

die Meldung geltenden Formen und Verfahren festzulegen. Es sollten jedoch in Artikel 14 spezifische Anforderungen aufgenommen werden, um (i) die Arten personenbezogener Daten anzugeben, die den für die NIS zuständigen Behörden gemeldet werden sollten (siehe Randnummern 53 und 63 oben), (ii) Sicherungen bezüglich der Verarbeitung personenbezogener Daten durch die für die NIS zuständigen Behörden vorzusehen, damit diese zur Erreichung des verfolgten Ziels verhältnismäßig bleibt und (iii) Einzelheiten zu den Verfahren der Zusammenarbeit der für die NIS zuständigen Behörden mit den Datenschutzbehörden für die Fälle vorzusehen, in denen der Vorfall den unbefugten Zugriff auf personenbezogene Daten umfasst (z. B. wie werden die Datenschutzbehörden informiert, welche Informationen sollten ihnen übermittelt werden, wie sollten sie in der Lage sein, ihre Antwort auf den Vorfall und mögliche Sanktionen zu koordinieren).

66. Was den weiteren Austausch personenbezogener Daten durch die für die NIS zuständigen Behörden mit anderen Empfängern (innerhalb und außerhalb des Kooperationsnetzwerks) angeht, muss sichergestellt werden, dass (i) die personenbezogenen Daten nur an Empfänger weitergeleitet werden, deren Verarbeitung zur Wahrnehmung ihrer Aufgaben in Übereinstimmung mit einer angemessenen Rechtsgrundlage erforderlich ist und dass (ii) diese Informationen auf das beschränkt werden, was zur Wahrnehmung ihrer Aufgaben erforderlich ist. Diesbezüglich kann die Offenlegung einiger oder aller vorliegenden personenbezogenen Daten durch die für die NIS zuständigen Behörden unter Berücksichtigung der Aufgaben und des Mandats nicht immer zur Zusammenarbeit mit anderen zuständigen Behörden notwendig sein. Die für die NIS zuständige Behörde muss vor der Offenlegung etwaiger personenbezogener Daten an externe Empfänger eine Einzelfallprüfung vornehmen, um festzustellen, ob und in welchem Ausmaß personenbezogene Daten diesem Empfänger mitgeteilt werden sollten. Der EDSB empfiehlt, dass dem Vorschlag spezifische Bestimmungen hinzugefügt werden, um diese Grundsätze hervorzuheben.

67. Ferner ist dem Grundsatz der Zweckbindung Rechnung zu tragen. Wenn die Organisation, die die Daten dem Netzwerk zum Austausch von Informationen ursprünglich zur Verfügung gestellt hat, die Zwecke, zu denen die Informationen verarbeitet werden, nicht mit ausreichender Gewissheit bestimmen kann und diese weiterübermittelt werden könnten, kann sie gezwungen sein, die Bereitstellung personenbezogener Daten über einen Vorfall zu Beginn stark einzuschränken und weitere Details nur als Antwort auf einzelne begründete Anfragen offenzulegen. Dies könnte die Zweckmäßigkeit des Netzwerks beachtlich reduzieren.

*Weitere Anforderungen an die Verarbeitung und den Austausch von Informationen*

68. Der EDSB unterstreicht, dass auch die anderen in den anwendbaren Rechtsvorschriften vorgesehenen Datenschutzanforderungen erfüllt werden müssen. Viele dieser Anforderungen müssten explizit im Vorschlag genannt werden, um effektive Sicherungen zu bieten. So müssten beispielsweise die für die NIS zuständigen Behörden sicherstellen, dass die personenbezogenen

Daten nicht länger als für den Zweck erforderlich aufbewahrt werden, für den sie erhoben werden. Dies wird es erforderlich machen, dass ein angemessener Zeitrahmen für die Aufbewahrung personenbezogener Daten zu den in der vorgeschlagenen Richtlinie vorgesehenen Zwecken definiert wird, insbesondere im Hinblick auf die Aufbewahrung durch die für die NIS zuständigen Behörden und innerhalb der sicheren Infrastruktur des Kooperationsnetzwerks.

