Formelle Kommentare des EDSB zu

- **Der Gemeinsamen Mitteilung der Europäischen Kommission und der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik an das Europäische Parlament und den Rat „Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit der Union wirksam erhöhen“** (nachstehend „die Gemeinsame Mitteilung“)[i];

- **dem Vorschlag der Kommission für eine Verordnung des Europäischen Parlaments und des Rates über die „EU-Cybersicherheitsagentur“ (ENISA) und zur Aufhebung der Verordnung (EU) 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik („Rechtsakt zur Cybersicherheit“)[ii];**

- **der Empfehlung der Kommission (EU) 2017/1584 vom 13. September 2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen** (nachstehend „die Empfehlung“)[iii];

- **der Mitteilung der Kommission an das Europäische Parlament und den Rat „Bestmögliche Netz- und Informationssicherheit - hin zu einer wirksamen Umsetzung der Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union“ (**nachstehend „die NIS-Mitteilung“**)**[iv].

Die Kommission verabschiedete diese Maßnahmen am 13. September 2017 in einer gemeinsamen Maßnahme, die als „Cybersicherheitspaket 2017“ bezeichnet wird.[v]

Das Paket enthält ferner einen **Vorschlag für eine Richtlinie zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln**[vi], auf den der EDSB in einem anderen Zusammenhang eingehen wird.

Am 18. Oktober verabschiedete die Kommission ein Maßnahmenpaket zur Sicherheitsunion, in dem einige der im Cybersicherheitspaket angekündigten Initiativen näher erläutert werden. Bei Bedarf wird der EDSB diese weiteren Elemente in diesen formellen Kommentaren aufgreifen. Es geht dabei im Wesentlichen um die angekündigten politischen Initiativen im Bereich Verschlüsselung.

I. Einleitung und Hintergrund

Am 13. September 2017 legten die Europäische Kommission und die Hohe Vertreterin ein Maßnahmenpaket vor, denn die EU muss sich *„… besser gegen Cyberangriffe wappnen und für eine wirksame Abschreckung in der EU und entsprechende strafrechtliche Verfolgung*

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

sorgen, um Bürgerinnen und Bürger, Unternehmen sowie öffentliche Einrichtungen in Europa besser zu schützen", das so genannte „Cybersicherheitspaket". Dieses Paket enthält die oben aufgeführten Instrumente.
Am 18. Oktober 2017 veröffentlichte die Kommission ihren Bericht über eine Sicherheitsunion[vii], in dem sie näher auf einige Elemente der Gemeinsamen Mitteilung einging. So stellte sie insbesondere eine ganze Reihe von Initiativen im Bereich Verschlüsselung vor.

Der EDSB hat von Anfang an die Entwicklungen bei der EU-Strategie zum Aufbau von Cybersicherheitskapazitäten verfolgt. Nachstehend einige Stellungnahmen, die der EDSB neben anderen formellen und informellen beratenden Dokumenten verfasst hat:

- Stellungnahme zu dem Vorschlag für eine Verordnung über ENISA, Dezember 2010.[viii]
- Formelle Kommentare des EDSB vom Oktober 2012 zur öffentlichen Konsultation der Kommission zur Verbesserung der Netz- und Informationssicherheit (NIS) in der EU.[ix]
- Stellungnahme vom Juni 2013 zur Gemeinsamen Mitteilung der Kommission und der Hohen Vertreterin zur Cybersicherheitsstrategie der EU und zum Vorschlag für eine NIS-Richtlinie.[x]
- Stellungnahme vom Dezember 2015 zur Verbreitung und Verwendung von eingreifenden Überwachungstechnologien.[xi]
- Leitfaden für Sicherheitsmaßnahmen für die Verarbeitung personenbezogener Daten[xii], März 2016.

Der EDSB stellt fest, dass das aktuelle Paket viele Elemente enthält, die mit Blick auf den Datenschutz und den Schutz der Privatsphäre relevant sind. Wir halten fest, dass sich die Kommission nicht an ihre Zusage gehalten hat, den EDSB vor der Annahme dieser Vorschläge zu konsultieren.

II. Gegenstand der Kommentare des EDSB

Das geltende Datenschutzrecht, darunter die Datenschutz-Grundverordnung[xiii], sieht in der Informationssicherheit eine Möglichkeit, natürliche Personen durch den Schutz ihrer personenbezogenen Daten zu schützen. Die Informationssicherheit gehört zu den im Gesetz verankerten „Grundsätzen" des Datenschutzes (Artikel 5 Absatz 1 Buchstabe f). Artikel 32 enthält für alle Akteure, die personenbezogene Daten verarbeiten („Verantwortliche"[xiv] und „Auftragsverarbeiter"[xv]), die Verpflichtung, *„... geeignete technische und organisatorische Maßnahmen zu ergreifen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten..."*. Artikel 33 und 34 sehen die Verpflichtung vor, unter bestimmten Bedingungen binnen 72 Stunden der zuständigen Aufsichtsbehörde Verletzungen des Schutzes personenbezogener Daten[xvi] zu melden, die zu einem Risiko für die betroffenen Personen führen, und die von einer Verletzung des Schutzes personenbezogener Daten betroffenen Personen unverzüglich von der Verletzung zu benachrichtigen, die voraussichtlich ein hohes Risiko für sie bedeutet.

Entsprechende Bestimmungen finden sich auch in der derzeit geltenden Verordnung (EG) Nr. 45/2001 über die Verarbeitung personenbezogener Daten durch Organe und Einrichtungen der EU[xvii] sowie in dem Vorschlag für eine neue Datenschutzverordnung für diese Organe und Einrichtungen der EU.

Artikel 4 der Richtlinie 2002/58/EG, deren Schwerpunkt der Datenschutz in der elektronischen Kommunikation ist, enthält Bestimmungen zur Cybersicherheit. Einige dieser Pflichten sind in

Artikel 17 des Vorschlags für eine E-Privacy-Verordnung[xviii] übergegangen, so z. B. die Verpflichtung, Endnutzer, sofern ein besonderes Risiko besteht, dass die Sicherheit von Netzen und elektronischen Kommunikationsdiensten beeinträchtigt werden könnte, über dieses Risiko zu informieren.

Zwar unterstreichen diese Instrumente die Bedeutung von Cybersicherheitsmaßnahmen für einen wirksamen Datenschutz, doch kann die Umsetzung von Sicherheitsmaßnahmen die Verarbeitung personenbezogener Daten zur Folge haben. Eine solche Verarbeitung muss mit dem Gesetz in Einklang stehen, und es müssen alle Grundsätze des Datenschutzes, darunter die Grundsätze von Zweckbindung und Datenminimierung, gewahrt sein.
In den vorliegenden formellen Kommentaren werden die genannten Instrumente vor dem Hintergrund des geltenden Rechtsrahmens und der obigen Erwägungen analysiert.

