Stellungnahme des Europäischen Datenschutzbeauftragten

zur Mitteilung der Europäischen Kommission an den Rat und das Europäische Parlament zur Errichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität

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],

gestützt auf den Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008[3] über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden,

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. EINLEITUNG

1.1. Konsultation des EDSB

1. Am 28. März 2012 nahm die Kommission eine Mitteilung mit folgendem Titel an: „Kriminalitätsbekämpfung im digitalen Zeitalter: Errichtung eines Europäischen Zentrums zur Bekämpfung von Cyberkriminalität“[4].

[1] ABl. L 281 vom 23.11.1995, S. 31.
[2] ABl. L 8 vom 12.1.2001, S. 1.
[3] ABl. L 350 vom 30.12.2008, S. 60.
[4] Cyberkriminalität ist im EU-Recht nicht definiert.

Postanschrift: Rue Wiertz 60 – 1047 Brüssel, Belgien
Dienststelle: Rue Montoyer 63
E-Mail: edps@edps.europa.eu – Website: www.edps.europa.eu
Tel.: +32 (0)2 283 19 00 – Fax: +32 (0)2 283 19 50

2. Der EDSB stellt fest, dass der Rat am 7.-8. Juni 2012 die Schlussfolgerungen zur Errichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität angenommen hat[5]. Der Rat billigt die Zielsetzungen der Mitteilung, unterstützt die Errichtung des Zentrums (nachfolgend auch als „EC3" bezeichnet) innerhalb von Europol und die Nutzung bestehender Strukturen zur Zusammenarbeit mit anderen Bereichen der Kriminalitätsbekämpfung, bestätigt, dass das EC3 als Anlaufstelle im Kampf gegen die Cyberkriminalität dienen soll, dass das EC3 eng mit den relevanten Agenturen und Akteuren auf internationaler Ebene zusammenarbeiten soll und ruft die Kommission in Konzertation mit Europol dazu auf, den Umfang der spezifischen Aufgaben auszuarbeiten, die erforderlich sind, um dafür zu sorgen, dass das EC3 vor Ende 2013 seinen Betrieb aufnehmen kann. In den Schlussfolgerungen wird jedoch nicht auf die Bedeutung der Grundrechte und insbesondere auf den Datenschutz im Zusammenhang mit der Errichtung des EC3 verwiesen.

3. Vor Annahme der Mitteilung der Kommission hatte der EDSB die Möglichkeit, informell zum Entwurf der Mitteilung Stellung zu nehmen. Im Rahmen dieser informellen Anmerkungen unterstrich der EDSB, dass der Datenschutz ein wesentlicher Aspekt ist, der bei der Einrichtung des Europäischen Zentrums zur Bekämpfung der Cyberkriminalität berücksichtigt werden muss. Leider wurden diese informellen Anmerkungen bei Ausarbeitung der Mitteilung nicht berücksichtigt. Außerdem wird in den Schlussfolgerungen des Rates gefordert, dass das Zentrum bereits im nächsten Jahr seinen Betrieb aufnehmen soll. Aus diesem Grund ist der Datenschutz bei den nächsten Schritten, die bereits in Kürze ergriffen werden, zu berücksichtigen.

4. In der vorliegenden Stellungnahme wird auf die Bedeutung des Datenschutzes bei der Errichtung des EC3 eingegangen. Sie enthält spezifische Vorschläge, die bei der Ausarbeitung des Mandats des EC3 und der legislativen Überprüfung des rechtlichen Rahmens von Europol berücksichtigt werden sollten. Aus diesem Grund nahm der EDSB gemäß Artikel 41 Absatz 2 der Verordnung (EG) Nr. 45/2005 die vorliegende Stellungnahme in Eigeninitiative an.

1.2. **Anwendungsbereich der Mitteilung**

5. In ihrer Mitteilung verkündete die Kommission als vorrangiges Ziel der Strategie der inneren Sicherheit die Absicht, ein Europäisches Zentrum zur Bekämpfung der Cyberkriminalität zu errichten.[6]

6. Die Mitteilung enthält eine unvollständige Liste der verschiedenen Formen der Cyberkriminalität mit denen sich das Zentrum vorrangig befassen sollte: von organisierten kriminellen Vereinigungen begangene Cyberstraftaten, insbesondere Straftaten mit hohen illegalen Erträgen (z. B. Online-Betrug), Cyberstraftaten mit schwerwiegenden Folgen für die Opfer (z. B. mit Hilfe des Internets begangener sexueller Missbrauch von Kindern) und Cyberstraftaten (einschließlich Cyberangriffe) gegen kritische Infrastrukturen und Informationssysteme in der Union.

---

[5] Schlussfolgerungen des Rates zur Errichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität, 3127. Sitzung des Rates JUSTIZ und INNERES, Luxemburg, 7. und 8. Juni 2012.

[6] EU-Strategie der inneren Sicherheit: Fünf Handlungsschwerpunkte für mehr Sicherheit in Europa. KOM(2010)673 endgültig, 22. November 2010. Siehe auch die Stellungnahme des EDSB zu dieser Mitteilung vom 17. Dezember 2010, ABl. C 101/6.