69. Ferner könnten die betroffenen Personen, wie in Artikel 10 und 11 der Richtlinie 95/46/EG festgelegt, über die Identität des für die Verarbeitung Verantwortlichen, den Zweck der Verarbeitung, die Arten der verarbeiteten Daten, die Empfänger der Daten und ihre Datenschutzrechte besser informiert werden, wenn eindeutige diesbezügliche Modalitäten im Text des Vorschlags selbst definiert würden. Derartige Details sollten dem Vorschlag zusammen mit einem Hinweis hinzugefügt werden, in dem die für die NIS zuständigen Behörden daran erinnert werden, dass sie weiterhin dafür verantwortlich sind, dass derartige Informationen über die Verarbeitung personenbezogener Daten leicht zugänglich sind, zum Beispiel mittels Veröffentlichung einer Datenschutzerklärung auf ihrer Website.

70. Ferner ist der EDSB der Ansicht, dass es von größter Bedeutung ist, dass die von den für die NIS zuständigen Behörden verarbeiteten Daten, die mit anderen Empfängern ausgetauscht werden, in der Phase der Verarbeitung angemessen gesichert sind. Der EDSB begrüßt es, dass Artikel 9 die Einrichtung eines sicheren Systems für den Informationsaustausch zur Unterstützung des Kooperationsnetzwerks beim Austausch sensibler und vertraulicher Informationen vorsieht. Der EDSB bedauert jedoch, dass der Vorschlag keine spezifischen Bestimmungen bezüglich des Sicherheitsniveaus vorsieht, das von den für die NIS zuständigen Behörden in Bezug auf deren Datenverarbeitung gewährleistet werden muss. Der EDSB empfiehlt den Gesetzgebern, in den Vorschlag eine spezifische Bestimmung in Bezug auf die Sicherheit der von für die NIS zuständigen Behörden erhobenen, verarbeiteten und ausgetauschten Informationen aufzunehmen. Ein Verweis auf die Sicherheitsanforderungen gemäß Artikel 17 der Richtlinie 95/46/EG sollte insbesondere bezüglich des Schutzes personenbezogener Daten durch die für die NIS zuständigen Behörden aufgenommen werden.

71. Gemäß Artikel 9 Absatz 2 kann die Kommission die Kriterien der Teilnahme der Mitgliedstaaten am sicheren System im Rahmen von delegierten Rechtsakten erlassen. Der EDSB unterstreicht, dass diese Kriterien definiert werden sollten, um sicherzustellen, dass ein hohes Niveau der Sicherheit und der Widerstandsfähigkeit gegen Cyberangriffe seitens aller Teilnehmer der Systeme für den Informationsaustausch während aller Verarbeitungsschritte gewährleistet ist. Der EDSB unterstreicht, dass die Kommission in Bezug auf ihre Teilnahme am sicheren System für den Informationsaustausch (insbesondere da sie gemäß Artikel 8 aktiv am Netzwerk teilnehmen wird, indem sie Informationen empfängt und austauscht) ebenfalls an diese Kriterien gebunden sein sollte. Zu diesen Kriterien zählen auch angemessene Maßnahmen zur Gewährleistung der Vertraulichkeit und Sicherheit, die von den Mitgliedstaaten und der Kommission umgesetzt werden müssen, um die

im System verarbeiteten personenbezogenen Daten gemäß Artikel 16 und 17 der Richtlinie 05/46/EG und Artikel 21 und 22 der Verordnung (EG) Nr. 45/2001 zu schützen. Der EDSB empfiehlt, dass dies in Artikel 9 des Vorschlags unterstrichen wird.

