universität wien

MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

„Datenschutz und IT-Security als Standortvorteil: Ein europäisches Modell“

verfasst von / submitted by

Paul Rockenbauer, BSc

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Diplom-Ingenieur (Dipl.-Ing.)

Wien, 2018 / Vienna 2018

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	A 066 926
Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet:	Masterstudium Wirtschaftsinformatik
Betreut von / Supervisor:	Univ.-Prof. Dipl.-Ing. Dr. Dr. Gerald Quirchmayr

Abstract

Privacy and cybersecurity play a core role in our daily lives. Our governments, economies and societies rely heavily on the effective and efficient operation of information technology and networks, especially the internet.
The degree of interdependence between the employed technologies is today much higher than ever before and more and more devices are generating and transmitting our personal data.
Consequently, a high degree of both privacy and cybersecurity is needed to protect individuals, processes, enterprises and whole economies. However, the awareness of these two topics in society and also in economy still is relatively low.
Hence, a new approach is needed. This master thesis contains an argumentation for a strengthened role of privacy and cybersecurity as competitive advantages in the Austrian and European market. The research discusses, whether and how privacy and cybersecurity can be enabled to play this role and which conditions are necessary.
Current regulations, such as the GDPR and the directive on network and information security and several national cyber security strategies, and the effects of new technology, such as Cloud Computing, on privacy and security were analysed. Furthermore, an empirical part, containing interviews with experts, was added to deepen the argumentation. According to the analyses, literature research and discussions within this masterthesis, privacy and cybersecurity are able to provide strong European competitive advantages, given the right conditions and circumstances.
Based on this analysis work, a framework, containing such central conditions, was designed and provided within a model, supported by a web-based tool.

Keywords

Privacy, cyber security, competitive advantage, General Data Protection Regulation, Directive on Network and Information Security, National Cyber Security Strategy, Cloud Computing

Kurzfassung

Datenschutz und IT-Sicherheit spielen in unserem Alltag zentrale Rollen.
Regierungen, Gesellschaften und ganze Wirtschaftsräume sind massiv vom Funktionieren von Netzwerken und Informationssystemen, wie vor allem dem Internet, abhängig.
Ein steigender Grad an Interdependenz zwischen den eingesetzten Technologien und immer mehr Geräte, die laufend personenbezogene Daten generieren, erhöhen die Herausforderung an Datenschutz und IT-Security im privaten, unternehmerischen und staatlichen Umfeld. Dennoch ist die Awareness für diesen Bereich in breiten Teilen der Bevölkerung relativ niedrig, es scheint also ein neuer Zugang nötig.
Diese Masterarbeit enthält eine Argumentation für die verstärkte Rolle von Datenschutz und IT-Sicherheit als Wettbewerbsvorteile für den österreichischen bzw. europäischen Standort und diskutiert, welche Faktoren für diese Stärkung notwendig sind.
Aktuelle rechtliche Regelungen, wie etwa die Datenschutz-Grundverordnung oder die NIS-Richtlinie und Cyber-Securitystrategien verschiedener Länder wurden dafür genauso analysiert, wie die Auswirkungen von Technologien - beispielsweise Cloud Computing - auf Datenschutz und IT-Security.
Ein empirischer Teil, der vier Expertengespräche beinhaltet, wurde zudem im Rahmen dieser Arbeit durchgeführt, um einen vertiefenden Einblick in die Materie zu gewinnen.
Nach der Literaturrecherche, den Analysen und den Gesprächen mit den Experten kommt die vorliegende Arbeit zum Schluss, dass Datenschutz und IT-Security unter den richtigen Rahmenbedingungen wesentliche europäische Standortvorteile darstellen können.
Auf der Analyse aufbauend wurde ein Framework, welches zentrale Rahmenbedingungen enthält, damit Datenschutz und IT-Security entsprechende positive Standortfaktoren darstellen können, wurde entwickelt und schließlich mittels eines Modells und Webtools zur Verfügung gestellt.

Schlüsselbegriffe

Datenschutz, IT-Sicherheit, Standortvorteil, Datenschutz-Grundverordnung, NIS-Richtlinie, Nationale Cybersecuritystrategie, Cloud Computing

Eigenständigkeitserklärung

Hiermit versichere ich ehrenwörtlich, die vorliegende Masterarbeit selbstständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich auch sonst keiner unerlaubter Hilfe bedient zu haben, dass ich dieses Masterarbeitsthema bisher weder im In- noch im Ausland in irgendeiner Form als Prüfungsarbeit vorgelegt habe und dass diese Arbeit mit der vom Begutachter beurteilten Arbeit vollständig übereinstimmt.

Wien, 25.01.2018

Unterschrift

Contents

1 Vorwort - Danksagung

Im Zuge meines Bachelor- und Masterstudiums der Wirtschaftsinformatik an der Universität Wien durfte und musste ich mich mit einer Vielzahl an Themen, Fachgebieten und Technologien beschäftigen. Prinzipien, Funktionsweisen und angewandtes Wissen im Bereich der Informatik, der Wirtschafts- und der Rechtswissenschaften zeichneten das Studium dabei in meinen Augen besonders aus. Auch die vorliegende Arbeit beschäftigt sich mit zutiefst interdisziplinären Themen. In den Bereichen Datenschutz und IT-Security treffen technische, wirtschaftliche, rechtliche und politische Fragestellungen aufeinander. Und genau das macht meiner Meinung nach die Faszination an Wirtschaftsinformatik als Schnittstellendisziplin aus: Technologische Entwicklungen isoliert zu betrachten, wäre ein Fehler. Sie haben oft beträchtlichen Einfluss auf Wirtschaft, Politik und Gesellschaft. Umso bedeutender ist es also, Rahmenbedingungen für die erfolgreiche Anwendung von Technologie und Technik zu definieren. Diese Arbeit stellt so einen Versuch auf einem kleinen Gebiet dar.
Am Ende eines langen Weges gilt es schließlich auch, persönliche Dankesworte auszusprechen.
Zu Beginn möchte ich mich bei meinem Betreuer, Univ.-Prof. Dipl.-Ing. Dr. Dr. Gerald Quirchmayr, bedanken, nicht nur für die großartige Betreuung dieser Masterarbeit, sondern für zahlreiche interessante Lehrveranstaltungen und inspirierende Gespräche im Rahmen der letzten Jahre.
Großer Dank gilt ebenso den Experten, die ich im Rahmen dieser Arbeit interviewen durfte.
Ein Studium zu absolvieren ist schließlich auch immer Teamwork. Insofern bedanke ich mich bei allen Kolleginnen und Kollegen, mit denen ich in den vergangenen Semestern Gruppenarbeiten absolviert und gemeinsam für Prüfungen gelernt habe. Diese Art von Austausch bereichert den Studienalltag ungemein und vermittelt viele wichtige Fertigkeiten.
Ohne die Unterstützung meiner Familie, speziell meiner Eltern, meiner Freundin, meines Bruders und meiner Großeltern, wären die Aufnahme eines Studiums und dessen erfolgreicher Abschluss nicht möglich gewesen. Ihnen sei an dieser Stelle herzlich gedankt.
Berufliche Tätigkeit und Studium miteinander in Einklang zu bringen ist ein besonderes
Kunststück, das sich selten einfach gestaltet. Unterstützt haben das meine stets sehr verständnisvollen Arbeitgeber, ganz besonders möchte ich mich an dieser Stelle bei Peter, René, Moritz und Cordula bedanken.
Abschließend gilt das Dankeswort meiner Studentenverbindung, der Katholisch-akademischen Verbindung Bajuvaria. Im Rahmen der dort verbrachten Zeit und des Engagements durfte ich eine Fülle an interessanten Persönlichkeiten treffen, wahre Freunde gewinnen und Fertigkeiten erlernen, die heutzutage im Studium wohl eher nicht ausreichend vermittelt werden können. Vielen Dank.

Vivat academia!

2 Einführung - Motivation

Datenschutz als Wettbewerbsvorteil - Privacy sells. Das gleichlautende Buch von Dr. Helmut Bäumler war eine der ersten Quellen, die im Zuge der Literaturrecherche für diese Arbeit gesichtet wurde. Dieses Buch aus dem Jahr 2002, im Zeithorizont der Informatik quasi steinalt, zeigte ein deutliches Bild: Datenschutz könne nicht nur als regulatorisches Hindernis, sondern als echter Standort- bzw. Wettbewerbsvorteil gesehen werden. Auch im Jahr 2016 erschien das Konzept noch einigermaßen visionär, obwohl es zum damaligen Zeitpunkt bereits 14 Jahre alt war. [2]
Generell ist die Bedeutung des Themas Datenschutz so aktuell wie selten zuvor. Immer mehr personenbezogene Daten werden von Geräten im Verbund des *Internet of Things* erzeugt. *Big Data* bzw. *Massendaten* können immer besser verarbeitet und interpretiert werden und stellen den Datenschutz vor rechtliche, technische aber auch politische und philosophische Fragestellungen. Dabei hat der Datenschutz für viele Adressaten einen eher fahlen Beigeschmack, gilt gar als Rand- oder Elitenthema und scheint wenig Bezug zur Lebensrealität vieler Personen zu haben.
Freilich stellt dies nicht der Wahrheit letzten Schluss dar. Menschen, die behaupten 'ohnehin nichts zu verbergen zu haben', teilen selten mit Begeisterung jedes noch so persönliche Detail ihres Privat- oder Berufslebens. Und Personen, die sich modernen Devices und somit dem *Internet of Things* komplett entziehen können, sind immer seltener anzutreffen.
Datenschutz geht also alle an und stellt ein breites gesellschaftliches, wirtschaftliches und politisches Thema dar. Als solches bietet es nicht nur Risiken und Gefahren, sondern kann auch als Positivum und Chance begriffen werden. Gerade der Standort Europa kann hier im Vergleich zu anderen Regionen und Wirtschaftsräumen der Welt handfeste Vorteile anbieten und somit einen Wettbewerbsvorteil aus Datenschutz generieren. Die ab Mai 2018 zwingend anzuwendende Datenschutz-Grundverordnung und die hochaktuellen begleitenden Gesetze der Mitgliedstaaten sowie die heftig geführten Diskussionen darüber zeigen die Brisanz der Thematik. [62]
Viele der Aussagen über den Datenschutz treffen ebenso auf den Bereich der IT-Sicherheit zu. Auch dieses Thema ist in der breiten Bevölkerung meist wenig beachtet, bis ein negatives Ereignis geschieht. Zwar kann sich ein Produkt oder Service mit besonders hoher IT-Security landläufig wohl stärker als mit vergleichsweise hohem Datenschutz in Werbung und Vermarktung durchsetzen, dennoch ist der Faktor Sicherheit wohl nicht unbedingt immer der erste Gedanke beim Download einer App.
Genauso wie beim Datenschutz gilt: Auch IT-Sicherheit kann einen österreichischen bzw. europäischen Standortvorteil darstellen. Die NIS-Richtline der EU verlangt von den Mitgliedstaaten die Implementierung einer nationalen Cybersicherheitsstrategie und ist ebenso ab Mai 2018 anzuwenden. Die Aktualität ist also auch in der Cybersecurity absolut gegeben. [51] Im Zuge der im Rahmen dieser Arbeit geführten Interviews, Dr. Bäumler konnte übrigens höchst erfreulicherweise persönlich als Gesprächspartner gewonnen werden, wurde eines

klar: Datenschutz und IT-Security gewinnen in der heutigen Gesellschaft rasant an Bedeutung. Wir können diese beiden Gebiete und Herausforderungen an uns vorbeiziehen lassen und die Entwicklung von innovativen Konzepten anderen überlassen, oder wir, als Österreich und als Europa, ergreifen die Chance und nehmen das Heft des Handels in unsere Hand. [22]
Diese Arbeit soll somit einen Beitrag zur sachlich orientierten, faktenbasierten Diskussion über Datenschutz und IT-Sicherheit sowie ihrer Eignung als Standortvorteile leisten.

3 Datenschutz als Wettbewerbs- und Standortvorteil

Data is the new oil.
Daten sind das neue Öl. Einer Reihe von Personen wird zugeschrieben, Urheber dieses vielgehörten Zitats zu sein. Am öftesten wird der Satz dem britischen Mathematiker Clive Humby zugesprochen, der 2006 hinzufügte, dass 'rohe' Daten, gleichsam dem Rohöl, von sehr begrenztem Nutzen seien. Vielmehr müssten sie analysiert und weiterverarbeitet werden, um zweckdienlich zu sein - eben gleich dem Rohöl, das zu Treibstoff, Plastik oder Chemikalien raffiniert werden muss. Die Öl-Daten Analogie trifft allerdings nur teilweise zu. Während das Öl als fossiler Rohstoff sprichwörtlich in der Erde ruht, werden Daten - quasi erneuerbaren Ressourcen gleich - ständig neu generiert. Wiederum passender ist der Vergleich im Bereich des wirtschaftlichen Nutzens des Rohstoffs. Daraus leiten sich spannende Fragestellungen ab. Wer sind die Förderer, wer die Verarbeiter der Ressource Daten? Welche Regelungen bedarf es in der Erhebung und Verarbeitung dieser Daten? Wenn Daten das 'neue Öl' sind, inwiefern gleicht der Datenschutz dann einem 'neuen Umweltschutz', wie manchmal kolportiert wird? Und kann aus diesem Datenschutz sogar in einem gewissen Maß ein Standortvorteil - quasi analog zu Green Tech und Innovation - generiert werden?

In diesem Kapitel soll ein Überblick über das Thema Datenschutz als Wettbewerbsvorteil gewährt werden. Dies umfasst anfangs einen historischen Aufriss über den Datenschutz sowie eine ausführliche Zusammenfassung und Analyse der im Zeitraum 2016-2018 wohl bedeutendsten Maßnahme der Datenschutzgesetzgebung, der Verordnung (EU) 2016/679 (besser bekannt als Datenschutz-Grundverordnung bzw. DSGVO). [62]
Weiters wird die nationale österreichische Umsetzung der Öffnungsklauseln und Regelungsspielräume der DSGVO, das Datenschutz-Anpassungsgesetz, zusammengefasst und analysiert. Auch die außereuropäische Datenschutzgesetzgebung wird, mit Fokus auf die USA und die Volksrepublik China, kurz behandelt. Im Zuge der Erstellung dieser Arbeit wurden auch einige Experteninterviews geführt, deren Einschätzungen zu Datenschutz und seine Möglichkeiten als Wettbewerbsvorteil den Weg in diese Arbeit und in dieses Kapitel gefunden haben.

3.1 Einführung aktuelle Situation - Motivation

Der Begriff Datenschutz ist mittlerweile allgegenwärtig geworden. Auf seine aktuelle Bedeutung wurde bereits eingegangen, ein Überblick im historischen Kontext folgt noch in diesem Kapitel.
Wie aber stellt sich die aktuelle Situation im Jahr 2017 dar?
Die Anforderungen an und die Herausforderungen für den Datenschutz sind wohl selten je so groß wie heutzutage gewesen. Technologie, die personenbezogene Daten generiert, erfasst und weiterverarbeitet durchdringt das alltägliche Leben wie nie zuvor. Im *Internet of Things*, auf Deutsch manchmal treffend als *Allesnetz* bezeichnet, vernetzen sich unzählige Gegenstände des täglichen

Lebens miteinander. Wie bei vielen technische Innovationen sind die daraus entstehenden Vorteile für Alltag, Arbeit und Freizeit enorm, allerdings dürfen auch potentielle Nachteile, etwa im Bereich des Datenschutzes, nicht verkannt werden. Nicht zuletzt deshalb kommt den technischen und rechtlichen Rahmenbedingungen große Bedeutung zu. Dabei soll technische Innovation keinesfalls von überbordender Regulierung ausgebremst werden, allerdings müssen klare Regelungen definieren, wie personenbezogene Daten im privaten, behördlichen und unternehmerischen Kontext geschützt werden müssen.
Dies ist aber keinesfalls so zu interpretieren, dass diese datenschutzrechtlichen Regeln Innovation und unternehmerischer Tätigkeit konträr entgegenstehen dürfen. Vielmehr soll ein hohes Niveau an Datenschutz und IT-Security einen echten Wettbewerbsvorteil für heimische Unternehmen darstellen. Die dazu notwendigen Rahmenbedingungen sollen in dieser Arbeit aufgezeigt werden.
Bei der grundsätzlichen Bedeutung von Datenschutz im betrieblichen Kontext für und in den Unternehmen selbst zeichnen sich unterschiedliche Bilder.
Laut einer Umfrage von Ernst & Young, über die die österreichische Tageszeitung 'Standard' im April 2017 berichtete, haben gerade österreichische Firmen in Sachen Datenschutz noch Nachholbedarf. [39]
Demzufolge wird die Priorität von betrieblichem Datenschutz und die Zuordnung als Thema für die oberste Managementebene bei mehr als zwei Drittel der Befragten erkannt, allerdings stehen ebenfalls laut Angaben der Unternehmen in mehr als der Hälfte der Fälle dafür nicht genügend Mittel und nicht genügend Personal zur Verfügung. Die E&Y Studie verortete Österreich im Bereich des Datenschutzes als international hinterherhinkend, nur ein Viertel der Unternehmen würde Datenschutzrisiken im Risikomanagement angemessen berücksichtigen. Datenschützer seien auch in großen Unternehmen oft Einzelkämpfer. [39]
Doch nicht nur in großen Unternehmen, auch im heimischen KMU-Segment herrscht Bedarf an Information. Laut einer Studie des Beratungsunternehmens Arthur D. Little und der WKO aus dem September 2017, die den Digitalisierungsstatus österreichischer Klein- und Mittelunternehmen erhob, sind mehr als 50 Prozent der befragten KMUs nicht mit der Datenschutz-Grundverordnung vertraut, deren Regelungen bereits ab Mai 2018 anzuwenden sind. [31, S. 42]
Ein gewisses Bewusstsein der Herausforderung scheint jedenfalls verankert, bei den größten Herausforderungen der digitalen Transformation an KMUs wurde von 10 Prozent der Teilnehmer die DSGVO genannt. [31, S. 21]
Diese Datenschutz-Grundverordnung der Europäischen Union (Verordnung (EU) 2016/679), die ab 25. Mai 2018 von den Mitgliedstaaten anzuwenden ist, stellt aktuell wohl das größte Projekt im datenschutzrechtlichen Bereich in Europa dar. [62]
In dieser Arbeit im Allgemeinen und in diesem Kapitel im Speziellen wird verstärkt auf Inhalt und Auswirkungen der DSGVO eingegangen und die Frage, inwieweit sie einen Beitrag zur Verankerung von Datenschutz als österreichischen bzw. europäischen Standortvorteil leisten kann, behandelt.

3.1.1 Datenschutz - ein kurzer geschichtlicher Überblick

Datenschutz ist kein Phänomen des digitalen Zeitalters. Bereits seit etlichen Jahrhunderten sind Vorgänge zum Schutze personenbezogener Daten bekannt, wie beispielsweise die ärztliche Schweigepflicht oder das Beichtgeheimnis.
In der römisch-katholischen Kirche stellt die Beichte ein Sakrament dar und das Beichtgeheimnis ist laut kanonischem Recht unverletzlich, dem Beichtvater ist es 'daher streng verboten, den Pönitenten durch Worte oder auf irgendeine andere Weise und aus irgendeinem Grund irgendwie zu verraten' [24, Can. 983 - §1].
Mit der zunehmenden elektronischen Verarbeitung von (personenbezogenen) Daten, die durch die technischen Entwicklungen vor allem seit Anfang der zweiten Hälfte des 20. Jahrhunderts ermöglicht wurde, stiegen ebenso die Herausforderungen an den Datenschutz.
Elektronische Erfassung und Verarbeitung großer Mengen an Daten eröffneten naturgemäß nicht nur Chancen, sondern auch Risiken, wie etwas missbräuchliche Verwendung dieser Prozesse sowie der dabei verwendeten Daten.
In Deutschland begann deshalb in den 1960er Jahren die Diskussion über den Schutz der Privatsphäre durch Schutz entsprechender Daten vor der Verarbeitung durch öffentliche Stellen. Hessen verabschiedete als erstes deutsches Bundesland 1970 ein Landesdatenschutzgesetz.
Wesentliche Eckpunkte umfassten u.a. den Schutz elektronischer Daten vor unbefugtem Zugriff, aber auch die Möglichkeit einer Korrektur unrichtiger Daten durch Betroffene sowie die Einsetzung eines Landesdatenschutzbeauftragten als Kontrollbehörde. [21]

1977 folgte das erste deutsche Bundesdatenschutzgesetz, 1981 waren Landesdatenschutzgesetze in allen damaligen Bundesländern der BRD implementiert worden. Die neuen Bundesländer folgten im Zeitraum 1990-1992. [21]
In diesem Zusammenhang von besonderer Bedeutung, oft sogar als Meilenstein in der Geschichte des deutschen Datenschutz bezeichnet, wird das sogenannte 'Volkszählungsurteil' 1983.
Im Zuge einer geplanten Volkszählung wurde diese nach etlichen Verfassungsbeschwerden vom Bundesverfassungsgericht als - teilweise - verfassungswidrig erklärt. [21]
So heißt es in der Begründung des Urteil u.a.: 'Die durch dieses Gesetz angeordnete Datenerhebung hat Beunruhigung auch in solchen Teilen der Bevölkerung ausgelöst, die als loyale Staatsbürger das Recht und die Pflicht des Staates respektieren, die für rationales und planvolles staatliches Handeln erforderlichen Informationen zu beschaffen. Dies mag teilweise daraus zu erklären sein, daß weiterhin Unkenntnis über Umfang und Verwendungszwecke der Befragung bestand und daß die Notwendigkeit zur verlässlichen Aufklärung der Auskunftspflichten nicht rechtzeitig erkannt worden ist, obwohl sich das allgemeine Bewußtsein durch die Entwicklung der automatisierten Datenverarbeitung seit den Mikrozensus-Erhebungen in den Jahren 1956 bis 1962 [...] erheblich verändert hatte. Die Möglichkeiten der modernen Datenverarbeitung sind weiterhin nur noch für Fachleute durchschaubar und können beim Staatsbürger die Furcht vor

einer unkontrollierbaren Persönlichkeitserfassung selbst dann auslösen, wenn der Gesetzgeber lediglich solche Angaben verlangt, die erforderlich und zumutbar sind' [6, S. 4f].

Ebenso wird der Begriff der Selbstbestimmung des Einzelnen in Zusammenhang mit Datenschutz erörtert:
'Individuelle Selbstbestimmung setzt aber - auch unter den Bedingungen moderner Informationsverarbeitungstechnologien - voraus, daß dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung [...] tatsächlich zu verhalten. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß' [6, S. 45f].
Schließlich folgerte das Bundesverfassungsgericht:
'Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen' [6, S. 46].
Damit war informationelle Selbstbestimmung höchstgerichtlich verankert, der Gesetzgeber durfte also ohne individuelle Einwilligung personenbezogene Daten nur dann verwenden bzw. die Selbstbestimmung beschränken, wenn dieses Recht ausdrücklich einer gesetzlichen Grundlage entsprach. [21].

Auf europäischer Ebene wurde mit der der EU-Richtline 95/46/EG (Datenschutzrichtlinie 95) eine Direktive geschaffen, die die Persönlichkeitsrechte im Datenschutz stärkte und ein harmonisiertes Datenschutzniveau aller Unionsstaaten vorschrieb, um den Austausch personenbezogener Daten innerhalb der Union zu ermöglichen. Der Austausch solcher sensibler Daten mit Drittstaaten wurde durch die Richtline 95/46/EG nur soweit erlaubt, als dass im Drittstaat ein entsprechendes Niveau an Datenschutz herrschen musste. [21]
So heißt es in Artikel 25, (1) der Richtline von 1995 :
'**Grundsätze**

(1) Die Mitgliedstaaten sehen vor, daß die Übermittlung personenbezogener Daten, die Gegenstand einer Verarbeitung sind oder nach der Übermittlung verarbeitet werden sollen, in ein Drittland vorbehaltlich der Beachtung der auf-

grund der anderen Bestimmungen dieser Richtlinie erlassenen einzelstaatlichen Vorschriften zulässig ist, wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet' [49, Art. 25 (1)].

Breite mediale Aufmerksamkeit erzielte der Austausch von Daten zwischen Unionsstaaten und den USA. Die Übereinkunft, dass Daten ohne Genehmigung in die USA übermittelt werden dürften, traf die Kommission mit dem sogenannten 'Safe-Harbor-Erlass' im Jahr 2000. [30]
Nach den Enthüllungen des ehemaligen CIA-Mitarbeiters Edward Snowden, der im Sommer 2013 umfassende Details zu Überwachungspraktiken von Geheimdiensten - wie beispielsweise der amerikanischen NSA - veröffentlichte, legte der österreichische Jurist Maximilian Schrems Beschwerde bei der irischen Datenschutzbehörde ein, da seiner Interpretation nach die von der Facebook-Zweigstelle für Europa, Facebook Irland, in die USA übermittelten Daten dort nicht sicher seien. [14]
Über den irischen High Court gelangte die Fragestellung an den EuGH, der im Oktober 2015 zum Ergebnis kam, dass einerseits die Safe-Harbor-Entscheidung nationale Stellen nicht daran hindere, die Erfüllung der in der Richtlinie 95/46/EG Stellen bei Übermittlung von Daten in Drittstaaten zu prüfen. Andererseits erklärte der Europäische Gerichtshof den Safe-Harbor-Entscheid selbst für nichtig, weil u.a. das notwendige Schutzniveau der Vereinigten Staaten im Bereich des Datenschutzes nicht als hinreichend begründet festgestellt wurde. [14]
Damit war eine neue Grundlage für Datenübermittlung als Nachfolge zu *Safe-Harbor* notwendig geworden. Diese wurde im Juli 2016 mit der Nachfolgevereinbarung *Privacy Shield* getroffen.
Zentrale Grundsätze dieser Vereinbarung waren strengere Auflagen für datenverarbeitende Unternehmen, klare Schutzvorkehrungen und Transparenzauflagen beim Zugriff auf Daten durch US-amerikanische Unternehmen, wirksamer Schutz des Rechts des Einzelnen sowie eine gemeinsame jährliche Überprüfung der Funktionsweise des Datenschutzschilds. [20]
Bedenken und Klarstellungsforderungen von Datenschützern wurden im Entstehungsprozess von *Privacy Shield* eingebracht, darunter befand sich beispielsweise die Stellungnahme WP 238 der Artikel 29 - Datenschutzgruppe [46], die den Entwurf der Grundlage für die Datenübermittlung in die USA zuerst datenschutzrechtlich geprüft hatte. In die finale Fassung wurden einige Vorschläge und Forderungen der Datenschutzgruppe übernommen, gänzlich unumstritten blieb der neue Rahmen allerdings nicht. [13]

Nach mehreren Jahren andauernden Reformdiskussionen und Verhandlungen trat schließlich im April 2016 die Verordnung (EU) 2016/679 - besser bekannt als Datenschutz-Grundverordnung - in Kraft. Sie ist ab dem 25.05.2018 verpflichtend in sämtlichen Mitgliedstaaten der Union anzuwenden. [62]

3.2 Verordnung (EU) 2016/679 - Die Datenschutz-Grundverordnung

Die Verordnung (EU) 2016/679, in Folge Datenschutz-Grundverordnung genannt, wurde im Mai 2016 kundgemacht und gilt ab dem 25.05.2018. Als 'Rückgrat des allgemeinen Datenschutzes der EU' [55, S. 4] gilt sie unmittelbar, enthält allerdings zahlreiche sogenannte *Öffnungsklauseln*, im Rahmen derer nationale Gesetzgeber bestimmte Dinge gesetzlich näher regeln können bzw. müssen. [55, S. 4] Der Leitfaden des BKA bzw. der DSB fasst drei Zielsetzungen der DSGVO zusammen: [55, S. 4]

- Einheitlicher Rechtsschutz aller Betroffenen in der Europäischen Union.
- Einheitliche Datenverarbeitungsregeln innerhalb der Europäischen Union.
- Gewährleistung eines einheitlichen und starken Vollzugs.