7. Was die Arbeit des Zentrums angeht, werden in der Mitteilung vier Kernaufgaben aufgeführt[7]:
   - ihre Funktion als Europäische Anlaufstelle für Informationen über Cyberstraftaten;
   - ihre Funktion als Europäische Sammelstelle für cyberkriminalitätsspezifisches Fachwissen zur Unterstützung der Mitgliedstaaten beim Aufbau geeigneter Kapazitäten;
   - die Unterstützung der von den Mitgliedstaaten durchgeführten Untersuchungen über Cyberstraftaten;
   - Sprachrohr aller mit Untersuchungen über Cyberstraftaten befassten Strafverfolgungs- und Justizbediensteten in der EU.

8. Die vom EC3 verarbeiteten Daten werden *aus umfangreichen öffentlichen, privaten und offenen Quellen zusammengetragen*, reichern die verfügbaren polizeilichen Daten an und betreffen *Informationen über Cyberstraftaten, über die Vorgehensweisen der Täter und über verdächtige Personen*. Das EC3 wird auch direkt mit anderen europäischen Agenturen und Einrichtungen zusammenarbeiten. Dies geschieht durch die Mitwirkung dieser Akteure im Programmausschuss des EC3 und durch eine je nach Bedarf erfolgende operative Zusammenarbeit.

9. Nach Ansicht der Kommission wäre das EC3 die optimale Schnittstelle zu den von Interpol ergriffenen Maßnahmen zur Bekämpfung der Cyberkriminalität und zu anderen internationalen Polizeidienststellen. Das EC3 sollte auch, gemeinsam mit Interpol und den strategischen Partnern in aller Welt an besser koordinierten Antworten für die Bekämpfung von Cyberstraftaten arbeiten.

10. Praktisch schlägt die Kommission vor, das EC3 als Teil von Europol einzurichten. Das EC3 wird *Teil von Europol*[8] und folglich dem Rechtsrahmen von Europol unterstellt sein[9].

11. Nach Ansicht der Kommission[10], bestehen die wichtigsten Neuerungen der aktuellen Aktivitäten von Europol, zu denen es aufgrund des vorgeschlagenen EC3 kommen wird, in: (i) mehr Ressourcen zur effizienten Einholung von Informationen aus verschiedenen Quellen (ii) Informationsaustausch mit Partnern außerhalb des Strafverfolgungsbereichs (hauptsächlich aus dem privaten Sektor).

1.3. Schwerpunkt der Stellungnahme

12. Der EDSB beabsichtigt mit dieser Stellungnahme:
   - die Kommission aufzufordern, den Bereich der Aktivitäten des EC3 zu klären, soweit diese für den Datenschutz relevant sind;
   - die vorgesehenen Aktivitäten im Kontext des aktuellen Rechtsrahmens von Europol zu bewerten, insbesondere deren Vereinbarkeit mit dem Rechtsrahmen;

[7] Mitteilung S. 4-5.

[8] Wie in der im Februar 2012 veröffentlichten Machbarkeitsstudie empfohlen, in der die verschiedenen verfügbaren Optionen bewerten wurden (Status quo, innerhalb von Europol, Teil von Europol, virtuelles Zentrum). http://ec.europa.eu/home-affairs/doc_centre/crime/docs/20120311_final_report_feasibility_study_for_a_european_cybercrime_centre.pdf.

[9] Entscheidung des Rats vom 6. April 2009 zur Errichtung des Europäischen Polizeiamts (Europol) (2009/371/JI).

[10] Pressemitteilung vom 28. März, Frequently Asked Questions: the new European Cybercrime Centre Reference: MEMO/12/221, Datum: 28.3.2012 http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/221.

- die relevanten Aspekte hervorzuheben, bei denen der Gesetzgeber im Kontext der zukünftigen Revision des rechtlichen Rahmens von Europol weiter ins Detail gehen sollte, um ein höheres Datenschutzniveau sicherzustellen.

13. Die Stellungnahme ist folgendermaßen aufgebaut: In Teil 2.1 wird ausgeführt, warum der Datenschutz ein wesentliches Element bei der Errichtung des EC3 ist. In Teil 2.2 wird auf die Vereinbarkeit der in der Mitteilung für das EC3 vorgesehenen Ziele mit dem Rechtsmandat von Europol eingegangen. Teil 2.3. befasst sich mit der Zusammenarbeit mit dem privaten Sektor und internationalen Partnern.

2. ANMERKUNGEN

2.1. Datenschutz als wesentliches Element der Errichtung des Zentrums

14. Der EDSB betrachtet die Bekämpfung der Cyberkriminalität als Grundstein der Gewährleistung von Sicherheit im digitalen Raum und der Schaffung des erforderlichen Vertrauens. Sie kann auch die Sicherheit im digitalen Raum fördern und folglich das Datenschutzniveau in diesem Bereich verbessern. Der Schutz natürlicher Personen im virtuellen Raum wird grundsätzlich davon profitieren, wenn das Zentrum seine Ziele erreicht und zugleich die Grundrechte, insbesondere das Recht auf Datenschutz, in vollem Umfang gewahrt werden. Vor diesem Hintergrund möchte der EDSB unterstreichen, dass er die Einrichtung von Mechanismen zur Bekämpfung der Cyberkriminalität, wie das vorgeschlagene Zentrum, unterstützt.

15. Die Bekämpfung der Cyberkriminalität wird häufig die Verarbeitung personenbezogener Daten im Rahmen der Ermittlungen erforderlich machen. Es besteht folglich die Gefahr von Eingriffen in die Privatsphäre der Bürger. Aus diesem Grund sollten bei den Zielsetzungen des EC3 auch die Bedenken bezüglich des Schutzes der Privatsphäre berücksichtigt werden.

