Zusammenfassung der 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 vollständige Text dieser Stellungnahme ist in englischer, französischer und deutscher Sprache auf der Internetpräsenz des EDSB unter http://www.edps.europa.eu erhältlich)

(2014/C 32/10)

1. **Einleitung**

1.1 *Konsultation des EDSB*

1. Am 7. Februar 2013 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 [1] (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 Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union [2] (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.

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 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

[1] JOIN(2013) 1 final.
[2] KOM(2013) 48 endgültig.

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

Peter HUSTINX

Europäischer Datenschutzbeauftragter