72. Der EDSB stellt fest, dass die vorgeschlagene Richtlinie die Verfahren zur Einrichtung, zum Betrieb und zum Management des Systems für den Informationsaustausch nicht explizit festlegt. Es sollte unter anderem geklärt werden, ob die Kommission bei der Einrichtung, dem Betrieb und der Instandhaltung der sicheren Infrastruktur eine Rolle spielen wird. Dies wird auch Auswirkungen auf die Verantwortlichkeiten der Kommission im Hinblick auf die etwaige Verarbeitung personenbezogener Daten im Rahmen dieser Infrastruktur nach Verordnung (EG) Nr. 45/2001 haben. Aus diesem Grund empfiehlt der EDSB, dass in Artikel 9 eine Beschreibung der jeweiligen Rollen und Verantwortlichkeiten der Kommission und der Mitgliedstaaten beim Aufbau, dem Betrieb und der Instandhaltung des sicheren Systems für den Informationsaustausch eingefügt wird. Der EDSB empfiehlt, dass der Vorschlag Mindestsicherheitsanforderungen und Datenschutzgrundsätze für die Datenqualität mit Bezug auf den Betrieb des Systems für den Informationsaustausch vorsieht. Ferner schlägt der EDSB vor, dass im Vorschlag explizit angeführt wird, dass die Gestaltung des Systems in Übereinstimmung mit den Grundsätzen des eingebauten Datenschutzes und der eingebauten Sicherheit erfolgen sollte.[44]

73. Abschließend begrüßt es der EDSB, dass Artikel 13 vorsieht, dass die Zusammenarbeit der Mitglieder des Kooperationsnetzwerks mit internationalen Partnern auf der Grundlage internationaler Vereinbarungen erfolgen soll, wodurch einem angemessenen Schutz der im Kooperationsnetz zirkulierenden personenbezogenen Daten Rechnung getragen wird. Der EDSB erinnert daran, dass jede Übermittlung personenbezogener Daten an Empfänger in Staaten außerhalb der EU gemäß den Artikeln 25 und 26 der Richtlinie 95/46/EG und Artikel 9 der Verordnung (EG) Nr. 45/2001 erfolgen muss.

## 4. SCHLUSSFOLGERUNGEN

74. Der EDSB begrüßt es, dass die Kommission und die Hohe Vertreterin der Europäischen Union für Außen- und Sicherheitspolitik eine umfassende Cybersicherheitsstrategie vorgelegt haben, die durch einen Vorschlag für eine Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit (NIS) in der EU ergänzt wird. Diese Strategie ergänzt die politischen Maßnahmen, die von der EU bereits im Bereich der Netz- und Informationssicherheit entwickelt wurden.

75. Der EDSB begrüßt es, dass die Strategie über den traditionellen Ansatz der Dichotomie von Sicherheit und Datenschutz hinausgeht, indem explizit der

[44] Siehe Text der gemeinsamen Mitteilung auf Seite 28 bezüglich der Empfehlungen an öffentliche und private Akteure zur Verabschiedung der Grundsätze für eingebaute Schutz- und Sicherheitsfunktionen.

Schutz der Privatsphäre und der Datenschutz als Grundwerte anerkannt werden, an denen sich die Cybersicherheitspolitik in der EU und auf internationaler Ebene orientieren sollte. Der EDSB stellt fest, dass die Cybersicherheitsstrategie und die vorgeschlagene Richtlinie über NIS wesentlich zur Wahrung der Rechte natürlicher Personen auf Schutz der Privatsphäre und Datenschutz in der Online-Umgebung beitragen können. Gleichzeitig muss sichergestellt werden, dass sie nicht zu Maßnahmen führen, die einen unrechtmäßigen Eingriff in die Rechte natürlicher Personen auf Privatsphäre und Datenschutz darstellen.

76. Der EDSB begrüßt auch, dass der Datenschutz in verschiedenen Teilen der Strategie erwähnt und in der vorgeschlagenen Richtlinie über NIS berücksichtigt wird. Es ist jedoch bedauerlich, dass die Strategie und die vorgeschlagene Richtlinie den Beitrag der bestehenden und erwarteten Datenschutzvorschriften zur Sicherheit nicht hervorheben und nicht umfassend sicherstellen, dass alle etwaigen Verpflichtungen aus der vorgeschlagenen Richtlinie oder anderen Elementen der Strategie die Datenschutzverpflichtungen ergänzen und sich nicht mit diesen überschneiden oder einander widersprechen.

