Exposé der Dissertation

nach dem Arbeitstitel

Rechtliche Fragestellungen in der nationalen Umsetzung der Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen (NIS-RL)

vorgelegt von

Ing. Mag.[a] Sylvia Mayer, MA

(0657279)

am

16. November 2017

angestrebter akademischer Grad

Doctor iuris (Dr. iur.)

Betreuer

Priv.-Doz. Dr. Bernhard Müller

Studienkennzahl lt. Studienblatt:	A 783 101
Studienrichtung lt. Studienblatt:	Rechtswissenschaften
Dissertationsfach:	Öffentliches Recht

1. Einleitung

Unsere Gesellschaft ist in zunehmendem Maße von bestimmten Diensten und Technologien abhängig. Egal ob die Versorgung mit Strom, Wasser, Bargeld oder Gesundheitsleistungen – diese so genannten kritischen Infrastrukturen sorgen für die Daseinsvorsorge und das Funktionieren unserer Gesellschaft und Ausfälle bzw. Störungen dieser Unternehmen können sich unmittelbar auf viele Menschen und auf schwerwiegende Art und Weise auswirken. Eben diese Dienste sind jedoch mittlerweile in hohem Maße abhängig von der Informations- und Kommunikationstechnologie (IKT) bzw. von IT-Systemen. Energienetze und Wasserpumpen werden über zentrale Server gesteuert, Patientendaten in Krankenhäusern ausschließlich über digitale Systeme verwaltet und Transaktionen mehrheitlich über bargeldlosen Zahlungsverkehr abgewickelt. Darüber hinaus zählt mittlerweile auch das Internet zur Grundlage unserer zivilen und wirtschaftlichen Gesellschaft. Es gibt in Österreich zum jetzigen Zeitpunkt nur mehr einen sehr geringen Anteil von Menschen, die nicht täglich im Internet arbeiten, ihre Mails abrufen oder über soziale Netzwerke kommunizieren.
Aus all diesen Gründen ist die Informations- und Kommunikationstechnologie einer der wichtigsten Grundpfeiler unserer Gesellschaft – und muss entsprechend vor Ausfällen und Angriffen geschützt werden.

Die Risiken von Cyber-Angriffen sind in den letzten Jahren stark gestiegen und werden auch in den kommenden Jahren eine der größten Risiken für Wirtschaft und Bevölkerung darstellen. Nach dem Allianz Risk Barometer stellen „Cyberkriminalität, IT-Ausfälle, Spionage, Datenmissbrauch“ 17 % der globalen Bedrohungen dar und befinden sich damit auf Rang 5 der Risiken mit weiterhin steigender Tendenz.

Der Staat ist in diesem Umfeld ein Akteur von vielen (neben z.B. Betreibern und Dienstleistern, Wirtschaft und Privaten als Nutzern). Ebenso wie der Staat müssen daher auch alle anderen Akteure ihre Verantwortung wahrnehmen. Trotzdem kommt dem Staat auch weiterhin eine besondere Rolle bei der Absicherung grundrechtlicher und wirtschaftlicher Freiheiten zu.

Die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (kurz "NIS-RL"), gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 114, wurde auf Vorschlag der Europäischen Kommission aus Februar 2013, nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente, nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses, gemäß dem ordentlichen Gesetzgebungsverfahren am 6. Juli 2016 beschlossen und im August 2016 im Amtsblatt der Europäischen Union kundgemacht bzw. veröffentlicht.

Ziel der Richtlinie ist vor allem, das allgemeine Niveau der Netz- und Informationssicherheit zu erhöhen und so zum Funktionieren des Binnenmarktes beizutragen.
Dazu soll jeder Mitgliedsstaat eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen festlegen und nationale Behörden einrichten, die für die Umsetzung der festgelegten Maßnahmen verantwortlich sind. Darunter fallen unter anderem die Koordination der österreichischen Strategie, die Wahrnehmung der grenzüberschreitenden Zusammenarbeit als Single Point of Contact, die Entgegennahme und Analyse von Meldungen über signifikante Sicherheitsvorfälle, die Erstellung von Lagebildern über diese Vorfälle sowie die Überprüfung der Sicherheitsmaßnahmen in Unternehmen.