3.2.1 Gliederungsübersicht DSGVO

Die Datenschutz-Grundverordnung wird in elf Kapitel gegliedert, die wiederum jeweils mehrere Artikel umfassen: [55, S. 5]

- Kapitel I: Allgemeine Bestimmungen - *Artikel 1 bis 4*
- Kapitel II: Grundsätze - *Artikel 5 bis 11*
- Kapitel III: Rechte der betroffenen Personen - *Artikel 12 bis 23*
- Kapitel IV: Verantwortlicher und Auftragsverarbeiter - *Artikel 23 bis 43*
- Kapitel V: Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen - *Artikel 44 bis 50*
- Kapitel VI: Unabhängige Aufsichtsbehörden - *Artikel 51 bis 59*
- Kapitel VII: Zusammenarbeit und Kohärenz - *Artikel 60 bis 76*
- Kapitel VIII: Rechtsbehelfe, Haftung und Sanktionen - *Artikel 77 bis 84*
- Kapitel IX: Vorschriften für besondere Verarbeitungssituationen - *Artikel 85 bis 91*
- Kapitel X: Delegierte Rechtsakte und Durchführungsrechtsakte - *Artikel 92 bis 93*
- Kapitel XI: Schlussbestimmungen - *Artikel 94 bis 99*

3.2.2 Inhaltliche Zusammenfassung DSGVO

3.2.2.1 Kapitel I: Allgemeine Bestimmungen

Im ersten Kapitel werden Gegenstand und Ziele, der sachliche sowie der räumliche Anwendungsbereich der Richtlinie, sowie Begriffsbestimmungen behandelt.
Als **Gegenstand** und somit grundlegender Zweck der Datenschutz-Grundverordnung wird der Erlass von 'Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten' [62, Art. 1 (1)] angeführt.
Die DSGVO soll Grundrechte natürlicher Personen schützen. Besonders hervorgehoben wird hierbei das Recht auf Schutz der personenbezogenen Daten. [62, Art. 1 (2)]

Sachlicher Anwendungsbereich der Verordnung ist die automatisierte und teilautomatisierte Verarbeitung personenbezogener Daten und weiters die nichtautomatisierte Verarbeitung ebensolcher Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. [62, Art. 2 (1)]
Keine Anwendung findet die DSGVO auf Verarbeitung personenbezogener Daten, die einen der folgenden Parameter aufweisen: [55, S. 6]

- Im Rahmen einer Tätigkeit außerhalb des Unionsrechts.
- Tätigkeiten im Rahmen der gemeinsamen Außen- und Sicherheitspolitik.
- Verwendung von Daten im Rahmen ausschließlicher persönlicher oder familiärer Tätigkeit.
- Tätigkeiten von zuständigen Behörden zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder Strafvollstreckung. Dazu gehören auch Maßnahmen zum Schutz vor und zur Abwehr von Gefahren für die öffentliche Sicherheit.

Der **räumliche Anwendungsbereich** umfasst die Verarbeitung personenbezogener Daten, soweit diese Verarbeitung im Rahmen einer Niederlassung eines *Verantwortlichen* oder *Auftragsverarbeiters* in der EU erfolgt. Dabei ist es nicht entscheidend, ob die Verarbeitung der Daten selbst in der EU stattfindet. [62, Art. 3 (1)]
Außerdem findet sie ebenfalls Anwendung, wenn die von der Verarbeitung Betroffenen sich in der Union befinden, die *Verantwortlichen* oder *Auftragsverarbeiter* aber nicht, wenn einer der zwei folgenden Parameter zutrifft: [62, Art. 3 (2)]

a) Die Datenverarbeitung steht im Zusammenhang damit, dass der Verantwortliche bzw. Auftragsverarbeiter in der EU Waren bzw. Dienstleistungen (auch unentgeltlich) anbietet.

b) Wenn das Verhalten betroffener Personen, welches in der Union erfolgt, in Zusammenhang mit der Datenverarbeitung beobachtet wird.

Außerdem findet die DSGVO Anwendung auf die Verarbeitung personenbezogener Daten, wenn der nicht in der EU niedergelassene Verantwortliche an einem Ort niedergelassen ist, der aufgrund völkerrechtlicher Bestimmungen dem Recht eines Mitgliedstaates unterliegt. [62, Art. 3 (3)]
Die Datenschutzgrundverordnung soll also nicht nur für Datenverarbeitungsvorgänge in der Union gelten, sondern auch, wenn beispielsweise ein US-amerikanischer Händler innerhalb der EU Waren oder Dienstleistungen anbietet. So soll unter anderem der steigenden Popularität des Online-Handels oder der erhöhten Inanspruchnahme von Cloud-Services, die von außerhalb der EU angeboten werden, Rechnung getragen werden.
Mit Begriffsbestimmungen schließt das erste Kapitel der DSGVO, hier wird eine Reihe von fachlichen Begriffen definiert. [62, Art. 4]
Der Leitfaden des BKA zur DSGVO spricht von zahlreichen Übernahmen aus der alten Datenschutzrichtlinie, nennt aber auch neue Definitionen, etwa die von Begriffen wie *Profiling*, *Pseudonymisierung*, *Verletzung des Schutzes personenbezogener Daten*, *Aufsichtsbehörde* oder *grenzüberschreitende Verarbeitung*. [55, S. 7]
An dieser Stelle seien die Definitionen des *Verantwortlichen* und des *Auftragsverarbeiters* explizit ausgeführt, da diese für das Verständnis zahlreicher weiterer Artikel von zentraler Bedeutung sind:
Verantwortlicher: 'Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden' [62, Art. 4].
Auftragsverarbeiter: 'Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet' [62, Art. 4].
Als *Verantwortliche* werden also die tatsächlich entscheidenden Stellen betitelt, die *Auftragsverarbeiter* mit der Verarbeitung von personenbezogenen Daten beauftragen können.

3.2.2.2 Kapitel II: Grundsätze

Im Rahmen des zweiten Kapitels werden die Grundsätze für die Verarbeitung der personenbezogenen Daten definiert. Dabei ähneln diese Grundsätze denjenigen

der alten Datenschutzrichtlinie. [55, S. 8] Exemplarisch erwähnt seien einige zentrale Prinzipien. So müssen personenbezogene Daten folgenden Grundsätzen entsprechen: **'Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz'** [62, Art. 5 (1)]. Damit sollen Datenverarbeitungsvorgänge transparent für betroffene Personengruppen gestaltet werden.
Die **Zweckbindung** ist der Grundsatz, welcher definiert, dass Daten nur für 'eindeutige und legitime Zwecke' [62, Art. 5 (1)] erhoben und weiterverarbeitet werden dürfen. Außerdem soll **Datenminimierung** betrieben werden, also 'das für die Zwecke der Verarbeitung notwendige Maß' [62, Art. 5 (1)] an Daten erhoben werden, diese Daten müssen natürlich auch dem Grundprinzip der **Richtigkeit** unterliegen. [62, Art. 5 (1)]
Speicherbegrenzung soll sicherstellen, dass personenbezogene Daten nur so lange gespeichert werden, wie für die Verarbeitungszwecke erforderlich ist. Die Verarbeitung selbst muss Schutz vor Missbrauch und unbeabsichtigten Störungen bieten, also den Grundsatz der **Integrität und Vertraulichkeit** erfüllen. [62, Art. 5 (1)]
Ebenso werden in diesem Kapitel Bedingungen für die **Rechtmäßigkeit der Verarbeitung** sowie **Bedingungen für die Einwilligung** bezüglich der Verarbeitung der personenbezogenen Daten klargestellt. [62, Art. 6, Art. 7, Art. 8]
Der Artikel 9 der DSGVO stellt klar, dass die Verarbeitung von personenbezogenen Daten grundsätzlich untersagt ist (es existiert eine Reihe von Ausnahmebestimmungen), aus denen sich sensible persönliche Eigenschaften, wie rassische und ethnische Herkunft, politische und religiöse Weltanschauung, sexuelle Orientierung oder beispielsweise auch Daten zum Gesundheitszustand einer Person ableiten lassen können. [62, Art. 9 (1)]

3.2.2.3 Kapitel III: Rechte der betroffenen Personen

Die Rechte der von Datenverarbeitung betroffenen Personen stehen im Mittelpunkt des dritten Kapitels der DSGVO, welches sich in fünf Abschnitte gliedert.

Abschnitt 1 Transparenz und Modalität
Innerhalb des ersten Abschnitts des dritten Kapitels wird vor allem die Wichtigkeit der Kommunikation und Transparenz der Rechte der betroffenen Personen durch die Verantwortlichen betont, die dafür entsprechende Maßnahmen zu treffen haben. [62, Art. 12]

Abschnitt 2 Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten
Im zweiten Abschnitt wird zuerst auf die Informationspflicht gegenüber betroffenen Personen bei der Erhebung von personenbezogenen Daten eingegangen. Betroffenen Personen müssen zum Zeitpunkt der Erhebung klar definierte Informa-

tionen mitgeteilt werden, wie beispielsweise Kontaktdaten des Verantwortlichen und - so vorhanden - des Datenschutzbeauftragten, Zwecke der Verarbeitung und andere wesentliche Rechte und Informationspflichten der betroffenen Person gegenüber. [62, Art. 13]
Diese Informations- und Auskunftspflichten waren bereits in der DSRL verankert, der EuGH bewertet diese Pflichten als Voraussetzungen zur Äußerung der Rechte sehr hoch. [55, S. 9]

Abschnitt 3 Berichtigung und Löschung
Im dritten Abschnitt wird auf mehrere konkrete Rechte eingegangen. Dazu zählen unter anderem das **Recht auf Berichtigung** unrichtiger personenbezogener Daten [62, Art. 16] und das **Recht auf Löschung bzw. das Recht auf Vergessenwerden** [62, Art. 17]. Letzteres Recht haben betroffene Personen gegenüber dem Verantwortlichen wenn gewisse Gründe, wie die Widerrufung der Einwilligung der Person, die unrechtmäßige Verarbeitung durch den Verantwortlichen, oder die nicht mehr vorhandene Notwendigkeit der Zwecke für die Verarbeitung bzw. Speicherung personenbezogener Daten zutreffen. [62, Art. 16, Art. 17].
Ebenso existiert das im Artikel 18 garantierte **Recht auf Einschränkung der Verarbeitung**, welches eine betroffene Person bei Vorliegen gegenüber gewisser Voraussetzungen gegenüber dem Verantwortlichen geltend machen kann. [62, Art. 18]
Außerdem wird mit Artikel 20 der DSGVO das **Recht auf Datenübertragung** eingeräumt. Dadurch sollen betroffene Personen ihre personenbezogenen Daten in einem strukturierten und maschinenlesbaren Format vom Verantwortlichen zur Verfügung gestellt bekommen. [62, Art. 20] So sollen technische Barrieren, etwa bei einem Servicewechsel hin zu einem anderen Anbieter, abgebaut werden. [55, S. 9]

Abschnitt 4 Widerspruchsrecht und automatisierte Entscheidungsfindung im Einzelfall
Im Kapitel III ist ebenso ein Widerspruchsrecht verankert. Einerseits haben betroffene Personen das Recht, aus in der Verordnung festgelegten Gründen in besonderen Situationen jederzeit gegen die Bearbeitung ihrer personenbezogenen Daten Widerspruch einzulegen. [62, Art. 21] Dies gilt auch für Profiling, welches die DSGVO als automatisierte Verarbeitung von personenbezogenen Daten definiert, aus denen persönliche Aspekte abgeleitet oder prognostiziert werden können. Solche Aspekte sind u.a. Gesundheit, Arbeitsleistung oder wirtschaftliche Lage. [62, Art. 4]
Grundsätzlich haben betroffene Personen außerdem das Recht, nicht einer ausschließlich auf automatisierter Verarbeitung basierten Entscheidung unterworfen zu sein, die dazu führt, rechtliche Wirkung gegenüber den Personen zu entfalten. Ausnahmen hierfür sind etwa, falls die Person dem eingewilligt hat oder etwa,

wenn es in spezifischer nationaler Gesetzgebung eines Mitgliedstaates vorgesehen ist und zusätzlich Maßnahmen zur Sicherung der Wahrung von Rechten und Freiheiten enthalten sind. [62, Art. 22]

Abschnitt 5 Beschränkungen
Diese Rechte der betroffenen Personen können durch Vorschriften der EU oder der Mitgliedstaaten in gewissen Fällen beschränkt werden. Es müssen dennoch Grundrechte und Grundfreiheiten sichergestellt werden und die gesetzten Maßnahmen verhältnismäßig und notwendig sein. Zusätzlich müssen solche Maßnahmen definierte Felder sicherstellen, wie etwa die nationale oder öffentliche Sicherheit, die Landesverteidigung oder die Strafvollstreckung. Außerdem müssen solche Vorgehensweisen spezifische Vorschriften zu den Kategorien personenbezogener Daten, Umfang der vorgenommenen Beschränkungen und zusätzlich definierte Angaben enthalten. [62, Art. 23]

3.2.2.4 Kapitel IV: Verantwortlicher und Auftragsverarbeiter

Die beiden Definitionen des Verantwortlichen und des Auftragsverarbeiters wurden bereits zu Beginn dieses Kapitels definiert.
Der Leitfaden des BKA nennt als grundsätzlichen Unterschied zur DSRL bzw. dem DSG 2000, dass Verantwortliche und Auftragsverarbeiter stärker in die Pflicht genommen werden. Als konkrete Beispiele wird unter anderem die in Artikel 27, Abschnitt 1 genannte Nennungspflicht eines Vertreters angeführt, falls Verantwortlicher oder Auftragsverarbeiter nicht im Gebiet der EU niedergelassen sind. [55, S. 10] [62, Art. 27 (1)]
Außerdem aufgezählt werden das *Verzeichnis von Verarbeitungstätigkeiten* und die *Datenschutz-Folgeabschätzung*, auf die jeweils nachfolgend eingegangen wird. [55, S. 10]

Abschnitt 1 - Allgemeine Pflichten
Der Verantwortliche wird im ersten Abschnitt des Kapitels IV dazu verpflichtet, technische und organisatorische Maßnahmen zu setzen, die die Eintrittswahrscheinlichkeit und Schwere der Risiken berücksichtigen müssen. Der Verantwortliche muss jederzeit nachweisen können, dass die Verarbeitung der personenbezogenen Daten, für die er sich verantwortlich zeichnet, der DSGVO entspricht. [62, Art. 24]
Ebenso gibt die DSGVO in diesem Abschnitt 'Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen' [62, Art. 25] vor. Dazu zählen etwa organisatorische bzw. technische Maßnahmen, die Grundsätze wie z.B. das Prinzip der Datenminimierung, etwa durch Pseudonymisierung, umsetzen. Außerdem müssen Verantwortliche ebenso Maßnahmen organisatorischer und technischer Natur treffen, um zu gewährleisten, dass durch aktivierte Voreinstellungen sichergestellt wird, dass nur für den Verarbeitungszweck erforderliche personenbezogene Daten aktiviert werden. [62, Art. 25]
Dieser *Privacy-by-default* Grundsatz kann auch durch entsprechende genehmigte

Zertifizierungsverfahren, welche in Abschnitt 5 behandelt werden, bestätigt werden.
Vertreter von nicht in der Union niedergelassenen Verantwortlichen bzw. Auftragsverarbeitern müssen - wie eingangs bereits erwähnt - schriftlich einen Verantwortlichen benennen, der in einem Mitgliedstaat niedergelassen ist. Dieser dient dann u.a. als Ansprechpartner für die zuständige Aufsichtsbehörde. [62, Art. 27]
Der Abschnitt geht außerdem auf die Auftragsverarbeiter ein, die eine Reihe an Anforderungen erfüllen müssen, um personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten zu dürfen. Zentrale Anforderungen an den Auftragsverarbeiter sind etwa geeignete technische und organisatorische Kapazitäten, keine Auftragsweitergabe an weitere Auftragsverarbeiter ohne Genehmigung des Verantwortlichen und das Vorhandensein einer vertraglichen Grundlage zwischen Verantwortlichem und Auftragsverarbeiter, die Verarbeitung betreffend. [62, Art. 28]
In der DSGVO wird nun auch ein Verzeichnis von Verarbeitungstätigkeiten eingefordert, welches vom Verantwortlichen bzw. seinem Vertreter zu führen ist und Angaben, etwa zum Zwecke der Verarbeitung, Kontaktdaten des Verantwortlichen, die Kategorien von personenbezogenen Daten oder auch die Übermittlung von relevanten Daten in ein Drittland enthält. [62, Art. 30]
Auch der Auftragsverarbeiter muss so ein Verzeichnis führen, welches Angaben zu allen im Auftrag des Verantwortlichen durchgeführten Verarbeitungstätigkeiten enthält. Das Führen eines solchen Verzeichnisses ist grundsätzlich für Unternehmen ab 250 Mitarbeitern verpflichtend, gilt aber auch für KMUs, wenn die vorgenommene Verarbeitung ein Risiko für die Rechte und Freiheiten der Betroffenen birgt, Daten besonderer Kategorien verarbeitet werden oder die Verarbeitung nicht nur gelegentlich erfolgt. [62, Art. 30 (5)]
Da die meisten KMUs allerdings regelmäßig - und somit nicht nur gelegentlich - personenbezogene Daten verarbeiten, dürften zahlreiche Betriebe mit weniger als 250 Mitarbeitern von der Führungspflicht solch eines Verzeichnisses betroffen sein. [16]
Die Wirtschaftskammer Steiermark erwähnte hier als plakative Beispiele die Lohnverrechnung oder Verarbeitung von Kundendaten. [61]
Abschließend wird im Abschnitt 1 die Zusammenarbeit des bzw. der Verantwortlichen und Auftragsverarbeiter mit der Aufsichtsbehörde auf Anfrage klargestellt. [62, Art. 31]

Abschnitt 2 - Sicherheit personenbezogener Daten

Abschnitt 2 behandelt die namensgebende Sicherheit personenbezogener Daten und den Umgang mit etwaigen Verletzungen des Datenschutzes. [62, Art. 32, 33, 34]
Grundsätzlich werden Verantwortliche und Auftragsverarbeiter verpflichtet, unter Berücksichtigung gewisser Parameter, wie zum Beispiel dem Stand der Technik, den Kosten der Implementierung oder der unterschiedlichen Eintrittswahrscheinlichkeit sowie der Schwere von Risiken ein angemessenes Schutzniveau für die

Sicherheit personenbezogener Daten zu bieten. Die DSGVO zählt hier im Rahmen des Artikel 32 beispielhaft bestimmte Maßnahmen, wie die Pseudonymisierung und Verschlüsselung, die rasche Datenwiederherstellung nach Zwischenfällen oder auch Evaluationsverfahren zur Gewährleistung des Schutzes auf.
Ebenso müssen bei der Beurteilung dieses Schutzniveaus Risiken bewertet werden, die mit der Verarbeitung selbst verbunden sind. Um die Erfüllung dieses Schutzniveaus nachzuweisen, können genehmigte Verhaltensregeln oder ein genehmigtes Zertifizierungsverfahren herangezogen werden, die im Abschnitt 4 dieses Kapitels behandelt werden. [62, Art. 32]
Im Falle der Verletzung des Schutzes personenbezogener Daten sind gemäß der Artikel 33 und 34 Meldungen bzw. Benachrichtigungen an die Aufsichtsbehörde sowie an die betroffenen Personen durchzuführen. Diese sind an die aufsehende Behörde möglichst unverzüglich, jedenfalls aber binnen 72 Stunden und an die betroffenen Personen ebenso möglichst unverzüglich durchzuführen und haben den Formvorgaben der DSGVO zu entsprechen. [62, Art. 33, Art. 44]

Abschnitt 3 - Datenschutz-Folgeabschätzung und vorherige Konsultation

Im Gegensatz zu Reaktionen nach eingetretenen Verletzungen des Datenschutzes hat die Datenschutz-Folgeabschätzung eine prophylaktische Aufgabe. Diese muss dann vom Verantwortlichen im Vorfeld abgegeben werden, falls die Form der Verarbeitung aufgrund mehrerer Parameter voraussichtlich ein hohes Risiko für Rechte bzw. Freiheiten von natürlichen Personen aufweist.
Die DSGVO zählt einige Fälle auf, die unbedingt eine Folgeabschätzung nach sich ziehen müssen und verpflichtet die entsprechende Aufsichtsbehörde, eine Liste mit Verarbeitungsvorgängen zu erstellen, für die eine Datenschutz-Folgeabschätzung notwendig ist. [62, Art. 35 (3)]
Die Folgeabschätzung muss naturgemäß gewisse Inhalte, wie eine systematische Beschreibung der Verarbeitungsvorgänge, eine Bewertung der Notwendigkeit bzw. Verhältnismäßigkeit dieser Vorgänge, eine Bewertung der Risiken und geplante Abhilfemaßnahmen sowie Garantien und Sicherheitsvorkehrung zur Bewältigung ebendieser Risiken enthalten. [62, Art. 35 (7)]
Wenn aus der Datenschutz-Folgeabschätzung ein potentiell hohes Risiko hervorgeht, muss der Verantwortliche vor der Verarbeitung die Aufsichtsbehörde konsultieren, die dem Verantwortlichen im Falle des Nicht-Einklangs der Verarbeitung mit der DSGVO innerhalb von acht Wochen u.a. schriftliche Empfehlungen zur Verfügung stellt. [62, Art. 36]

Abschnitt 4 - Datenschutzbeauftragter

Ein wesentlicher Eckpunkt der DSGVO dreht sich um die Benennung bzw. die Rolle des Datenschutzbeauftragten. Dieser kann grundsätzlich jederzeit freiwillig benannt werden, ist für eine Reihe von Organisationen und Unternehmen allerdings verpflichtend vorgesehen.

Jedenfalls ist ein Datenschutzbeauftragter vom Verantwortlichen und Auftragsverarbeiter zu benennen für: [62, Art. 37 (1)] [60]

1. Behörden und öffentliche Stellen, die Verarbeitungen personenbezogener Daten durchführen (Ausnahmen: Gerichte im Zuge ihrer justiziellen Tätigkeiten).

2. Verantwortliche bzw. Auftragsverarbeiter (also auch Unternehmen), deren Kerntätigkeiten Verarbeitungstätigkeiten umfassen, die eine umfangreiche regelmäßige und systemische Überwachung von Personen notwendig machen. Die Wirtschaftskammer Österreich führt beispielhaft Banken, Versicherungen, Kreditauskunfteien und Berufsdetektive an.

3. Verantwortliche bzw. Auftragsverarbeiter (also auch Unternehmen), deren Kerntätigkeit die Verarbeitung sensibler Daten oder personenbezogener Daten über strafrechtliche Verurteilungen und Strafdaten umfasst. Hier erwähnt die WKO als Beispiel einer solchen Kategorie Krankenanstalten.