III. Kommentare des EDSB

1. Allgemeine Überlegungen zum Cybersicherheitspaket einschließlich der Gemeinsamen Mitteilung

- *Die Umsetzung einer wirksamen Cybersicherheit in der EU darf nicht hinausgeschoben werden*

Unsere Gesellschaft verlässt sich zunehmend auf den Austausch von Informationen über Kommunikationsnetze, meist mit dem globalen Internet verbunden, um die Lieferung und Nutzung wesentlicher Dienste wie Energie und Herstellung und Verteilung von Waren sowie Verkehr zu straffen. Die Verarbeitung von Informationen und Daten, darunter personenbezogene Daten, gilt als Fundament der Digitalen Wirtschaft. Ein herausragendes Beispiel für die Rolle, die das Internet und Online-Dienste spielen sollen, ist die jüngst angenommene Erklärung von Tallinn zur E-Government, deren Ziel es ist, für Bürger und Unternehmen in der EU hochwertige, nutzerzentrierte digitale Behördendienste zu gewährleisten. Sie sieht in Maßnahmen in den Bereichen Vertrauenswürdigkeit und Sicherheit den Schlüssel, mit dem erfolgreich gewährleistet werden kann, dass *„…Anliegen der Informationssicherheit und des Datenschutzes bei der nach einem risikogestützten Ansatz und unter Verwendung der neuesten Techniken erfolgenden Gestaltung öffentlicher Dienstleistungen und Informations- und Kommunikationstechnologie-(IKT)Lösungen für öffentliche Verwaltungen berücksichtigt werden…“*.

In vielen Zusammenhängen ist der Zugang zum Internet ein wesentlicher Faktor für die umfassende Teilhabe an wirtschaftlichen und gesellschaftlichen Aktivitäten geworden.

Cybersicherheit ist nicht länger nur ein Anliegen von Experten; vielmehr anerkennt eine große Mehrheit von EU-Bürgern ihre Bedeutung, wie jüngst in einer Eurobarometererhebung deutlich wurde:[xix] 87 % der Befragten halten Cyberkriminalität für eine wichtige Herausforderung für die innere Sicherheit der EU, und der Missbrauch personenbezogener Daten ist nach wie vor das größte Problem für Internetnutzer.

Wir begrüßen daher und betrachten als wesentlich und nicht länger hinausschiebbar die Bemühungen um *„… die Erhöhung der Sicherheit des Internets und der privaten Netz- und Informationssysteme, die für das Funktionieren unserer Gesellschaft und Wirtschaft unverzichtbar sind …“*, wie es in der Begründung des Pakets heißt.

Wir stellen fest, dass in der Gemeinsamen Mitteilung eine Reihe von Maßnahmen hervorgehoben wird, mit denen die Reaktion auf geschehene Cybervorfälle verbessert werden

soll. Wir räumen ein, dass eine gut vorbereitete Reaktion, die auf guter Planung, der Schulung von Mitarbeitern und der Einrichtung geeigneter Prozesse und Verfahren im Vorhinein beruht, den von einem Vorfall verursachten Schaden erheblich begrenzen und eine weitere Schadensausbreitung verhindern helfen kann.

Wir erinnern jedoch daran, dass angemessene Maßnahmen zur Verhinderung von Vorfällen, wie z. B. eine ordnungsgemäße Wartung von IT-Systemen, noch wirksamer sein können, da sie Angriffe stoppen, bevor irgendein Schaden eintreten kann. In diesem Zusammenhang sei der Hinweis erlaubt, dass die Wannacry-Angriffe im Mai 2017 keine Systeme betrafen, die das empfindliche Funktionsmerkmal (das in vielen Systemen gar nicht verwendet wurde) entweder abgeschaltet oder ein Update installiert hatten, das schon rund einen Monat vor den Angriffen zur Verfügung gestanden und die von dem Angreifer genutzte Schwachstelle beseitigt hatte.[xx] Wir unterstreichen daher die Bedeutung des Aufbaus dem neuesten Stand der Technik entsprechender Risikomanagementsysteme für Informationssicherheit, der Erarbeitung und Anwendung geeigneter Strategien für alle Systeme und der Zuweisung von Verantwortlichkeiten in allen Organisationen. Diese Maßnahmen entsprechen dem in den relevanten Datenschutzrechtsvorschriften und in anderen Instrumenten zum Thema Informationssicherheit formulierten Sicherheitskonzept.
Wannacry und andere Cybersicherheitsvorfälle aus der jüngsten Zeit machen deutlich, dass die Zielsetzungen der Cybersicherheitsstrategie von 2013, nämlich bessere Robustheit und Abwehrbereitschaft im öffentlichen und privaten Sektor, noch immer gültig sind und weiterhin erhebliche Anstrengungen erfordern. Investitionen in Bildung und geeignete Präventivmaßnahmen sollten die Grundlage bilden, auf der eine wirksame und schnelle Reaktion auf sich abzeichnende Vorfälle den Schaden begrenzen hilft. Die Cybersicherheitsstrategie sollte beiden Wegen folgen und kann vielleicht von einer gründlichen Analyse von Vorfällen aus der Vergangenheit profitieren, bei der die Faktoren ermittelt werden können, die für das Fehlen geeigneter Vorbereitungs- und Präventivmaßnahmen in den am stärksten betroffenen Organisationen verantwortlich waren. Maßnahmen zur Verbesserung von Kompetenzen im Bereich Cybersicherheit sowie von Cyberhygiene und Problembewusstsein können auf unsere umfassende Unterstützung zählen.

Die Beseitigung oder Verringerung inhärenter Schwächen von Produkten und Diensten kann sich bei der Prävention von Cybersicherheitsvorfällen als besonders wirksam erweisen. Die Gemeinsame Mitteilung erwähnt mehrere Konzepte, die zur Bekämpfung inhärenter Schwächen des derzeitigen Marktes für Produkte und Dienste beitragen können:

- Befolgung des Grundsatzes der „eingebauten Sicherheit“,
- Aufstellung des Grundsatzes der „Sorgfaltspflicht“,
- Zuweisung an Marktakteure einer Haftpflicht für Ausfälle.