Der Anwendungsbereich der Richtlinie gliedert sich in so genannte Betreiber wesentlicher Dienste und Anbieter digitaler Dienste. Unter den Betreibern wesentlicher Dienste werden so genannte kritische Infrastrukturen aus den Bereichen Energie, Transport, Wasser, Gesundheit, Digitales, Finanzen und Finanzmarktinfrastrukturen verstanden, die eine wesentliche Bedeutung für die Aufrechterhaltung gesellschaftlicher Funktionen haben und deren Ausfall oder Störung schwerwiegende Auswirkungen auf die Bevölkerung haben könnte. Anbieter digitaler Dienste sind in der Richtlinie als Online-Marktplätze, Online-Suchmaschinen und Cloud Service Provider geregelt.

Diese Betreiber und Anbieter werden in der Richtlinie konkreten Verpflichtungen unterworfen, nämlich der Meldung schwerwiegender Störfälle in ihren IKT-Systemen sowie das Treffen geeigneter technischer und organisatorischer Sicherheitsmaßnahmen, um Ausfälle zu verhindern.

2. Problemstellung

Die Umsetzung der Richtlinie in nationales Recht muss mit der bereits bestehenden österreichischen Rechtslage im Einklang sein. Einerseits sind bestehende verfassungsrechtliche und einfachgesetzliche Normen, die IT-Sicherheit oder sonstige Rahmenbedingungen regeln, zu berücksichtigen. Ebenso muss bei Vorliegen mehrerer Optionen zur Umsetzung jene gewählt werden, die aufgrund existierender Strukturen und Organisationen geeignet erscheint.

In Bezug auf die Richtlinie im Allgemeinen soll eine rechtspolitische Diskussion über die immer stärker in Erscheinung tretende „Kompetenzblindheit“ der Europäischen Union geführt werden, wodurch ein zunehmender Eingriff in innerstaatliche Kompetenzen erfolgt.

Einer rechtspolitischen Diskussion soll des Weiteren das am 01.07.2017 in Kraft getretene Bundesgesetz über die Grundsätze der Deregulierung zugeführt werden, das unter anderem vorgibt, dass Rechtsakte der Europäischen Union nicht ohne Grund übererfüllt werden. In Anbetracht des Vorhabens des österreichischen Gesetzgebers, über die NIS-RL hinaus weitere Sektoren in den Anwendungsbereich des NIS-Gesetzes miteinzubeziehen, sind Zielsetzung und Begründung der beiden einander möglicherweise widersprechenden Regelungen gegenüberzustellen.

Zu untersuchen sind außerdem einerseits kompetenzrechtliche Zuständigkeiten nach den Art. 10 – 15 B-VG. Die Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit – als möglicherweise primärer Tatbestand der Cyber Sicherheit – ist gemäß Art. 10 Abs. 1 Z 7 B-VG sowohl in Gesetzgebung als auch Vollziehung Zuständigkeit des Bundes und damit unproblematisch hinsichtlich der Umsetzung der Richtlinie in Form eines Bundesgesetzes. Fraglich sind darüber hinaus jedoch Fachmaterien wie beispielsweise der Sektor Gesundheit sowie das Elektrizitätswesen, bei denen möglicherweise eine Zuständigkeit in Gesetzgebung der Länder gegeben ist. Dabei wird zu untersuchen sein, ob eigene landesgesetzliche (Ausführungs-)Regelungen notwendig sein werden. Ebenso soll rechtspolitisch diskutiert werden, inwieweit die Schaffung einer eigenen Bundeskompetenz in Bezug auf Cyber Sicherheit Sinn machen könnte, um eine unnötige Zersplitterung – auch in künftigen Rechtsmaterien – zu vermeiden.