16. Der EDSB ist davon überzeugt, dass effektive Maßnahmen zur Bekämpfung der Cyberkriminalität ohne solide ergänzende Datenschutzmaßnahmen nicht umgesetzt werden können. Es werden angemessene Garantien dafür benötigt, dass die Überwachung und Verarbeitung personenbezogener Daten grundsätzlich nur zielgerichtet erfolgt und dass dem Missbrauch dieses Mechanismuses durch angemessene Maßnahmen vorgebeugt wird. Der EDSB möchte sicherstellen, dass diese Überwachung innerhalb eines klaren Rahmenwerks mit angemessenen Datenschutzgarantien erfolgt.

17. Leider wird in der Mitteilung der Datenschutz nicht als ein bei den Aktivitäten des Zentrums zu berücksichtigendes Element erwähnt. Der EDSB fordert die Kommission auf zu berücksichtigen, dass die Aktivitäten des EC3 auf soliden Datenschutzbestimmungen basieren sollten und dass dies bei dessen Errichtung sich sowohl im Mandat des Zentrums als auch bei der vorgesehenen Überprüfung des rechtlichen Rahmens von Europol widerspiegeln sollte.

2.2. Vereinbarkeit der Zielsetzungen des EC3 mit dem offiziellen Auftrag von Europol

Vom Europol Cyber Crime Center zum EC3

18. Der EDSB stellt fest, dass kein spezifisches Rechtsinstrument zur Errichtung des EC3 vorgesehen ist. Das Zentrum wird auf bestehenden Strukturen basieren. Das Zentrum wird im Sitz von Europol eingerichtet und die Aktivitäten des EC3 müssen deshalb mit den Bestimmungen des Europol-Ratsbeschlusses vereinbar sein, einschließlich des Rahmens für den Datenschutz von Europol.

19. Europol unterstützt die Mitgliedstaaten bei der Bekämpfung der Cyberkriminalität seit 2002, als das High Tech Crime Centre von Europol eingerichtet wurde. In der Folge hat Europol eine europäische Plattform entwickelt, um den Bedürfnissen der Mitgliedstaaten im Zusammenhang mit der Bekämpfung der Cyberkriminalität nachzukommen.

20. Laut dem allgemeinen Bericht über die Tätigkeit von Europol 2011[11] wurde 2011 ein „Europol Cyber Crime Centre" eingerichtet, und gemäß den im Bericht aufgeführten Ergebnissen hat dieses Zentrum bereits einen wichtigen Beitrag zur Bekämpfung der Cyberkriminalität geleistet[12]. Dies führt zu der Frage, was im Hinblick auf die Tätigkeiten und Aufgaben in der Mitteilung der Kommission neu ist, da das Europol Cyber Crime Centre bereits seit 2011 innerhalb von Europol besteht.

21. In der Mitteilung wird auf diese bereits bestehende Tätigkeit von Europol nicht Bezug genommen, sie scheint vielmehr auf die Errichtung einer gänzlich neuen Struktur innerhalb von Europol ausgerichtet zu sein. In diesem Sinne fordert der EDSB mehr Klarheit bezüglich der neuen für das EC3 vorgesehenen Tätigkeit sowie eine Analyse der Auswirkungen in Bezug auf den Datenschutz.

Straftaten, bei denen das EC3 Ermittlungen durchführen wird

22. Der EDSB stellt fest, wie wichtig es ist, zu überprüfen, ob die in der Mitteilung enthaltenen Ziele des EC3 mit dem aktuellen rechtlichen Rahmen von Europol und insbesondere mit dem aktuellen Auftrag vereinbar sind.

23. Gemäß Artikel 4 Absatz 1 des Europol-Beschlusses und des Anhangs zählt auch die Bekämpfung von „Computerkriminalität" zum Zuständigkeitsbereich von Europol. Das Konzept von „Computerkriminalität" ist allerdings nicht definiert, weder im Europol-Beschluss noch in irgendeinem anderen EU-Rechtsakt. Die Begriffe „Computerkriminalität" und „Cyberkriminalität" sind miteinander verbunden, jedoch nicht notwendigerweise identisch. Es kann auch nicht automatisch davon ausgegangen werden, dass alle Aufgaben, die das EC3 übernehmen soll, auch unter die Aufgaben von Europol fallen.

---

[11] Allgemeiner Bericht über die Tätigkeit von Europol 2011, 10036/12, ENFOPOL 141, Brüssel, 24. Mai 2012.

[12] „*In 2011, Europol supported major cybercrime operations Crossbill (malware) and Mariposa II (Butterfly bots). In the area of online child exploitation, Europol supported Operation Rescue in a successful bid to take down a worldwide network of child sex-offenders. Operation Icarus is another such operation involving 23 countries*." (Europol unterstützte 2011 im Bereich der Cyberkriminalität die wichtigen Ermittlungen Crossbill ('Malware') und Mariposa II ('Butterfly Bots'). Im Bereich der Online-Ausbeutung von Kindern unterstützte Europol die Operation Rescue, bei der es gelang, ein weltweites Netzwerk von pädophilen Sexualstraftätern zu Fall zu bringen. Die Operation Icarus ist eine weitere derartige Operation unter Beteiligung von 23 Staaten.) Siehe S. 59 des Europol-Berichts für 2011, der weitere Informationen enthält.