Wir bestärken die Kommission in ihrer Absicht, zur Förderung dieser Zielsetzungen Strategien auszuarbeiten und umzusetzen sowie Legislativmaßnahmen vorzuschlagen. Dies entspräche und ergänzte im Unionsrecht bereits für den Schutz personenbezogener Daten vorhandene Konzepte, so z. B. die Verpflichtung, den Grundsatz des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen zu wahren und die entsprechenden Sanktionen und Verantwortlichkeiten zu regeln.

Unabhängige Sicherheitsexperten können eine wichtige Rolle bei der Aufdeckung, Bewertung und Untersuchung von Schwachstellen in der Cybersicherheit spielen. Ihre Arbeit sollte nicht durch unangemessen gestaltete Rechtsvorschriften behindert werden, die das Risiko einer Verfolgung wegen durchaus legitimer Tätigkeiten bergen. Wir begrüßen die Anerkennung dieser Notwendigkeit in der Gemeinsamen Mitteilung.

- *Zum geplanten Netz von Cybersicherheitskompetenzzentren mit einem Europäischen Kompetenzzentrum für Cybersicherheitsforschung*

Wir nehmen den Plan zur Kenntnis, *„ein Netz von Cybersicherheitskompetenzzentren unter dem Dach des Europäischen Kompetenzzentrums für Cybersicherheitsforschung"* zu schaffen, *„die Entwicklung und Verbreitung von Cybersicherheitstechnik zu fördern und die Bemühungen um den Aufbau von Kapazitäten in diesem Bereich auf EU-Ebene und auf nationaler Ebene zu ergänzen"*. Wir nehmen auch zur Kenntnis, dass die Kommission 2018 mit einer Folgenabschätzung beginnen will.

Wir werden uns zu einem späteren Zeitpunkt mit diesem Vorschlag befassen, sobald einschlägige politische Instrumente einschließlich rechtlicher Instrumente vorliegen, und wir stehen in unserer Beratungsfunktion der Kommission gerne für eine weitere Zusammenarbeit zur Verfügung.

Bei dieser Gelegenheit begrüßen wir, dass die Notwendigkeit betont wird, Verschlüsselungsfähigkeiten in Produkten und Diensten als wesentliche Elemente zum Schutz der Information und der Grundrechte der Menschen durch Schutz ihrer personenbezogenen Daten zu entwickeln und zu bewerten.

- *Zur Schaffung einer wirksamen Abschreckung zur Erhöhung der Cybersicherheit*

Wir teilen zwar die Auffassung, dass Bedarf an einer wirksamen Strafverfolgung mit Schwerpunkt auf Enttarnung, Rückverfolgbarkeit und Verfolgung von Cyberkriminellen besteht, doch weisen wir nachdrücklich darauf hin, dass sie unter vollständiger Achtung der Charta der Grundrechte der EU und der darin verankerten Rechte auf Privatsphäre und auf den Schutz personenbezogener Daten zu erfolgen hat. Wir möchten bei dieser Gelegenheit an einen Rat des EDSB in seinem „Toolkit zur Beurteilung der Erforderlichkeit von Maßnahmen" erinnern, nämlich die Auswirkungen neuer Bestimmungen und Maßnahmen auf die Grundrechte von Personen bei der Verarbeitung ihrer personenbezogenen Daten zu prüfen, die Fälle zu ermitteln, in denen eine Einschränkung dieses Rechts tatsächlich erforderlich ist, und angemessene Garantien als Gegengewicht zum Eindringen der geplanten Maßnahme in die Privatsphäre zu schaffen.

In der Gemeinsamen Mitteilung werden Maßnahmen im Bereich elektronischer Beweismittel angekündigt. Zu dem Rechtsakt zu grenzüberschreitendem Zugang zu elektronischen Beweismitteln, den die Kommission im Januar 2018 annehmen wird, werden wir eine getrennte Stellungnahme herausgeben.

In dem Bericht „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion, Elfter Fortschrittsbericht" geht es um das Problem von Strafverfolgungs- und Justizbehörden, die in ihren Ermittlungen mit von mutmaßlichen Straftätern verwendeten Verschlüsselungen zu tun haben. Wir halten die Pläne der Kommission fest, Vorschläge für *„rechtliche Maßnahmen zur Erleichterung des Zugangs zu verschlüsseltem Beweismaterial"* und *„technische Maßnahmen zur Verbesserung der Verschlüsselungsfähigkeiten"* zu unterbreiten. Zu diesen Plänen gehören auch die Verbesserung der Entschlüsselungsfähigkeiten von Europol und besonderes Augenmerk für von der EU finanzierte Forschung und Entwicklung in einschlägigen Technologien. Ferner halten wir fest, dass die Kommission zudem ein *„Netzwerk von Fachwissenszentren"* zu diesem Thema vorschlägt, in dem nationale Fähigkeiten und Fachkenntnisse ausgetauscht werden können. Dieses Netzwerk sollte, so der Vorschlag der Kommission, ein *„Instrumentarium an alternativen Ermittlungstechniken"* entwickeln und

austauschen, deren Verzeichnis beim Europäischen Zentrum zur Bekämpfung der Cyberkriminalität bei Europol angesiedelt sein sollte. Neben anderen Maßnahmen hält die Kommission es für *„erforderlich, angesichts der ständigen Weiterentwicklung der Verschlüsselungstechniken, ihrer zunehmenden Nutzung durch Straftäter und ihrer Auswirkungen auf strafrechtliche Ermittlungen eine fortlaufende Bewertung der technischen und rechtlichen Aspekte der Rolle der Verschlüsselung in strafrechtlichen Ermittlungen durchzuführen"*. Die Kommission wird *„die Einrichtung einer Beobachtungsfunktion in Zusammenarbeit mit dem Europäischen Zentrum zur Bekämpfung der Cyberkriminalität (EC3) bei Europol, dem Europäischen Justiziellen Netz gegen Cyberkriminalität (EJCN) und Eurojust unterstützen"*.

Wir begrüßen die Tatsache, dass die Kommission eine Reihe von Maßnahmen zur Unterstützung der Behörden der Mitgliedstaaten im Umgang mit Verschlüsselungstechniken bei strafrechtlichen Ermittlungen vorzuschlagen gedenkt, *„ohne jedoch die Nutzung von Verschlüsselungstechniken zu untersagen, einzuschränken oder zu schwächen"*. **Wir begrüßen und unterstützen folgende Erklärung der Kommission: *„Maßnahmen, die die Verschlüsselung schwächen oder Auswirkungen auf eine größere oder unabsehbare Anzahl von Menschen haben könnten, werden nicht berücksichtigt"*.** Unserer Auffassung nach können die von der Kommission erwogenen Maßnahmen unter vollständiger Wahrung der Grundrechte sowie der Grundsätze von Notwendigkeit und Verhältnismäßigkeit durchgeführt werden.