In Artikel 37 (4) der DSGVO existiert eine Öffnungsklausel, die den Mitgliedstaaten erlaubt, weitere Anwendungsfelder für die verpflichtende Benennung eines Datenschutzbeauftragten durch Verantwortliche oder Auftragsverarbeiter zu bestimmen. [62, Art. 37 (4)]
Grundsätzlich können Datenschutzbeauftragte beim Verantwortlichen oder Auftragsverarbeiter angestellt sein, oder auch mittels eines Dienstleistungsvertrags ihre Leistungen erbringen. [62, Art. 37 (6)]
Der Datenschutzbeauftragte hat laut DSGVO eine klar definierte Stellung inne und ebenso klar definierte Aufgaben zu erfüllen.
So muss er etwa von Verantwortlichen und Auftragsverarbeiter ordnungsgemäß und frühzeitig in alle Fragen in Zusammenhang mit dem Schutz personenbezogener Daten eingebunden werden, erforderliche Ressourcen und Zugangsberechtigungen zur Erfüllung seiner Aufgaben bekommen, weisungsfrei bezüglich seiner Aufgaben agieren können und unmittelbar der höchsten Managementebene berichten. Er ist bei der Erfüllung seiner Aufgaben an die Vertraulichkeit bzw. Wahrung der Geheimhaltung gebunden und kann auch andere Pflichten wahrnehmen, sofern vom Verantwortlichen bzw. Auftragsverarbeiter sichergestellt wird, dass solche Pflichten nicht zu einem Interessenkonflikt führen. [62, Art. 38]
Die in der DSGVO definierten Aufgaben des Datenschutzbeauftragen umfassen zumindest die Unterrichtung und Beratung der Verantwortlichen bzw. Auftragsverarbeitern und der durchführenden Beschäftigungen, der Überwachung der DSGVO-Einhaltung sowie Beratungstätigkeit, etwa im Zusammenhang mit der Datenschutz-Folgeabschätzung.
Weitere Aufgaben umfassen die Zusammenarbeit mit der Aufsichtsbehörde und die Tätigkeit als Anlaufstelle für diese Behörde für etwaige Fragen in Zusammenhang mit der Verarbeitung personenbezogener Daten. [62, Art. 39]

Abschnitt 5 - Verhaltensregeln und Zertifizierung

Der Abschnitt 5 des Kapitels IV umfasst einerseits das System der Verhaltensregeln, welches bereits in Artikel 27 der DSRL vorhanden war und baut dieses weiter aus. [55, S. 12]
Kategorien von Verantwortlichen bzw. Auftragsverarbeitern vertretende Verbände und Vereinigungen können demnach Verhaltensregeln ausarbeiten, mit denen die Anwendung der DSGVO in bestimmen Bereichen präzisiert wird. [62, Art. 40]
Diese Verhaltensregeln können bei der Aufsichtsbehörde eingereicht werden und werden von dieser bzw. einer akkreditierten Stelle auf ihre Einhaltung überwacht. [55, S. 12]
Andererseits behandelt Abschnitt 5 das Themenfeld der datenschutzspezifischen Zertifizierungsverfahren, sowie von Datenschutzsiegeln und Datenschutzprüfzeichen. Diese sollen zum Nachweis der Einhaltung der DSGVO bei Verarbeitungstätigkeiten durch Verantwortliche oder Auftragsgeber dienen. [62, Art. 42] Solche Zertifizierungen müssen laut DSGVO über freiwillige und transparente Verfahren zugänglich sein und mindern nicht die Verantwortung des Verantwortlichen bzw. des Auftragsgebers für die Einhaltung der DSGVO. Sie werden für eine Höchstdauer von drei Jahren erteilt und können unter denselben Bedingungen entsprechend verlängert oder - so die Voraussetzungen nicht mehr gegeben sind - widerrufen werden. [62, Art. 42 (7)]
Diese Zertifizierungen werden von einer geeigneten Zertifizierungsstelle vergeben, die über entsprechend fachliche Kompetenz verfügt und von der zuständigen Aufsichtsbehörde oder der nationalen Akkreditierungsstelle akkreditiert werden muss. Solch eine Akkreditierung wird für maximal fünf Jahre gewährt und kann unter denselben Bedingungen entsprechend verlängert werden. [62, Art. 43]

3.2.2.5 Kapitel V: Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen

Kapitel V der Datenschutz-Grundverordnung regelt die Voraussetzungen für die Übermittlung personenbezogener Daten an Drittländer bzw. internationale Organisationen und soll so sicherstellen, dass übermittelte Daten beim Empfänger außerhalb der EU demselben Schutzregime wie innerhalb der Union unterliegen sollen. [55, S. 13]
Personenbezogene Daten dürfen an ein Drittland bzw. eine internationale Organisation übermittelt werden, wenn dieses Drittland bzw. die internationale Organisation einem Kommissionsbeschluss nach über ein entsprechendes Schutzniveau verfügt. Dieser Beschluss findet im Rahmen eines Durchführungsrechtsaktes nach einer Beurteilung der Angemessenheit des Schutzniveaus statt. [62, Art. 45 (1)]

Existiert kein solcher Durchführungsrechtsakt, dürfen personenbezogene Daten vom jeweiligen Verantwortlichen bzw. Auftragsverarbeiter nur dann in ein Drittland bzw. an eine internationale Organisation übermittelt werden, sofern der Verantwortliche bzw. der Auftragsverarbeiter geeignete Garantien vorgesehen hat, den Betroffenen wirksame Rechtsbehelfe zur Verfügung stehen und diese ihre Rechte entsprechend durchsetzen können. Beispielhafte Garantien werden von der DSGVO genannt, etwa ein rechtlich bindendes und durchsetzbares Dokument zwischen den Behörden, bestimmte Standarddatenschutzklauseln oder verbindliche interne Datenschutzvorschriften gem. Artikel 47. [62, Art. 46]
Außerdem definieren die folgenden Artikel 49 und 50 Ausnahmen für die Übermittlung sowie Aufgaben der Kommission und der Aufsichtsbehörden zur internationalen Zusammenarbeit zum Schutz personenbezogener Daten. [62, Art. 49, Art. 50]

3.2.2.6 Kapitel VI: Unabhängige Aufsichtsbehörden

Abschnitt 1 - Unabhängigkeit
Kapitel VI definiert, dass mindestens eine unabhängige Behörde pro Mitgliedstaat für die Einhaltung der Datenschutz-Grundverordnung zuständig ist. [62, Art. 51 (1) (2)]
Diese Behörde ist bei der Erfüllung ihrer Aufgaben und der Befugnisausübung unabhängig und ihre Mitglieder werden im Rahmen eines transparenten Verfahrens vom Parlament, der Regierung, vom Staatsoberhaupt oder einer unabhängigen Stelle, die nach jeweiligem nationalen Recht mit dieser Aufgabe betraut ist, ernannt. [62, Art. 52, Art. 53 (1)]

Abschnitt 2 - Zuständigkeit, Aufgaben und Befugnisse
Die Zuständigkeit der jeweiligen Aufsichtsbehörde erstreckt sich auf das Hoheitsgebiet des Mitgliedstaats. [62, Art. 55 (1)]
Die Behörde besitzt - im Vergleich zu den Regelungen im Zeitraum vor der DSGVO, also u.a. der DSRL - erheblich erweiterte Aufgaben sowie Befugnisse. [55, S. 14]
Die Aufgaben der Behörde umfassen nach DSGVO u.a.: [62, Art. 57 (1)]

- Überwachung und Durchsetzung der Anwendung der DSGVO.
- Sensibilisierung der Öffentlichkeit mit Risiken und Rechten im Zusammenhang mit der Verarbeitung personenbezogener Daten - mit besonderem Augenmaß auf Kinder.
- Beratung von Einrichtungen wie der Regierung oder des nationalen Parlaments über gesetzgeberische und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen.

- Sensibilisierung von Verantwortlichen bzw. Auftragsverarbeitern ihrer Pflichten gegenüber.
- Anfragebeantwortungen betroffener Personen gegenüber, v.a. deren Rechte laut DSGVO betreffend.
- Befassung mit Beschwerden von betreffenden Personen, Stellen, Organisationen oder Verbänden gemäß Artikel 80. Dies umfasst u.a. die Untersuchung des Beschwerdegegenstandes und die Unterrichtung des Beschwerdeführers.
- Zusammenarbeit mit anderen Aufsichtsbehörden, etwa durch Informationsaustausch und das Leisten von gegenseitiger Amtshilfe.
- Untersuchungen über die Anwendung der DSGVO.
- Beobachtung von Entwicklungen, besonders im Bereich der IKT, soweit sich diese auf den Schutz personenbezogener Daten auswirken.
- Festlegung von Standardvertragsklauseln im Sinne der DSGVO.
- Erstellung und Führung einer Liste von Verarbeitungsarten, für die im Sinne der DSGVO eine Datenschutz-Folgeabschätzung notwendig ist.
- Beratung für Verantwortliche bzw. Auftragsgeber für Verarbeitungsvorgänge mit lt. Datenschutz-Folgeabschätzung hohem Risiko.
- Förderung der Ausarbeitung von Verhaltensregeln gemäß Artikel 40 DSGVO und Abgabe von Stellungnahmen zu ebenjenen.
- Billigung der Einführung von Datenschutzmechanismen, -siegeln und -prüfzeichen gemäß Artikel 42 Absatz 1 und deren Zertifizierungskriterien. Außerdem gegebenenfalls die regelmäßige Überprüfung der erteilten Zertifizierungen.
- Die Definition von Kriterien für die Akkreditierung einer Stelle für die Überwachung von Verhaltensregeln sowie einer Zertifizierungsstelle.
- Weitere Aufgaben, wie Beiträge zur Ausschusstätigkeit zu leisten oder ein internes Verzeichnis über Verstöße gegen die DSGVO zu führen.

Zur Erreichung dieser Aufgaben besitzt die Behörde Befugnisse, die in Untersuchungsbefugnisse, Abhilfebefugnisse sowie Genehmigungs- und Beratungsbefugnisse unterteilt werden. [62, Art. 58]
Untersuchungsbefugnisse berechtigen die Aufsichtsbehörde etwa, Verantwortliche bzw. Auftragsverarbeiter anzuweisen, Informationen bereitzustellen, Zugang zu personenbezogenen Daten sowie Geschäftsräumen zu erhalten oder Untersuchungen in Form einer Datenschutzüberprüfung durchzuführen. [62, Art.

58 (1)]
Abhilfebefugnisse gestatten es der Behörde unter anderem, Verantwortliche bzw. Auftragsverarbeiter zu warnen, dass in Zukunft beabsichtigte Verarbeitungen voraussichtlich gegen die DSGVO verstoßen werden und zu verwarnen, wenn dies bereits passiert ist. Die Behörde kann das Ineinklangbringen von Verarbeitungsvorgängen mit der DSGVO anordnen, eine vorübergehende oder endgültige Verarbeitungsbeschränkung verordnen, Berichtigungen und Löschungen anordnen sowie Zertifizierungen widerrufen oder die Aussetzung der Übermittlung von Daten in ein Drittland anweisen. Anstelle oder zusätzlich der Maßnahmen kann die Aufsichtsbehörde eine Geldbuße verhängen, wobei jedenfalls die Umstände des Einzelfalls zu berücksichtigen sind. [62, Art. 58 (2)]
Genehmigungs- und beratende Befugnisse gestatten es der Aufsichtsbehörde, in etlichen Bereichen Konsultationen zu leisten und Genehmigungen zu erteilen. Beispiele für Ersteres umfassen Beratungen gemäß dem Verfahren der vorherigen Konsultation - Artikel 36 DSGVO - oder Stellungnahmen zu Fragen den Schutz personenbezogener Daten betreffend an das nationale Parlament, die Regierung, sonstige Stellen oder an die Öffentlichkeit zu richten.
Genehmigend tätig wird die Aufsichtsbehörde etwa bei der Akkreditierung von Zertifizierungsstellen, der Festlegung von Standarddatenschutzklauseln oder der Billigung von Entwürfen zu Verhaltensregeln und Kriterien für Zertifizierungen. [62, Art. 58 (3)]
Weitere Befugnisse der Behörde können im Rahmen einer Öffnungsklausel von den einzelnen Mitgliedstaaten vorgesehen werden. [62, Art. 58 (6)]

3.2.2.7 Kapitel VII: Zusammenarbeit und Kohärenz

Abschnitt 1 - Zusammenarbeit
Kapitel VII Abschnitt 1 behandelt die Zusammenarbeit zwischen der federführenden - also der hauptverantwortlichen - Aufsichtsbehörde und anderen betroffenen Behörden. Diese sind dazu angehalten, sich im Rahmen ihrer Zusammenarbeit um einen Konsens zu bemühen und sich untereinander auszutauschen. Die federführende Behörde kann bei den anderen betroffenen Behörden dabei jederzeit um Amtshilfe ansuchen und gemeinsame Maßnahmen, etwa zur Durchführung von Untersuchungen in Bezug auf einen Verantwortlichen bzw. Auftragsverarbeiter mit Sitz in einem anderen Mitgliedstaat, durchführen. Zur einheitlichen Anwendung gewähren sich die Aufsichtsbehörden der einzelnen Mitgliedstaaten grundsätzlich Amtshilfe, die nur in speziellen Fällen abgelehnt werden darf. [62, Art. 60, Art. 61, Art. 62]

Abschnitt 2 - Kohärenz
Durch die im Abschnitt 2 des Kapitels VII definierten Maßnahmen des Kohärenzverfahrens soll die einheitliche Anwendung und die Zusammenarbeit

der Behörden untereinander und mit der Kommission geregelt werden. Dazu werden Maßnahmen des Ausschusses, wie Stellungnahme und Streitbeilegung, sowie Dringlichkeitsverfahren und Informationsaustausch behandelt. [62, Art. 63-67]

Abschnitt 3 - Europäischer Datenschutzausschuss
Im Rahmen der Anwendung der DSGVO wird ein Europäischer Datenschutzausschuss mit eigener Rechtspersönlichkeit eingerichtet, der aus dem Leiter der Aufsichtsbehörde jedes Mitgliedstaats und dem Europäischen Datenschutzbeauftragten besteht. Falls in einem Mitgliedstaat mehr als eine zuständige Aufsichtsbehörde existiert, wird ein gemeinsamer Vertreter entsandt. [62, Art. 68]
Der Ausschuss agiert unabhängig und hat in Artikel 70 formulierte Aufgaben. Eine zentrale Aufgabe ist die Sicherstellung der einheitlichen Anwendung der DSGVO. Diese Aufgabe soll durch Beratungsleistungen der Kommission gegenüber, der Bereitstellung von Leitlinien und Empfehlungen und 'best practice'-Verfahren in diversen Bereichen der DSGVO und Abgabe von Stellungnahme für die Kommission erfüllt werden. Außerdem werden Förderungen von Schulungsprogrammen und Maßnahmen des Personalaustauschs zwischen Aufsichtsbehörden und Förderung von Know-how Austausch mit Aufsichtsbehörden auch über die Union hinaus angeführt. [62, Art. 70]
Der Ausschuss leitet seine Stellungnahmen, Leitlinien u.ä. an die Kommission weiter und veröffentlicht sie, außerdem konsultiert er gegebenenfalls sogenannte 'interessierte Kreise' [62, Art. 70] und gibt ihnen die Möglichkeit, ihrerseits Stellungnahmen abzugeben. [62, Art. 70]
Zudem werden in diesem Kapitel Verfahrensweisen, Berichterstattungspflichten, der Vorsitz des Ausschusses und weitere Formalitäten definiert. [62, Art. 71 - Art. 76]

3.2.2.8 Kapitel VIII: Rechtsbehelfe, Haftung und Sanktionen

In Kapitel VII werden zu Beginn Rechtsbehelfe und Beschwerderechte behandelt. Unabhängig von anderen (etwa verwaltungsrechtlichen oder gerichtlichen) Rechtsbehelfen verankert die DSGVO ein Beschwerderecht jeder betroffenen Person direkt bei der entsprechenden Aufsichtsbehörde. [62, Art. 77]
Durch Artikel 78 wird der Rechtsweg vor Gericht gegen rechtsverbindliche Beschlüsse von Aufsichtsbehörden ermöglicht, der gleichsam natürlichen und juristischen Personen offensteht. Falls die Aufsichtsbehörde auf eine Beschwerde nicht reagiert bzw. die betroffene Person als Beschwerdeführer nicht binnen drei Monaten über Stand oder Ergebnis einer Beschwerde gem. Artikel 77 informiert, existiert ebenfalls ein wirksamer gerichtlicher Rechtsbehelf. [62, Art. 78]
Ebenso verankert die DSGVO das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche bzw. Auftragsverarbeiter. Das ist dann möglich, wenn eine betroffene Personen der Ansicht ist, dass ihre Rechte lt.

DSGVO im Rahmen einer Verarbeitung ihrer personenbezogenen Daten verletzt wurden. [62, Art. 79]
Das im Artikel 80 verankerte Recht auf Beschwerde durch eine Organisation ohne Gewinnerzielungsabsicht, so im Recht des Mitgliedstaat vorgesehen, wurde im Rahmen der Maßnahmen des österreichischen Datenschutz-Anpassungsgesetzes 2018 nicht vorgesehen. [62, Art. 80 (2)] [37]
Schadenersatzrechte für materiellen und immateriellen Schaden werden in der DSGVO ebenso verankert und es werden explizit die Haftungen für Verantwortliche und Auftragsverarbeiter klargestellt. Der Verantwortliche haftet grundsätzlich für Schäden, die aus mit der DSGVO nicht in Einklang stehenden Verarbeitungen entstehen; der Auftragsverarbeiter nur dann, wenn er seinen in der Verordnung definierten Pflichten nicht entspricht oder die rechtmäßig erteilten Anweisungen des Verantwortlichen ignoriert bzw. ihnen zuwider handelt. [62, Art. 82 (1) (2)]
Bei Beteiligung mehrerer Verantwortlicher oder Auftragsverarbeiter haftet jeder Beteiligte für den gesamten Schaden. [62, Art. 82 (4)]
Abschließend werden in Kapitel VII die Bedingungen für Geldbußen genannt. Diese werden von der Aufsichtsbehörde verhängt und sollen 'wirksam, verhältnismäßig und abschreckend' sein. [62, Art. 83 (1)]
Grundsätzlich bleiben Geldbußen zusätzlich zu anderen Maßnahmen jedenfalls Einzelfallentscheidungen, bei denen stets verschiedene Faktoren zu berücksichtigen sind. Dazu zählen etwa Art, Dauer und Schwere des Verstoßes, Vorsätzlichkeit oder Fahrlässigkeit, Maßnahmen, welche zur Minderung getroffen wurden, frühere Verstöße, Kooperation mit der Aufsichtsbehörde oder die Kategorie betroffener personenbezogener Daten. [62, Art. 83 (2)]
Die vielfach zitierte Höhe der Geldbußen wird ebenfalls in Artikel 83 festgelegt. Für bestimmte definierte Verstöße wird eine Buße von bis zu 10 Mio. Euro oder - im Falle, dass ein Unternehmen betroffen ist - von bis zu 2 Prozent des weltweit erzielten Jahresumsatzes fällig. Bei weiteren definierten Verstößen kann die Geldbuße sogar auf bis zu 20 Mio. Euro oder 4 Prozent des Jahresumsatzes steigen, wobei auch hier der jeweils höhere Betrag gewählt wird. [62, Art. 83 (4) (5) (6)]
Ebenso wird eine Öffnungsklausel für die Mitgliedstaaten implementiert, die die Möglichkeit schafft, auch gegen Behörden und öffentliche Stellen Geldbußen zu verhängen. [62, Art. 83 (7)]

3.2.2.9 Kapitel IX: Vorschriften für besondere Verarbeitungssituationen

Im Rahmen des Kapitels IX werden besondere Verarbeitungssituationen benannt und Vorschriften für diese erlassen. Dazu zählen etwa die Freiheit der Meinungsäußerung und die Informationsfreiheit, etwa für journalistische, wissenschaftliche oder künstlerische Zwecke. Weiters umfasst das Kapitel etwa Vorschriften zur Datenverarbeitung im Kontext von Beschäftigung, Geheimhaltungspflichten oder bestehenden Datenschutzvorschriften von Kirchen und religiösen Gemeinschaften. [62, Art. 85 - 91]

3.2.2.10 Kapitel X: Delegierte Rechtsakte und Durchführungsrechtsakte und Kapitel XI: Schlussbestimmungen

Die beiden abschließenden Kapitel X und XI der DSGVO behandeln Bestimmungen zu delegierten Rechtsakten und Durchführungsrechtsakten sowie die Schlussbestimmungen, die etwa die Richtlinie 95/46EG aufheben und das Inkrafttreten der Datenschutz-Grundverordnung am 24.05.2016 bzw. die verpflichtende Anwendung ab 25.05.2018 beinhalten. [62, Art. 92 - 99]

3.2.3 Inhaltliche Analyse DSGVO

Da der Datenschutz im Allgemeinen und die Datenschutzgesetzgebung im Speziellen ein Feld mannigfaltiger, aufeinanderprallender Interessen darstellen, erscheint es kaum verwunderlich, dass die DSGVO von unterschiedlichen Stellen sehr differenziert bewertet wird.
Dabei unterliegt Datenschutzgesetzgebung stets der Herausforderung, rechtliche Rahmenbedingungen für technische Entwicklungen vorzugeben und dabei nach bester Möglichkeit mit dem Tempo des Fortschritts mitzuhalten. Dass dies ein schwieriges Unterfangen ist, betonte etwa Dr. Bäumler im Gespräch im Rahmen dieser Arbeit mehrmals. [22]
Im Zuge der Experteninterviews für diese Arbeit wurde die Datenschutz-Grundverordnung grundsätzlich positiv bewertet. [22] [34] [23]
Weitere positive Rückmeldungen kamen etwa von der Bundesdatenschutzbeauftragten Deutschlands, Andrea Voßhoff, sowie vom ehemaligen Staatssekretär im Bundeswirtschaftsministerium, Rainer Sontowski.
Voßhoff erwartete in einem Statement im April 2016 Rechtssicherheit und gleiche Bedingungen für sämtliche Marktteilnehmer von der DSGVO. Ebenso würde der Flickenteppich der Regelungen einzelner Mitgliedstaaten nun harmonisiert. Die deutsche Bundesdatenschutzbeauftragte bezeichnete den Datenschutz als Qualitätsmerkmal, er 'könne auch als Standortvorteil genutzt werden' [64]. Des Weiteren forderte sie vom deutschen Wirtschaftsministerium, Datenschutz-

konzepte im Rahmen eines Wettbewerbs ausschreiben zu lassen. [64]
Der Staatssekretär im Bundeswirtschaftsministerium, Rainer Sontowski, bezeichnete die DSGVO als Meilenstein, die entsprechende Rahmenbedingungen für gerechten Handel im Spannungsfeld Big Data - Datenschutz möglich mache. [64]
Die EU-Justizkommissarin Vera Jourova sprach im Dezember 2015 in Pressemitteilungen, dass die Bürger wieder 'Herr ihrer Daten' [36] würden, die Stärkung des 'Rechts auf Vergessenwerden' betonte die Kommissarin besonders. [36]
Deutlich kritischer äußerte sich etwa Prof. Dr. Tomas Hoeren, Informations- und Medienrechtswissenschaftler an der Universität Münster. Hoeren bezeichnete die DSGVO auf dem Euroforum-Datenschutzkongress im April 2016 als 'größte Katastrophe des 21. Jahrhunderts' [65].
Konkret kritisierte er etwa die Regelungen zur verpflichtenden Datenportabilität von einem Dienstleister zum anderen als sinnlose Maßnahme, die der 'neue' Dienstleister eventuell gar nicht akzeptieren würde. Das 'Recht auf Vergessen' sei laut Hoeren bereits größtenteils im BDSG verankert, außerdem kritisierte er, dass die 120 neuen Informationspflichten auch für 'jeden Sportverein, für jeden Webseiten-Betreiber' [65] gelte und die Grundverordnung in den Verhandlungen stets weiter reduziert worden wäre. Auch die als Pluspunkt betonte Harmonisierung des Datenschutzrechts sah er aufgrund der Öffnungsklauseln und nationalen Regelungsspielräume als kaum gegeben an. [65]
Ebenso kritisch fiel beispielsweise eine rechtswissenschaftliche Untersuchung der Universität Kassel aus.
Die Projektgruppe *Verfassungsverträgliche Technikgestaltung* untersuchte unter der Leitung von Prof. Dr. Alexander Roßnagel die Datenschutz-Grundverordnung und kam zum Ergebnis, dass die DGSVO keines ihrer Ziele erreichen würde. [29]
Die drei wesentlichen Gründe dafür sind laut der Analyse: [29]

- Die hohe Anzahl an Öffnungsklauseln und Regelungsspielräumen, die die Analyse mit 70 beziffert. Dadurch unterscheiden sich die nationalen Regelungen deutlich voneinander.
- Die DSGVO enthalte laut der Projektgruppe nur sehr abstrakte Antworten auf die gestellten Fragen, dadurch würde es zu unterschiedlichen Anwendungen von Behörden, der Judikative und der Unternehmen in den Mitgliedstaaten kommen.
- Außerdem seien laut Analyse die Regelungen der DSGVO dermaßen technikneutral, dass die Risiken der IT nicht entsprechend erfasst werden würden. Prof. Roßnagel führte konkret an, dass Datenschutzherausforderungen in Bereichen wie Cloud Computing, soziale Netzwerke oder Big Data ignoriert werden würden.

Des Weiteren bemängelte die juristische Analyse der Universität Kassel die

zunehmende Rechtsunsicherheit, die durch die Gültigkeit der DSGVO und des nationalen - in diesem Fall also deutschen - Rechts entstehe. Das nationale Recht würde nämlich weiter gelten, außer, es stehe in Widerspruch gegenüber der Datenschutz-Grundverordnung. Dennoch gilt das Recht des Mitgliedstaats im Falle eines vermeintlichen Widerspruchs oder einer andersartigen Regelung, wenn es die DGSVO im Zuge einer Öffnungsklausel präzisiert. Dadurch kommt Prof. Roßnagel zum Schluss, dass es zu Unklarheiten kommen könnte, welche Rechtsmaterie nun anwendbar sei. [29]
Ebenso forderten die Rechtswissenschaftler den deutschen Gesetzgeber auf, Übersichtlichkeit in die Rechtslage zu bringen, die das Datenschutzniveau sichern sollen. [29] Aufgrund der entdeckten Unklarheiten gab Prof. Roßnagel im September 2016 ein Buch mit dem Titel 'Europäische Datenschutz-Grundverordnung: Vorrang des Unionsrechts - Anwendbarkeit des nationalen Rechts' heraus, in welchem etwa Fragen des Anwendungsvorrangs der DSGVO und zur Gültigkeit nationaler Regelungen behandelt wurden, um eine Übersicht zu schaffen. [53]

3.3 Das Datenschutz-Anpassungsgesetz 2018

Die Datenschutz-Grundverordnung gilt als Verordnung der Europäischen Union grundsätzlich unmittelbar. Dennoch sind in der DSGVO etliche Regelungsspielräume bzw. Öffnungsklauseln enthalten, die es den jeweiligen Mitgliedstaaten ermöglichen, anpassend legislativ tätig zu werden.
Für das nationale österreichische Recht wurden die entsprechenden Regelungen mit den Maßnahmen des Datenschutz-Anpassungsgesetzes 2018 getroffen. Nach dem vorparlamentarischen Begutachtungsverfahren mit der Möglichkeit für unterschiedliche Institutionen, Organisationen, Unternehmer und Bürger eine Stellungnahmen abzugeben, erfolgte am 07.06.2017 das Einlangen im Nationalrat. Es wurde am 26.06.2017 im Verfassungsausschuss behandelt und am 29.06.2017 im Rahmen der 190. Sitzung des Nationalrats mit den Stimmen der Abgeordneten der SPÖ und ÖVP (Gegenstimmen: FPÖ, Die Grünen, NEOS und Team Stronach) in dritter Lesung angenommen. Am 06.07.2017 erfolgte der Beschluss im Bundesrat, der Länderkammer des österreichischen Parlaments. [42]
Ursprünglich umfasste die Regierungsvorlage unter dem Titel 'Datenschutz-Anpassungsgesetz 2018' Änderungen des Bundes-Verfassungsgesetzes, das Erlassen des Datenschutzgesetzes und die Aufhebung des Datenschutzgesetzes 2000. Aufgrund der politischen Situation und dem absehbaren Nichtzustandekommen der notwendigen Zweidrittelmehrheit wurde das Gesetz als 'Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (Datenschutz-Anpassungsgesetz 2018)' [45] beschlossen.
Dazu wurde im Ausschuss ein Abänderungseintrag erfolgreich eingebracht. [44]

3.3.1 Inhaltliche Zusammenfassung Datenschutz-Anpassungsgesetz 2018

Das Datenschutz-Anpassungsgesetz 2018, mit dem das DSG2000 zum DSG abgeändert wurde, umfasst 5 Hauptstücke, die sich wiederum in einzelne Abschnitte gliedern.
Das 1. Hauptstück handelt von der Durchführung der DSGVO und weiteren, ergänzenden Regelungen. Im 2. Hauptstück werden Organe wie Datenschutzrat bzw. -behörde behandelt. Das 3. Hauptstück umfasst die Verarbeitung personenbezogener Daten für polizeiliche und militärische Zwecke sowie Maßnahmen des Strafvollzugs, während die beiden abschließenden Hauptstücke Nummer 4 und 5 besondere Strafbestimmungen und die Schlussbestimmungen zum Inhalt haben. [37]
Nun folgend wird kurz auf wesentliche Eckpunkte in der österreichischen Regelung eingegangen.