24. In Ermangelung einer rechtlichen Definition von Cyberkriminalität in den EU-Rechtsvorschriften ist der EDSB der Ansicht, dass es wichtig ist, die Kompetenzen des Zentrums zu definieren. Es sollte zumindest geklärt werden, welche „Arten von Cyberkriminalität" untersucht werden sollen. Dabei sollte beispielsweise festgelegt werden, ob sich das EC3 mit bestimmten Straftaten, die bereits im EU-Rechtsrahmen vorgesehen sind, befassen soll oder nicht:

    - Rahmenbeschluss 2005/222/JI des Rates über Angriffe auf Informationssysteme[13] und die vorgeschlagene Richtlinie[14], die den Rahmenbeschluss ersetzen wird. Der Rahmenbeschluss umfasst beispielsweise den rechtswidrigen Zugang zu Informationssystemen, den rechtswidrigen Systemeingriff und die rechtswidrige Bearbeitung von Daten;
    - Richtlinie 2011/92/EU zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornografie[15]. Dies umfasst beispielsweise Bilder von sexuellem Kindesmissbrauch, die mit Hilfe von neuen Technologien und dem Internet verbreitet werden;
    - Beschluss 2001/413/JI des Rates zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln. Dies umfasst beispielsweise die Ausführung oder Veranlassung einer Übertragung von Geld oder monetären Werten mit der Absicht, dem Zuwiderhandelnden oder einem Dritten einen unzulässigen Vermögensvorteil zu verschaffen, durch die unrechtmäßige Eingabe, Veränderung, Löschung oder Unterdrückung von Computerdaten, insbesondere von Identifikationsdaten, oder das unrechtmäßige Eingreifen in den Ablauf eines Computerprogramms oder den Betrieb eines Computersystems.

25. Außerdem arbeitet die Kommission derzeit als Teil der Europäischen Strategie für das Identitätsmanagement an einem Vorschlag zur Kriminalisierung des Identitätsdiebstahls. Darüber hinaus wird in der Budapester Konvention zur Cyberkriminalität von 2001[16] eine Reihe von Straftaten erwähnt, 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. Es sollte geklärt werden, ob auch all diese Straftaten abgedeckt sind.

26. Da das Rechtsinstrument, das die Rechtsgrundlage für die Tätigkeit des Zentrums darstellen wird, der aktuelle Europol-Rechtsrahmen ist, der derzeit überarbeitet wird[17], empfiehlt der EDSB, dass im Rahmen dieses Überarbeitungsverfahrens unter anderem auch die Definition der Kompetenzen des EC3 berücksichtigt wird.

---

[13] Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme, ABl. L 69, 16.3.2005, S. 67-71.

[14] Der Vorschlag 2010/273 für eine Richtlinie des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme und zur Aufhebung des Rahmenbeschlusses 2005/222/JI des Rates befindet sich derzeit im ordentlichen Gesetzgebungsverfahren.

[15] Richtlinie 2011/92/EU vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates, ABl. L 335 vom 27.11.2011, S. 1-14.

[16] Konvention zur Cyberkriminalität, Budapest, 23.11.2001.
http://conventions.coe.int/Treaty/en/Treaties/html/185.htm

[17] Gemäß Artikel 88 Absatz 2 des Vertrags über die Arbeitsweise der Europäischen Union legen das Europäische Parlament und der Rat gemäß dem ordentlichen Gesetzgebungsverfahren den Aufbau, die Arbeitsweise, den Tätigkeitsbereich und die Aufgaben von Europol fest. Das Arbeitsprogramm der Europäischen Kommission 2012 umfasst diese Rechtsetzungsinitiative unter Punkt 64.
http://ec.europa.eu/atwork/programmes/docs/cwp2012_annex_en.pdf

27. Der EDSB empfiehlt außerdem, dass bis zur Anwendbarkeit des überarbeiteten Rechtsrahmens der Tätigkeitsbereich des EC3 zumindest in der Form eines Mandats definiert werden sollte[18]. Dieses Mandat sollte vor Beginn der Tätigkeit des EC3 (gemäß Mitteilung, vor Ende 2013) festgelegt werden und sollte unter anderem festlegen, welche Straftaten in die Zuständigkeit des EC3 fallen und welche nicht.

Operative Unterstützungsaktivitäten des EC3

28. Das EC3 wird - laut Mitteilung - „*operative Unterstützung*" für Untersuchungen über Cyberstraftaten leisten und beispielsweise die Einsetzung gemeinsamer Untersuchungsteams fördern. Eine der vorgeschlagenen Aufgaben ist es, „*hochwertige computerforensische Unterstützung in Form von Anlagen, Speichermöglichkeiten und Tools sowie Sachverständigenwissen auf dem Gebiet der Datenverschlüsselung für Untersuchungen über Cyberdelikte zur Verfügung zu stellen*."[19] Ein weiteres in der Mitteilung enthaltenes Beispiel ist die Arbeit eines Europol-Analysten, der bei einer früheren Ermittlung die Sicherheitsvorkehrungen eines Computersystems „geknackt"[20] hat.

29. Die allgemeine Rechtsgrundlage in Artikel 88 AEUV[21] definiert die Aufgaben von Europol und wird im Europol-Beschluss weiter ausgeführt. Artikel 5 Absatz 2 des Europol-Beschlusses definiert dessen Aufgaben im Detail, wozu auch die Unterstützung der Mitgliedstaaten mittels Unterstützung, Beratung und Nachforschungen bezüglich „*kriminaltechnischen und kriminalwissenschaftlichen Methoden und Analysen sowie Ermittlungsmethoden*" zählen sowie „*die Unterstützung der Mitgliedstaaten bei der Erhebung und Analyse von Informationen aus dem Internet, um bei der Aufdeckung von kriminellen Handlungen zu helfen, die durch das Internet erleichtert oder über das Internet begangen wurden*".