Ein zentraler Punkt des zu erstellenden Bundesgesetzes wird dessen Anwendungsbereich sein. Dazu müssen die Mitgliedsstaaten entsprechend den Vorgaben der NIS-RL ihre nationalen Betreiber auswählen, die in ihren Staaten einen wesentlichen Dienst erbringen. Dazu bestehen innerstaatlich mehrere Möglichkeiten. Einerseits könnte der Gesetzgeber

selbst bzw. durch Verordnungsermächtigung im Rahmen einer Verordnung eine Liste der Betreiber erstellen und diese kundmachen. Dies würde jedoch dem Schutz dieser Betreiber zuwiderlaufen, weil eine Veröffentlichung dieser Liste erst recht potenzielle Angriffsziele für Angreifer darstellen könnte. Die zweite Möglichkeit – die auch im deutschen IT-Sicherheitsgesetz Anwendung gefunden hat – ist, in einer Verordnung (aufgrund einer gesetzlichen Verordnungsermächtigung im Bundesgesetz) spezifische Kriterien festzulegen, anhand derer die nationalen Betreiber selbst entscheiden müssen, ob sie in den Anwendungsbereich fallen und daher der Meldepflicht unterliegen. Der Nachteil dieser Alternative besteht in der möglichen Rechtsunsicherheit der Unternehmen, die nie gänzlich davon überzeugt sein können, tatsächlich im Anwendungsbereich zu liegen. Dies erscheint insofern problematisch, als an die Nichterfüllung von Verpflichtungen verwaltungsrechtliche Sanktionen geknüpft sein werden. Die dritte Möglichkeit liegt in der Festlegung der Kriterien in einer Verordnung und der darauf basierenden Identifizierung der Betreiber durch die Behörden selbst. In weiterer Folge müssten die Betreiber möglicherweise durch Bescheid über deren Rolle als Betreiber eines wesentlichen Dienstes in Kenntnis gesetzt werden. Diese Fragestellung sollte vor dem Hintergrund des Legalitätsprinzips diskutiert werden, insbesondere in Bezug auf die Judikatur des Verfassungsgerichtshofes zum „differenzierten Legalitätsprinzip“ (VfGH 11.3.1999, V40/98 ua.), demnach in Bereichen, in denen eine exaktere Determinierung möglich ist und in denen das Rechtsschutzbedürfnis (wie etwa im Strafrecht) eine besonders genaue Determinierung verlangt, eine weit gehende gesetzliche Vorherbestimmung als erforderlich anzusehen ist.

Weitere rechtliche Fragen im Zuge der Umsetzung könnten sich in Bezug auf bereits bestehende Verpflichtungen zur Meldung von sicherheitsrelevanten Vorfällen sowie bestehende verpflichtende Sicherheitsstandards für Unternehmen in der europäischen und österreichischen Rechtsordnung stellen. Zu nennen ist hier beispielsweise die Richtlinie 2015/2366 des europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt. Gem. Art. 95 haben Zahlungsdienstleister einen Rahmen angemessener Risikominderungsmaßnahmen und Kontrollmechanismen zur Beherrschung der operationellen und der sicherheitsrelevanten Risiken zu schaffen. Als Teil dieses Rahmens müssen die Zahlungsdienstleister wirksame Verfahren für das Management von Vorfällen – auch zur Aufdeckung und Klassifizierung schwerer Betriebs- und Sicherheitsvorfälle – festlegen und anwenden. Gem. Art. 96 haben die Zahlungsdienstleister im Falle eines schwerwiegenden Betriebs- oder eines Sicherheitsvorfalles unverzüglich die zuständige Behörde im Herkunftsmitgliedstaat zu unterrichten. In der nationalen Rechtsordnung existieren beispielsweise Verpflichtungen zum Treffen angemessener Sicherheitsvorkehrungen im Gesundheitstelematikgesetz oder im Eisenbahngesetz, Meldepflichten unter anderem im Bankwesengesetz. Insbesondere die Abgrenzung zu meldepflichtigen Vorfällen nach der Datenschutzgrundverordnung, die im Mai 2018 in Kraft treten wird, wird näher zu untersuchen sein, da ein und derselbe Vorfall Meldepflichten und Sanktionierungen nach beiden Rechtsmaterien auslösen und gegebenenfalls dem Verbot der Doppelbestrafung widersprechen könnte.