3.3.1.1 1. Hauptstück - Durchführung DSGVO und ergänzende Regelungen

In Artikel 8 der DSGVO ist eine Minimalgrenze des vollendeten sechzehnten Lebensjahres vorgegeben, allerdings existiert eine Öffnungsklausel für Regelungen durch Mitgliedstaaten. [62, Art. 8]
Diese wurde vom österreichischen Gesetzgeber auch genutzt, im DSG ist eine Einwilligung bereits ab dem vierzehnten Lebensjahr rechtmäßig. [37, §4 Abs. 4]. Dies soll laut Abg. z. NR Eva-Maria Himmelbauer die Lebensrealität widerspiegeln - 14jährige Jugendliche kaufen z.B. regelmäßig Apps für ihre Smartphones und sollen auch - um die Benutzung zu ermöglichen - den Datenschutzbestimmungen zustimmen können. [16]
Außerdem werden Regelungen zum Datenschutzbeauftragten präzisiert. Nennenswert ist, dass Datenschutzbeauftragte des öffentlichen Bereichs einen regelmäßigen Austausch von Erfahrungen zu pflegen haben. Damit soll vor allem ein einheitlicher Datenschutzstandard gewährleistet werden. [37, §5]
Weitere Regelungen und Spezifikationen umfassen das Datengeheimnis [37, §6], sowie Datenverarbeitung zu spezifischen (Forschungs-)Zwecken. [37, §7-§11]

3.3.1.2 2. Hauptstück - Organe

Neben der - laut Datenschutz-Grundverordnung - unbedingt notwendigen Datenschutzbehörde bleibt auch der Datenschutzrat als Beratungsgremium des Bundeskanzleramts erhalten. [37, §14]
Das DSG definiert die neue Zusammensetzung, es entsenden u.a. im Hauptausschuss des Parlaments vertretene politische Parteien, die Länder, die AK und die WKO sowie weitere Institutionen in Datenschutzfragen versierte Mitglieder in dieses Gremium. [37, §15]
Weitere Kompetenzen, Regelungen und Aufgaben die Datenschutzbehörde betreffend werden ebenso im 2. Hauptstück behandelt und diese wird als nationale

Aufsichtsbehörde gemäß Datenschutz-Grundverordnung [62, Art. 51] eingerichtet. [37, §18]
Zu den Befugnissen der DSB zählen auch explizit Beratungsbefugnisse und Möglichkeiten, Verantwortliche bzw. Auftragsverarbeiter vor geplanten Vorgängen zu warnen bzw. Anweisungen zu erteilen, Verarbeitungsvorgänge in Einklang mit der DSGVO zu bringen. [37, §33]

3.3.1.3 3. - 5. Hauptstück

Das 3. Hauptstück umfasst Regelungen zur Verarbeitung personenbezogener Daten für 'Zwecke der Sicherheitspolizei einschließlich des polizeilichen Staatsschutzes, des militärischen Eigenschutzes, der Aufklärung und Verfolgung von Straftaten, der Strafvollstreckung und des Maßnahmenvollzugs'. [37, 3. Hauptstück]
Auf diese spezifischen Fälle wird an dieser Stelle nicht gesondert eingegangen.
Im 4. Hauptstück sind besondere Strafbestimmungen geregelt. Sofern nicht strengere Strafbestimmungen gemäß DSGVO fällig sind, werden verschiedene Tatbestände definiert, welche Verwaltungsstrafen von bis zu 50.000 Euro nach sich ziehen können. [37, §62]
Datenverarbeitung in Gewinn- bzw. Schädigungsabsicht kann dabei u.a. mit einer Freiheitsstrafe von bis zu einem Jahr geahndet werden. [37, §63]
Schluss- und Übergangsbestimmungen sind im abschließenden 5. Hauptstück angeführt. [37, §64-§70]

3.3.2 Inhaltliche Analyse Datenschutz-Anpassungsgesetz 2018

Datenschutz ist ein grundsätzlich kontroversiell debattiertes Themengebiet, in dessen Bereich Interessen vieler Gruppierungen, Organisationen, Institutionen und Individuen aufeinandertreffen. Dies drückt sich nicht nur in der Debatte um die DSGVO, sondern auch um jene des Datenschutz-Anpassungsgesetzes 2018 und dessen Regelungen aus.
Allein für den Ministerialentwurf des Datenschutz-Anpassungsgesetzes 2018 gelangten im Rahmen des parlamentarischen Begutachtungsverfahrens weit über 100 Stellungnahmen mit den unterschiedlichsten inhaltlichen Stoßrichtungen ein. [43]
Um eine ausgewogene inhaltliche Analyse zu ermöglichen, sollen an dieser Stelle vermehrt Punkte aus den Stellungnahmen bzw. Bewertungen der **Wirtschaftskammer Österreich** als Interessenvertretung heimischer Unternehmen auf der einen Seite, und Positionen der **ARGE Daten** als gemeinnütziger Verein und Gesellschaft für Datenschutz auf der anderen Seite, berücksichtigt werden.
Ein umstrittener Punkt ist - abgesehen von inhaltlichen Bestimmungen - das kurze Begutachtungsverfahren der Novelle. Naturgemäß wurde diese Vorgehensweise vor allem von den Oppositionsparteien kritisiert, die dadurch zahlreiche, spät eingelangte Stellungnahmen nicht gebührend berücksichtigt sahen. [41]

Dem entgegengesetzt wird, unter anderem von Seiten der WKO [52] und der Abg. z. NR Eva-Maria Himmelbauer [16], dass den Betroffenen, vor allem also den Unternehmen, gegenüber Rechtssicherheit bestehen müsse.
Dieses Argument wiegt insofern schwer, da die DSGVO ab 25.05.2018 in Kraft tritt und in Österreich am 15.10.2017 Nationalratswahlen stattfanden, die das politische Kräftespiel dementsprechend veränderte. Da die Phase der Regierungsbildung nach einer Wahl ebenso mehrere Wochen bis Monate in Anspruch nehmen könne, würde die Anpassung nationaler Gesetze an die DSGVO wohl erst 2018 erfolgen. Dies würde betroffene Organisationen und Unternehmen vor große Rechtsunsicherheiten stellen. Auch SPÖ-Abgeordneter Peter Wittmann betonte die Wichtigkeit, sich auf die die veränderte Rechtslage einstellen zu können. [41]
Insofern erscheint die kurze Begutachtungsphase verständlich, wäre aber bei ausreichend langfristiger Planung vermutlich vermeidbar gewesen. Die Herausforderung, in politisch unsicheren Zeiten diese Novelle rasch zu verabschieden, manifestierte sich bereits in der Tatsache, dass die ursprünglich vorgesehenen verfassungsrechtlichen Änderungen ihren Weg nicht in die Novelle fanden, da die dafür notwendige Zwei-Drittel-Mehrheit (wofür die Zustimmung einer Oppositionspartei notwendig gewesen wäre) nicht erreicht werden konnte.

Aus unternehmerischer Standortperspektive fällt das Urteil über das Anpassungsgesetz grundsätzlich positiv aus.
Die WKO betonte in einer Meldung nach dem Beschluss im Nationalrat Ende Juni 2017 wie bereits erwähnt die positiven Aspekte der raschen Beschlussfassung, vor allem die geschaffene Rechtssicherheit für die österreichischen Unternehmen. Einige Öffnungsklauseln der DSGVO, die zusätzliche Aufgaben für Betriebe bedeutet hätte, wurden nicht in Anspruch genommen, etwa die der zusätzlich möglichen verpflichtenden Datenschutzbeauftragten oder die in Österreich nicht mögliche antragslose Verbandsbeschwerdemöglichkeit. [37]
Diese nicht vorhandene Beschwerdemöglichkeit über Verbraucherverbände wurde von anderen Fraktionen, wie zum Beispiel dem Datenschutz-Juristen Maximilian Schrems, kritisiert. [54]
Zu den weiteren positiven Punkten zählte die Wirtschaftskammer die Möglichkeit, Geldbußen gegen juristische Personen zu verhängen und nicht parallel etwa Geschäftsführer (und damit Privatpersonen) zu bestrafen. Auch das Kumulationsverbot und die Möglichkeit, Verwarnungen statt Geldbußen zu erteilen, wurden positiv erwähnt. [52]
Im gesamtändernden Abänderungsantrag wurde von der WKÖ u.a. die Absenkung des Einwilligungsalters auf 14 Jahre goutiert, dies erwähnt im Interview im Rahmen dieser Arbeit ebenso Abg. z. NR Eva-Maria Himmelbauer positiv. [16] [52]
Außerdem sah die WKO positiv, dass rechtskräftig erteilte Genehmigungen der DSB gem. §§ 13, 46 und 47 DSG 2000 aufrecht blieben. [52]

Die ARGE Daten stieß mit den einleitenden Worten ihrer Stellungnahme grundsätzlich in eine ähnliche Richtung und bezeichnete als Leitprinzip der nationalen Gesetzgebung zur DSGVO die Schaffung von Rechtssicherheit. Sie be-

tonte, dass es den heimischen Unternehmen mit dieser Rechtssicherheit ermöglicht werden solle, bis 25.05.2018 optimal die notwendigen Vorkehrungen zu treffen. [47, S. 2]
Ein Kritikpunkt, der auch im Interview mit Abg. z. NR Eva-Maria Himmelbauer angesprochen wurde, war, dass die Datenschutzbehörde zugleich als Kontroll- und als Strafbehörde fungiert, also keine Trennung der Aufgaben vorgenommen wurde, wie sie beispielsweise in Bereichen des Kartellrechts existiert. Laut Abg. z. NR Himmelbauer ist aber für eine sehr ähnliche Fragestellung in Bezug auf Strafkompetenz einer Kontrollbehörde für die FMA ein Verfahren beim VwGH anhängig. [16]
Viele weitere Punkte der Stellungnahme zielten allerdings auf Unvereinbarkeiten zwischen den Regelungen des österreichischen Datenschutz-Anpassungsgesetzes und der Datenschutz-Grundverordnung ab, bzw. waren vergleichsweise wesentlich kritischer als die angeführten Punkte der WKO.
Als problematisch beurteilte die Stellungnahme die weitere Nichtregelung von Scoringsystemen. Darunter versteht man Systeme, die Individuen aufgrund verschiedener Informationen beurteilen, etwa im Rahmen von Kreditbeurteilungssystemen zur Bonitätsprüfung. Verschiedene Parameter, die laut der ARGE DATEN-Stellungnahme zu einer schlechteren Bewertung führen würden, sind etwa ein junges Alter, die 'falsche' Wohngegend oder das arbeitsrechtliche Anstellungsverhältnis als Arbeiter. [47, S. 2]
Ähnliche Vorgänge erwähnte im Zuge des Interviews im Rahmen dieser Arbeit Landesdatenschutzbeauftragte Marit Hansen, die die sogenannte 'Preisdiskriminierung' als greifbaren Effekt von unzureichendem Datenschutz benannte. [34]
Ebenso kritisch gab sich die Stellungnahme der ARGE Daten in Bezug auf **Whistleblowing-Hotlines**, die sie insofern verunmöglicht sah, als dass die Verarbeitung personenbezogener Daten über Straftaten behördliche Aufsicht erfordern würde. Hier wurde eine Klarstellung gefordert. [47, S. 3f]
Bezüglich des **Grundrechts auf Datenschutz** sprach sich die ARGE-Stellungnahme gegen eine Beibehaltung des Grundrechts aus dem alten DSG 2000 aus - zum einen, da dies bereits in der Grundrechtecharta, der EMRK und der DSGVO verankert war und die Rechtslage somit verkomplizieren würde; zum anderen, weil sich die Einschränkungstatbestände laut Stellungnahme nicht mit der DSGVO decken würden. [47, S. 4]
Eine weitere, kritisch gesehene österreichische Regelung ist eine Besonderheit im Zuge der **Bestellung von Datenschutzbeauftragten im öffentlichen Dienst**. Hier sieht die österreichische Gesetzgebung vor, dass der Datenschutzbeauftragte dem jeweiligen Ministerium bzw. der jeweiligen nachgeordneten Dienststelle angehören muss. Dies ARGE DATEN sah in diesem Passus eine nicht notwendige Einschränkung und wollte diese Möglichkeit auch einem externen Personenkreis ermöglichen. [47, S. 5]
Die ARGE DATEN sah zudem Schwierigkeiten bei der Kompatibilität der nationalen österreichischen Regelungen mit der DSGVO im Bereich der **Befugnisse der Datenschutzbehörde**. So könne gemäß dem Datenschutzgesetz 2018 die DSB nur im begründeten Verdachtsfall bei Verstoß gegen die DSGVO tätig werden. Darin sah die Stellungnahme eine nicht erlaubte Einschränkung der

Mindestbefugnisse. [47, S. 5]
Scharfe Kritik übte die ARGE DATEN an der fehlenden Möglichkeit der österreichischen Datenschutzbehörde, gegenüber **Behörden und öffentlichen Stellen Geldbußen** auszusprechen. So sei die Datenschutzgesetzgebung im öffentlichen Bereich als zahnlos anzusehen. [47, S. 8]

Insgesamt existieren also zu den Regelungen des Datenschutz-Anpassungsgesetzes mannigfaltige Stellungnahmen und Meinungen, ob die getroffenen Anpassungen nun begrüßenswert seien, oder eben nicht. Konsens ist jedenfalls, dass die Begutachtungsfrist relativ kurz gesetzt wurde - wohl der politischen Situation geschuldet. Nach den sitzungsfreien Sommerwochen wäre der Beschluss im Nationalrat wohl aufgrund der Wahl am 15.10.2017 und den darauffolgenden Regierungsverhandlungen erst verhältnismäßig kurz vor Beginn der Anwendbarkeit der DSGVO getroffen worden - und für Unternehmen würde sehr lange keine Rechtssicherheit über die anzuwendenden nationalen Regelungen bestehen. Auch der Inhalt der Maßnahmen des österreichischen Datenschutz-Anpassungsgesetzes 2018 wurde - abschließend zusammengefasst - kontroversiell diskutiert. Einerseits wurden die Regelungen negativ konnotiert 'Minimalversion' genannt [54], auf der anderen Seite wurde genau diese enge Anlegung an die ursprüngliche DSGVO von zahlreichen Seiten als sehr positiv bezeichnet, da *gold plating* verhindert und wenig zusätzliche, belastende Regulierungen vom österreichischen Gesetzgeber verabschiedet worden wären.

3.4 Vergleich Datenschutzrecht/Privacy im internationalen Kontext

3.4.1 Datenschutz(recht) in den USA

Datenschutz weist im internationalen Vergleich schon historisch bedingt einen unterschiedlichen Stellenwert auf. Ein kurzer geschichtlicher Umriss des Datenschutzes wurde bereits zu Beginn dieses Kapitels gegeben, wobei der Fokus eher auf die europäischen bzw. deutschen Entwicklungen gelegt wurde.
In den USA wurde der Bedarf nach modernen rechtlichen Rahmenbedingungen für Datenschutz in den 1960er Jahren erkannt. Beispiele für frühe Regelungen waren der *Freedom of Information Act* 1966 und der *Privacy Act* 1974, in denen allerdings hauptsächlich Auskunftsrechte für Betroffene und Einschränkungen für Bundesbehörden behandelt wurden. [57, S. 3]
Bis dato wurde allerdings kein - mit europäischem Ausmaß vergleichbares - Datenschutzgesetz auf Bundesebene verabschiedet. Das Gewirr unterschiedlicher Regelungen auf Ebene des Bundes und der Bundesstaaten erschweren eine Übersicht über die Rechtslage. Der in der Folge des 11. September erlassene *Patriot Act* ermöglichte Sicherheitsbehörden eine Ausweitung ihrer Kontrollrechte. Die von Edward Snowden 2013 veröffentlichten Informationen zur Überwachungstätigkeit der NSA zeigten erneut den schwachen Stand von Daten-

schutzsystemen und -regelungen in den Vereinigten Staaten auf, dessen historischer Vorsprung in Sachen Datenschutzrecht egalisiert worden war. Ein unionsähnliches Datenschutzniveau ist also nicht existent. [57, S. 3]
Die *New York Times* verglich in einem Artikel vom Jänner 2016 das Schutzniveau von Onlinedaten in den USA mit dem in den EU-Mitgliedstaaten anhand mehrerer Beispielfälle. Eingangs wurde erwähnt, dass ein grundsätzlicher Unterschied zwischen dem Schutz von Onlinedaten in den USA und in 'Europa' (Anm.: gemeint ist wohl EU/EWR) herrscht. In den Vereinigten Staaten würden ganz unterschiedliche Gesetzesmaterien spezifische Sektoren, wie beispielsweise den Gesundheitsbereich, betreffen. In der EU würde Datenschutz hingegen als Grundrecht angesehen. [56]
Anhand von einigen Beispielen wurde der Unterschied deutlich gemacht. So könnte in der Union ein Suchmaschinentreffer über eine längst vergangene, kurzzeitige Verhaftung ohne Verurteilung oder Eintrag in ein Strafregister aufgrund des 'Rechts auf Vergessen' mittels einer Anfrage bei der Suchmaschine gelöscht werden; in den USA hingegen existieren laut Artikel keinerlei solche grundsätzlich verankerten Möglichkeiten. [56]
Auch das Recht auf Auskunft, also welche Daten ein konkretes Unternehmen über eine betroffene Person besitzt, sei als solches in der EU, nicht aber in den USA verankert. In den Vereinigten Staaten existieren in manchen Bereichen aber Industriestandards zum Thema. [56]
Dieses unterschiedliche Schutzniveau spielte und spielt naturgemäß bei der Übermittlung personenbezogener Daten von Europa in die USA eine große Rolle, wie die bereits erwähnten Debatten um *Safe Harbor* und dem Nachfolger, *Privacy Shield*, zeigen.
Zusammenfassend ist den Vereinigten Staaten - trotz einstigem Vorsprung in der Datenschutzgesetzgebung in den 1960er und 1970er Jahren - kein, dem EU-Zustand vergleichbares, Datenschutzniveau zu attestieren. Datenschutz als Wettbewerbsvorteil könnte also aus dieser Perspektive ein europäisches Alleinstellungsmerkmal darstellen.

3.4.2 Datenschutz(recht) international (exkl. USA)

Auch in anderen Regionen der Welt ist es um den Datenschutz oft weniger gut bestellt als in der Europäischen Union. Dies korrespondiert in vielen Ländern wohl auch mit den weniger stark ausgeprägten Bürgerrechten bzw. Abwehrrechten gegenüber dem Staat.
Ein prominentes Beispiel hierfür ist die Volksrepublik China, in welcher das Thema Datenschutz durch die zunehmende Anzahl an Nutzern von Onlinediensten rasant an Bedeutung gewinnt. Im August 2017 betrug die Internetnutzerzahl geschätzte 731 Millionen Personen. Dabei stellt das speziell in China wenig ausgeprägte Bewusstsein für Datenschutz bei gleichzeitiger selbstverständlicher Nutzung potentiell kritischer Services, wie etwa Bezahldienste, ein besonderes Problem dar. [58]

Dennoch wächst das Bedürfnis nach Datenschutz auch in der Volksrepublik, ein Datenleak vom Juni 2017, der vor allem Apple-User betraf, führte gerade in der Mittelschicht zu einem erhöhten Bewusstsein in Bezug auf leichtsinnige Datenweitergabe. Einen einheitlichen, landesweiten gesetzliche Rahmen sucht man allerdings, wie in den USA, vergebens. Zwar wurde vom chinesischen Staatsrat ein Gesetzesentwurf 2003 in Auftrag gegeben, der Stillstand in dieser Causa dauert allerdings bereits seit 2008 an. Aktuell herrscht ein Durcheinander zahlreicher branchenspezifischer Regelungen. [58]
Bewegung in die Sache kommt insofern, als dass verschiedene Standards in der Informationssicherheit und für die Weitergabe an Daten in das Ausland von Seiten der Regierung entworfen wurden, welche alleine aufgrund wirtschaftlicher Interessen am Funktionieren eines intakten und vertrauensvollen Datennetzwerks angewiesen ist. Dennoch werden vor allem Unternehmen und User haftbar gemacht, eine Kontrolle von Behörden bzw. des Staates wurde bis dato nicht ermöglicht - und ist in einem totalitären Einparteiensystem wohl so schnell auch nicht zu erwarten. [58]
Gerade in Bezug auf Clouddienste muss besondere Vorsicht an den Tag gelegt werden, da hier auch im betrieblichen Umfeld schnell die Übersicht, wo welche personenbezogenen Daten verarbeitet bzw. gespeichert werden, verloren geht. Im Abschnitt Cloud Computing dieser Arbeit wird gesondert auf diese Problematik eingegangen, an dieser Stelle sei allerdings erwähnt, dass neben den USA und China besonders vor Indien, in dem de facto keine Datenschutzgesetzgebung existiert, sowie weiteren unsicheren Drittstaaten von Expertenseite ausdrücklich gewarnt wird. [48]
Auch hier gilt also: Ein hohes Maß an Datenschutz kann wohl nur der europäische bzw. der Unionsmarkt bieten. Datenschutz als Wettbewerbsvorteil bleibt auch im Vergleich mit Regionen und Ländern außerhalb der USA ein europäisches Merkmal.

4 IT-Security als Wettbewerbs- und Standortvorteil

Data is the new oil - Daten sind das neue Öl. Mit diesem Satz wurde das Datenschutz-Kapitel der vorliegenden Arbeit begonnen und es ist auch für das nun folgende Kapitel relevant. Daten, als 'neues Öl' dementsprechend wertvoll zu besitzen, müssen auch entsprechend geschützt werden, sei es vor Verlust bzw. Beschädigung durch Unfälle, sei es vor böswilligen Zugriffen.
Damit auch die Sicherheit der Informationstechnologie einen Beitrag zum Wettbewerbsvorteil für die Standorte Österreich und die Europäische Union leisten kann, muss eine durchdachte Strategie verfolgt werden, die Behörden, Unternehmen und Privatpersonen berücksichtigt. In diesem Kapitel werden deshalb zuerst Empfehlungen der ENISA, der Unionsbehörde für Netzwerk- und Informationssicherheit, zusammengefasst. Diese behandeln die vier Phasen des *Lifecycles* einer NCSS: Entwicklung, Implementierung, Evaluierung und Anpassung. [17] [32]
Danach werden drei aktuelle nationale Cybersicherheitsstrategien (Großbritannien, Deutschland, Österreich) inhaltlich aufbereitet und analysiert, bevor die NIS-Richtlinie der EU, mit der ein gemeinsames hohes Schutzniveau in Netz- und Informationssystemen in der EU erreicht werden soll, behandelt wird. Genauso wie die DSGVO ab Mai 2018 anzuwenden ist, muss die NIS-Richtlinie bis Mai 2018 in den Mitgliedstaaten in nationales Recht umgesetzt werden. [51]
Auch das Thema IT-Security und die Frage, inwieweit ein hohes Niveau an IT-Sicherheit einen Standortvorteil bedeuten kann, wurde in den Experteninterviews im Rahmen dieser Arbeit behandelt. Deren Fachkenntnisse finden sich am Ende dieses Kapitels und innerhalb des Modells wieder, um dazu beizutragen, die Frage nach den Rahmenbedingungen für IT-Sicherheit als Wettbewerbs- und Standortvorteil zu klären.

4.1 Einführung aktuelle Situation - Motivation

Gleich dem Datenschutz ist wohl auch die Bedeutung von IT-Sicherheit für das Alltagsleben heute so hoch wie nie zuvor. Die elektronische Verarbeitung personenbezogener Daten, etwa durch Unternehmen oder Behörden, ist dabei freilich nichts Neues und kein Phänomen der letzten Jahre. Doch die Vernetzung von immer mehr (Daten generierender) Endgeräte, die vermehrte Abwicklung hochsensibler (Unternehmens-) Prozesse im Cyberspace sowie die immer stärker vorhandene Möglichkeit, große Mengen an personenbezogenen Daten zu verarbeiten und zu verknüpfen hat in den letzten Jahren massiv zugenommen. Das eher verbraucherorientierte *Internet of Things* und das betriebliche *industrial Internet of Things* ermöglichen Vernetzungen und eröffnen neue, innovative Möglichkeiten im privaten und unternehmerischen Umfeld.
Dennoch besitzt der vermehrte Grad an Vernetzung auch eine Schattenseite. Starke Interdependenzen zwischen elektronischen (Informations-)Systemen können große Abhängigkeit und eine Vielzahl an potentiellen Schwachstellen bei einem unvorhergesehenen Ereignis bedeuten. Zudem bieten vernetzte Geräte und Systeme oft Möglichkeiten für Angreifer, Verbindungen zu stören, Daten zu stehlen

oder anderen beträchtlichen Schaden anzurichten.
Das Thema IT-Security zieht sich also durch die unterschiedlichsten Lebensbereiche und umfasst so gut wie alle Akteure einer Gesellschaft, von den staatlichen Stellen und Behörden, über große Unternehmen und international agierende Konzerne, bis hin zu kleinen KMUs sowie zum einzelnen Individuum. Hier herrscht in einigen heimischen Bereichen noch Nachholbedarf. So zitierte die Tageszeitung 'Der Standard' Ende Mai 2017 eine Umfrage von PwC, die den österreichischen Unternehmen noch Verbesserungsnotwendigkeiten attestierte. Zwar sei ein Umdenken in Sicht, dass IT-Sicherheit elementarer Bestandteil geschäftlicher Rahmenbedingungen sein müsse, allerdings hinke der heimische Markt in Punkto Investitionen in IT-Security und Mitarbeiterschulungen dem internationalen Umfeld hinterher. Die Budgetmittel für diesen Bereich würden weltweit im betrieblichen Vergleich um ungefähr zwei Drittel gesteigert, in Österreich hingegen nur um ein Drittel. Weltweit würden Unternehmen rund 60 Prozent ihrer Mitarbeiter im Bereich IT-Sicherheit schulen, laut Angaben der befragten heimischen Unternehmen war es hierzulande nur ein Drittel. [40]
Es ist also bedeutend, eine wohlüberlegte Strategie für IT-Sicherheit für die jeweils eigene Ebene zu entwickeln. Dies bedeutet freilich nicht dasselbe für jeden Akteur - eine Privatperson, ein KMU und eine Behörde werden und sollten hier unterschiedliche Planungen vollziehen bzw. Maßnahmen treffen. Dennoch soll die Überlegung verdeutlichen, dass jeder Akteur für seinen Teilbereich Überlegungen zu Cybersecurity anstellen sollte. Der Staat hat schließlich Rahmenbedingungen für Bürger und Unternehmen zu setzen sowie die Pflicht, eine umfassende nationale Cybersicherheits Strategie (NCSS) zu konzipieren. Dazu verpflichtet die Mitgliedstaaten der Europäischen Union auch die NIS-Richtlinie, die im Zuge dieses Kapitels noch ausführlich behandelt wird. [51]

4.2 Vergleich internationaler Modelle im europäischen Kontext

Die Entwicklung einer nationalen Cybersecurity Strategie kann über mehrere Ansätze verfolgt werden. Expertise hierfür bietet die European Union Agency for Network and Information Security - kurz: ENISA. ENISA ist eine Expertenorganisation für Cybersecurity in Europa, hat ihren Sitz in Heraklion/Kreta und besitzt ein Außenbüro in Athen. [15]
Als solche stellt sie ihr Fachwissen aus diversen Bereichen der Informationssicherheit für unterschiedliche Zielgruppen, wie beispielsweise die EU, die Mitgliedstaaten, private Unternehmen und generell für die europäischen Bürger zur Verfügung. [32, S. ii]
Die ENISA benennt zwei Schlüsselphasen in der Implementierung und Verwaltung einer NCSS. Die erste Phase umfasst die *Entwicklung und Ausführung* der Strategie, die zweite inkludiert *Evaluierung und Anpassung*. [17, S. 7]
Außerdem definiert die Agency drei Modelle, wie eine NCSS eingeführt und entwickelt werden kann: [17, S. 7]

- Das **lineare Modell** besteht aus den Phasen *Entwicklung*, *Implementierung*, *Evaluierung* und schlussendlich aus dem *Erlöschen* bzw. der *Ersetzung* der NCSS.
- Der **NCSS-Lifecycle** funktioniert anfangs ähnlich dem linearen Modell, allerdings wird das Ergebnis aus der Evaluierungsphase dazu genützt, die Strategie zu warten und anzupassen.
- Das **Hybrid-Modell** ermöglicht mehrere laufende Verbesserungskreisläufe auf unterschiedlichen Ebenen.