30. Gemäß Artikel 6 des Europol-Ratsbeschlusses kann das Europol-Personal in unterstützender Funktion an gemeinsamen Ermittlungsgruppen teilnehmen, nicht jedoch an der Ergreifung von Zwangsmaßnahmen.

31. Die im Ratsbeschluss definierten Aufgaben von Europol sind generell beschränkt auf die Unterstützung durch Bereitstellung der Kenntnis bewährter Praktiken und Analyse von Informationen. Die Grenze zwischen operativen und unterstützenden Tätigkeiten ist im Bereich der Cyberkriminalität jedoch ganz unklar: Sicherheitsvorkehrungen eines Computersystems zu „*knacken*" oder „*operative Unterstützung*" zu leisten, kann in einigen Fällen über die Bereitstellung von Unterstützung und Kenntnis hinausgehen. Folglich empfiehlt der EDSB:

    - im Kontext der Bekämpfung der Cyberkriminalität eindeutig zu definieren, welche Art der operativen Unterstützung das Personal des Zentrums erbringen kann und in welchem Ausmaß, ob allein oder in Zusammenarbeit mit gemeinsamen Ermittlungsteams und

[18] Gemäß Artikel 37 Absatz 7 Buchstabe c des Europol-Ratsbeschlusses trifft der Verwaltungsrat Entscheidungen oder erlässt Durchführungsmaßnahmen nach Maßgabe dieses Beschlusses.
[19] Mitteilung, S. 5.
[20] Ebenda.
[21] Gemäß Artikel 88 Absatz 1 hat Europol den Auftrag, die Tätigkeit der Polizeibehörden und der anderen Strafverfolgungsbehörden der Mitgliedstaaten sowie deren gegenseitige Zusammenarbeit bei der Verhütung und Bekämpfung der zwei oder mehr Mitgliedstaaten betreffenden schweren Kriminalität, des Terrorismus und der Kriminalitätsformen, die ein gemeinsames Interesse verletzen, das Gegenstand einer Politik der Union ist, zu unterstützen.

- klare Verfahren für die Bereitstellung operativer Unterstützung festzulegen, die auf der einen Seite die Einhaltung der Rechte natürlicher Personen und insbesondere des Rechts auf Datenschutz sicherstellen und auf der anderen Seite Garantien dafür vorsehen, dass die Beweismittel rechtmäßig eingeholt werden und vor einem Gericht verwendet werden können.

Verwendung von Technologien zum Schutz der Privatsphäre

32. Die praktische Umsetzung der Tätigkeit des EC3 wird wahrscheinlich auf der Verwendung einer fortschrittlichen IT-Infrastruktur basieren, mit der – zur Unterstützung der in der Mitteilung vorgesehenen Aktionen – große Menge personenbezogener Daten verarbeitet werden. Die Technologien zum Schutz der Privatsphäre können als Mittel zur Erzielung eines korrekten Gleichgewichts zwischen der Erreichung der Zielsetzungen des EC3 und der Wahrung der Rechte natürlicher Personen betrachtet werden.

33. Der EDSB empfiehlt dringend, dass die IT-Infrastruktur vorab sorgfältig geprüft wird und dass konkrete Maßnahmen zur Anwendung der Technologien zum Schutz der Privatsphäre vorgesehen werden. Dieser Ansatz ist mit dem Ansatz des „eingebauten Datenschutzes" vereinbar, der im jüngsten Vorschlag der Kommission zur Überprüfung des Rahmens für den Datenschutz vorgesehen ist.[22] Dies ist in diesem Fall, angesichts der kurzen Frist vor Aufnahme der Tätigkeit durch das Zentrum und der Tatsache, dass der überarbeitete rechtliche Rahmen von Europol sehr wahrscheinlich noch nicht anwendbar sein wird, besonders wichtig.

34. Der Ansatz des „eingebauten Datenschutzes" wird folglich dazu beitragen, die Angemessenheit der Tätigkeit des Zentrums zu gewährleisten und den Eingriff in die Grundrechte zu minimieren.

2.3. Zusammenarbeit zwischen dem EC3 und dem privaten Sektor und internationalen Partnern

35. In Kapitel 2.1 der Mitteilung wird das Ziel des EC3 beschrieben, die Anlaufstelle für die Bekämpfung der Cyberkriminalität zu werden. Insbesondere ist vorgesehen, dass eine der Funktionen des EC3 in der Einholung von Informationen über Cyberkriminalität aus *„umfangreichen öffentlichen, privaten und offenen Quellen"* und zur Anreicherung der verfügbaren polizeilichen Daten bestehen wird. Aus der Mitteilung geht hervor, dass diese Informationen auch der Cyberkriminalität verdächtigte Personen betreffen können. Folglich wird das EC3 in diesem Zusammenhang personenbezogene Daten im Sinne von Artikel 2 Buchstabe a des Beschlusses 2008/977/JI[23] verarbeiten.

36. Der EDSB stellt fest, dass der Europol-Beschluss den Austausch personenbezogener Daten zwischen Europol und dem privaten Sektor streng regelt und in den meisten Fällen, wie nachfolgend noch näher ausgeführt werden wird, der Datenaustausch

[22] Artikel 19 des Vorschlags 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/2012/010 endgültig - 2012/0010 (COD).