Wir möchten an dieser Stelle nochmals unsere Auffassung zum Ausdruck bringen, dass eine Schwächung der Verschlüsselung zur Bekämpfung von Cyberkriminalität keine realistische Option ist und daher nach Alternativen gesucht werden sollte.[xxi] Wir halten fest, dass diese Auffassung auch in den Begründungen der Kommissionsvorschläge zum Ausdruck kommt und von Experten weitgehend geteilt wird.[xxii] Wir begrüßen weitere Untersuchungen und sind gerne bereit, unserer Beratungsaufgabe nachzukommen und einschlägige Vorschläge zu prüfen. **Wir sind insbesondere der Ansicht, dass die geplante Beobachtungsstelle eine wichtige Rolle beim Schutz der Grundrechte natürlicher Personen spielen kann und erwarten, bei ihrer Vorbereitung konsultiert zu werden.** In unserer Funktion als Aufsichtsbehörde bei Europol für die Verarbeitung personenbezogener Daten werden wir darüber hinaus dafür sorgen, dass die Maßnahmen bei ihrer Umsetzung in der Praxis die Grundrechte natürlicher Personen achten.

In der Gemeinsamen Mitteilung wird vorgeschlagen, dass das künftige Europäische Kompetenzzentrum für Cybersicherheitsforschung und sein Netzwerk nicht nur die Sicherheit von *„Produkten und Diensten, die von Bürgern, Unternehmen und Regierungen im Digitalen Binnenmarkt genutzt werden"* unterstützen, sondern auch die Cyberabwehrdimension der EU. Wir empfehlen Überlegungen dahingehend, dass die Ergebnisse des Zentrums, die eigentlich zur Verteidigung der EU-Bürger gedacht sind, gegen diese eingesetzt werden könnten, falls sie in die falschen Hände geraten oder missbräuchlich verwendet werden.

In unserer Stellungnahme zu eingreifenden Überwachungstechnologien[xxiii] haben wir bereits auf EU-Maßnahmen im Zusammenhang mit potenziell schädlichen Produkten und Diensten insbesondere im Bereich der Cybersicherheit hingewiesen und festgestellt, dass für Technologien zur Cyberüberwachung die gleichen Erwägungen gelten sollten wie für Güter mit doppeltem Verwendungszweck. Wir haben vor den Risiken gewarnt, die mit der Entwicklung, Verwendung und Vermarktung von Hacking-Tools einhergehen, die stark in das Leben der Menschen eindringen und eine große Gefahr für die Grundrechte und Grundfreiheiten natürlicher Personen darstellen. Wir vertraten die Auffassung dass *„für die Verwendung von Überwachungsinstrumenten eine spezielle Gesetzgebung gelten (sollte), in der die vertretbaren Grenzen der Verbreitung und Verwendung solcher Technologien bestimmt und die*

erforderlichen Schutzmechanismen für eine solche Verwendung festgelegt werden". Ferner sagten wir: *„Im Zusammenhang mit dem doppelten Verwendungszweck sollten Standards entwickelt werden, um zu bewerten, wie die IKT oder die betreffenden Informationen verwendet werden könnten und welche möglichen Auswirkungen sie auf die Grundrechte in der EU hätten"*. Wir nehmen zur Kenntnis, dass das Europäische Parlament einen Bericht über den Vorschlag der Kommission zur Neufassung des Rechtstextes über Ausfuhrkontrollen bei Gütern mit doppeltem Verwendungszweck[xxiv] erwägt, mit dem bestimmte Kategorien von Cyberüberwachungsinstrumenten in die Regelung aufgenommen würden[xxv].

Abgesehen von der externen Dimension können ausgefeilte Tools für die Ausnutzung von Sicherheitsschwachstellen oder -fehlfunktionen auch Risiken für ihre Hersteller bedeuten. Neuere Berichte[xxvi] über Hacking-Tools, die von einer staatlichen Sicherheitsagentur entwickelt wurden und dann nach außen durchgedrungen waren und für bösartige Cyberangriffe eingesetzt wurden, von denen Zehntausende von Computern und kritischen Infrastrukturen betroffen waren, der Betrieb von Krankenhäusern beeinträchtigt und E-Government-Einrichtungen blockiert wurden, belegen diese Risiken ganz eindeutig.

In der Gemeinsamen Mitteilung wird nicht erläutert, wie mit den Risiken im Zusammenhang mit der geplanten Unterstützung der EU für die Mitgliedstaaten *„beim Aufbau von Cybersicherheitskapazitäten mit doppeltem Verwendungszweck"* umgegangen werden soll. Wir empfehlen nachdrücklich eine gründliche Analyse der Risiken einer solchen Strategie und fordern die Kommission auf, eine gründliche Folgenabschätzung vorzunehmen, bevor etwaige Maßnahmen auf den Weg gebracht werden.

- *Zur Anwendung von Sicherheits- und Meldepflichten und die Beziehung zu Sicherheit und Meldungen von Verletzungen des Schutzes personenbezogener Daten in der DS-GVO*

Organisationen, die den Sicherheits- und Informationspflichten der NIS-Richtlinie unterliegen, haben zu gewährleisten, dass gleichzeitig die Bestimmungen über den Schutz personenbezogener Daten und über die Meldung von Verletzungen des Schutzes personenbezogener Daten eingehalten werden. Die beiden Instrumente verfolgen unterschiedliche Zielsetzungen, und bei ihrer Umsetzung muss unterschiedlichen Risiken Rechnung getragen werden, doch müssen Organisationen, die beiden Instrumenten unterliegen, Maßnahmen ergreifen, die geeignet sind, allen Vorgaben Genüge zu tun. Unternehmen und Behörden, die personenbezogene Daten verarbeiten, sollten einen integrierten Ansatz wählen, wenn es um die Vorgaben für Sicherheit und Datenschutz bei der Prävention von Netzwerk- und Informationsvorfällen und den Umgang damit geht.
Wir empfehlen der Kommission und den Mitgliedstaaten, diese Notwendigkeit operativer Synergien bei der Gestaltung von Maßnahmen zur wirksamen Umsetzung der Cybersicherheitsbestimmungen zu berücksichtigen, also bei Meldemechanismen und der Zusammenarbeit zwischen Datenschutzbehörden und zuständigen Behörden der Mitgliedstaaten, wie in der NIS-Richtlinie aufgeführt.