77. Ferner stellt der EDSB fest, dass aufgrund des Mangels einer aufmerksamen Erwägung und vollumfänglichen Berücksichtigung anderer paralleler Initiativen und laufender Rechtssetzungsverfahren, wie der Datenschutzreform und der vorgeschlagenen Verordnung über die elektronische Identifizierung und Vertrauensdienste, es der Cybersicherheitsstrategie nicht gelingt, einen wirklich umfassenden und ganzheitlichen Überblick über die Cybersicherheit in der EU zu geben und die Risiken der Fortführung eines fragmentierten und bereichsbezogenen Ansatzes aus dem Weg zu räumen. Der EDSB stellt auch fest, dass die vorgeschlagene Richtlinie über die NIS auch noch keinen umfassenden Ansatz im Hinblick auf die Sicherheit in der EU enthält und dass die in den Datenschutzvorschriften vorgesehenen Verpflichtungen vermutlich die umfassendste Netzwerk- und Sicherheitsverpflichtung im EU-Recht darstellen.

78. Ferner bedauert es der EDSB, dass die wichtige Rolle der Datenschutzbehörden bei der Umsetzung und der Vollstreckung der Sicherheitsverpflichtungen und der Förderung der Cybersicherheit nicht ausreichend berücksichtigt wird.

79. Was die Cybersicherheitsstrategie angeht, unterstreicht der EDSB Folgendes:

- Eine klare Definition der Begriffe „Widerstandsfähigkeit gegenüber Cyberangriffen“, „Cyberkriminalität“ und „Cyberverteidigung“ ist besonders wichtig, da diese Begriffe zur Begründung bestimmter besonderer Maßnahmen verwendet werden, die einen Eingriff in die Grundrechte darstellen, einschließlich der Rechte auf Schutz der Privatsphäre und Datenschutz. Die in der Strategie und im Übereinkommen über Cyberkriminalität verwendeten Begriffe sind jedoch sehr breitgefasst. Es wäre jedoch ratsam, eine klare und restriktive

Definition von „Cyberkriminalität“ vorzusehen anstelle einer derart weitgefassten Begriffsbestimmung.

- Die Datenschutzvorschriften sollten auf alle Maßnahmen der Strategie Anwendung finden, sofern sie Maßnahmen betreffen, welche die Verarbeitung personenbezogener Daten zulassen. Obgleich die Datenschutzvorschriften in den Abschnitten zur Cyberkriminalität und zur Cyberverteidigung nicht explizit erwähnt werden, unterstreicht der EDSB, dass viele der in diesen Bereichen geplanten Maßnahmen die Verarbeitung personenbezogener Daten umfassen und sie folglich in den Geltungsbereich der anwendbaren Datenschutzbestimmungen fallen. Er stellt auch fest, dass viele der Maßnahmen darin bestehen, Koordinierungsmechanismen einzurichten, welche die Umsetzung angemessener Datenschutzsicherungen im Hinblick auf die Verfahren zum Austausch personenbezogener Daten erforderlich machen.

- Die Datenschutzbehörden spielen eine wichtige Rolle im Kontext der Cybersicherheit. Als Hüter des Rechts auf Schutz der Privatsphäre und Datenschutz der natürlichen Personen setzen sich die Datenschutzbehörden aktiv für den Schutz personenbezogener Daten sowohl offline als auch online ein. Deshalb sollten sie in ihrer Rolle als Überwachungsorgane in Bezug auf die Umsetzungsmaßnahmen, die die Verarbeitung personenbezogener Daten umfassen (wie die Einführung des EU-Pilotprojekts zur Bekämpfung von Botnets und Schadprogrammen), angemessen eingebunden werden. Weitere Akteure im Bereich der Cybersicherheit sollten bei der Wahrnehmung ihrer Aufgaben ebenfalls mit ihnen zusammenarbeiten, zum Beispiel beim Austausch bewährter Praktiken und Sensibilisierungsmaßnahmen. Der EDSB und die nationalen Behörden sollten auch angemessen an der Konferenz mit hochrangigen Vertretern beteiligt werden, die für 2014 einberufen werden wird, um den Fortschritt bei der Umsetzung der Strategie zu bewerten.

80. Im Hinblick auf die vorgeschlagene Richtlinie über NIS empfiehlt der EDSB den Gesetzgebern Folgendes:

- Es sollte für mehr Klarheit und Gewissheit in Artikel 3 Absatz 8 bezüglich der Definition der Marktteilnehmer gesorgt werden, die in den Geltungsbereich des Vorschlags fallen und eine erschöpfende Liste vorgesehen werden, die alle relevanten Akteure umfasst, um so einen vollständig harmonisierten und integrierten Ansatz an die Sicherheit in der EU zu gewährleisten.