[23] Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl. L 350 vom 30.12.2008, S. 60-71.

zwischen Europol und dem privaten Sektor nur unter Vermittlung der nationalen Strafverfolgungsbehörden erfolgen kann.

37. Der EDSB prüft in diesem Kapitel, wie die rechtlichen Beschränkungen, die im Europol-Beschluss enthalten sind, durch das EC3 in der Praxis angewandt werden sollten.

Zusammenarbeit mit dem privaten Sektor

38. Die Mitteilung sieht vor, dass Europol Daten aus allen verfügbaren (privaten, öffentlichen oder offenen) Quellen zusammentragen wird, um polizeiliche Daten anzureichern. Der EDSB stellt mit Besorgnis fest, dass dieser Ansatz dem allgemeinen Trend entspricht, sicherstellen zu wollen, dass der Grundsatz der Verfügbarkeit von Informationen zur Verbesserung der Effizienz der Strafverfolgungsbehörden garantiert wird, ohne dass ein Gleichgewicht mit den Grundsätzen der Verhältnismäßigkeit und der Notwendigkeit gemäß Artikel 8 der Charta der Grundrechte der Europäischen Union, Artikel 8 EMRK und Artikel 16 AEUV hergestellt wird.

39. Die Bekämpfung der Cyberkriminalität wird häufig die Zusammenarbeit des privaten Sektors erforderlich machen, da die meisten der sachdienlichen Daten im Zusammenhang mit Ermittlungen bezüglich Cyberstraftaten von privaten Stellen gespeichert werden, die im Rahmen ihres Geschäftsbetriebs oder zur Einhaltung spezifischer rechtlicher Auflagen Aufzeichnungen über elektronische Transaktionen und Kommunikationen führen. So speichern beispielsweise Telekom-Netzbetreiber Internetkommunikations- und Telekomdaten zu geschäftlichen Zwecken oder unter Einhaltung der Vorratsdaten-Richtlinie[24].

40. Es ist offensichtlich, dass die Bekämpfung der Cyberkriminalität ein Zweck ist, der in keiner Verbindung zur Geschäftstätigkeit dieser Unternehmen steht. Deshalb müssen Fragen im Zusammenhang mit der rechtmäßigen Verarbeitung und der Vereinbarkeit der Nutzung personenbezogener Daten berücksichtigt werden, da die Erfassung und die weitere Nutzung der Daten zur Bekämpfung der Cyberkriminalität zu einer Verletzung des Rechts auf den Schutz personenbezogener Daten führen könnten.

41. Der EDSB ist in der Vergangenheit bereits mehrfach auf die Zusammenarbeit mit dem privaten Sektor im Rahmen von Strafverfolgungsaktivitäten eingegangen[25], wobei

[24] Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. L 105, S. 54.

[25] Stellungnahme des Europäischen Datenschutzbeauftragten vom 23. Juni 2008 zum Vorschlag für einen Beschluss des Europäischen Parlaments und des Rates über ein mehrjähriges Gemeinschaftsprogramm zum Schutz der Kinder bei der Nutzung des Internets und anderer Kommunikationstechnologien. ABl. C 2 vom 7.1.2009, S. 2-6.
Stellungnahme des Europäischen Datenschutzbeauftragten zu den laufenden Verhandlungen der Europäischen Union über ein Abkommen zur Bekämpfung von Produkt- und Markenpiraterie (Anti-Counterfeiting Trade Agreement, ACTA). ABl. C 147 vom 5.6.2010, S. 1-13.
Stellungnahme des Europäischen Datenschutzbeauftragten vom 7. Oktober 2011 über Netzneutralität, Verkehrssteuerung und den Schutz der Privatsphäre und personenbezogener Daten. ABl. C 34 vom 8.2.2012, S. 1-17.
Stellungnahme des Europäischen Datenschutzbeauftragten vom 24. April 2012 zum Vorschlag für einen Beschluss des Rates über den Abschluss des Handelsübereinkommens zur Bekämpfung von Produkt- und Markenpiraterie zwischen der Europäischen Union und ihren Mitgliedstaaten, Australien, Kanada, Japan, der Republik Korea, den Vereinigten Mexikanischen Staaten, dem Königreich Marokko, Neuseeland, der Republik

deren sensible Natur unterstrichen wurde. Der EDSB ist insbesondere besorgt im Hinblick auf die Fragen, die durch eine Beteiligung eines kommerziellen Akteurs aufgeworfen werden, der eine spezifische Dienstleistung anbietet, in einem Bereich wie der Strafverfolgung, in dem grundsätzlich nur die zuständigen Behörden entsprechend den gemäß nationalem Recht vorgesehenen Bedingungen beteiligt sein sollten.

42. Außerdem scheint die Mitteilung auf eine direkte Interaktion zwischen dem EC3 und dem privaten Sektor abzuzielen. Europol und folglich auch das EC3 sind jedoch nicht berechtigt, direkt ohne Einschränkungen mit privaten Akteuren zu interagieren. Artikel 25 des Europol-Ratsbeschlusses legt fest, dass Europol, soweit dies für die rechtmäßige Erfüllung seiner Aufgaben erforderlich ist, Informationen, einschließlich personenbezogener Daten von privaten Parteien, nur unter bestimmten Bedingungen verarbeiten darf.