Genauer gesagt sind wir der Auffassung, dass **die Beziehung zwischen der NIS-Richtlinie und der DS-GVO im Hinblick auf Informationssicherheit und Meldungen von Verletzungen des Schutzes personenbezogener Daten noch weiter geklärt werden sollte.**[xxvii] Gemäß Artikel 1 Absatz 7 der NIS-Richtlinie gilt die Bestimmung über Sicherheits- und/oder Meldeanforderungen für Anbieter digitaler Dienste oder Betreiber wesentlicher Dienste nach der Richtlinie nicht, wenn ein sektorspezifischer Rechtsakt der EU Sicherheits- und/oder Meldeanforderungen vorsieht, sofern diese Anforderungen den in der NIS-Richtlinie enthaltenen Pflichten mindestens gleichwertig sind. Dieser Grundsatz wird in der Mitteilung

der Kommission aufgegriffen, wo es heißt, dass eine *Lex specialis* Vorrang vor den Bedingungen für Sicherheits- und Meldeanforderungen der NIS-Richtlinie hätte.[xxviii]

Allerdings werden die Verpflichtungen gemäß der DS-GVO von der NIS-Richtlinie oder irgendwelchen sektorspezifischen Rechtsvorschriften nicht berührt. In der NIS-Mitteilung wird eingeräumt, dass die Meldepflichten der NIS-Richtlinie *„unbeschadet der Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde gemäß Artikel 33 DS-GVO"* gelten.

Wir meinen, dass diese Formulierung mehrdeutig ist und möchten daher klarstellen, wie wir die Beziehung zwischen den beiden Rechtsinstrumenten bezüglich dieser Pflichten sehen.

Nach unserer Auffassung kann die DS-GVO nicht als sektorspezifischer Rechtsakt im Sinne von Artikel 1 Absatz 7 der NIS-Richtlinie gelten. Schon dem Titel der DS-GVO ist zu entnehmen, dass sie allgemein anzuwenden ist und für alle Stellen gilt, die personenbezogene Daten verarbeiten, ohne die Einschränkungen im Geltungsbereich der NIS-Richtlinie und einiger ihrer Einzelbestimmungen.[xxix]

Das bringt mit sich, dass alle in der DS-GVO geregelten Pflichten, einschließlich der die Sicherheit personenbezogener Daten und Verletzungen des Schutzes personenbezogener Daten betreffenden, zusätzlich zu allen denkbaren Pflichten gemäß der NIS-Richtlinie gelten.
Des Weiteren kann die parallele Anwendung von DS-GVO und NIS-Richtlinie zu praktischen Problemen für Organisationen führen, die beiden Rechtsakten unterliegen:

- Artikel 32 DS-GVO befasst sich mit den Bedingungen, unter denen Verantwortliche und Auftragsverarbeiter gehalten sind, geeignete technische und organisatorische Maßnahmen zu ergreifen, um ein dem Risiko für die natürlichen Personen, deren Daten verarbeitet werden, angemessenes Schutzniveau zu gewährleisten. Die NIS-Richtlinie[xxx] verfolgt einen risikogestützten Ansatz zur Vermeidung und Minimierung der Auswirkungen von Vorfällen im Zusammenhang mit der Sicherheit der Netz- und Informationssysteme auf die bereitgestellten Dienste. Auch wenn sich die Ergebnisse der beiden Bewertungen in gewissem Umfang vielleicht überschneiden, geht es doch um den Schutz von zwei verschiedenen Gütern (Grundrechte natürlicher Personen bei der DS-GVO und Dienstkontinuität bei der NIS-Richtlinie) und muss die Organisation diesen Unterschied bei der Durchführung ihrer Bewertung des Sicherheitsrisikos berücksichtigen.

- Die Verpflichtungen zur Meldung von Vorfällen nach der NIS-Richtlinie und die Verpflichtung zur Meldung von Verletzungen des Schutzes personenbezogener Daten nach der DS-GVO[xxxi] werden durch unterschiedliche Umstände ausgelöst, verfolgen einen sich teilweise überschneidenden, aber dennoch unterschiedlichen Zweck, und unterschiedliche Behörden sind Empfänger der Meldung[xxxii].

  Während die DS-GVO eine Meldung bei der zuständigen Datenschutzbehörde verlangt, wenn ein Risiko für personenbezogene Daten besteht, verlangt die NIS-Richtlinie von Betreibern wesentlicher Dienste und Anbietern digitaler Dienste eine Meldung gemäß der Richtlinie bei den zuständigen Behörden, sobald erhebliche Auswirkungen auf die bereitgestellten wesentlichen Dienste bestehen bzw. Vorfälle sich in erheblichem Maße auf die von ihnen bereitgestellten Dienste auswirken. Es bestehen also unterschiedliche Kriterien für die Beurteilung der verschiedenen Meldepflichten. Im Mittelpunkt der NIS-Richtlinie stehen die Sicherheit von Informationssystemen und die Wiederaufnahme des Dienstes, während der Schwerpunkt der DS-GVO auf dem Schutz

natürlicher Personen und ihrer personenbezogenen Daten liegt. Darüber hinaus verlangt die DS-GVO unter bestimmten Umständen und Bedingungen auch die Unterrichtung möglicherweise betroffener Personen.[xxxiii]

Wir raten in jedem Fall zu mehr Klarheit gegenüber den anvisierten Organisationen (Betreiber wesentlicher Dienste und Anbieter digitaler Dienste) und den Mitgliedstaaten bezüglich der Tatsache, dass die Sicherheits- und Meldeanforderungen nach der NIS-Richtlinie diejenigen nach der DS-GVO nicht aufheben oder ersetzen, sondern dass vielmehr beide Rechtstexte gelten und einer wirksamen integrierten Umsetzung bedürfen.
In diesem Zusammenhang schließen wir uns der Kommission in der Aufforderung an die mit der NIS-Richtlinie eingesetzte Koordinierungsgruppe an, im Einklang mit Artikel 5 Absatz 6 der NIS-Richtlinie die Mitgliedstaaten dabei zu unterstützen, einen einheitlichen Ansatz für die Ermittlung der Betreiber wesentlicher Dienste zu verfolgen.