Die ENISA wählte aufgrund ihrer Erfahrung aus Befragungen und Interviews daraus den *NCSS-Lifecycle*, da sie in diesem Modell die Anforderungen an eine nationale Cybersecurity-Strategie am besten abgebildet sah. Eine weitere Begründung war, dass solche Strategien rasch auf neu entstehende Bedrohungen reagieren und sich ihnen anpassen können müssten. [17, S. 7]
Insgesamt publizierte ENISA zwei Guides, 2012 den **National Cyber Security Strategies - Practical Guide on Development and Execution** und 2014 **An evaluation Framework for National Cyber Security Strategies**, die die zwei oben genannten Schlüsselphasen einer NCSS abbilden sollten und auf die nun überblicksmäßig gesondert eingegangen wird. [17] [32]

4.2.1 ENISA - NCSS Practical Guide on Development and Execution

Der Guide zur Entwicklung und Ausführung/Implementierung von NCSS wurde von der ENISA im Dezember 2012 publiziert. Im Rahmen der Erstellung kamen die Experten der Behörde zum Schluss, dass die Entwicklung einer NCSS durchaus eine große Herausforderung an Staat und Behörden darstelle, welche eine gut durchdachte Koordinierung und Abstimmung zwischen den unterschiedlichen Stakeholdern bedürfe. Dies umfasse sowohl Organisationen, Einrichtungen und Unternehmen aus dem öffentlichen, als auch aus dem privaten Sektor. Die Strategie müsse schlussendlich Staaten helfen, die Bemühungen aller eingebundenen Organisationen zu bündeln und zu verwalten, um Cyberrisiken auf nationaler Ebene bewältigen zu können. [17, S. 34]
Im Zuge dessen wurden von der ENISA 20 konkrete Aktionspunkte definiert, die Strategieverantwortliche im Zuge der Erstellung der NCSS befolgen sollten: [17, S. 34]

1. Definition von Vision, Umfang, Zielen und Prioritäten.
2. Befolgung eines nationalen Risk-Assessment-Approachs.
3. Bestandsaufnahme von existierenden Strategien, Regulierungen und Ressourcen.

4. Entwicklung einer klaren Verwaltungsstruktur.
5. Stakeholder identifizieren und einbinden.
6. Etablierung von vertrauenswürdigen Mechanismen zum Informationsaustausch.
7. Entwicklung von Cybersecurity-Krisenplänen.
8. Organisation von Cybersecurity-Krisenübungen.
9. Etablierung von grundlegenden Sicherheitsanforderungen.
10. Implementierung von Störungsmeldungs-Mechanismen.
11. Das Bewusstsein von Bürgern schärfen.
12. Forschung und Entwicklung fördern.
13. Trainings- und Erziehungsprogramme stärken.
14. Etablierung von Kapazitäten zur Störungsbewältigung.
15. Cyber-Kriminalität thematisieren.
16. Engagement in internationaler Kooperation.
17. Public-Private Partnership ermöglichen.
18. Sicherheit mit Datenschutz in Einklang bringen.
19. Evaluierung der NCSS.
20. Anpassung der NCSS.

Diese Aktionspunkte entsprechen dem PDCA-Modell und seinen Phasen *Plan*, *Do*, *Check* und *Act*. Die vier Phasen sollen der Entwicklung kontinuierlichen Verbesserung der Strategien dienen. Während die Entwicklung (*Plan*) und die Umsetzung (*Do*) vorrangig in diesem Guide behandelt wurden, sind die Abschnitte Evaluierung (*Check*) und Anpassung (*Act*) Schwerpunkte des nächsten ENISA-Guides zum NCSS-Lifecycle.

4.2.2 ENISA - Evaluation Framework National Cyber Security Strategies

Im November 2014 veröffentlichte die ENISA ein *Evaluation Framework* für Nationale Cybersecurity Strategien. Dieser Guide soll, wie bereits mehrfach erwähnt, Maßnahmen zur zweiten, von ENISA definierten Schlüsselphase, hinsichtlich Implementierung und Verwaltung von NCSS umfassen, also *Evaluierung und Anpassung* der Strategie. [32]
Für die jeweiligen NCSS bietet ENISA Hilfestellungen für Design, Implementierung und Evaluierung an. Das *Evaluation Framework for National Cyber Security Strategies* der ENISA aus dem Jahr 2014 analysierte vorhandene nationale Strategien zur Cybersicherheit, die zu jenem Zeitpunkt von 18 EU-Staaten verabschiedet worden waren, teilweise bereits in ihrer zweiten Iteration. [32, S. iii]
Dabei wurde die Evaluierung des *NCSS lifecycles* anhand von vier Zielen verfolgt: [32, S. iii]

- Eine Bestandsaufnahme von aktuellen Zugängen zur NCSS-Evaluierung vornehmen.
- Empfehlungen und positive Erfahrungswerte zur Implementierung und Evaluierung von NCSS präsentieren.
- Ein *Evaluation Framework* zu entwerfen und zu entwickeln.
- Dieses Framework mit aussagekräftigen Key Performance Indikatoren (KPIs) zu untermauern, um die unterschiedlichen Bedürfnisse und Reifegrade der einzelnen Mitgliedstaaten zu berücksichtigen bzw. abzubilden.

Dazu wurden 18 NCSS von Unionsmitgliedern, sowie 8 Strategien von außerhalb der EU analysiert. Die zentralen Ziele eines solchen Frameworks, die gemessen werden sollten, umfassen: [32, S. iii]

- Kapazitäten und Strategien zur Cyberverteidigung aufbauen.
- Widerstandsfähigkeit im Bereich Cybersecurity entwickeln.
- Cyberkriminalität reduzieren.
- Wirtschaft & Industrie im Bereich Cybersecurity unterstützen.
- Kritische IT-Infrastrukturen absichern.

Bei der Entwicklung eines NCSS-Evaluierungsframeworks stieß das ENISA-Team auf die Herausforderung, dass die Auswirkungen und Ziele einer nationalen Cybersicherheitsstrategie teils sehr unterschiedlich ausfallen können. Unterschiedliche Staaten legen ihre Prioritäten im Bereich Cybersicherheit anders fest, es existiert keine universelle Vorschrift oder Strategie, die ideal in jedem

Unionsstaat auf jede Situation anwendbar ist. ENISA begegnete dieser Herausforderung mit einem breiten Evaluierungsframework, mit dem einerseits die NCSS im Sinne von Effektivität evaluiert werden kann, man andererseits aber auch die Überprüfungsmöglichkeit hat, ob der Einsatz von Ressourcen (wie etwa Zeit oder Arbeitsaufwand) zur Erreichung eines spezifischen Ziels angemessen beiträgt. [32, S. 36]
Die ENISA-Ausarbeitung bietet laut Eigenbeschreibung also ein generisches Framework mit einem konsistenten Logikmodell und Handlungsvorschlägen zu jeweiligen KPIs. Es umfasst außerdem bspw. Hinweise, wie man mit möglichen Fallstricken und Problemfeldern umgehen bzw. sie vermeiden kann, wenn es um die Evaluierung von NCSS geht. Zusammen mit dem *Practical Guide* zur Entwicklung und Ausführung von Cybersecuritystrategien komplettiert das Framework mit den beiden Schritten Evaluierung und Anpassung den *Cyber Security Strategy Lifecycle*. [32, S. 36]

4.2.3 AUT - Österreichische Strategie für Cyber Sicherheit

In Österreich liegt die politische Verantwortung für Cybersecurity in den Händen des Bundeskanzleramts (BKA), welches zur Ausgestaltung eine Cyber Sicherheit Plattform ins Leben gerufen hat. Die aktuelle Strategie für Cybersicherheit stammt aus dem Jahr 2013 und wird als 'umfassendes und proaktives Konzept zum Schutz des Cyber-Raums und der Menschen im virtuellen Raum' beschrieben. [5, S. 4f]
Um neuere Entwicklungen ergänzt wird das aktuelle Bild der Cybersecurity in Österreich durch einen jährlichen Bericht Cyber-Sicherheit. [3]
Die folgende Übersicht befasst sich primär mit der Strategie für Cyber Sicherheit 2013.

4.2.3.1 Einleitung

Einführend zur Strategie werden verschiedene schützenswerte Bereiche des täglichen Lebens aufgezählt, die von digitalen Infrastrukturen abhängen. Die Wirtschaft ist aufgrund des technischen Fortschritts und ihrer internen Geschäftsprozesse, die öffentliche Verwaltung aufgrund der Zurverfügungstellung ihrer Dienstleistungen über das Internet von digitaler Infrastruktur abhängig. Die Bevölkerung muss auf die Datensicherheit vertrauen können und ebenso wird die Funktion des offenen und freien Internets und der Schutz personenbezogener Daten als Grundlage für Wohlstand, Sicherheit und Förderung der Menschenrechte erwähnt.
Die Daseinsvorsorge wird ebenfalls als stark von digitaler Infrastruktur abhängiger Bereich angeführt. Als Bedrohungen im Cyber Raum treten laut der österreichischen Strategie nichtstaatliche Akteure, wie Kriminelle oder Terroristen, aber auch staatliche Angreifer, zum Beispiel Geheimdienste oder Streitkräfte, auf.

Die Strategie für Cyber Sicherheit leitet sich dabei aus der Sicherheitsstrategie ab und orientiert sich an Prinzipien des Schutzes kritischer Infrastrukturen. [5, S. 4f]

4.2.3.2 Chancen und Risiken im Cyber Raum

Die österreichische Strategie bezeichnet den Cyberspace als 'vitalen Aktionsraum für den Staat, die Wirtschaft und die Gesellschaft'. [5, S. 6]
Bedeutung erlangt er als **Informations- und Kommunikationsraum**, innerhalb dessen die Verbreitung von Informationsbeständen ermöglicht wird. Er ist außerdem **sozialer Interaktionsraum** und **Wirtschafts- und Handelsraum**, der sich innerhalb von verhältnismäßig kurzer Zeit zu einem unglaublich bedeutenden Marktplatz entwickelt hat. Ebenso beeinflusst der Cyberspace das Verhältnis Staat zu Gesellschaft und ist so **politischer Partizipationsraum**. Der Staat erreicht mittels Formen des E-Governments Bürger und vereinfacht somit den Zugang zu staatlichen Leistungen. Die Bevölkerung erhält digitale Formen der Interaktion zur politischen Teilhabe.
Der Cyber Raum wird abschließend auch als **Steuerungsraum** bezeichnet. Gemeint ist damit, dass quasi die gesamte Verkehrs-, Wirtschafts-, Bildungs-, Sicherheits-, Gesundheits- und Industrieinfrastruktur überwacht, betrieben und gewartet werden kann. [5, S. 6]
Auch an dieser Stelle betont die österreichische Strategie also die Wichtigkeit von Cybersicherheit in Kombination mit der reibungslosen Funktionsweise kritischer Infrastruktur.

4.2.3.3 Prinzipien

Die österreichische NCSS sieht Cyber Sicherheitspolitik als Bereich, der in vielen Lebens- und Politikbereichen mitgedacht werden muss und definiert, welche Aspekte solch eine Sicherheitspolitik umfassen soll. Dabei wird als wünschenswertes Ziel eine IT-Sicherheitspolitik definiert, welche:

- **umfassend** (also Aspekte wie äußere, innere, zivile und militärische Aspekte verknüpfend)
- **integriert** (sprich arbeitsteilig zwischen Akteuren wie Staat, Wirtschaft und Wissenschaft)
- **proaktiv** (vorbeugend, um Bedrohungen präventiv zu verhindern)
- und **solidarisch** (verbunden mit Sicherheitspolitiken auf europäischer und internationaler Ebene)

sein muss. [5, S. 7]
Davon werden folgende Prinzipien abgeleitet: [5, S. 7]

- **Rechtsstaatlichkeit**: Staatliches Handeln muss auch im Bereich der Cybersecurity den hohen rechtsstaatlichen Standards Österreichs - inklusive den Menschenrechten - entsprechen. Besonders betont wird u.a. das Recht auf Privatsphäre und Datenschutz.

- **Subsidiarität**: Der Staat trägt nicht die alleinige Verantwortung für den Schutz des Cyberspace, subsidiär sind Betreiber von IKT für den Schutz der eigenen Systeme verantwortlich und sollen sich selbst dazu verpflichten. Regulierung soll nur wenn absolut notwendig angewandt werden.

- **Selbstregulierung**: Anschließend dazu soll die Eigeninitiative der Unternehmen und Organisationen bei der Anhebung des Schutzniveaus möglichst ausgeprägt sein, etwa durch Standardisierungen oder *Code of Conducts*. Die staatliche Aufgabe ist es, den Ordnungsrahmen zum IKT-Schutz zu schaffen und die Begleitung der Selbstregulierung im Privatbereich sicherzustellen.

- **Verhältnismäßigkeit**: Schutzmaßnahmen zur Hebung der IT-Security müssen kostentechnisch in einem ausgeglichenen Bezug zum jeweiligen Risiko stehen.

4.2.3.4 Strategische Ziele

Die österreichische NCSS verfolgt mehrere strategische Ziele, welche sie mit Maßnahmensetzung in bestimmten Handlungsfeldern erreichen will: [5, S. 9]
Ein **sicherer, resilienter und verlässlicher Cyber Raum**, in dem ein vertraulicher und zuverlässiger Datenaustausch gewährleistet werden kann, wird als Ziel ausgerufen, wobei prioritäre IKT-Systeme redundant ausgelegt werden sollen.
Die Strategie verfolgt weiters einen **gesamtstaatlichen Ansatz der zuständigen Bundesministerien**, der die österreichischen **IKT-Infrastrukturen** vor seinen Gefährdern sichert. Staatliche und private Stellen sollen partnerschaftlich zusammenarbeiten.
Das **Rechtsgut Cyber Sicherheit** wird von allen beteiligten Partnern unter Einsatz wirksamer und verhältnismäßiger Mittel geschützt. [5, S. 9]
Eine **'Kultur der Cyber Sicherheit'** soll durch **Awareness-Maßnahmen** implementiert werden.
Österreich soll durch Aufbau von Wissen, Fähigkeiten und Kapazitäten sowie durch zu verstärkende Kooperationen und Förderung neuer Initiativen ein **Wegbereiter bei der Umsetzung von Maßnahmen zur Sicherheit der digitalen Gesellschaft** werden. An dieser Stelle wird betont, dass dadurch die *'Attraktivität des Standorts durch hohe Verfügbarkeit, Integrität und Vertraulichkeit*

der IKT Infrastruktur' deutlich steigt.
Weiters soll Österreich eine **aktive Rolle bei der internationalen Zusammenarbeit** spielen, seine **E-Government Maßnahmen** weiter ausbauen und sicherer gestalten. Die **Unternehmen** sollen Integrität ihrer Anwendungen und anvertraute Daten ihrer Kunden schützen, während die **Bevölkerung** sich ihrer individuellen Verantwortung bewusst sein soll.

4.2.3.5 Handlungsfelder und Maßnahmen

Abgeleitet von den Zielen und an den Prinzipien orientiert ergeben sich in der österreichischen NCSS nun eine Reihe von Handlungsfeldern mit Zielausrichtungen und durchzuführenden Maßnahmen: [5, S. 10-16]

Handlungsfeld 1 - Strukturen und Prozesse [5, S. 10f]
Zielausrichtung des H1 ist die Schaffung organisationsübergreifender Abläufe im Bereich der Cybersicherheit, die eine übergeordnete Koordinierung auf politisch-strategischer sowie auf operativer Ebene ermöglichen sollen.
Maßnahmen zur Zielerreichung sind zum einen die Einrichtung einer Cyber Sicherheit Steuerungsgruppe, die unter Federführung des BKA die Maßnahmen zur Cybersicherheit auf politisch-strategischer Ebene koordiniert. Zum anderen soll eine Koordinationsstruktur auch auf der operativen Ebene implementiert werden, in deren Verantwortung die Erstellung eines regelmäßigen Lagebildes Cyber Sicherheit fällt. Im Rahmen dieser Struktur sollen Einrichtungen zusammenarbeiten, deren Aufgabe im Schutz von Computersystemen besteht, beispielsweise CERTs wie GovCERT bzw. MilCERT, das Cyber Crime Competence Center (C4) oder auch private CERTs wie CERT.at, das BRZ-CERT und etwa CERTs großer Bankinstitute.
Weiters soll ein Cyber Krisenmanagement, ähnlich dem staatlichem Krisen- und Katastrophenmanagement SKKM strukturiert, etabliert werden, das Krisenmanagement- und Kontinuitätspläne für den Bereich Business Continutiy entwirft und Cyber Übungen durchführt.
Abschließend sollen im Rahmen des H1 bestehende Cyber Strukturen, wie etwa GovCERTs, MilCERTs oder das C4 sowie der gesamte österreichische CERT-Verbund weiter gestärkt werden. [5, S. 10]

Handlungsfeld 2 - Governance [5, S. 12]
Die **Zielausrichtung** von H2 liegt darin, Rollen und Kompetenzen von staatlichen und nicht-staatlichen Akteuren im Cyberspace zu definieren und für die Kooperation geeignete Rahmenbedingungen zu schaffen.
Maßnahmen zur Zielerreichung sind die Schaffung eines zeitgemäßen ordnungspolitischen Rahmens, dem ein Bericht der Cyber Sicherheit Steuerungs-

gruppe über die Notwendigkeit zur Schaffung rechtlicher Grundlagen, regulatorischer Maßnahmen und nicht-rechtlicher Verpflichtungen (wie z.B. *Codes of Conduct*) vorangeht; außerdem die Festlegung von Mindestsicherheitsstandards sowie die Erstellung eines jährlichen Berichtes zur Cyber Sicherheit durch die Cyber Sicherheit Steuerungsgruppe.

Handlungsfeld 3 - Kooperation Staat, Wirtschaft und Gesellschaft [5, S. 12f]
Zielausrichtung von H3 ist es, eine Kooperation aller Cybersicherheit tangierender Bereiche, wie Unternehmen, Bürgern und öffentlichem Sektor mit einem permanenten wechselseitigen Informationsaustausch zu schaffen. Damit soll die Verwendung von IKT sicherer gestaltet werden.
Die **Maßnahmen zur Zielerreichung** in H3 umfassen zuallererst die Einrichtung einer 'Cyber Sicherheit Plattform', die zur laufenden Kommunikation mit allen Stakeholdern dienen soll und auf bestehende Initiativen als Public-Private-Partnership aufgebaut werden soll.
KMUs sollen mittels eigener Schwerpunktprogramme für das für sie oft als wenig relevant erscheinende Thema IT-Sicherheit sensibilisiert werden und schlussendlich soll eine 'Cyber Sicherheit Kommunikationsstrategie' ausgearbeitet werde, die zur Optimierung der Stakeholder-Kommunikation von der Steuerungsgruppe vorbereitet werden soll.

Handlungsfeld 4 - Schutz kritischer Infrastrukturen [5, S. 14]
Zielausrichtung der Handlungsfelds 4 ist die Erhöhung der Widerstandskraft der IKT kritischer Infrastrukturen. Durch ein gesondertes Programm (*APCIP*) sollen solche Infrastrukturen betreibende Unternehmen angehalten werden, umfassende Sicherheitsarchitekturen zu implementieren.
Eine beschriebene **Maßnahme zur Zielerreichung** ist die Resilienzerhöhung von kritischer Infrastruktur. Diese soll dadurch erreicht werden, dass bestimmte Infrastrukturbetreiber in Prozesse des nationalen Cyber Krisenmanagements eingebunden werden sollen und eine strategische Sicherheitsarchitektur einrichten. Die Krisenkommunikation soll ausgebaut und Cyber Sicherheitsstandards für Unternehmen ausformuliert werden. Gesetzlich nach einem Konsultationsprozess mit den Stakeholdern zu schaffende Grundlagen, wonach schwere Cyber Vorfälle meldepflichtig werden sollen, sind laut österreichischer Strategie ebenso zu schaffen, wie ein Instrumentarium zur laufenden Überprüfungen der Dispositionen von *APCIP* und des *SKKM* im Hinblick auf aktuelle Bedrohungen im Bereich Cybersecurity.

Handlungsfeld 5 - Sensibilisierung und Ausbildung [5, S. 14f]
Als **Zielausrichtung** des H5 wird die Bewusstseinsbildung für die Notwendigkeit von Cybersicherheit sowie die Aufbau einer Kompetenz in diesem Feld in der Lehre sowie eine verstärkte Behandlung in Schulen und weiteren Bildungsstätten definiert.
Es existieren dafür zwei **Maßnahmen zur Zielerreichung**. Zuerst soll die 'Cyber Sicherheit Kultur' [5, S.14] gestärkt werden, dies plant die Strategie mittels Sensibilisierungsinitiativen, Beratungs- und Präventionsangeboten sowie dem Webportal IKT-Sicherheit umzusetzen.
Die zweite Maßnahme besteht in der 'Verankerung von Cyber Sicherheit und Medienkompetenz auf allen Ebenen der Aus- und Weiterbildung'. [5, S. 15]. Dies soll durch Integration eines Modells namens 'Digitaler Kompetenzen' [5, S. 15] in die Lehrpläne aller Schulpläne geschehen, im Rahmen dessen Kompetenzen im Bereich IKT-Sicherheit behandelt werden.
Eine vermehrte Ausbildung von Spezialisten wird ebenso angestrebt, wie die Schulung von IKT-Systemadministratoren in Bereichen wie dem Erkennen von relevanten Vorfällen aus dem Bereich Cybersecurity (*Human Sensor Programm*).

Handlungsfeld 6 - Forschung und Entwicklung [5, S. 15f]
Die **Zielausrichtung** des Handlungsfelds 6 ist das Vorhaben vermehrter Behandlung von Cybersecurity-Themen in der Cyberforschung und in der Sicherheitsforschung allgemein, zum Beispiel in Programmen wie *KIRAS*.
Maßnahmen zur Zielerreichung umfassen gemeinsame Projekte von Stakeholdern aus Verwaltung, Wirtschaft und Forschung innerhalb dieser Grundlagen und technologische Werkzeuge zur Hebung des IT-Sicherheitsstandards. Ebenso soll auf eine aktive Themenführerschaft bei Sicherheitsforschungsprogrammen der EU hingearbeitet werden.

Handlungsfeld 7 - Internationale Zusammenarbeit [5, S. 16]
Die **Zielausrichtung** des letzten Handlungsfelds H7 bezieht sich auf internationale Zusammenarbeit und weltweite Vernetzung. Eine aktive Cyber Außenpolitik soll betrieben und im Rahmen von Partnerschaften mit EU, VN, OSZE, Europarat, OECD und NATO koordiniert und gezielt verfolgt werden.
Maßnahmen zur Zielerreichung sind, wie bereits in der Zielausrichtung erwähnt, die einer Umsetzung aktiver Cyber Außenpolitik. Beispiele dafür wären die Beteiligung an der Erarbeitung und Umsetzung der Cyber Sicherheitsstrategie der EU und die Umsetzungsmaßnahmen für die Europaratskonvention über Cyberkriminalität. Auch länderübergreifende Cyberübungen sollen fokussiert werden. Koordiniert sollen die außenpolitischen Maßnahmen vom BMEIA werden.

4.2.3.6 Umsetzung [5, S. 17]

Der Umsetzungsauftrag der BKA-Strategie lautet, drei Monate nach Beschluss der ÖSCS einen Implementierungsplan zu erarbeitet, wobei die Umsetzung der konkreten Maßnahmen von der Steuerungsgruppe koordiniert und von den einzelnen Stellen durchgeführt wird. Alle zwei Jahre erarbeitet die Steuerungsgruppe einen Umsetzungsbericht an die Bundesregierung, anhand dem auch die Aktualität der ÖSCS überprüft, evaluiert und gegebenenfalls adaptiert wird.

4.2.3.7 Conclusio AUT

Die nationale Cybersecurity Strategie Österreichs verfolgt mehrere Zielsetzungen. Ein sicherer, resilienter Cyberspace soll verlässlichen Datenaustausch ermöglichen. Die NCSS begreift den Cyberspace als Interaktions- bzw. Informationsraum verschiedenster Akteure und benennt Staat, Wirtschaft und Gesellschaft als 'Mitspieler'. Als Prinzipien der österreichischen NCSS sind **Rechtsstaatlichkeit**, **Subsidiarität**, **Selbstregulierung** und **Verhältnismäßigkeit** definiert. Wie zum Beispiel in der noch folgenden britischen Strategie wird also die Verantwortlichkeit für Cybersecurity subsidiär auf verschiedenen Ebenen gesehen.
Die ENISA fasst zusammen, dass die österreichische NCSS eine Stärkung der Wettbewerbsfähigkeit der Unternehmen generell verfolgt, speziell Unterstützung für KMUs soll ausgebaut werden, ein Beispiel dafür ist etwa die Initiative *it-safe.at*. [33, S. 1]
Die österreichische Strategie legt einen besonderen Fokus auf die Computer Emergency Response Teams (CERTs) und deren Zusammenarbeit untereinander. So sollen CERTs aus unterschiedlichsten Bereichen, wie die der Streitkräfte, staatlich-behördliche oder private CERTs (etwa jene großer Bankinstitute) mit dem Cyber Crime Competence Center C4 des BMI kooperieren und im Rahmen eines CERT-Verbunds regen Erfahrungstausch betreiben.
Außerdem ist im Rahmen der österreichischen NCSS eine Schwerpunktsetzung im Bereich des Schutzes kritischer Infrastrukturen feststellbar. Ein eigener Masterplan zum Schutz solcher Infrastrukturen (*APCIP*) soll betreibende Unternehmen anhalten, Sicherheitsarchitekturen innerhalb des Betriebes zu implementieren, zu verbessern und gewisse Prozesse in das nationale Cyber Krisenmanagement einzubauen.
Gerade im Bereich der Sensibilisierung bzw. der Schaffung von Awareness, ebenso ein Handlungsfeld der österreichischen Strategie, gibt es noch starken Handlungsbedarf. So meldete KPMG im September 2017 als Ergebnis einer Studie zur Cybersicherheit in Österreich, dass unter 240 befragten Cybersecurity-Experten österreichischer Unternehmen 40 Prozent angaben, keinen Überblick über alle IoT-Geräte im Betrieb zu haben. Ebenso zeichnet sich laut Studie ein stark verschärftes Bedrohungsbild ab. So stieg der Anteil von Cyberkriminalität betroffener Unternehmen im Vergleich zum Vorjahreszeitraum von 49 Prozent massiv auf 72 Prozent an, die Hälfte der untersuchten Betriebe litt in Folge der Angriffe an einer Unterbrechung von Geschäftsprozessen. [67]

Allerdings vermeldete die Studie auch positive Tendenzen im Bereich Cybersecurity in Österreich, an die eine eventuelle neue NCSS anknüpfen kann.
So wird das Thema Cybersecurity in knapp drei Viertel der Unternehmen auf oberster Managementebene diskutiert. Allerdings sehen nur 43 Prozent gesetzliche Maßnahmen wie NIS und DSGVO als hilfreich im Kampf gegen Kriminalität im Cyberspace an und Cybersicherheit wird nach wie vor (von ca. zwei Drittel der Führungsebene) als eher technische Angelegenheit betrachtet. Oft werden dadurch Chancen im Bereich IT-Sicherheit verkannt, diese Problematik sollte eine neue österreichische NCSS aufgreifen und stärker, wie zum Beispiel in Großbritannien, auf die Möglichkeiten der Vermarktung von Cybersecurity hinarbeiten. [67]
Auch im Bereich Bildung wird anzusetzen sein, wobei Österreich in der Vergangenheit nicht nur mit negativen Schlagzeilen, wie schlechten Platzierungen in Universitätsrankings, kämpfen musste, sondern auch durchaus positive Meldungen verbuchen konnte. So konnte die österreichische Teilnehmergruppe, bestehend aus Schülern und Studenten, 2014 und 2015 etwa die *European Cyber Security Challenge* gewinnen. [19]
Solch internationale Wettbewerbe stellen mitunter sehr geeignete Maßnahmen dar, das Berufsfeld Cybersecurity zu attraktivieren sowie High Potentials direkt mit zukünftigen Arbeitgebern zu vernetzen.