    - Gemäß Artikel 25 Absatz 3 Buchstabe a dürfen Daten von privaten Parteien, die nach dem Recht eines Mitgliedstaats erstellt wurden, von Europol nur verarbeitet werden, wenn sie über die nationale Stelle dieses Mitgliedstaats gemäß dem innerstaatlichen Recht übermittelt werden. Dieser Artikel untersagt es Europol explizit, zur Einholung von Informationen direkt mit privaten Parteien in Verbindung zu treten.
    - Gemäß Artikel 25 Absatz 3 Buchstabe b dürfen personenbezogene Daten von privaten Parteien, die nach dem Recht eines Drittstaats erstellt wurden, mit dem Europol ein Kooperationsabkommen geschlossen hat, nur über die Kontaktstelle des betreffenden Staates übermittelt werden.
    - Gemäß Artikel 25 Absatz 3 Buchstabe c dürfen personenbezogene Daten von privaten Parteien, die nach dem Recht eines Drittstaats erstellt wurden, mit dem Europol kein Kooperationsabkommen geschlossen hat, von Europol nur verarbeitet werden, wenn die betroffene private Partei in eine Liste aufgenommen wurde, die vom Verwaltungsrat von Europol ausgearbeitet wird und sofern Europol und die betroffene private Partei eine Vereinbarung über die Übermittlung von Informationen geschlossen haben, in der bestätigt wird, dass die personenbezogenen Daten von dieser privaten Partei rechtmäßig erhoben und übermittelt werden, und in der angegeben wird, dass die übermittelten personenbezogenen Daten nur für die rechtmäßige Erfüllung der Aufgaben von Europol benutzt werden dürfen. In Artikel 25 Absatz 6 wird klargestellt, dass Europol diese Informationen nur zum Zwecke ihrer Aufnahme in das Europol-Informationssystem und anderer analytischen Arbeitsdateien oder Systeme, auf die im genannten Artikel Bezug genommen wird, verarbeiten darf.
    - Gemäß Artikel 25 Absatz 4 kann Europol personenbezogene Daten aus öffentlich zugänglichen Quellen verarbeiten.

43. Eine direkte Interaktion mit privaten Akteuren wäre zudem komplex, da diese verschiedenen nationalen Rechtsvorschriften und verschiedenen Verfahrensgarantien unterliegen würden, je nachdem, in welchem Mitgliedstaat der private Akteur seinen Sitz hat (so kann beispielsweise in einem Staat die Offenlegung einer besonderen Datenart nur auf der Grundlage von einer richterlichen Genehmigung erfolgen, während dies in einem anderen Staat nicht erforderlich ist).

Singapur, der Schweizerischen Eidgenossenschaft und den Vereinigten Staaten von Amerika, veröffentlicht unter www.edps.europa.eu.

44. Der EDSB stellt fest, dass die Einschränkung, wonach Europol nur Daten verarbeiten darf, die über nationale Stellen eingeholt wurden, die Interaktion vereinfachen und zum Datenschutz beitragen wird, da die nationalen Stellen normalerweise sicherstellen, dass der Informationsaustausch mit dem EC3 auf rechtmäßige Weise erfolgt und dass entsprechend den Rechtsvorschriften eines jeden Mitgliedstaates angemessene Garantien vorgesehen werden. Deshalb empfiehlt der EDSB, dass diese Garantie sowohl im Mandat des EC3 als auch bei der Revision des Europol-Rechtsrahmens beibehalten wird.

Zusammenarbeit mit internationalen Partnern

45. Ermittlungen im Zusammenhang mit Cyberstraftaten machen häufig die Erfassung und Verarbeitung von Daten erforderlich, die aus verschiedenen Ländern stammen (wovon einige nicht zur Europäischen Union gehören könnten). Der Mitteilung ist zu entnehmen, dass eines der Ziele des EC3 darin besteht, das Sprachrohr der europäischen Cyberkriminalitätsermittler aus Strafverfolgungs- und Justizbehörden zu werden. Um dieses Ziel zu erreichen, wäre das EC3 die optimale Schnittstelle zu den von Interpol ergriffenen Maßnahmen zur Bekämpfung der Cyberkriminalität und zu anderen internationalen Polizeidienststellen, die in diesem Bereich tätig sind.

46. Grundsätzlich ist diese Tätigkeit mit Artikel 23 des Europol-Ratsbeschlusses vereinbar, der vorsieht, dass Europol Informationen, auch personenbezogene Daten, mit Drittstaaten und einigen konkreten Organisationen austauschen darf sofern dies zur rechtmäßigen Erfüllung ihrer Aufgaben erforderlich ist.

47. So sieht Artikel 23 Absatz 3 insbesondere vor, dass Europol personenbezogene Daten von Drittstaaten und Organisationen entgegennehmen und verwenden darf. Gemäß Artikel 23 Absatz 6 ist Europol berechtigt, personenbezogene Daten an Drittstaaten und Organisationen zu übermitteln, falls folgende Bedingungen erfüllt sind:
    - vorherige Zustimmung des Mitgliedstaates, der die betroffenen Daten ursprünglich an Europol übermittelt hat;
    - soweit dies in Einzelfällen zur Verhütung oder Bekämpfung von Straftaten, für die Europol zuständig ist, unbedingt erforderlich ist;
    - wenn Europol mit der betreffenden Einrichtung ein Abkommen geschlossen hat, das die Übermittlung solcher Daten auf der Grundlage einer Feststellung zulässt, dass diese Stelle ein angemessenes Datenschutzniveau gewährleistet;
    - der Direktor von Europol kann, nach Feststellung der Angemessenheit des Datenschutzniveaus der empfangenden Stelle, die Übermittlung personenbezogener Daten genehmigen, wenn er die Übermittlung der Daten zur Wahrung der grundlegenden Interessen der betreffenden Mitgliedstaaten im Rahmen der Ziele von Europol oder zur Abwehr einer unmittelbaren kriminellen oder terroristischen Bedrohung für unbedingt erforderlich hält.