Darüber hinaus ist den Mitgliedsstaaten die Höhe der Sanktionierung der Verwaltungsübertretungen offengehalten. Orientiert man sich hierbei an der Datenschutzgrundverordnung – die ähnliche Verwaltungsübertretungen regelt und sanktioniert - und deren Strafhöhen, kommt es zu unverhältnismäßigen Differenzen zu den Geldstrafen im nationalen gerichtlichen Strafrecht. Ähnlich hohe Strafen wie in der Datenschutzgrundverordnung sind in der nationalen Rechtsordnung auch im Banken- und

Kapitalmarkt vorgesehen. Nach der ständigen Judikatur des Verfassungsgerichtshofes sind hohe Strafen nur von ordentlichen Gerichten zu verhängen, nicht von einer Verwaltungsbehörde. Der Verfassungsgerichtshof prüft in Bezug darauf aktuell eine Strafbestimmung des Bankwesengesetzes (BWG), konkret § 99d, auf ihre Verfassungsmäßigkeit.
Ebenso wird der für Meldeprozesse erforderliche Austausch von personenbezogenen Daten (IP-Adressen) zwischen privaten Unternehmen und das dabei bestehende Verhältnis zur Datenschutzgrundverordnung zu diskutieren sein.

Eine für die Unternehmen wichtige Frage stellt die Geltung des so genannten Offizialprinzips gemäß der Strafprozessordnung im Rahmen der Meldepflicht dar, demnach die Kriminalpolizei bei jedem Verdacht einer Straftat Ermittlungen einzuleiten hat. Da dies nicht immer im Interesse der Betreiber liegt, wird nach Möglichkeiten gesucht, diese Ermittlungspflicht – insbesondere bei freiwilligen Meldungen – hintanzuhalten.

Grundsätzlich soll auch das bisher in Österreich vorherrschende Prinzip der Public Private Partnership – dem Schutz kritischer Infrastruktur ohne konkrete Verpflichtungen für die Betreiber – dem nunmehr in Kraft tretenden Verpflichtungen für diese Unternehmen durch die NIS-RL gegenübergestellt werden. Insbesondere wird zu untersuchen sein, inwieweit eine Differenzierung zwischen physischer Sicherheit (für die es keine Verpflichtungen gibt) und Sicherheit der IT-Systeme verfassungsrechtlich zulässig ist. Darüber hinaus sind diese Eingriffe bzw. deren Zulässigkeit in Bezug der verfassungsrechtlich gewährleisteten Rechte auf Freiheit des Eigentums und der Erwerbsausübung zu diskutieren.

3. Stand der Forschung

Die gegenständliche Richtlinie muss von den Mitgliedsstaaten bis spätestens Mai 2018 in nationales Recht umgesetzt werden. Dementsprechend wurde bereits im Februar 2016 unter der Federführung des Bundeskanzleramtes eine interministerielle Arbeitsgruppe eingesetzt, die an einem Entwurf für das so genannte Bundesgesetz zur Gewährleistung der Sicherheit von Netz- und Informationssystemen (auch „Cybersicherheitsgesetz“) arbeitet. Parallel dazu arbeitet auf europäischer Ebene die EU-Kooperationsgruppe (Vertreter aller Mitgliedsstaaten sowie der Europäischen Kommission) an Dokumenten zur Unterstützung der Mitgliedsstaaten, vor allem in Bezug auf die Identifizierung der Betreiber wesentlicher Dienste.

Aufgrund des Umstandes, dass das Bundesgesetz zur Umsetzung der Richtlinie (Mai 2018) vor Fertigstellung gegenständlicher Dissertation (WS 2018/2019) in Kraft treten wird, wird das Gesetz sodann in die Betrachtungen der Dissertation mit aufgenommen. Nichtsdestotrotz werden alle Umsetzungsoptionen der NIS-RL sowie rechtliche Fragestellungen im Rahmen der Umsetzung diskutiert.

4. Methode

Im ersten Teil werden die Vorgaben der NIS-RL sowie deren Erwägungsgründe vollständig durch eine systematische Inhaltsanalyse (qualitativ, deduktiv) erfasst und diskutiert.

Im zweiten Teil erfolgte eine Untersuchung der nationalen Rechtslage nach bereits bestehenden Regelungen, die im Zuge der Umsetzung berücksichtigt werden müssen, sowie der Schnittstellen zu sonstigen zu beachtenden EU-Rechtsakten.

Den Kernbereich bildet der dritte Teil des Dissertationsvorhabens, in dem rechtliche Fragestellungen und Schwierigkeiten, die sich durch in Kraft befindliche nationale Normen ergeben, rechtsdogmatisch analysiert und beantwortet werden.