4.2.4 GER - Cyber-Sicherheitsstrategie für Deutschland 2016

Die aktuell gültige deutsche IT-Sicherheitsstrategie wurde im November 2016 von der Bundesregierung beschlossen und war davor vom Bundesminister des Innern vorgelegt worden. Sie soll den 'ressortübergreifenden strategischen Rahmen für die Aktivitäten der Bundesregierung mit Bezügen zur Cyber-Sicherheit' [25] bilden und setzt so die Vorgängerstrategie aus dem Jahr 2011 fort. Zentraler Leitgedanke ist die Sicherung der Handlungsfähigkeit und Souveränität Deutschlands im Digitalisierungs-Zeitalter. [25]

4.2.4.1 Einleitung

Die Strategie beginnt mit der Feststellung der Veränderungskraft der Digitalisierung auf Staat, Wirtschaft und Gesellschaft. Der Staat - und damit die Bundesregierung - gibt sich die Aufgabe, Veränderungsprozesse im Interesse der Bürger zusammen mit weiteren Akteuren, wie zum Beispiel der Wirtschaft, zu bewerten, zu gestalten und geeignete Rahmenbedingungen zu schaffen.
Es werden sowohl Chancen als auch Risiken durch die Digitalisierung erwähnt und Vertrauen als zu erreichendes Ziel definiert. Eine absolute Sicherheit schließt die Strategie von vorne aus.
Als wesentliche betroffene Gruppen werden die Bürger benannt, die oftmals die von ihnen verwendeten Technologien nicht nachvollziehen können bzw. die Unternehmen, die auch in Zukunft ihr Know-how schützen und Produk-

tionsprozesse beherrschen müssen, selbst wenn selbstlernende Maschinen oder Cloud-Technologien eingesetzt werden. [26, S. 4]

4.2.4.2 Einschätzung Cyber-Bedrohungslage

Generell wird von der deutschen NCSS ein steigendes Bedrohungsbild sowohl in Menge, als auch in Qualität der Cyberangriffe auf Staat, Wirtschaft und Gesellschaft Deutschlands attestiert. Die Auswirkungen bleiben dabei nicht im Cyberraum, sondern können Bereiche wie Funktionsfähigkeit von Verwaltung, Streitkräften, Sicherheitsbehörden, kritischer Infrastruktur, Finanzmärkte und etliche weitere umfassen.
Die Bedrohung geht dabei in der Annahme dieser Strategie von kriminellen und terroristischen, aber auch von militärisch-nachrichtendienstlichen - also fremdstaatlichen - Gruppierungen aus. Durch die Austragung politischer Konflikte im Cyberspace erschwert sich die politische Bewertung von Cyberattacken und verhältnismäßiger Gegenmaßnahmen.
Ebenso wird erwähnt, dass viele Angriffe unzureichend abgesicherte IT-Systeme trifft. Angriffswerkzeuge sind vergleichsweise einfach erreichbar und somit ergeben sich neue Bedürfnisse für Abwehrprogramme. Cyberattacken sind zudem oft nur mit hohem Aufwand und bedeutender Zeitverzögerung festzustellen. [26, S. 7]

4.2.4.3 Leitlinien Cyber-Sicherheitsstrategie

Eine zentrale Leitlinie der NCSS Deutschlands ist, wie bereits eingangs erwähnt, die Sicherung der Handlungsfähigkeit und Souveränität im Zeitalter der Digitalisierung. Die Sicherheitspolitik für den Cyberspace soll die Chancen der Digitalisierung ausschöpfen, indem ihre Risiken beherrscht werden.
Allgemein wird die Aufgabe formuliert, im Cyberspace durch Schutz vor Gefährdungen Freiheit für Wirtschaft und Gesellschaft bieten zu können - dafür sind neue Lösungsansätze zu erforschen und in politische Lösungen einzuarbeiten.
Wie in anderen NCSS wird ein subsidiäres Verantwortungsbild gezeichnet, innerhalb dessen die Verantwortung zuallererst im Bereich des Betreibers bzw. Anwenders liegt. Eine Beachtung von Basisregeln kann eine große Zahl von Cyber-Attacken mit verhältnismäßig geringem Aufwand abwehren.
Eine Zusammenarbeit in Sachen Cybersicherheit ist zwischen Staat, Wirtschaft, Wissenschaft und Gesellschaft nötig, die auch gemeinsam Verantwortung tragen. Internationale bzw. europäische Kooperationen werden als unverzichtbar bezeichnet, da Bedrohungen im Cyberspace ebenso selten auf Staatsgrenzen Rücksicht nehmen und internationale Interdependenzen bestehen. [26, S. 8f]
Aus diesen Leitlinien werden vier Handlungsfelder gebildet, welche die Schwer-

punkte deutscher Cybersicherheitspolitik darstellen sollen: [26, S. 9]

- Handlungsfeld 1: Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung.
- Handlungsfeld 2: Gemeinsamer Auftrag Cyber-Sicherheit von Staat und Wirtschaft.
- Handlungsfeld 3: Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur.
- Handlungsfeld 4: Aktive Positionierung Deutschlands in der europäischen und internationalen Cyber-Sicherheitspolitik.

4.2.4.4 Handlungsfelder Cyber-Sicherheitsstrategie

Handlungsfeld 1: Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung [26, S. 13-19]

Unter HF1 werden Maßnahmen zum selbstbestimmten Handeln im Cyberraum subsummiert, die im Kontext digitaler Autonomie und somit digitaler Bildung über sämtliche Altersgruppen hinweg stehen. Nutzerfreundliche Lösungen mit hoher Usability werden angesprochen, die idealerweise 'Made in Germany' sein sollten. [26, S. 13]

Digitale Kompetenz bei allen Anwendern fördern [26, S. 14]
Die Schaffung von digitaler Kompetenz durch digitale Bildung stellt einen wesentlichen Bestandteil des HF1 dar. Die Vermittlung solcher Kompetenzen soll als fester Bestandteil in Bereich Schule, duale Ausbildung, Hochschule und weiterer Erwachsenenbildung Platz finden.
Während für den schulischen und universitären Bereich die Länder als zuständig genannt werden, will der Bund die duale Ausbildung an die Gegebenheiten anpassen. Die Notwendigkeit einer verstärkten Kooperation Bund-Länder wird betont.
Außerdem sollen Lehrstühle und Kompetenzzentren im MINT-Bereich, v.a. im Bereich Informatik, ausgebaut werden. Kooperationen mit der Wirtschaft sollen über Drittmittel bzw. Stiftungsfinanzierung einen Teil der Kosten beitragen.

Digitaler Sorglosigkeit entgegenwirken [26, S. 14]
Die vielzitierte Schafftung von *Awareness* steht im Zentrum dieses Unterpunktes im HF1. Zielgruppengerechte Sensibilisierung soll durch Kooperation mit Initiativen vorangetrieben werden. Als besonders verantwortliche Behörde für öffentliche Maßnahmen und Warnungen wird das BSI genannt.
Wesentliche Vermittler von Awareness sollen betriebliche IT-Sicherheitsbeauftragte - gleichwertig den Datenschutzbeauftragten in deren Bereich - darstellen.

Voraussetzungen für sichere elektronische Kommunikation und sichere Webangebote schaffen [26, S. 15]
Die Notwendigkeit des Einsatzes einer sicheren Verschlüsselung für Webangebote wird in diesem Unterpunkt gefordert. Vertrauliche elektronische Kommunikation ist laut der deutschen NCSS Basis für 'Wahrnehmung der Kommunikationsrechte, des Rechts auf Privatsphäre und der Persönlichkeitsrechte der Bürgerinnen und Bürger' [26, S. 15].
Fördern will die Bundesregierung dies durch Abbau von Hemmnissen beim Einsatz von Lösungen zur Verschlüsselung. Daneben sollen deutsche Sicherheitsbehörden im Einzelfall rechtlich befugt und technisch in der Lage sein, verschlüsselte Kommunikation zu dechiffrieren.

Sichere elektronische Identitäten[26, S. 16]
Zur Herausforderung der sicheren elektronischen Kommunikation sollen parallel Konzepte für eine sichere Identifikation erweitert werden, um im Internet eine entsprechende Authentifizierung zu ermöglichen. Aktuell werden von der Bundesregierung bereits Dokumente mit Online-Ausweisfunktion bereitgestellt, diese Möglichkeiten sollen weiterentwickelt werden und die derzeitig wohl gängigste Form der Identifikation - Benutzer/Passwort - zu ersetzen. [26, S. 16]
Auch die Vorsitzende des ULD, Marit Hansen, verwies im Gespräch auf die Möglichkeiten des deutschen Personalausweises und der *attribute based credentials*. Hier ermöglichen technische Innovationen Datenminimierung, beispielsweise bei Alterskontrollen, allerdings müsse laut Hansen der Bekanntheitsgrad innerhalb der Bevölkerung noch massiv erhöht werden. [34]

Zertifizierung und Zulassung stärken - Einführung Gütesiegel IT-Sicherheit [26, S. 17]
Analog zu bereits existierenden Zertifizierungen von IT-Sicherheitsprodukten soll ein Zertifizierungsverfahren für sichere IT-Verbraucherprodukte eingeführt werden, wofür das BSI entsprechende Richtlinien bzw. Kriterien ausarbeitet.
Ziel ist - trotz Herausforderungen wie beispielsweise kurzer Technologiezyklen - ein einheitliches Gütesiegel zur Unterstützung bei Kaufentscheidungen zu schaffen, sowohl bei IT-Produkten, als auch bei IT-Dienstleistungen. [26, S. 17]
Der Referatsleiter für Zertifizierungen im ULD, Henry Krasemann, verwies im Gespräch auf die Nützlichkeit von öffentlich wirksamen Siegeln und Zertifizierungen á la Stiftung Warentest für Produkte für den Privatkunden, merkte allerdings zusätzlich an, dass Werbung hierfür relativ schnell verpuffen könne. Wichtiger sei das Thema grundsätzlich, etwa in Schulklassen, zu vermitteln und die Bevölkerung zu sensibilisieren. Viel könne etwa in einem 30 Sekunden dauernden Werbespot gar nicht dargestellt werden. [23]

Digitalisierung sicher gestalten [26, S. 18]
Die Digitalisierung umfasst quasi alle Bereiche des Lebens und ist aus der Arbeits-, aber auch Freizeitwelt kaum mehr wegzudenken. Um den Herausforderungen in Hinblick auf die IT-Sicherheit rechtzeitig zu begegnen, sollen

einerseits entsprechende Produkthaftungsregeln und Sicherheitsvorgaben für Hersteller und Anbieter von Hard- und Software geschaffen werden - darunter fällt auch die Berücksichtigung von Security-Aspekten am Beginn der Produktentwicklung, sogenanntes *Security by Design*.
Andererseits sollen bei der Gesetzes- und Verordnungserstellung bereits die Auswirkungen digitaler Entwicklungen, besonders in Sachen IT-Security, berücksichtigt werden.

IT-Sicherheitsforschung vorantreiben [26, S. 18]
Herausforderungen an die IT-Sicherheit bedürfen laut deutscher NCSS ganzheitliche Ansätze und Lösungen. Die Bedeutung der IT-Security-Forschung nimmt dementsprechend zu. In diesem Bereich hat die deutsche Bundesregierung das Rahmenprogramm *Selbstbestimmt und sicher in der digitalen Welt 2015-2020* [26, S. 18] initiiert und plant, dieses weiter auszubauen.
Weiter intensiviert werden auch Investitionen in die existierenden IT-Sicherheits-Forschungskompetenzzentren *CRISP* in Darmstadt, *CISPA* in Saarbrücken und *KASTEL* in Karlsruhe. Den militärischen Part übernimmt dabei der Cyber-Cluster der Universität der Bundeswehr München.
Diese Technologien sollen kommerziell genutzt werden um einen möglichst hohen volkswirtschaftlichen Nutzen zu erzielen.

Handlungsfeld 2: Gemeinsamer Auftrag Staat - Wirtschaft [26, S. 20-25]

Im Rahmen des HF2 werden gemeinsame Auftragsfelder und Schnittstellen von Regierung, Behörden und staatlichen Stellen mit Unternehmen bzw. Betrieben definiert und behandelt. Besonderes Augenmerk erhalten dabei die Betreiber kritischer Infrastrukturen. [26, S. 20f]

Kritische Infrastrukturen sichern [26, S. 22]
Der Schutz von kritischen Infrastrukturen wird prominent als zentraler Aktivitätspunkt der Zusammenarbeit zwischen Staat und Wirtschaft positioniert. Vertrauensvoller Austausch von Informationen im Rahmen der privat-öffentlichen Partnerschaft *UP KRITIS* auf sämtlichen Ebenen und die Schaffung von Mindeststandards und Meldewegen werden betont.

Unternehmen in Deutschland schützen [26, S. 22]
Unterstützungsangebote für Unternehmen fallen in diesen Unterpunkt des HF2. Gerade Unternehmen aus dem Bereich der mittelständischen Betriebe sollen sich wirksam gegenüber Bedrohungen aus dem Cyberspace schützen, damit diese im Gegenzug ihr volles Geschäftspotential nutzen können. Vertrauensbildende Maßnahmen zwischen Behörden und Unternehmen sind dafür essentiell.
Im Bereich dieser Zusammenarbeit existieren bereits einige Initiativen, welche

weiter ausgebaut werden sollen, darunter zum Beispiel das 'German Competence Center against Cyber Crime' G4C, die 'IT-Sicherheit in der Wirtschaft' oder die 'Initiative Wirtschaftsschutz'. [26, S. 18]

Die deutsche IT-Wirtschaft stärken [26, S. 23]
Die Cyber-Sicherheit Deutschlands soll zusammen mit einer innovativen IT-Wirtschaft wachsen, diesbezüglich sollen Schlüsseltechnologien identifiziert und die Wettbewerbsfähigkeit der Unternehmen gestärkt werden.
'IT Security Made in Germany' [26, S. 23] soll als Markenzeichen gefördert und eigene Kapazitäten sollen, wo es möglich und sinnvoll ist, gestärkt werden.

Mit den Providern zusammenarbeiten [26, S. 24]
Als Schlüsselfeld des HF2 wird die staatliche Zusammenarbeit mit Providern zur Erkennung von Gefahren aus dem Cyberspace angeführt. Die Erkennung von Anomalien soll die Sicherheit im Netz erhöhen.

IT-Sicherheitsdienstleister einbeziehen [26, S. 25]
Im Zentrum dieses Punktes der Strategie steht der Austausch von Fachwissen zwischen Staat und Wirtschaft, da gerade in diesem Bereich ein Mangel an Fachkräften herrscht. Im Planungsstatus befinden sich dafür personelle Austauschprogramme der Bundesregierung mit Unternehmen, wobei natürlich die Wahrung von staatlichen auf der einen bzw. betrieblichen Geheimnissen auf der anderen Seite sichergestellt werden muss.

Plattform für vertrauensvollen Informationsaustausch schaffen [26, S. 25]
Zusammenarbeit zwischen staatlichen Stellen und Unternehmen bedarf, wie mehrfach erwähnt, regen Informationsaustausch, wofür eine Kooperationsplattform, auch zum Austausch von Lageinformationen, geschaffen werden soll.

Handlungsfeld 3: Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur [26, S. 26-37]
Eine effiziente, zeitgemäße Cyber-Sicherheitsarchitektur steht im Zentrum des HF3. Dazu zählt eine subsidiäre Rollenverteilung und Zusammenarbeit zwischen den Akteuren auf Bundes-, Länder- und Kommunalebene sowie anderen Akteuren, wie den Unternehmen. Cybersicherheit wird als gesamtstaatliche Aufgabe verstanden, die entsprechende Verantwortlichkeiten und Notwendigkeit von enger Kooperation kennt. [26, S. 27]

Das Nationale Cyber-Abwehrzentrum weiterentwickeln [26, S. 28]
Bereits 2011 wurde das Nationale Cyber-Abwehrzentrum - Cyber-AZ - gegründet. Es dient vornehmlich dem Informationsaustausch zwischen Behörden des Bundes und soll weiter ausgebaut werden, weiters sollen dazu eigene Auswertungskompetenzen, u.a. zur Erstellung eines Cyber-Lagebildes, entstehen.

Im Angriffsfall soll das Cyber-AZ als Krisenreaktionszentrum dienen, da eine Abwehr gezielter Cyberangriffe koordinierte Zusammenarbeit bedarf. In diesen Prozess sollen die Länder ihre Fähigkeiten einbringen.

Die Fähigkeit zur Analyse und Reaktion vor Ort stärken [26, S. 29]
Rasche, über übliche Maßnahmen hinausgehende Unterstützung vor Ort durch staatliche Stellen, ist laut der deutschen Strategie nach Angriffen in der Vergangenheit nur selten erfolgt. Dies soll sich durch die Implementierung von *Mobile Incident Response Teams*, (*MIRTs*) des BSI ändern. Diese sollen zeitnah Behörden oder Betreiber wichtiger Einrichtungen, wie kritischer Infrastrukturen, unterstützen können. Damit soll rasche und effiziente Business Continuity gewährleistet werden.
Darüber hinaus soll das Bundeskriminalamt für Sicherheitsermittlungen eine Einheit aufstellen (Quick Reaction Force - *QRF*), die rasch unaufschiebbare Maßnahmen für Strafverfolgungsbehörden umsetzen kann.
Im militärischen Bereich übernimmt die Aufgabe der Abwehr und Unterstützung vor Ort der militärische Nachrichtendienst MAD. Auch der Bundesnachrichtendienst BND soll im Rahmen seiner legalen Möglichkeiten Cyber-Angriffe in Vorbereitungs- und Durchführungsphase beobachten.

Strafverfolgung im Cyber-Raum intensivieren [26, S. 30]
Behörden aus dem Bereich von Justiz und Strafverfolgung sollen weitere technische und fachliche Fähigkeiten vermittelt bekommen, um die Strafverfolgung im Cyberraum zu intensivieren. Dazu zählen u.a. die Bereiche der Personalgewinnung und des Aufbaus von effizienten Analysesystemen. Neue Technologien dürfen laut deutscher NCSS zu keiner Fähigkeitslücke führen, sondern müssen von den Sicherheitsbehörden immer mitberücksichtigt und gegebenenfalls in das Portfolio der Kompetenzen einbezogen werden.

Cyber-Spionage und Cyber-Sabotage effektiv bekämpfen [26, S. 31]
Deutschland wird laut Strategie den 'Weg des verstärkten 360-Grad-Blickes' [26, S. 31] in Sachen Spionageabwehr fortsetzen. Darunter versteht die Regierung die grundsätzliche Beobachtung aller fremden nachrichtendienstlichen Aktivitäten in Deutschland. Cyberangriffe als Beschaffung von Informationen durch diverse fremde Organisationen oder staatliche Stellen sollen unter anderem so abgewehrt werden. Ein weiterer, besonderer Schwerpunkt gilt der Bekämpfung von Cyber-Attacken mit extremistischem bzw. terroristischem Hintergrund.

Ein Frühwarnsystem gegen Cyber-Angriffe aus dem Ausland implementieren [26, S. 32]
Unter Federführung des BND soll ein Frühwarnsystem zur Bedrohungserkennung und Einleitung von Abwehrmaßnahmen eingerichtet werden. Die Bewertung der Attacken soll außerdem der besseren Erstellung eines Lagebildes dienen.

Gründung der Zentralen Stelle für Informationstechnik im Sicherheitsbereich - ZITiS [26, S. 32]
Zur Effizienzsteigerung der Cybersicherheitskompetenz im nationalen Sicherheitsbereich und zur Schaffung wichtiger Synergieeffekte soll die zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) geschaffen werden. Diese soll Behörden in den drei Bereichen Entwicklung, Unterstützung und Beratung zur Seite stehen, selbst aber keine operativen Kompetenzen erhalten.

Verteidigungsaspekte der Cyber-Sicherheit stärken [26, S. 33]
Die Cyberverteidigung Deutschlands ist als Teil der gesamtstaatlichen Verteidigung Aufgabengebiet der Bundeswehr. Hier existieren aber natürlich auch Überschneidungen mit der Cyber-Sicherheitsarchitektur.
Die Strategie gibt vor, Cyber-Verteidigung und Cyber-Abwehr in sämtliche Planungen und Strukturen zu integrieren. Die Bundeswehr soll zusätzlich ihre Fähigkeiten ausbauen und organisatorisch die bisher eher zersplitterten Strukturen in einer Abteilung des Verteidigungsministeriums sowie in einem militärischen Organisationsbereich zusammenführen.

CERT-Strukturen in Deutschland stärken [26, S. 34]
Als Unterpunkt des HF3 findet sich in der deutschen Strategie ebenso ein Bekenntnis zur Stärkung der deutschen CERT-Strukturen. Zentrale Koordinierungs- und Ansprechstelle für Deutschland ist das BSI mit dem verknüpften CERT-Bund. Dieses bietet Dienstleistungen für Betreiber kritischer Infrastrukturen und andere Unternehmen an, es existieren aber auch auf anderer Behördenebene oder in wissenschaftlichen bzw. akademischen Einrichtungen wiederum eigene CERTs. Mit diesen soll der Grad der Vernetzung gesteigert werden.

Die Bundesverwaltung sichern [26, S. 35]
Die Bundesverwaltung und ihre Stellen müssen sich aufgrund der zunehmenden Digitalisierung, Vernetzung und Interdependenzen besonders auf neue Sicherheitserfordernisse in der IT einstellen. Der *Umsetzungsplan Bund* gibt dabei verbindliche Richtlinien für sämtliche Bundesbehörden mit technischen und organisatorischen Aspekten vor.
Weiter existiert das Gesamtprojekt *IT-Konsolidierung Bund*, im Rahmen dessen die Zusammenführung der IT-Betriebe der unmittelbaren Bundesverwaltung erfolgen soll. Das Projekt *Netze des Bundes* soll außerdem eine einheitliche und sichere Netzinfrastruktur schaffen. Auch die mobile Kommunikation steht im Fokus der Sicherheitsbestrebungen, hier sind vor allem Maßnahmen im Sensibilisierungsbereich der Mitarbeiter und im Beschaffungsprozess von IT-Produkten geplant.

Zusammenarbeit Bund-Länder [26, S. 36]
Mit einem stark ausgeprägten Föderalismus in Politik und Verwaltung kommt der Zusammenarbeit zwischen Bund und Ländern in Deutschland auch in den IT-Security Agenden erhöhte Beachtung bei. Das BSI als Bundesbehörde soll zusätzlich zu vorhandenen Strukturen den Landesbehörden Unterstützung leisten

können, bis dato war dies nur als Unterstützung von Polizei- und Strafverfolgungsbehörden der Fall.
Der Herausforderung der oftmals unterschiedlichen Standards und Richtlinien will Deutschland mit der 'Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung' [26, S. 36] beikommen, die einen Maßstab für alle Bundes- und Länderverwaltungsbehörden darstellt. Der bisher freiwillige Datenaustausch zwischen Bundesländern und der Bundesebene soll verpflichtend verankert werden.
Auch die kleinsten öffentlichen Verwaltungsstrukturen, die Kommunen, sollen über die Länder vom Know-how der Bundesbehörden profitieren. Das BSI soll daraus wiederum ein kommunales Lagebild entwickeln.

Ressourcen einsetzen, Personal gewinnen und entwickeln [26, S. 37]
Die deutsche NCSS sieht im Bereich der Cyber-Sicherheit massive Investitionen nötig, um auf den drei Verwaltungsebenen Bund, Länder und Kommunen einen entsprechenden Grad von IT-Sicherheit zu implementieren. Der Personalgewinnung bzw. -entwicklung soll eine entscheidende Rolle zukommen, der öffentliche Dienst soll sich als Arbeitgeber offensiver bewerben und mit Ausbildungseinrichtungen kooperieren.
In Zusammenarbeit von Wissenschaft, Wirtschaft und Staat sollen sogenannte 'Cyber-Cluster' entstehen. Besonders hervorgehoben wird die Bedeutung des Studiengangs 'Cyber-Sicherheit' an der Universität der Bundeswehr München.
Die Cyber-Reserve der Bundeswehr soll auch für Personen, die bisher keinen Wehrdienst geleistet haben, geöffnet werden.

Handlungsfeld 4: Aktive deutsche Positionierung europäischer und internationaler Cyber-Sicherheitspolitik [26, S. 38-43]
Das HF4 soll die Priorität von internationaler Zusammenarbeit in sicherheitspolitischen IT-Agenden abbilden. Hier wird eine aktive Rolle Deutschlands, etwa im Rahmen der Mitgliedschaft in der Europäischen Union, der NATO und der Vereinten Nationen gefordert. [26, S. 38f]

Eine wirksame europäische Cyber-Sicherheitspolitik aktiv gestalten [26, S. 40]
Im Rahmen von Maßnahmen für eine europäische IT-Sicherheitspolitik wird vor allem auch 'eine auf Datensicherheit beruhende europäische Daten-Standortpolitik' [26, S. 40] proklamiert, weiters auch die 'Berücksichtigung von Datenschutz bei europäischen Regeln für den internationalen Datenaustausch' [26, S. 40].
Innerhalb dieses Unterpunktes findet sich somit ein angedeutetes Bekenntnis zur europäischen Standortpositionierung über den Faktor IT-Sicherheit und auch Datenschutz.
Auch eine vermehrte Berücksichtigung von Cyber-Sicherheit im Rahmen der gemeinsamen Außen- und Sicherheitspolitik sowie die grenzüberschreitende An-

wendung elektronischer Identifizierung und Kennzeichnung, etwa bei Unternehmens- und Behördensiegeln, sollen Eckpfeiler deutschen Handels darstellen.

Die Cyber-Verteidigungspolitik der NATO weiterentwickeln [26, S. 40]
Ebenso kurz angeführt wird der Zuwachs der Bedeutung von cyber-verteidigungspolitischen Maßnahmen im Rahmen der NATO. In den Rahmen der Adaptierung an veränderte Bedrohungslagen will sich Deutschland gestaltend einbringen.