Wir halten fest, dass die Kommission ferner eine Konsultation zu einer Durchführungsverordnung in die Wege geleitet hat, die nähere Angaben zu den Elementen enthalten soll, die von Anbietern digitaler Dienste im Umgang mit Risiken für die Sicherheit von Netz- und Informationssystemen zu berücksichtigen sind, sowie zu den Parametern, anhand derer entschieden wird, ob ein Vorfall erhebliche Auswirkungen hat.[xxxiv] Wir fordern die Kommission auf, zu gewährleisten, dass die künftige Durchführungsverordnung einen Ansatz unterstützt, der nicht nur im Einklang mit den Rechtsvorschriften über Pflichten bei Verletzungen des Schutzes personenbezogener Daten sowie den praktischen Leitlinien in dieser Frage, die die Datenschutzbehörden in der Artikel 29-Datenschutzgruppe und der künftige Europäische Datenschutzausschuss (EDSA) bereitstellen, steht, sondern tatsächlich davon profitiert und sie ergänzt.

Im Sinne eines einheitlichen Ansatzes bei der Umsetzung der NIS-Richtlinie und der DS-GVO empfehlen wir eine engere Zusammenarbeit zwischen den Datenschutzbehörden und den nach NIS zuständigen nationalen Behörden, ENISA und den CSIRT, damit etwas gegen die Fragmentierung der verschiedenen Rahmen für die Sicherheits- und Meldepflichten der Organisationen unternommen wird und sie in der Entwicklung von Methoden und Instrumenten für einen integrierten Ansatz im Umgang mit Risiken für die Informationssicherheit und Verletzungen des Schutzes personenbezogener Daten unterstützt werden, der tatsächlich im Einklang mit den Anforderungen der NIS, der DS-GVO und aller anderen anwendbaren Rechtsvorschriften steht.

IV. Zum vorgeschlagenen Rechtsakt zur Cybersicherheit *(nachstehend „der Vorschlag“)*.

1. Zur Reform von ENISA

Wir begrüßen das ständige Mandat und die der ENISA zugewiesenen neuen Aufgaben und Ressourcen. Wir nehmen zur Kenntnis, dass ihre wachsende Rolle bei der Unterstützung und Beratung bei der Ausarbeitung und Überprüfung der Unionspolitik und des Unionsrechts auf dem Gebiet der Cybersicherheit für einen wirksameren Schutz der digitalen Ressourcen der EU und der Maßnahmen, die sie tragen, entscheidend sein kann. Wir sind der Ansicht, dass ein starkes Mandat in der Politikgestaltung ein angemessenes Governance-Modell für die Agentur erfordert, das für die Koordinierung mit anderen Organisationen sorgt, die Aufgaben in verwandten Bereichen wahrnehmen, sowie eine umfassende Kontrolle durch die Organe der Union, insbesondere im Hinblick auf die Vorbereitung und Umsetzung von Rechtsvorschriften.

Die vorgeschlagene Verordnung würde der ENISA neben einer erweiterten politischen Rolle auch eine operative Funktion als Wissenszentrum für Vorfälle gemäß der NIS-Richtlinie, der

eIDAS-Verordnung und der Richtlinie über den Europäischen Kodex für elektronische Kommunikation zusprechen (Artikel 5 Absatz 5 des Vorschlags).

Wir begrüßen Artikel 7, in dem der ENISA die Aufgabe übertragen wird, auf operativer Ebene unter anderem mit den Organen, Einrichtungen und sonstigen Stellen der Union und den für die Aufsicht über den Datenschutz zuständigen Stellen zusammenzuarbeiten, um Fragen von gemeinsamem Interesse anzugehen.

Artikel 20 bekräftigt die Existenz und Rolle einer Ständigen Gruppe der Interessenträger, die sich aus anerkannten Sachverständigen als Vertreter einschlägiger Interessenträger zusammensetzt, darunter auch Vertreter der Datenschutz-Aufsichtsbehörden. Auch wenn diese Gruppe nur beratende Funktion hat, sind wir der Ansicht, dass eine stärkere Vertretung von Datenschutz-Aufsichtsbehörden der Gruppe sehr von Vorteil wäre und die Qualität ihrer Beratung verbessern würde.

Wir stellen fest, dass es in dem Vorschlag einige Änderungen bei den Zuständigkeiten von ENISA für den Schutz der Privatsphäre und personenbezogener Daten gegeben hat.

Auch wenn es im verfügenden Teil keine wirklichen Änderungen bei den Aufgaben der ENISA im Bereich Schutz der Privatsphäre und personenbezogener Daten gegeben hat (siehe Artikel 3 Buchstabe e der Verordnung 526/2013 und Artikel 7 Absatz 2 des Vorschlags), wurden solche Aufgaben doch in vielen Erwägungsgründen der Verordnung 526/2013 direkt erwähnt (Erwägungsgründe 13, 16). Diese Erwägungsgründe finden sich im Vorschlag nicht mehr, und in Artikel 10 zu den Aufgaben der ENISA in Bezug auf Forschung und Innovation ist vom Schutz der Privatsphäre und personenbezogener Daten keine Rede mehr.

Wir bedauern, dass diese Aufgabe im Bereich Forschung und Beratung verschwunden ist, und dass diese Tatsache zur Folge haben kann, dass die Arbeiten der ENISA an Technologien für einen besseren Schutz von Privatsphäre und personenbezogenen Daten (PET)[xxxv] und eher allgemein am Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen[xxxvi] unterbrochen werden, denn wir sind entschieden der Auffassung, dass derartige Forschungs-und Beratungstätigkeiten intensiviert werden müssen, insbesondere im Hinblick auf die mit der DS-GVO begründeten Verpflichtung zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen. Derzeit gibt es keine Einrichtungen der EU, die diese Lücke füllen könnten.

Wir empfehlen dem Gesetzgeber Überlegungen dazu, wie diese politische Aufgabe am besten fortgeführt und ausgebaut werden kann, entweder durch eine explizite Bekräftigung der Rolle der ENISA im verfügenden Teil des Vorschlags oder durch Übertragung der Zuständigkeiten für den Schutz personenbezogener Daten an eine andere Einrichtung der EU. Zum Schutz personenbezogener Daten gehört zwar die Sicherheit, er ist aber nicht darauf beschränkt, und ein Mandat zu diesem politischen Aspekt sollte in einen einschlägigen Kontext eingebettet sein und mit angemessenen Ressourcen einhergehen.

Der EDSB, der gemäß Artikel 46 Buchstabe e der Verordnung (EG) Nr. 45/2001 die Aufgabe hat, *„relevante Entwicklungen zu überwachen, insoweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie“,* ist auch weiterhin bereit, seinen Beitrag zu leisten und auszubauen, entweder in enger Zusammenarbeit mit der ENISA oder auf eine andere vom Gesetzgeber vorgesehene Weise, sofern angemessene Ressourcen bereitgestellt werden.