- In Artikel 1 Absatz 2 Buchstabe c sollte geklärt werden, dass die vorgeschlagene Richtlinie für EU-Organe und Einrichtungen Anwendung findet und es sollte ein Verweis auf die Verordnung (EG) Nr. 45/2011 in Artikel 1 Absatz 5 des Vorschlags aufgenommen werden.

- Es sollte eine horizontalere Rolle dieses Vorschlags im Hinblick auf die Sicherheit anerkannt werden, indem in Artikel 1 explizit ausgeführt wird, dass diese unbeschadet bestehender oder zukünftiger detaillierter

Vorschriften in spezifischen Bereichen gelten (wie diejenigen für Anbieter von Vertrauensdiensten in der vorgeschlagenen Verordnung zur elektronischen Identifizierung).

- Es sollte ein Erwägungsgrund hinzugefügt werden, der vorschreibt, dass der eingebaute Datenschutz schon in einer frühen Phase der Ausarbeitung der Mechanismen, die im Rahmen des Vorschlags eingerichtet werden und im gesamten Zyklus der Prozesse, Verfahren, Organisationen, Techniken und Infrastrukturen berücksichtigt werden muss, wobei der vorgeschlagenen Datenschutzverordnung Rechnung getragen werden muss.

- Die Definitionen der Begriffe „Netze und Informationssysteme“ in Artikel 3 Absatz 1 und „Sicherheitsvorfall“ in Artikel 3 Absatz 4 sollten geklärt werden und in Artikel 5 Absatz 2 sollte die Verpflichtung zur Einrichtung eines „Risikobewertungsplans“ durch die „Einrichtung und Beibehaltung eines Risikomanagementrahmens“ ersetzt werden.

- In Artikel 1 Absatz 6 des Vorschlags sollte angegeben werden, dass die Verarbeitung personenbezogener Daten gemäß Artikel 7 Buchstabe e der Richtlinie 95/46/EG gerechtfertigt wäre, da sie notwendig ist, um die mit dieser vorgeschlagenen Richtlinie verfolgten Ziele des öffentlichen Interesses zu erreichen. Den Grundsätzen der Notwendigkeit und der Verhältnismäßigkeit muss jedoch gebührlich Rechnung getragen werden, so dass nur Daten, die zur Erreichung des verfolgten Ziels unbedingt erforderlich sind, verarbeitet werden.

- In Artikel 14 müssen die Umstände dargelegt werden, unter denen eine Meldung erforderlich ist, sowie der Inhalt und das Format der Meldung, einschließlich der Arten von personenbezogenen Daten, die gemeldet werden sollten, sowie ob oder ob nicht und in welchem Maß die Meldung und die Belege Einzelheiten zu den personenbezogen Daten enthalten, die Gegenstand eines spezifischen Sicherheitsvorfalls sind (z. B. IP-Adressen). Es muss die Tatsache berücksichtigt werden, dass es den für die NIS zuständigen Behörden gestattet werden sollte, personenbezogene Daten im Zusammenhang mit einem Sicherheitsvorfall nur dann zu erheben und zu verarbeiten, wenn dies unbedingt erforderlich ist. Es sollten ferner im Vorschlag angemessene Sicherungen vorgesehen werden, um einen angemessenen Schutz der Daten sicherzustellen, die von den für die NIS zuständigen Behörden verarbeitet werden.

- In Artikel 14 sollte geklärt werden, dass Meldungen von Sicherheitsvorfällen gemäß Artikel 14 Absatz 2 unbeschadet der Verpflichtung zur Meldung der Verletzung des Schutzes personenbezogener Daten gemäß den anwendbaren Datenschutzvorschriften Anwendung finden. Es sollten in dem Vorschlag die wichtigsten Aspekte des Verfahrens der Kooperation zwischen der für die NIS zuständigen Behörden und den Datenschutzbehörden im Hinblick auf Fälle dargelegt werden, in denen ein Sicherheitsvorfall zu einer Verletzung personenbezogener Daten geführt hat.