Cyber-Sicherheit international aktiv mitgestalten [26, S. 41]
Ebenso soll Deutschland im Rahmen seiner Möglichkeiten innerhalb der Vereinten Nationen und der OSZE Prozesse zur Erschwerung von Wirtschaftsspionage über den Cyberspace sowie Cyber-Angriffe durch Schaffung bzw. Durchsetzung internationaler Regelungen über deutsche und europäische Grenzen hinweg anstoßen.
Weiters ist laut Strategie von der Bundesregierung die Schaffung eines deutschen Instituts für internationale Cyber-Sicherheit geplant, welches der Regierung als Berater zur Seite stehen wird.

Bilaterale/regionale Unterstützung & Kooperation zum Auf- und Ausbau von Cyberfähigkeiten (Cyber Capacity Building) [26, S. 42]
Mit ausgewählten Partnerstaaten und -regionen will Deutschland im Rahmen von Unterstützungskooperationen den Aufbau der Netzrobustheit und Netzresilienz unterstützen. Deutschland soll so seine Vertrauenswürdigkeit international einsetzten, um das 'Cyber Capacity Building' [26, S. 42] zu stärken. Davon umfasst sind Maßnahmen wie die Entwicklung eigener Cybersecurity-Strategien, Zertifizierungen, die Intensivierung von Forschungstätigkeiten oder etwa Maßnahmen der Aus- und Weiterbildung im Bereich der Cybersecurity.

Internationale Strafverfolgung stärken [26, S. 43]
Der deutsche Einsatz auf internationalem Parkett soll auch der Bekämpfung der Cyber-Kriminalität dienen. Konkrete Maßnahmen in diesem Bereich sind beispielsweise die Optimierung internationaler rechtlicher Rahmenbedingungen, die Implementierung handlungsfähiger grenzüberschreitender Strafverfolgung durch einfache und rasche Rechtshilfeersuchen oder der Beitritt möglichst vieler Staaten zur Budapester Konvention - dem Übereinkommen des Europarates über Computerkriminalität.

4.2.4.5 Conclusio GER

Die 2016 beschlossene deutsche NCSS setzt die Stoßrichtung der vorherigen Version aus dem Jahr 2011 fort und verfolgt den Leitgedanken der Sicherung der Handlungsfähigkeit und Souveränität Deutschlands im Cyberspace. Auch in dieser Strategie werden die Veränderungspotentiale der Digitalisierung und ihre Auswirkungen auf Staat, Wirtschaft und Gesellschaft betont. Gleich zu Beginn wird die Priorität von Maßnahmen betont, die der digitalen Sorglosigkeit

entgegentreten und digitale Kompetenz als festen Bestandteil in Schulen, der dualen Ausbildung, auf Hochschulen und innerhalb der Erwachsenenbildung verankern.
Als starke Industrienation verwundert es nicht, dass ein zentraler Fokus Deutschlands auf dem Schutz der Unternehmen gegenüber Cyberkriminalität, wie beispielsweise Wirtschaftsspionage, liegt. Auch der Schutz kritischer Infrastrukturen wird ausführlich behandelt. Eine eigene Quick Reaction Force (*QRF*) des Bundesamts für Sicherheitsermittlungen und Mobile Incident Responce Teams (*MIRTs*) des Bundesamts für Sicherheit in der Informationstechnik sollen die rasche Analyse und Reaktion vor Ort des Geschehens einer Bedrohung aus dem Cyberspace ermöglichen.
Im Gegensatz etwa zur britischen NCSS spielt eine multilaterale Einbindung der Cyberverteidigungspolitik innerhalb der EU eine größere Rolle. Zur österreichischen Strategie hin stellt die deutsche Einbindung in die Strukturen der NATO naturgemäß einen Unterschied dar. Ohnehin ist die internationale Kooperation ein wesentlicher Eckpfeiler der NCSS Deutschlands, mit bilateraler Unterstützung will Deutschland seine Vertrauenswürdigkeit und seinen guten Ruf international dafür einsetzen, ausgewählte Partnerstaaten und -regionen bei einem *Cyber Capacity Building* zu unterstützen.
Auch die ENISA leitet aus der deutschen NCSS (allerdings aus der Vorgängerversion) Ziele wie die Förderung der Sicherheit der Digitalwirtschaft und Industrie ab. Stakeholder innerhalb Deutschlands NCSS sind neben staatlichen Stellen und der Regierung eine eigene Task Force IT Security in der Industrie. Ebenso führt die EU-Behörde den hohen Stellenwert der internationalen Kooperation und den Wunsch nach Standards und Normen im Bereich Cybersecurity an. [33]

4.2.5 UK - National Cyber Security Strategy 2016-2021

Das Vereinigte Königreich gilt gemeinhin als weltweites Vorbild in Sachen IT-Security. Im November 2016 veröffentlichte die Regierung eine NCSS für den Zeitraum 2016-2021, an der mehrere Behörden und Ministerien federführend beteiligt waren. [8]
Bereits die Kurzbeschreibung auf der Regierungswebseite weist darauf hin, dass der Anspruch darin begründet liegt, Großbritannien zu einem der sichersten Orte weltweit zu machen, um Wirtschaft im Cyberspace zu betreiben. [8]
Philip Hammond, als britischer Schatzkanzler einer der politisch Hauptverantwortlichen für die NCSS, schreibt in seinem Vorwort: 'Government has a clear leadership role, but we will also foster a wider commercial ecosystem, recognising where industry can innovate faster than us. This includes a drive to get the best young minds into cyber security.' [7, S. 6]
Er betont also, dass der Führungsauftrag im Kontext der IT-Sicherheit zwar klar bei der Regierung liegt, aber ebenso die Industrie und die Wirtschaft eine wichtige Rolle als Partner und Innovator spielen. Alleine auch der Umstand, dass der britische Schatzkanzler als Finanz- und Wirtschaftsminister maßgeblich an dieser Strategie beteiligt ist, zeigt, dass das Vereinigte Königreich den Faktor

Cybersecurity klar als wirtschaftlichen Standortvorteil betrachtet.

4.2.5.1 Bedrohungs- und Risikoanalyse

Die NCSS 2016-2021 erwähnt, dass bereits im Rahmen der letzten Cybersicherheitsstrategie aus dem Jahr 2011 die Bedeutung des technologischen Wandels erkannt wurde, diese nun noch rascher zugenommen hat und weiterhin zunimmt. Internetbasierte Technologien ermöglichen ganz neue ökonomische und soziale Entwicklungen, bieten aber sozusagen als Kehrseite der Medaille auch eine große Angriffsfläche. [7, S. 17]
Im Rahmen der Bedrohungsanalyse soll auf solche Entwicklungen eingegangen werden, wobei betont wird, dass Bedrohungen für den britischen Cyberspace von unterschiedlichsten Gruppierungen ausgehen. [7, S. 17]

Cyberkriminalität [7, S. 17f]
Prinzipiell unterscheidet die NCSS 2016-2021 des Vereinigten Königreichs zwischen zwei miteinander verwobenen Formen der Cyberkriminalität.
Sogenannte **'cyber-dependent crimes'** [7, S. 17] stellen Straftaten dar, die ausschließlich durch Informations- und Kommunikationstechnologie durchgeführt werden können. Dies bedeutet, das IKT-Geräte sowohl Werkzeug als auch Ziel der kriminellen Tätigkeit darstellen. Unter dem Begriff **'cyber-enabled crimes'** [7, S. 17] werden hingegen 'traditionelle' kriminelle Akte subsumiert, welche durch IKT eine größere Intensität oder Reichweite erlangen können.
Die NCSS ortet einen Großteil dieser kriminellen Aktivitäten Großbritannien gegenüber bei russischsprachigen kriminellen Vereinigungen aus Osteuropa (*OCGs*), eine steigende Tendenz ist aber aus den Regionen südliches Asien, Westafrika und innerhalb des Vereinigten Königreichs selbst bemerkbar. Die dafür verantwortlichen Personen sind oft sehr schwer juristisch zur Rechenschaft zu ziehen, da sie eben oftmals in Ländern beheimatet sind, mit denen nur rudimentäre oder gar keine Auslieferungs- bzw. Rechtshilfeabkommen existieren.
Die Verantwortlichkeit für die Entwicklung und Verbreitung von Malware wird bei den *OCGs* gesehen, zwar verteilt sich der Schaden auf gesamt Großbritannien und ist daher auf den ersten Blick nicht eindeutig erkennbar, die kumulierten Effekte seien aber signifikant. Die Heftigkeit und Aggressivität dieser Attacken nehme zu, besonders benannt werden *Distributed Denial of Service* (*ddos*) Angriffe, die oft erpresserischen Vorhaben dienen.

Fremdstaatliche und fremdstaatlich unterstütze Angriffe [7, S. 18]

Angriffe von fremden Staaten bzw. durch diese fremden Staaten unterstützte Angriffe bedrohen die Cybersicherheit von Großbritannien, besonders in den Bereichen Politik, Diplomatie und Wirtschaft.

Insbesondere stehen die Regierung, der Verteidigungsbereich, der Finanzsektor, Energie- und Telekommunikationsbranche im Fokus.
Innerhalb der NCSS wird betont, dass nur eine Handvoll Fremdstaaten im Moment die technischen Kapazitäten besitzen, das Vereinigte Königreich ernsthaft direkt mit einem Cyberangriff zu gefährden. Nichtsdestotrotz sind einige andere staatliche Programme in Entwicklung, die Interessen von Großbritannien in naher Zukunft gefährden könnten, besonders Cyberspionage wird hierbei angeführt.
Über die Spionage hinaus haben laut der Strategie einige wenige Parteien Möglichkeiten für offensive Kapazitäten, also Möglichkeiten zur Cyberkriegsführung, geschaffen. Diese könnten vor allem in dem Glauben benutzt werden, dass deren Einsatz zu relativ geringen Konsequenzen führen würde und somit andere ermutigen, dementsprechend nachzuziehen. Solche Attacken bezeichnet der Strategiebericht als selten, aber ansteigend und attestiert ihnen eine große Schockwirkung.

Terroristisch motivierte Cyberkriminalität [7, S. 19]
Terroristische Gruppierungen sind und bleiben laut NCSS 2016-2021 ebenso auch über den Cyberspace potentielle Angreifer auf Großbritannien und seine Interessen. Ihr technisches Know-how wird dabei als relativ gering eingeschätzt, dennoch war in der Vergangenheit der Schaden dieser Aktivitäten unverhältnismäßig hoch. Diese Terroristen sind nämlich in der Lage, relativ leicht mediale Aufmerksamkeit und eine Atmosphäre der Furcht zu generieren.
Für die Zukunft wird ein Beibehalten der terroristischen Präferenz auf physische und nicht auf Cyber-Ziele erwartet. Dennoch steigt die Gefahr terroristisch motivierter Cyberangriffe alleine schon durch das Heranwachsen einer Generation, die in IKT ungleich bessere Kenntnisse als die vorhergehende besitzt. Wenn sich Angehörige dieser Generation radikalisieren, steigt laut der NCSS auch die Gefahr, ebenso die einer Attacke eines sogenannten 'einsamen Wolfes' oder eines Insiders, der mit terroristischen Gruppierungen zusammenarbeitet. Grundsätzlich ist jedenfalls zwischen terroristischer Cyberkriminalität und der Verbreitung 'physischer' terroristischer Propaganda über das Internet zu differenzieren.

Hacktivists [7, S. 19]
Als sogenannte *Hacktivisten* werden dezentral orientierte Gruppen bezeichnet, die an einer (meist ideologischen) Frage orientiert sind. Die Opfer ihrer Angriffe wählen sie aufgrund von ihnen so wahrgenommenen Missständen aus, wobei sie meist störende Attacken, wie z.B. DDOS durchführen. Einzelgruppierungen konnten ihren Zielen in der Vergangenheit dadurch bereits wesentliche, gravierende Schäden zufügen.

Script Kiddies [7, S. 20]
Script Kiddies - also Individuen mit eher geringen Fachkenntnissen, die Cyberattacken mit von anderen Personen geschriebenen Programmen durchführen - werden vom strategischen Bericht nicht als wesentliche Bedrohung der Wirtschaft

oder Gesellschaft gesehen. Nichtsdestotrotz können sie durch den Zugang zu Tools und Ressourcen Organisationen bzw. Unternehmen über das Internet im Verhältnis zum Aufwand des Angriffs überdurchschnittlich hohen Schaden zufügen.

4.2.5.2 Schwachstellenanalyse

Bevor eine Gegenstrategie zu Cyberkriminalität und -attacken entworfen werden kann, muss ebenso ein Bild über Schwachstellen im System dokumentiert werden, welches erlaubt, schwerwiegende Angriffsflächen zu identifizieren und entsprechende Gegenmaßnahmen abzustimmen.

Steigende Anzahl der Endgeräte - Internet of Things [7, S. 22]
Während zur Zeit der Erstellung der letzten britischen NCSS im Jahr 2011 die meisten Personen Cybersecurity in Hinblick von Endgeräten wie Laptops oder PCs betrachteten, ist das Internet heutzutage wesentlich stärker in unseren Alltag integriert.
Im gleichen Maße, wie das *Internet of Things* neue Möglichkeiten realisiert, kann es auch dazu missbraucht werden, Angriffe auf nun wesentlich einfacher zu erreichende Ziele über den Cyberspace durchzuführen. Solche Attacken können dramatische Auswirkungen, bis hin zu schweren Verletzungen und den Tod von Menschen, nach sich führen.
Ebenso steigt mit dem technischen Fortschritt und der Integrierung des *Industrial Internet of Things* das Risiko von Angriffen auf Industrie- und gewerbliche Ziele. Auch hier sind Geräte bzw. Prozesse relativ einfach angreifbar, die in der Vergangenheit von außen nur sehr schwierig zugänglich waren.

Geringe Cyberhygiene und Compliance [7, S. 22]
Gerade in Großbritannien - das zweifelsfrei hier eine Vorbildrolle einnimmt - ist die Awareness über die Existenz und die Gefährlichkeit von Cyberattacken in den letzten Jahren bedeutend gestiegen - nicht zuletzt trugen diverse Regierungsprogramme höchstwahrscheinlich ihren Teil dazu bei.
Ein wesentlicher, von der NCSS an dieser Stelle genannter Punkt ist, dass der Erfolg zahlreicher Cyberangriffe weniger an dem ausgeklügelten Angriff, als an der Verletzlichkeit des Angegriffenen liegt. Hier müssen Unternehmen und Organisationen sich ihrer Verantwortung bewusst werden, die sie für ihre Systeme und die eigenen bzw. ihnen anvertrauten Daten tragen. Eine dem wirtschaftlichen und organisatorischen Aufwand entsprechende Vorbereitung von Schutzmaßnahmen ist zur Erreichung dieser *Cyberhygiene* unabdingbar.

Ungenügendes Training und mangelhafte Fähigkeiten [7, S. 22f]
In diesem Abschnitt wird vom strategischen Bericht auf ein Fehlen von Wissen und Fähigkeiten im Bereich der Cybersecurity sowohl im privaten, als auch im öffentlichen Sektor hingewiesen. Auf die hohe Priorität der Entwicklung von

Specialist skills, die mit dem technologischen Fortschritt mithalten können, wird hingewiesen. Die *skill gap* wird gar als Verletzbarkeit nationalen Ausmaßes bezeichnet.

Legacy Systems und Benutzung alter Softwareversionen [7, S. 23]
Die Benutzung nicht aktualisierter bzw. veralteter Systeme ist eine bedeutende Sicherheitslücke, die zahlreiche Organisationen, Unternehmen und Privatpersonen betrifft. Alte Versionen von Software, die nicht aktualisiert werden bzw. für die eventuell gar keine Aktualisierung (mehr) existiert, bieten potentiellen Angreifern oft einfache Ziele.
Die NCSS zitiert an dieser Stelle den jährlichen Cisco Report aus dem Jahr 2016, für den 115.000 mit dem Internet verbundene Cisco-Endgeräte überprüft wurden, von denen 106.000 bekannte Schwachstellen innerhalb der auf ihnen laufenden Software besaßen.

Einfache Verfügbarkeit von Hacking-Ressourcen [7, S. 23]
Durch die Möglichkeit, über das Internet vergleichsweise einfach an Hacking-Tools und Anleitungen zu deren Nutzung zu gelangen, können Personen mit dementsprechenden Vorhaben Cyberangriffe einfacher realisieren.

4.2.5.3 Conclusio Bedrohungs-, Risiko- und Schwachstellenanalyse [7, S. 23]

Insgesamt schätzt der strategische Bericht ein, dass Großbritannien durch die in der Vergangenheit eingeführten Strategien und Institutionen einen gewissen Schutzfaktor gegen Cyberangriffe etabliert hat. Dennoch folgt die Warnung, dass das Vereinigte Königreich den Bedrohungen aus diesem Bereich keinesfalls einen Schritt voraus ist, sondern sich stetig wachsenden Gefahren gegenüber sieht.
Die Angriffskapazitäten der potentiell gefährlichen Gegner, also einiger ausgewählter Staaten und kriminellen Organisationen, ist laut Einschätzung der NCSS gestiegen. Die gemeinsame Herausforderung der Sicherstellung von Gegenmaßnahmen, die flexibel und effizient auf Bedrohungen reagieren und ebenso die Ursachen von Schwachstellen bekämpfen können, wird betont.

4.2.5.4 Die britische Cybersecurity-Strategie

Als Reaktion auf die oben benannten Bedrohungen und Schwachstellen definiert der NCSS-Bericht einen strategischen Ansatz für die Jahre 2016-2021. Als Vision für das Jahr 2021 beschreibt die Strategie dabei, dass Großbritannien sicher und unnachgiebig gegenüber Bedrohungen über den Cyberspace ist und außerdem einen wirtschaftlich erfolgreichen und selbstbewussten Zugang zur digitalen Welt besitzt. [7, S. 25]
Um diese Vision realisieren zu können, werden folgende zu erreichende Ziele

abgeleitet, auf die im späteren Verlauf noch genauer eingegangen wird: [7, S. 25]

- **DEFEND** - Verteidigen:
  Das Vereinigte Königreich und seine Netzwerke, Daten und IT-Systeme sollen gegen die stetig zunehmenden Bedrohungen von Cyberangriffen effizient verteidigt werden. Betont wird dabei, dass Bürger, Unternehmen und der öffentliche Sektor das Wissen und die Kompetenzen besitzen sollen, sich selbst zu verteidigen.

- **DETER** - Abschrecken:
  Großbritannien soll ein schwierig zu knackendes Ziel für Cyberangriffe darstellen. Angriffe gegen seine Systeme, Daten und IT-Infrastrukturen sollen entdeckt, verstanden und untersucht werden, um schließlich feindliche Aktivitäten aufzudecken und zu zerstören. Offensive Gegenschläge im Cyberspace werden als klare Handlungsmöglichkeit benannt.

- **DEVELOP** - Entwickeln:
  Die Bedeutung der innovativen und wachsenden Cybersecurity Industrie Großbritanniens und des damit verbundenen akademischen Bereiches wird als Ziel für 2021 betont. Die Entwicklung von Fähigkeiten und Ausbildung von Fachkräften im Bereich der IT-Security soll die Bedürfnisse im privaten und öffentliche Bereich zufrieden stellen und die State-of-the-Art Expertise Großbritanniens soll das gesamte Land dazu befähigen, mit den zukünftigen Gefahren und Herausforderungen gut umzugehen.

Die Bedeutung internationaler Kooperationen zur Erreichung dieser Ziele wird von der Strategie betont, ebenso wird aus diesem Grund eine große Anzahl an Prinzipien definiert. Wesentlicher Eckpfeiler dieser Prinzipien ist die Doktrin, dass alle Aktionen und Strategien Großbritanniens dazu dienen müssen, sowohl die Sicherheit, als auch den Wohlstand des Landes zu sichern. Ein Cyberangriff auf das Vereinigte Königreich wird von den Behörden mit einer konventionellen Attacke gleichgesetzt und soll mit allen als notwendig erachteten Mitteln abgewehrt werden. [7, S. 25]
Dabei definiert die NCSS, dass alle Handlungen nationalem und internationalem Recht entsprechen werden und dass die britischen Werte wie Demokratie, Freiheit, Menschenrechte und Meinungsfreiheit dabei hochgehalten werden. Besonders wird auch der Schutz der Daten britischer Bürger betont. [7, S. 25]
Wie an zahlreichen Stellen zuvor wird dabei die Zusammenarbeit von Regierungsbehörden mit Unternehmen und anderen Institutionen hervorgehoben. [7, S. 26]
Die NCSS unterscheidet weiters zwischen verschiedenen Rollen und Verantwortlichkeiten im Bereich der IT-Sicherheit.
Individuen, also Bürger, Angestellte und Konsumenten, sollen ihrer persönlichen Verantwortlichkeit nachkommen, alle zumutbaren Schritte zur Erhöhung der

IT-Sicherheit in ihrem Bereich durchzuführen. Hierbei soll die Aufmerksamkeit nicht nur der Hardware wie Smartphones und anderen Endgeräten, sondern auch den individuellen Daten und Systemen dienen. [7, S. 26]
Unternehmen und Organisationen aus dem privaten und öffentlichen Sektor verwalten Daten und stellen Dienstleistungen, Services und Systeme in der digitalen Welt zur Verfügung. Aus dieser Rolle ergibt sich die Verantwortung, mit den anvertrauten Daten sorgfältig umzugehen, ihre Systeme gegen Angriffe zu verteidigen und ihre Funktionsfähigkeit schnellstmöglich wiederherzustellen. [7, S. 26]
Die **Regierung** des Vereinigten Königreichs sieht laut der NCSS als ihre primäre Aufgabe, das Land vor den Angriffen anderer Staaten zu verteidigen, die Bürger und die Wirtschaft vor Schaden zu bewahren und die nationalen und internationalen Rahmenbedingungen zu schaffen, um britische Interessen durchzusetzen. Als Verantwortungsträger für zahlreiche kritische Daten und als Informationsgeber den Bürgern gegenüber ergeben sich weitere, wesentliche Pflichten. Auch wenn zahlreiche Schlüsselsektoren der Wirtschaft in privaten Händen liegen, muss laut der Strategie die Regierung als letztverantwortliche Instanz für deren Widerstand gegenüber Cyberangriffen in Zusammenhang mit nationalen Interessen dienen. [7, S. 26f]
Betont werden auch die sich verändernden Rollen des Marktes und der Regierungsbehörden im Vergleich zur NCSS aus dem Jahr 2011. In der damaligen Strategie wurde die Rolle des Marktes Entscheidungen zu fällen und die Richtung vorzugeben stärker betont. In der Zwischenzeit führt die NCSS aus, dass zwar bereits viel erreicht wurde, vor allem in Sachen Schaffung von Awareness und Verständnis für die nötigen Gegenmaßnahmen, allerdings wird die Kombination aus Marktkräften und Förderung durch die Regierung als nicht effektiv angesehen, die langfristigen Interessen Großbritanniens im Cyberspace sicherzustellen, da der Markt laut NCSS-Interpretation der Cybersecurity einen zu geringen Stellenwert geben würde. [7, S. 27]
Deswegen wird in der NCSS 2016-2021 der Regierung in diesem Bereich eine größere Rolle zuteil, etwa im Bereich von Investitionen in innovative Unternehmen im Bereich Cybersecurity oder Erhöhung von Standards im Datenschutz. [7, S. 27]
Ebenso wurde mit dem *National Cyber Security Centre* (NCSC), das seine Tätigkeit am 1. Oktober 2016 aufnahm, eine einzelne zentrale Anlaufstelle für Cybersecurity auf nationaler Ebene geschaffen. Für alle diese Maßnahmen hat Großbritannien im Zuge des Strategic Defence and Security Review 2015 1,9 Milliarden Pfund für die fünf Jahre der NCSS budgetiert. [7, S. 28f]
Um die Ziele der britischen NCSS 2016-2021 zu erreichen, wird die Implementierung in drei verschiedene Hauptzielbereiche unterteilt. In der Kategorie **DEFEND** sollen alle Verteidigungsmaßnahmen für den Cyberspace zusammengefasst werden, der Bereich **DETER** dient der Abschreckung der Gegner und mit **DEVELOP** sollen die Kapazitäten Großbritanniens im Bereich IT-Security ausgedehnt werden. [7, S. 31]

4.2.5.5 DEFEND - Verteidigung

Die Elemente aus dem DEFEND-Zielbereich sollen die Netzwerke, Daten und Systeme Großbritanniens aus dem öffentlichen, privaten und wirtschaftlichen Bereich schützen und widerstandsfähig gegenüber Cyberattacken machen. [7, S. 33]
Die Regierung will Maßnahmen setzen, um sicherzustellen, dass Bürger, Unternehmen, Organisationen aus dem öffentlichen und privaten Sektor sowie weitere Institutionen Zugang zu den richtigen Informationen haben, um sich selbst entsprechend gegen Cyberangriffe zu verteidigen. Als Kompetenz- und Beratungszentrum soll hierfür das bereits erwähnte *National Cyber Security Centre* dienen, mit Hilfe dessen maßgeschneiderte Lösungen bzw. Unterstützungen für IT-Security und die Verteidigung des Cyberspaces gewährleistet werden sollen. Die Zusammenarbeit zwischen Regierung, Industrie und internationalen Partnern soll einen hohen Stellenwert besitzen. [7, S. 33]

Active Cyber Defence - ACD

ACD bezeichnet jenen Teilbereich der DEFEND-Ziele, mit dem Sicherheitsmaßnahmen zur Stärkung von Netzwerken und Systemen gegenüber einer Cyberattacke implementiert werden. Als *Netzwerk* wird dabei im Rahmen dieser NCSS der gesamte Cyberspace Großbritanniens bezeichnet. [7, S. 33]
Dabei soll das Vereinigte Königreich zu einem nur schwierig zu attackierenden Ziel für staatlich unterstützte Angreifer werden, indem die Widerstandsfähigkeit der Netzwerke im Land erhöht wird. Die große Mehrheit von Malware-Angriffen mit niedrigem Niveau soll durch Blockade der Kommunikation zwischen Hackern und deren Opfern abgewehrt werden. Außerdem sollen die Fähigkeiten, fremdstaatlich gestützte und kriminelle Attacken größeren Ausmaßes zu zerstören und gegebenenfalls ebenso offensive Maßnahmen einzuleiten, ausgebaut werden. Eine große Rolle soll auch die Sicherung der nationalen kritischen Infrastruktur gegenüber Cyber-Bedrohungen spielen. [7, S. 33f]
Um diese Zielen sicherzustellen, will die Regierung im Rahmen der NCSS ihre Zusammenarbeit mit der Industrie und speziell mit Communication Service Providers (CSPs), also Kommunikationsdienstleistern, verstärken um die Auswirkungen bzw. Schäden von Attacken auf die Kommunikationsinfrastruktur zu minimieren. Eine konkrete Maßnahme ist beispielsweise die Beschränkung des Zugangs zu Webseiten, welche bekannte Quellen von Malware darstellen (sog. *DNS blocking*). Die Prävention von *Phishing*, konkret von *Spoofing*, also dem Fall einer vorgetäuschten Herkunftsquelle eines E-Mails, etwa einer Bank, soll durch Implementierung eines E-Mail Verifizierungssystems für Regierungsbehörden sichergestellt werden, welches auch der Industrie als Anreiz dienen soll. [7, S. 34f]
Im Rahmen von Partnerschaften mit der Industrie will die NCSS die Sicherheit des gesamte *Software Ökosystems* des Landes erhöhen, etwa indem ein höherer Fokus an den Einbau von IT-Securitymaßnahmen in die Supply Chain eines Unternehmens gelegt wird. [7, S. 34]