Eine Option, Forschung und Beratung zu Technologien für einen besseren Schutz von Privatsphäre und personenbezogenen Daten (PET) zu verbessern, wäre ein stärkeres Mandat für den EDSB, das nach Möglichkeit in die derzeitige Reform der Verordnung (EG) Nr. 45/2001 einfließen sollte, und, aufbauend auf den bereits bestehenden Aufgaben, die Überwachung und Förderung der Entwicklung von PET und von Methoden für Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen. Diese Aufgabe könnte in Absprache mit einschlägigen nationalen Forschungsarbeiten von Wissenschaft, Industrie und Behörden einschließlich Datenschutzbehörden unter der Voraussetzung wahrgenommen werden, dass die Haushaltsbehörden die erforderlichen Ressourcen zuweisen.

2. Europäischer Rahmen für die Cybersicherheitszertifizierung

Verbesserung bei der Transparenz bei den Angaben zur *Vertrauenswürdigkeit*, eines des Hauptziele des neuen Vorschlags, stärkt die Fähigkeit von Nutzern, Anbietern digitaler Dienste zu vertrauen, die personenbezogene Daten verarbeiten, und trägt zur Fähigkeit von Verantwortlichen bei, Auftragsverarbeiter auszuwählen, die Garantien bieten, um der Sicherheitsverpflichtung des Datenschutzrechts Genüge zu tun.

Gemäß Artikel 43 des Vorschlags für den Rechtsakt zur Cybersicherheit soll ein System für die Cybersicherheitszertifizierung geschaffen werden, *„das der Bescheinigung dient, dass die (...) zertifizierten IKT-Produkte und Dienste auf einer bestimmten Vertrauenswürdigkeitsstufe den festgelegten Anforderungen an ihre Fähigkeit genügen, Handlungen zu widerstehen“*, die darauf abzielen, die Sicherheit zu beeinträchtigen. Gegenstand der Zertifizierung sind Produkte und Dienste, Ziel ist es, Handlungen zu widerstehen, die darauf abzielen, zentrale Sicherheitsziele zu gefährden, und bei der Zertifizierung geht es um drei Stufen der Vertrauenswürdigkeit. Nationale Aufsichtsbehörden für die Zertifizierung sind unter anderem zuständig für die Bearbeitung von Beschwerden, die von natürlichen oder juristischen Personen in Bezug auf Zertifikate eingereicht werden, die von Konformitätsbewertungsstellen in ihrem Hoheitsgebiet ausgestellt wurden, und können im Einklang mit dem einzelstaatlichen Recht Sanktionen verhängen.[xxxvii]

Dieses System weicht erheblich von dem Ansatz der DS-GVO ab. Die Zertifizierung eines oder mehrerer Verarbeitungsvorgänge gemäß Artikel 42 DS-GVO kann dazu beitragen, unter gewissen Umständen die Einhaltung der DS-GVO selber nachzuweisen, und zwar in Anwendung des Grundsatzes der Rechenschaftspflicht. Die Artikel 29-Datenschutzgruppe arbeitet derzeit an einem Leitfaden für die Zertifizierungs-und Akkreditierungskriterien in der DS-GVO. Neben anderen Elementen können die nach der DS-GVO anerkannten Zertifizierungsregelungen die Pflichten gemäß Artikel 32 DS-GVO über die Sicherheit der Verarbeitung abdecken. Gegenstand der Zertifizierung nach der DS-GVO sind Verarbeitungen personenbezogener Daten; Sicherheit ist dabei nur ein Thema, und das Konzept der Vertrauenswürdigkeitsstufen findet keine Anwendung.

Da möglicherweise ein- und dieselbe Organisation Zertifizierungen nach beiden Rechtsakten anstrebt, ist es von allergrößter Bedeutung, dass bei Technik und Governance Synergien hergestellt werden, damit Zertifizierungen nach dem Europäischen Rahmen für die Cybersicherheitszertifizierung und nach der DS-GVO von den Organisationen, die beiden Instrumenten Genüge tun möchten, nicht als widersprüchlich oder nicht zusammenhängend wahrgenommen werden. Der unterschiedliche Geltungsbereich der Zertifizierungssysteme verhindert zwar deren nahtlose Integration, doch sollten die an ihrer Umsetzung beteiligten Einrichtungen der EU dafür sorgen, dass sie einander ergänzen und verstärken. Kommission und ENISA sind aufgefordert, sich mit der Artikel 29-Datenschutzgruppe und dem künftigen EDSA wegen einer möglichen Zusammenarbeit in Verbindung zu setzen. Bevor die

Kommission einen Durchführungsrechtsakt zu einem Zertifizierungssystem gemäß Artikel 44 des vorgeschlagenen Rechtsakts zur Cybersicherheit erwägt, kann sie gerne den EDSB konsultieren und seine Ansichten berücksichtigen.

Eine Zusammenarbeit mit Datenschutzbehörden würde bei Bedarf eine wirksamere Aufsicht über beide Arten zuständiger Behörden erlauben. Der Rechtsakt zur Cybersicherheit sollte Datenschutzbehörden ausdrücklich zu den Behörden zählen, mit denen zusammenzuarbeiten ist (Artikel 50 Absatz 6 Buchstabe d).

Brüssel, den 15. Dezember 2017

Wojciech Rafał WIEWIÓROWSKI

Endnoten

[i] Gemeinsame Mitteilung der Kommission und der Hohen Vertreterin der Europäischen Union für Außen- und Sicherheitspolitik, JOIN/2017/0450 final, 13. 09.2017, http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=JOIN:2017:450:FIN

[ii] Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die „EU-Cybersicherheitsagentur" (ENISA) und zur Aufhebung der Verordnung (EU) 526/2013 sowie über die Zertifizierung von Informations- und Kommunikationstechnik („Rechtsakt zur Cybersicherheit"), COM/2017/0477 final, 13.09.2017, http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52017PC0477R(01)

[iii] Empfehlung der Kommission (EU) 2017/1584 vom 13. September 2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen, ABl. L 239 vom 19.9.2017, S. 36.