48. Der EDSB stellt fest, dass gemäß diesen Bestimmungen das EC3 keine personenbezogenen Daten austauschen sollte, es sei denn dies ist in Einzelfällen gerechtfertigt und sofern die empfangende Stelle ein angemessenes Datenschutzniveau garantiert. Diese Bedingungen müssen auch ausgehend von den im Beschluss 2009/934/JI des Rates zur Regelung der Beziehungen von Europol zu anderen Stellen enthaltenen Umsetzungsbestimmungen geprüft werden.

49. Vor diesem Hintergrund und angesichts der Bedeutung, die der Informationsaustausch auf internationaler Ebene bei der Bekämpfung der Cyberkriminalität hat, empfiehlt der EDSB, dass geprüft wird, ob die aktuellen internationalen, von Europol unterzeichneten Übereinkommen den erforderlichen Informationsaustausch in der in diesem Kontext erforderlichen Menge und Geschwindigkeit zulassen. Der EDSB stellt auch fest, dass das vom EC3-Umsetzungsteam auszuarbeitende Mandat spezifisch auf die internationale Zusammenarbeit eingehen sollte, da eine der Hauptaufgaben des EC3 darin bestehen wird, das Sprachrohr der europäischen Ermittler im Bereich der Cyberkriminalität und die Anlaufstelle für internationale Partner zu sein.

3. SCHLUSSFOLGERUNGEN

50. Der EDSB betrachtet die Bekämpfung der Cyberkriminalität als Grundstein der Gewährleistung von Sicherheit im digitalen Raum und zur Schaffung des erforderlichen Vertrauens. Der EDSB stellt fest, dass die Vereinbarkeit mit den Datenschutzbestimmungen als wesentlicher Bestandteil der Bekämpfung der Cyberkriminalität und nicht als Einschränkung ihrer Effizienz betrachtet werden sollte.

51. In der Mitteilung wird Bezug genommen auf die Errichtung eines neuen Europäischen Zentrums zur Bekämpfung der Cyberkriminalität innerhalb von Europol, während bereits seit einer Reihe von Jahren ein „Europol Cyber Crime Centre“ besteht. Der EDSB würde mehr Klarheit im Hinblick auf die neuen Kapazitäten und Tätigkeiten begrüßen, die das neue EC3 von dem bestehenden „Europol Cyber Crime Centre“ unterscheiden.

52. Der EDSB empfiehlt, dass die Kompetenzen des EC3 eindeutig definiert werden und nicht nur mittels Verweis auf das Konzept der „Computerkriminalität“, das Teil des aktuellen Rechtsrahmens von Europol ist. Auch die Definition der Kompetenzen und der Datenschutzgarantien des EC3 sollten Teil der Überarbeitung der Europol-Rechtsvorschriften sein. Bis die neuen Europol-Rechtsvorschriften anwendbar sein werden, empfiehlt der EDSB der Kommission, diese Kompetenzen und Datenschutzgarantien im Mandat des Zentrums festzulegen. Dies sollte Folgendes umfassen:

    - eine klare Definition der Datenverarbeitungsaufgaben (insbesondere Ermittlungen und operative Unterstützungstätigkeiten), die vom Personal des Zentrums allein oder in Zusammenarbeit mit gemeinsamen Ermittlungsgruppen durchgeführt werden könnten und

    - klare Verfahren, die auf der einen Seite die Einhaltung der Rechte natürlicher Personen (einschließlich des Rechts auf Datenschutz) sicherstellen und auf der anderen Seite Garantien dafür vorsehen, dass die Beweismittel rechtmäßig eingeholt wurden und vor einem Gericht verwendet werden können.

53. Der EDSB ist der Ansicht, dass der Austausch personenbezogener Daten zwischen dem EC3 und Akteuren, die über *„umfangreiche, öffentliche, private und offene Quellen*“ verfügen, spezifische Datenschutzrisiken aufwirft, da dies häufig zur Verarbeitung von Daten führen wird, die zu kommerziellen Zwecken zusammengetragen wurden, sowie eine internationale Datenübertragung mit sich bringt. Diese Risiken werden vom aktuellen Europol-Beschluss angegangen, der vorsieht, dass Europol generell keine Daten direkt mit dem privaten Sektor und nur

unter sehr konkreten Umständen mit spezifischen internationalen Organisationen austauschen darf.

54. Vor diesem Hintergrund und angesichts der Bedeutung dieser beiden Tätigkeiten für das EC3 empfiehlt der EDSB, dass in Übereinstimmung mit den bestehenden Bestimmungen der Europol-Entscheidung angemessene Datenschutzgarantien vorgesehen werden. Diese Garantien sollten in dem vom Umsetzungsteam auszuarbeitenden Mandat des EC3 eingegliedert werden (und später im überarbeiteten Europol-Rechtsrahmen) und dürfen auf keinen Fall zu einem niedrigeren Datenschutzniveau führen.

Brüssel, den 29. Juni 2012

(**unterzeichnet**)

Peter HUSTINX
Der Europäische Datenschutzbeauftragte