5. Forschungsfragen

Im Rahmen der Dissertation sollen folgende Forschungsfragen behandelt werden:

- Welche Umsetzungsoptionen ermöglicht die NIS-RL bzw. in welcher Form kann die Umsetzung in nationales Recht erfolgen?
- Welche nationalen Regelungen bestehen bereits hinsichtlich des Schutzes kritischer Infrastruktur und der Cyber Sicherheit?
- Welche rechtlichen Schwierigkeiten und Fragestellungen ergeben sich aufgrund der bestehenden österreichischen Rechtlage im Zuge der Umsetzung?

6. Vorläufiges Inhaltsverzeichnis

1. Einleitung
2. Grundlagen der Untersuchung
    a. Aufbau der Arbeit
    b. Untersuchungsbedingungen
    c. Forschungsinteresse und Forschungsfragen
    d. Methodische Vorgangsweise
3. Analyse der Richtlinie für Netz- und Informationssicherheit
    a. Kompetenzgrundlage der Europäischen Union
    b. Entwicklung
    c. Erwägungsgründe
    d. Analyse der Inhalte
4. Bisherige nationale Regelungen und Strukturen zum Schutz kritischer Infrastruktur und zur Cyber Sicherheit in Österreich
    a. Verfassungsrechtliche Kompetenzen
        i. Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit (Art. 10 Abs. 1 Z 7 B-VG)
        ii. Militärische Landesverteidigung (Art. 79 Abs. 1 B-VG)
        iii. Assistenzeinsatz (Art. 79 Abs. 2 Z 1 lit. b B-VG)
        iv. Sonstige Kompetenztatbestände (z. B. Gesundheitsversorgung etc.)
        v. Notwendigkeit einer Bundeskompetenz für Cyber Sicherheit
    b. Einfachgesetzliche Aufgaben und Befugnisse in Bezug auf den Schutz kritischer Infrastruktur und Cyber Sicherheit
        i. Bundesministeriengesetz
        ii. Sicherheitspolizeigesetz
        iii. Militärbefugnisgesetz
    c. Kritische Infrastrukturen in Österreich
        i. Definition (Sicherheitspolizeigesetz, Strafgesetzbuch)
        ii. Identifizierung kritischer Infrastruktur
    d. Bestehende Verpflichtungen für kritische Infrastrukturbetreiber in Österreich
        i. Unternehmensgesetzbuch
        ii. Gesundheitstelematikgesetz
        iii. Eisenbahngesetz
        iv. Telekommunikationsgesetz

e. Bestehende Organisationen und Strukturen
    i. Computer Emergency Response Teams (CERTs) und deren rechtlicher Rahmen
f. Public Private Partnership vs. Auferlegung von Verpflichtungen
    i. Rechtliche Verantwortlichkeit des Staates für Betreiber kritischer Infrastruktur
    ii. Prinzip der Subsidiarität und Selbstverpflichtung
    iii. Eingriff in verfassungsrechtlich gewährleistete Rechte der Betreiber und Anbieter
        1. Erwerbsausübungsfreiheit
        2. Eigentumsfreiheit

5. Schnittstellen zu anderen relevante Unionsrechtsakten
    a. Richtlinie 114/2008 zum Schutz kritischer Infrastruktur
    b. Datenschutzgrundverordnung
    c. Richtlinie 2015/2366 für Zahlungsdienste im Binnenmarkt
6. Schwierigkeiten und rechtliche Fragestellungen in der nationalen Umsetzung
    a. Verfassungsrechtliche Kompetenzen
    b. Identifizierung des Anwendungsbereiches
    c. Implementierung einer Meldeverpflichtung
    d. Möglichkeiten der Vereinheitlichung von Meldewegen aus verschiedenen Bundesgesetzen
    e. Festlegung von Mindestsicherheitsstandards
    f. Einbindung privater Organisationen in Form einer Beleihung
    g. Offizialprinzip als Herausforderung des Informationsaustausches