[iv] MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT, Bestmögliche Netz- und Informationssicherheit - hin zu einer wirksamen Umsetzung der Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, COM/2017/0476 final, 13.9.2017, http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=COM:2017:476:FIN

[v] https://ec.europa.eu/digital-single-market/en/cyber-security

[vi] Vorschlag für eine RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln und zur Ersetzung des Rahmenbeschlusses 2001/413/JI des Rates, COM(2017)489, 13.9.2017, http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52017PC0489

[vii] Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat und den Rat, „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion, Elfter Fortschrittsbericht", COM(2017) 608 final, http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52017DC0608

[viii] Stellungnahme des EDSB vom 10. Dezember 2010 zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Europäische Agentur für Netz- und Informationssicherheit (ENISA) https://edps.europa.eu/sites/edp/files/publication/10-12-20_enisa_de.pdf

[ix] Kommentare des EDSB vom 12. Oktober 2012 zur öffentlichen Konsultation der GD Connect zur Verbesserung der Netz- und Informationssicherheit (NIS) in der EU: https://edps.europa.eu/sites/edp/files/publication/12-10-10_comments_nis_en.pdf

[x] Stellungnahme vom Juni 2013 zur Gemeinsamen Mitteilung der Kommission und der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik „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: https://edps.europa.eu/sites/edp/files/publication/13-06-14_cyber_security_de.pdf

[xi] Stellungnahme des EDSB vom 15. Dezember 2015 zur Verbreitung und Verwendung von eingreifenden Überwachungstechnologien: https://edps.europa.eu/sites/edp/files/publication/15-12-15_intrusive_surveillance_de.pdf

[xii] Guidance on Security Measures for Personal Data Processing - Article 22 of Regulation 45/2001 (Leitlinien vom 21. März 2016 zu Sicherheitsmaßnahmen für die Verarbeitung personenbezogener Daten - Artikel 22 der Verordnung (EG) Nr. 45/2001 (nur EN)): https://edps.europa.eu/sites/edp/files/publication/16-03-21_guidance_isrm_en.pdf

[xiii] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119 vom 4.5.2016, S. 1.

[xiv] Siehe die Definition von „Verantwortlicher" in Artikel 4 Absatz 7 DS-GVO.

[xv] Siehe die Definition von „Auftragsverarbeiter" in Artikel 4 Absatz 8 DS-GVO.

[xvi] Siehe die Definition von „Verletzung des Schutzes personenbezogener Daten" in Artikel 4 Absatz 12 DS-GVO.

[xvii] 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, ABl. L 8 vom 12.1.2001, S. 1.

[xviii] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), COM(2017) 010 final, 10.1.2017, http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:52017PC0010

[xix] Special Eurobarometer 464a, Europeans' attitudes towards cyber security, published September 2017,

[xx] CERT-EU Security Advisory 2017-012 of May 22, 2017, WannaCry Ransomware Campaign

Exploiting SMB Vulnerability, https://cert.europa.eu/static/SecurityAdvisories/2017/CERT-EU-SA2017-012.pdf

[xxi] Rede von Giovanni Buttarelli, EDSB, „Chiffrement, Sécurité et Libertés at Assemblée nationale française, Paris, France“: https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/encryption-protects-security-and-privacy_en

[xxii] Scientific Opinion No. 2/2017 of 24 March 2017 of the High Level Group of Scientific Advisors to the Commission on Cybersecurity in the European Digital Single Market, section 4.1.3, https://ec.europa.eu/research/sam/pdf/sam_cybersecurity_report.pdf-

[xxiii] Vgl. Endnote **Error! Bookmark not defined.**.

[xxiv] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über eine Unionsregelung für die Kontrolle der Ausfuhr, der Verbringung, der Vermittlung, der technischen Unterstützung und der Durchfuhr betreffend Güter mit doppeltem Verwendungszweck (Neufassung), COM(2016) 616 final, 28.9.2016

[xxv] 2016/0295(COD) Unionsregelung für die Kontrolle der Ausfuhr, der Verbringung, der Vermittlung, der technischen Unterstützung und der Durchfuhr betreffend Güter mit doppeltem Verwendungszweck. Neufassung,

[xxvi] Siehe beispielsweise: https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html

[xxvii] Vgl. Endnote **Error! Bookmark not defined.**.

[xxviii] Beispiele solcher sektorspezifischen Rechtsvorschriften finden sich in der Mitteilung sowie in der NIS-Richtlinie:

- Verpflichtungen gemäß der Richtlinie 2002/21/EG für öffentliche Kommunikationsnetze und öffentlich zugängliche elektronische Kommunikationsnetze.
- Verpflichtungen gemäß der eIDAS-Verordnung 910/2014.
- Meldungen gemäß der Richtlinie 2014/64/EG über Märkte für Finanzinstrumente.
- Verpflichtungen gemäß der Verordnung 648/2012 des Europäischen Parlaments und des Rates über zentrale Gegenparteien und Transaktionsregister.
- Verpflichtungen gemäß der zweiten Zahlungsdiensterichtlinie.

[xxix] Beispielsweise Artikel 16 Absatz 11 der NIS-Richtlinie.

[xxx] Siehe die Artikel 14 und 16 der NIS-Richtlinie.

[xxxi] Die Artikel 29-Datenschutzgruppe hat einen Entwurf von Leitlinien für die Auslegung der Bestimmungen der DS-GVO zu Verletzungen des Schutzes personenbezogener Daten vorgelegt: http://ec.europa.eu/newsroom/document.cfm?doc_id=47741 Eine endgültige Fassung soll in den kommenden Monaten erscheinen.

[xxxii] Siehe ferner ENISA, Incident notification for DSPs in the context of the NIS Directive - A comprehensive guideline on how to implement incident notification for Digital Service Providers, in the context of the NIS Directive, February 2017, p. 20, abrufbar unter www.enisa.eu: *„Es kann vorkommen, dass DSB denselben Vorfall bei beiden zuständigen Behörden melden müssen. Theoretisch deckt die DS-GVO den Schutz personenbezogener Daten und die NIS-Richtlinie die Vertraulichkeit des angebotenen Dienstes und der zugrunde liegenden Daten (die meist personenbezogene Daten sind) ab. In der DS-GVO ist kein „Light Touch Approach“ zu finden, wie es ihn in der NIS-Richtlinie gibt“.*

[xxxiii] Siehe Artikel 34 DS-GVO.

[xxxiv] https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-4460501_et

[xxxv] z. B. Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies of March 2016 and subsequent measures on PETS; Privacy Enhancing Technologies: Evolution and State of the Art, March 2017, https://www.enisa.europa.eu/publications/pets-evolution-and-state-of-the-art

[xxxvi] z. B. Report on Privacy and Data Protection by Design, January 2015, https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

[xxxvii] Siehe Artikel 50 Absatz 7 und Artikel 54 des Vorschlags für den Rechtsakt zur Cybersicherheit.