- Artikel 14 Absatz 8 sollte so geändert werden, dass der Ausschluss von Kleinstunternehmen aus dem Geltungsbereich der Meldung nicht auf diejenigen Wirtschaftsteilnehmer zutrifft, die eine wesentliche Rolle bei der Erbringung von Diensten der Informationsgesellschaft spielen, z. B. aufgrund der Art der von ihnen bearbeiteten Informationen (z. B. biometrische oder sensible Daten).

- Es sollten Bestimmungen zur Regelung des weiteren Austausches personenbezogener Daten durch die für die NIS zuständigen Behörden mit anderen Empfängern hinzugefügt werden, um sicherzustellen, dass (i) die personenbezogenen Daten nur an Empfänger weitergeleitet werden, deren Verarbeitung zur Wahrnehmung ihrer Aufgaben in Übereinstimmung mit einer angemessenen Rechtsgrundlage erforderlich ist und dass (ii) diese Informationen auf das beschränkt werden, was zu Wahrnehmung ihrer Aufgaben erforderlich ist. Es sollte berücksichtigt werden, wie Einrichtungen, die Daten an das System für den Informationsaustausch übermitteln, die Einhaltung des Grundsatzes der Zweckbindung sicherstellen.

- Es sollte der Zeitrahmen für die Aufbewahrung personenbezogener Daten zu den in der vorgeschlagenen Richtlinie vorgesehenen Zwecken definiert werden, insbesondere im Hinblick auf die Aufbewahrung durch die für die NIS zuständigen Behörden und innerhalb der sicheren Infrastruktur des Kooperationsnetzwerks.

- Die für die NIS zuständigen Behörden sollten an ihre Verpflichtung erinnert werden, die betroffenen Personen angemessen über die Verarbeitung ihrer personenbezogenen Daten zu informieren, zum Beispiel, indem auf ihrer Website eine Datenschutzerklärung veröffentlicht wird.

- Es sollte eine Bestimmung bezüglich des Sicherheitsniveaus hinzugefügt werden, welches von den für die NIS zuständigen Behörden in Bezug auf die erhobenen, verarbeiteten und ausgetauschten Daten gewährleistet werden muss. Ein Verweis auf die Sicherheitsanforderungen gemäß Artikel 17 der Richtlinie 95/46/EG sollte insbesondere bezüglich des Schutzes personenbezogener Daten durch die für die NIS zuständigen Behörden vorgesehen werden.

- In Artikel 9 Absatz 2 sollte geklärt werden, dass die Kriterien für die Teilnahme der Mitgliedstaaten am sicheren System für den Informationsaustausch sicherstellen sollten, dass ein hohes Maß der Sicherheit und der Widerstandsfähigkeit gegenüber Cyberangriffen von allen Teilnehmern der Systeme für den Informationsaustausch während aller Verarbeitungsschritte gewährleistet wird. Diese Kriterien sollten angemessene Maßnahmen zur Wahrung der Vertraulichkeit und Sicherheit gemäß Artikel 16 und 17 der Richtlinie 95/46/EG und Artikel 21 und 22 der Verordnung (EG) Nr. 45/2001 umfassen. Die Kommission sollte explizit verpflichtet werden, diese Kriterien im Hinblick auf ihre

Teilnahme am sicheren System für den Informationsaustausch in ihrer Rolle als für die Verarbeitung Verantwortliche zu erfüllen.

- In Artikel 9 sollte eine Beschreibung der Rollen und Verantwortlichkeiten der Kommission und der Mitgliedstaaten bei der Einrichtung, dem Betrieb und der Instandhaltung des sicheren Systems zum Informationsaustausch hinzugefügt werden, und es sollte vorgesehen werden, dass die Gestaltung des Systems den Grundsätzen des eingebauten Datenschutzes und der eingebauten Sicherheit entspricht.

- In Artikel 13 sollte hinzugefügt werden, dass jede Übermittlung personenbezogener Daten an Empfänger in Staaten außerhalb der EU in Übereinstimmung mit den Artikeln 25 und 26 der Richtlinie 95/46/EG und Artikel 9 der Verordnung (EG) Nr. 45/2001 erfolgen muss.

Brüssel, den 14. Juni 2013

**(unterzeichnet)**

Peter HUSTINX
Der Europäische Datenschutzbeauftragte