7. Zeit- und Arbeitsplan

Stand November 2017	Themenwahl Literatur- und Judikaturrecherche Erstellung eines Exposés Absolvierung der Lehrveranstaltungen der Studieneingangsphase gem. § 4 Abs. 1 lit a bis d des Studienplans
SS 2018	Weiterführende Literatur- und Judikaturrecherche Erstellung Kapitel 1 – 4 Absolvierung der übrigen Lehrveranstaltungen laut Studienplan (§ 4 Abs. 1 lit e)
SS 2018	Erstellung Kapitel 5 - 6
WS 2018/2019	Überarbeitung und Fertigstellung der Dissertation Abgabe der Dissertation Defensio

8. Ausgewählte Literatur

Arbeitsprogramm der Österreichischen Bundesregierung 2013-2018." (2013).

Bartsch, Frey. "Staatliche Lösungsansätze" in "Cyberstrategien für Unternehmen und Behörden".

Bendiek. "Cybersicherheit und internationale Beziehungen. Zur Sorgfaltsverantwortung in der Außen- und Sicherheitspolitik" - ZBP Zeitschrift für Politikberatung.

Berger. "Zwischen Strafverfolgung und nachrichtendienstlicher Analyse. Konsequenzen aus der Europäisierung der Cybersicherheitspolitik für Deutschland." - Integration

Bräutigam, Wilmer. "Big Brother is watching you? - Meldepflichten Im Geplanten It-Sicherheitsgesetz." *Zeitschrift für Rechtspolitik* 02/2015.

Brisch. "Der Beitrag des Rechts zur IT-Sicherheit: Rechtsrahmen, Anforderungen, Grenzen".

Einzinger, Skopik, Fiedler. "Keine Cyber-Sicherheit ohne Datenschutz." *Datenschutz und Datensicherheit - DuD* 11/2015.

Gitter, Meißner, Spauschus. "Das It-Sicherheitsgesetz." *Datenschutz und Datensicherheit - DuD* 1/2016 (2016): 7-11.

Grobauer, Kossakowski, Schreck. "Klassifikation von IT-Sicherheitsvorfällen." *Datenschutz und Datensicherheit - DuD* 01/2016.

Heidrich, Wegener. "Datenschutzrechtliche Aspekte bei der Weitergabe von IP-Adressen." *Datenschutz und Datensicherheit - DuD* 03/2010: 172-77.

Hellwig. "Anforderung an die Modellierung der Kommunikation von CERTs".

Huber, Hellwig, Quirchmayr. "Wissensaustausch und Vertrauen unter Computer Emergency Response Teams - Eine europäische Herausforderung." *Datenschutz und Datensicherheit - DuD* 3/2016 (2016).

Hübner. "Wie wirken Standards und Normen im Recht?". *Datenschutz und Datensicherheit - DuD* 01/2011.

Kerstens, Reuter, Schröder. "Gesetze und Standards im Umfeld der Informationssicherheit".

Kilian, Detlef. "Vorbereitung und Durchführung von IT-Sicherheitsaudits." *IT-Sicherheit und Datenschutz* 10/2007 (2007).

Krabbes. "Die Zertifizierung in der Informationssicherheit" in "Zertifizierung als Erfolgsfaktor".

Leisterer, Schneider. "Informationshandeln des Staates im Recht der IT-Sicherheit"

"Österreichische Strategie für Cyber Sicherheit." (2013).

"Österreichisches Programm zum Schutz Kritischer Infrastruktur (APCIP)." (2014).

Das Europäische Parlament. "Richtlinie (EU) 2016/1148 Des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung eines hohen gemeinsamen
Schneider. "Meldepflichten im IT-Sicherheitsrecht".

Sicherheitsniveaus von Netz- und Informationssystemen in der Union." (06.07.2016 2016).

Skopik, Fiedler, Lendl. "Cyber Attack Information Sharing." *Datenschutz und Datensicherheit - DuD* 04/2014.

"Verordnung (EU) Nr. 526/2013 des Europäischen Parlaments und des Rates vom 21. Mai 2013 über die Agentur der Europäischen Union für Netz- Und Informationssicherheit (ENISA), European Union, 2015, S. 1-26.".

Wischmeyer. "Informationssicherheitsrecht. IT-Sicherheitsgesetz und NIS-Richtlinie als Bausteine eines Ordnungsrechts für die Informationsgesellschaft".