Building a more secure internet

Die Bedeutung des *Internet of Things* für den Themenkomplex Cybersecurity wurde schon mehrfach angesprochen, die NCSS erklärt es in diesem Zusammenhang als Ziel, dass Online-Produkte *secure by default* sind, also bereits standardmäßig integrierte Securitymechanismen in Soft- und Hardwarekomponenten besitzen. Dies steht natürlich im Spannungsfeld der Interessen mehrerer Seiten, so sollen am Ende des Prozesses leistbare, aber eben von Beginn an sichere Produkte angeboten werden - stets unter der Berücksichtigung der offenen Art und Natur des Internet. [7, S. 35]

Einige Beispiele des Approaches in diesem Bereich sind etwa die Entwicklung von *Secure Internet Services* durch die Regierung, die sich so nicht darauf verlassen müsse, dass das Internet andernfürsich sicher sei. Weiters sollen Sicherheitsmechanismen bei verkauften Produkten standardmäßig aktiviert sein und müssen erst aktiv vom User deaktiviert werden, nicht umgekehrt. Außerdem soll in Technologien wie *Trusted Platform Services* (*TPM*) und Industriestandards wie *Fast Identity Online* (*FIDO*) investiert werden, welche nicht Passwörter, sondern Geräte und andere innovative Authentifizierungsmaßnahmen für User verwenden. [7, S. 36f]

Protecting Government

Die Regierung und ihre Behörden halten große Mengen an sensiblen Daten, betreiben wichtige Netzwerke und sind wesentliche Dienstleister für die gesamte Nation. Darum besitzt die Modernisierung öffentlicher Services hohen Stellenwert auch innerhalb der NCSS - das erklärte Ziel der Regierung ist es, Großbritannien zur *World Leading Digital Nation* zu machen. Als häufiges Ziel von Cyberangriffen müssen die Regierungsbehörden die jeweils verhältnismäßigen Cybersecurity-Level implementieren, auch, um das Vertrauen der Bevölkerung in die digitalen Dienstleistungen zu halten. [7, S. 37]

Maßnahmen zur Erreichung dieses Ziels sind laut der NCSS die Beseitigung von Risiken aus Legacy-Systemen, die Erstellung eines genauen Abbildes aller relevanten Systeme und Zugangsrollen und Implementierung von 'Best-practice'-Vorgaben des NCSC und ebenso die entsprechende Schulung der Mitarbeiter der Behörden bzw. des öffentlichen Dienstes, da Cyber-Security neben der technischen eine ebenso wichtige menschliche Komponente besitzt. Zwei besonders hervorgehobene prioritäre Bereiche dafür sind der Gesundheitssektor und die Streitkräfte. [7, S. 38f]

Protecting Critical National Infrastructure and other priority Sectors

Eine intakte IT-Sicherheit bedeutender Unternehmen und Organisationen in Großbritannien ist von hoher Priorität für den reibungslosen Ablauf des täglichen Lebens und der wirtschaftlichen Funktionen des Landes. Angriffe auf Infrastruktur dieser ausgewählten Gruppe und deren *Critical National Infrastructure* (*CNI*)

würden große Schäden für die Stabilität der britischen Wirtschaft, die internationale Reputation Großbritanniens oder sogar das Leben seiner Bevölkerung bedeuten. Deswegen setzt die NCSS eine hohe Priorität auf den Schutz dieser CNI, zu der etwa die erfolgreichsten britischen Unternehmen, Verwalter von sensiblen Daten wie z.B. manche NGOs, wichtige Medien oder auch Digital Service Provider zählen. [7, S. 39f]
Zwar will die Regierung nicht die Kontroll- und Verantwortungskompetenzen bei privaten Unternehmen und Organisationen zwangsweise übernehmen, diese aber in Sachen IT-Security durch gezielte Informationen, die Entwicklung von Richtlinien und die Durchführung von Krisenübungen unterstützen. [7, S. 40-42x]

Changing public and business behaviours
Einige Unternehmen und Organisationen haben in Großbritannien eine Vorreiterrolle in Sachen IT-Security inne, doch der NCSS-Bericht kommt ebenso zum Schluss, dass die große Masse an Firmen bzw. Organisationen keine adäquate Einschätzung bzw. Umsetzung von IT-Sicherheitsmaßnahmen besitzt, respektive betreibt. [7, S. 42]
Deswegen setzt sich die Regierung die Bestärkung von Individuen und Organisationen zur Beschäftigung mit dem Thema zum Ziel. Dies soll für die breite Öffentlichkeit etwa durch entsprechend populärer Verbreitung einfacher und klarer Handlungsanweisungen sichergestellt werden, für Unternehmen will man die klaren betriebswirtschaftlichen Vorteile von IT-Security und die Kosten von potentiellen Schäden aufzeigen. [7, S. 42f]
Ein Beispiel einer solchen Marketing-Maßnahme stellt die Kampagne *Cyber Aware* dar. [7, S. 43]

Managing Incidents and understanding the Threat
Im Falle eines Angriffes bzw. Vorfalles im Bereich Cybersecurity muss die Zusammenarbeit und der Informationsfluss zwischen Regierung, Unternehmen und Öffentlichkeit klar definiert und laut der NCSS einheitlicher und simpler gestaltet werden. Die Wichtigkeit der Zusammenarbeit mit dem privaten Sektor im Krisenfall wird betont, ebenso die Kooperation mit anderen Computer Emergency Response Teams (CERTs). [7, S. 44]
Zur Zielerreichung soll ein einzelner *Incident Management Approach* mit klar definierten Prozessabläufen und -verantwortlichkeiten entwickelt werden. [7, S. 35]

4.2.5.6 DETER - Abschreckung
Der zentrale Grundsatz des DETER-Zielelements der NCSS ist es, die politischen, diplomatischen, ökonomischen und/oder strategischen Kosten eines Cyberangriffes massiv zu erhöhen, um präventiv eine Vielzahl an potentiellen Tätern

abzuschrecken. Abschreckung im Cyberspace dient den gleichen Zielen und beinhaltet dieselben Prinzipien wie physische Abschreckungspolitik und soll auch mit dieser zusammenwirken. [7, S. 47]
Ein wesentlicher Punkt der Abschreckung liegt im Bereich der **Cyberkriminalität**. Hier muss laut NCSS als Teil der Abschreckungspolitik den potentiellen Tätern klar gemacht werden, dass eine Straftat im Cyberspace - gleichsam einer 'analogen' Straftat - polizeilich mit aller Härte verfolgt wird. Dafür sollen die Behörden auch die Funktionsweisen und Abläufe von Cybercrime-Modellen verstehen, um aus Großbritannien ein *High-Cost, High-Risk* Land für Cyberkriminalität zu machen. [7, S. 47f]
Einen weiteren Eckpfeiler der Abschreckung bilden Gegenmaßnahmen zu fremdstaatlichen bzw. fremdstaatlich unterstützen Cyberangriffen. Entscheidende Maßnahmen der NCSS sind dafür verstärkte internationale Kooperation und die Stärkung von Cybersecurity-Legistik auf völkerrechtlicher Ebene. [7, S. 49f]
Die Abschreckung **terroristischer Cyberattacken** ist ein weiterer zentraler Eckpunkt von DETER. Hierfür soll die - momentan noch überschaubare - Bedrohung durch terroristisch motivierte Gegner auf IT-Security Ebene identifiziert und zerstört werden, v.a. auch durch starke internationale Kooperation. [7, S. 50]
Ebenso will Großbritannien erweiterte Kapazitäten in den Bereichen der **offensiven Möglichkeiten im Cyberspace** und von **Verschlüsselungstechnologien** erlangen.
Erstere sollen Möglichkeiten eröffnen, in feindliche Netzwerke und Systeme vorzudringen, um dort Schaden anzurichten. Diese Möglichkeiten bilden einen Aspekt des Offensivsystems ab, zu dem auch physische Kapazitäten zur Abhaltung von gegnerischen Angriffen zählen. Hierfür existiert bereits das *National Offensive Cyber Programme* (NOCP), dessen Kapazitäten ausgeweitet werden sollen. [7, S. 51f]

4.2.5.7 DEVELOP - Entwicklung

Das DEVELOP-Element beschreibt, wie Großbritannien im Zuge seiner NCSS Werkzeuge und Fähigkeiten zur IT-Security erwerben und ausbauen will.
Ein zentraler Punkt hierfür ist die **Stärkung von Cybersecurity-Skills**, die die Regierung durch gezielte Förderung von Ausbildungsprogrammen heben will, um daraus eine blühende Cybersecurity Start-up Szene zu entwickeln. So soll der Mangel an Experten und Nachwuchskräften in diesem Bereich bekämpft werden. Diese Aufgabe kann laut britischer NCSS nur der private Sektor - also Unternehmen - bewältigen, aber der Staat kann Ausbildung und Innovation fördern. Dies bedarf freilich eines viel längeren Zielsetzungshorizontes, weniger von fünf, als mehr von zwanzig Jahren. [7, S. 55f]
Die **Förderung von Wachstum in der Cybersecuritybranche** stellt einen weiteren Handlungsschwerpunkt der NCSS dar. Großbritannien wird als innovativer und führender Standort für Cybersecurity-Technologien und -Produkte

beschrieben, der seinen Platz aber auch in Zukunft weiter behaupten muss. Ebenso müssen Finanzierungslücken von KMUs aus dem Bereich IT-Security überwunden werden, viele am Markt eingeführte Technologien finden außerdem nur schwierig *Early Adopters*. Diese Herausforderungen will die NCSS mit einer gezielten Zusammenarbeit der Regierung mit wissenschaftlichen Institutionen und der Industrie lösen. Einige Maßnahmen zur Erreichung sind etwa die Schaffung zweier Innovationszentren, die Zurverfügungstellung von Testanlagen für Unternehmen oder Förderungen von 165 Mio. Pfund aus dem *Defence and Cyber Innovation Fund*. [7, S. 57-59]
Außerdem soll die **Förderung von Cybersecurity-Forschung** die wichtige akademische Basis für Fortschritt in der IT-Sicherheit bilden. Für diese Zielerreichung sollen Zusammenarbeit und innovative Finanzierungsmodelle für Forschung gefördert bzw. die Forschung und ihre Ergebnisse vermarktet werden. [7, S. 59]
Die Stärkung der Cybersecurity-Forschung soll auch der Etablierung der bereits erwähnten *Secure by Default*-Produkten dienen, die standardmäßig aktivierte Sicherheitseinstellungen auf hohem Niveau haben, welche User erst bewusst deaktivieren müssen (*opt-out*-Modell). [7, S. 59]
Schlussendlich muss durch sogenanntes **Effective Horizon Scanning** die sich stets im Wandel befindliche Cyber-, geopolitische sowie technologische Landschaft im Auge behalten werden. Marktveränderungen, die auf britische Cybersecurity-Kompetenzen großflächige Auswirkungen haben könnten, sollen durch engmaschiges Monitoring fünf bis zehn Jahre im Voraus vorhergesagt werden können. [7, S. 60f]

4.2.5.8 Conclusio UK

Die britische Cybersecurity-Strategie verfolgt eine klare Zielsetzung. Die Vision Großbritanniens lautet, dem Land einen wirtschaftlich erfolgreichen und selbstbewussten Zugang zur digitalen Welt zu geben. 2021 soll das Vereinigte Königreich sicher und belastbar gegenüber Bedrohungen aus dem Cyberraum und zeitgleich dort wirtschaftlich erfolgreich agieren können bzw. die Rahmenbedingungen für Unternehmen dazu bieten.
Die drei Eckpfeiler der britischen NCSS sind mit DEFEND, DETER und DEVELOP gesetzt und zeigen den ganzheitlichen Zugang der Verantwortlichen zum Thema Cybersecurity. DEFEND, also Verteidigung, bedeutet, dass Behörden, Unternehmen und Bürger sich Wissen und Fähigkeiten aneignen, um sich selbst im Cyberspace zu verteidigen.
DETER bedeutet Abschreckung und soll Großbritannien als nur schwer anzugreifendes Ziel im Cyberspace gestalten. Bedrohungen sollen erkannt, verstanden und gegebenenfalls auch durch offensive Kapazitäten zerstört werden.
Der dritte Schwerpunkt, DEVELOP, betont die Notwendigkeit einer innovativen Cybersecurity-Wirtschaft verknüpft mit wissenschaftlicher Kompetenz in diesem Themenbereich. Ziel der Strategie ist das Schaffen eines Cyber-Ökosystems, in dem Start-ups mit entsprechend Kapital und Unterstützung ausgestattet werden, um innovative Sicherheitslösungen schaffen zu können. Diese inno-

vativen Konzepte sollen zwischen den Behörden, den Unternehmen und dem wissenschaftlichen Bereich ausgetauscht werden.
Im Zuge der Evaluierung der vorherigen NCSS aus dem Jahr 2011 wurde ebenso die veränderte Rolle des Marktes betont, der zwar viel erreicht hätte, aber die Priorität von Cybersecurity noch als zu gering einschätzen würde, weswegen hier eine stärkere staatliche Zielsetzung erfolgen müsse.
Die Zielsetzungen der aktuellen und der vergangenen britischen NCSS sind sehr klar marktwirtschaftlich orientiert. Im NCSS-Vergleich der ENISA aus dem Jahr 2014 werden die britischen Cybersecurity-Ziele aufgezählt, hier wird das Erreichen einer internationalen Führungsrolle betont, weiters müsse das Vereinigte Königreich ein sicherer Ort werden, um Geschäfte im Cyberspace abzuwickeln. [33, S. 12]
Zusammenfassend kann der Zugang Großbritanniens zum Thema Cybersecurity als innovativ und sehr fortschrittlich bezeichnet werden. Einer - durchaus selbstkritischen - Evaluierung der vorherigen Strategie aus dem Jahr 2011 folgen eine klar definierte Vision und konkrete Schwerpunkte mit entsprechenden Zuständigkeiten. Cybersecurity wird als Notwendigkeit und als klarer Wettbewerbsvorteil gesehen, um die Zukunft des Wirtschaftsstandorts Großbritannien erfolgreich zu gestalten.
Sicherheitslösungen für private Unternehmen, die einem gewissen Gefahrenpotential unterliegen, müssen *business driven* sein. [33, S. 12] Sie sollen also vom jeweiligen Betrieb selbst entwickelt bzw. beauftragt werden und so Lösungen erzielen, welche den Bedürfnissen der Praxis entsprechen.
Insgesamt ist für das Thema Cybersecurity subsidiär jeder Akteur auf seiner Ebene mitverantwortlich. Der Bürger im Rahmen seiner Privatnutzung von IT und Internet, die Unternehmen bzw. ebenso die einzelnen Behörden in Bezug auf Daten, Geschäftsgeheimnisse und kritische Infrastruktur und der Staat im Rahmen der Abwehr und gegebenenfalls der Zerstörung von Gefahren, die den britischen Cyberspace bedrohen.
Im Gegensatz etwa zur deutschen oder österreichischen NCSS besitzt die britische Strategie auch ein Kapitel *beyond 2021*, um die zukünftigen Bedrohungslagen und Chancen im Bereich Cybersecurity zumindest kurz zu umreißen. Durch *Effective Horizon Scanning* sollen sich neu ergebende Marktveränderungen mit Auswirkungen auf die britischen Kompetenzen in der Cybersecurity durch engmaschiges Monitoring zumindest fünf bis zehn Jahre im Vorhinein erkannt werden können.
Der gleichen Qualität wie Evaluierung und Planung der NCSS muss allerdings auch die Implementierung und Verwaltung entsprechen, zuletzt gab es gerade im Bereich der Streitkräfte einige kritische Nachrichten. So meldeten Medien, dass Systeme des neuen britische Flugzeugträgers *HMS Queen Elizabeth* noch mit Windows XP betrieben würden. Das Betriebssystem, das aufgrund der ausgelaufenen Supportphase nicht mehr mit kritischen Updates versorgt wird, ist Cyberangriffen im hohen Maße ausgeliefert. [4]

4.3 Richtlinie (EU) 2016/1148 - Die NIS-Richtline

Ebenfalls ab Mai 2018, also im gleichen Monat wie die Datenschutz-Grundverordnung, ist die Richtlinie (EU) 2016/1148, umgangssprachlich *NIS-Richtlinie* genannt, anzuwenden. [51]
Die 'Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union' [51, S. 1] verfolgt u.a. das Ziel, die Sicherheit und Verlässlichkeit von Netz- und Informationssysteme zu erhalten bzw. zu verbessern, damit diese ihre wichtige Rolle für Wirtschaft und Gesellschaft wahrnehmen können. [51, S. 1]
EU-weite, gemeinsame Mindestanforderungen in definierten Bereichen sollen für Betreiber *wesentlicher Dienste* und Anbieter *digitaler Dienste* geschaffen werden. [51, S. 2]

4.3.1 Gliederungsübersicht NIS-Richtlinie

Die NIS-Richtlinie wird in sieben Kapitel gegliedert, die wiederum jeweils mehrere Artikel umfassen: [51]

- Kapitel I: Allgemeine Bestimmungen - *Artikel 1 bis 6*
- Kapitel II: Nationale Rahmen für die Sicherheit von Netz- und Informationssystemen - *Artikel 7 bis 10*
- Kapitel III: Zusammenarbeit - *Artikel 11 bis 13*
- Kapitel IV: Sicherheit der Netz- und Informationssysteme der Betreiber wesentlicher Dienste - *Artikel 14 bis 15*
- Kapitel V: Sicherheit der Netz- und Informationssysteme der Anbieter digitaler Dienste - *Artikel 16 bis 18*
- Kapitel VI: Normung und freiwillige Meldung - *Artikel 19 bis 20*
- Kapitel VII: Schlussbestimmungen - *Artikel 21 bis 27*

4.3.2 Inhaltliche Zusammenfassung NIS-Richtlinie

4.3.2.1 Kapitel I: Allgemeine Bestimmungen

In den allgemeinen Bestimmungen zu Beginn der Richtlinie werden grundsätzliche Regelungen behandelt, etwa Gegenstand und Anwendungsbereich. Wie bereits erwähnt wurde, ist die Zielsetzung der Richtlinie ein 'hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen in der Union' [51, Art. 1 (1)]. Um dies zu erreichen, werden alle Mitgliedstaaten der Union verpflichtet, eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen zu erarbeiten. Außerdem soll eine Kooperationsgruppe zur Koordination der Zusammenarbeit und des Austauschs von Information geschaffen und ein Netzwerk von Computer-Notfallteams implementiert werden. Ziel dieses *CSIRTs*-Netzwerks ist die Schaffung einer Vertrauensbasis in diesem Bereich zwischen den Unionsstaaten und die Verstärkung von Kooperationsmöglichkeiten. [51, Art. 1 (2)]
In Artikel 3 wird die sogenannte *Mindestharmonisierung* geregelt, die besagt, dass die einzelnen Mitgliedstaaten strengere Bestimmungen bzw. höhere Sicherheitsniveauregelungen erlassen können, als bereits in der NIS-Richtlinie geregelt. [51, Art. 3]
In Artikel 4 sind zahlreiche Begriffsbestimmungen definiert, von denen zwei besonders bedeutende, weil auch für Kapitel IV und V wesentliche, Begriffe explizit erwähnt seien.
Betreiber wesentlicher Dienste sind Einrichtung öffentlicher oder privater Art, die einer im Anhang II der NIS-Richtlinie angeführten Aufzählung entsprechen. Dazu zählen etwa bestimmte Unternehmen aus dem Energiesektor, wie einige Verteilernetzbetreiber, Elektrizitätsunternehmen etc.; wesentliche Verkehrsunternehmen, zum Beispiel aus den Bereichen Luft-, Schienen- oder Straßenverkehr; oder auch gewisse Einrichtungen im Gesundheitswesen, der Trinkwasserversorgung, des Bank- und Finanzmarktes und der digitalen Infrastruktur. [51, Art. 4] [51, Anh. II]
Vereinfacht ausgedrückt handelt es sich bei den *Betreibern wesentlicher Dienste* also um wesentliche Betreibereinrichtungen aus dem Bereich der kritischen Infrastrukturen.
Anbieter digitaler Dienste sind juristische Personen, die ebensolche *digitale Dienste* anbieten. Diese Dienste werden in der EU-Richtlinie 2015/1535 als 'Dienstleistung der Informationsgesellschaft, d. h. jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung' [50, Art. 1] definiert. [51, Art. 4]
Die Mitgliedstaaten der Union sind im Rahmen des Artikels 5 verpflichtet, bis November 2018 die Betreiber der oben angeführten und im Anhang definierten wesentlichen Dienste in ihrem jeweiligen Hoheitsgebiet zu ermitteln. Die dadurch erstellte Liste muss ab diesem Zeitpunkt mindestens alle zwei Jahre aktualisiert werden. [51, Art. 5].

4.3.2.2 Kapitel II: Nationale Rahmen für die Sicherheit von Netz- und Informationssystemen

Mittels der NIS-Richtlinie werden alle Mitgliedstaaten der Union ebenso verpflichtet, eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen zu erarbeiten. Diese Strategie soll unterschiedliche Aspekte behandeln, wie beispielsweise Ziele und Prioritäten für die nationale Strategie, einen Steuerungsrahmen zur Erreichung ebenjener Ziele, aber auch etwa Forschungs- und Entwicklungspläne in Zusammenhang mit der Strategie anzugeben und einen Risikobewertungsplan auszuarbeiten. [51, Art. 7]
Bei der Erstellung der Strategie können die Mitgliedstaaten die ENISA um Unterstützung ansuchen. [51, Art. 7]
Ebenso, wie im Rahmen der DSGVO (mindestens) eine zuständige Datenschutzbehörde pro Unionsmitglied zu melden ist, muss im Rahmen der NIS-Richtlinie eine *zuständige Behörde* für den Bereich Netzwerk- und Informationssicherheit benannt werden, welche die Anwendung der Richtlinie auf nationaler Ebene überwacht. Auch eine *zentrale Anlaufstelle* muss damit beauftragt werden, die grenzüberschreitende Zusammenarbeit der Behörden, etwa im Bereich des *CSIRTs*-Netzwerks, zu gewährleisten. Diese Anlaufstelle kann gleichzeitig die ebenso zu benennende zuständige Behörde sein. [51, Art. 8]
Außerdem müssen von den Mitgliedstaaten Computer-Notfallteams (*CSIRTs*) definiert werden, deren Aufgaben und Pflichten im Anhang I der Richtlinie klargestellt sind. Die Zusammenarbeit der *CSIRTs* innerhalb des *CSIRTs-Netzwerks* der Union muss von den Mitgliedstaaten gewährleistet werden. [51, Art. 9] [51, Anh. I]

4.3.2.3 Kapitel III: Zusammenarbeit

Die Zusammenarbeit auf Unionsebene regelt das Kapitel III der NIS-Richtlinie. Die bereits in Kapitel I erwähnte Kooperationsgruppe wird in Artikel 11 definiert, als ihre Aufgabe wird die Unterstützung der strategischen Zusammenarbeit und des Informationsaustauschs zwischen den Mitgliedstaates der Union benannt. [51, Art. 11]
Das ebenso bereits erwähnte Netzwerk der *CSIRTs* wird in Artikel 12 behandelt und sein Aufbau aufgetragen. Die wesentlichen Aufgaben umfassen unter anderem den Informationsaustausch zwischen den *CSIRTs*, Unterstützung der einzelnen Mitglieder der Union bei grenzüberschreitenden Vorfällen, Bestimmung weiterer Formen der Zusammenarbeit auf operativer Ebene, sowie die Unterrichtung der in Artikel 11 definierten Kooperationsgruppe. [51, Art. 12]

4.3.2.4 Kapitel IV: Sicherheit der Netz- und Informationssysteme der Betreiber wesentlicher Dienste

Die *Betreiber wesentlicher Dienste*, also kurz gesprochen Einrichtungen, die besonders definierte kritische Infrastrukturen betreiben, haben spezielle Aufgaben inne, welche Artikel 14 definiert.
Die Mitgliedstaaten müssen dafür Sorge tragen, dass die Betreiber Maßnahmen zur Bewältigung von Risiken für die Netzwerk- und Informationssysteme tragen. Auch die Gewährleistung einer möglichst geringen Auswirkung von Sicherheitsvorfällen auf diese Systeme wird als Sicherstellungspflicht der Mitgliedstaaten den Betreibern gegenüber erwähnt. [51, Art. 12]
Die Richtlinie verpflichtet die benannten Betreiber von kritischen Infrastrukturen also mittelbar zur Sicherstellung von *Business Continuity*.
Ebenso ist eine Meldeverpflichtung von Sicherheitsvorfälle mit gravierenden Auswirkungen auf ihre angebotenen Dienst verankert, solche müssen der entsprechenden Behörde bzw. dem *CSIRT* gemeldet werden und eigene, in Artikel 14 angeführte, Parameter beinhalten. [51, Art. 14 (3) (4)]
Nach dem Eingang einer solchen Meldung müssen andere Mitgliedstaaten - sofern diese betroffen sind - durch die Behörde bzw. das *CSIRT* benachrichtigt werden. Ebenso ist in der Richtlinie verankert, dass, sofern zur Prävention bzw. Bewältigung notwendig, die Öffentlichkeit von der Behörde bzw. dem *CSIRT* unterrichtet werden kann. [51, Art. 14 (5) (6)]
Kapitel IV umfasst außerdem, dass jeweiligen Behörden von den Mitgliedstaaten die jeweiligen rechtlichen und organisatorischen Kapazitäten erhalten, um ihren Pflichten entsprechend nachkommen zu können. [51, Art. 15]
Im selben Artikel 15 findet sich ebenso eine nennenswerte Verbindung zum Themenkomplex Datenschutz bzw. den Datenschutzbehörden. Mit diesen müssen die für die Aufgaben der NIS-Richtlinien zuständigen Behörden nämlich eng zusammenarbeiten, falls der jeweilige Sicherheitsvorfall zur Verletzung des Schutzes personenbezogener Daten führt. [51, Art. 15 (4)]

4.3.2.5 Kapitel V: Sicherheit der Netz- und Informationssysteme der Anbieter digitaler Dienste

Nach den Betreibern spezieller kritischer Dienste werden in Kapitel V der NIS-Richtlinie Sicherheitsanfordernisse und Regelungen für allgemeine Anbieter digitaler Dienstleistungen benannt.
In diesem Kapitel wird die Pflicht der Mitgliedstaaten verankert, sicherzustellen, dass Anbieter jeglicher digitaler Dienste Maßnahmen organisatorischer und technischer Natur treffen, um den Risiken für Netz- und Informationssicherheit entgegenzutreten. Besonderer Wert wird dabei unter anderem auf *Sicherheit der Systeme und Anlagen*, *Bewältigung von Sicherheitsvorfällen* und dem bereits erwähnten *Business continuity management* gelegt. [51, Art. 16 (1)]
Anbieter digitaler Dienste werden verpflichtet, Sicherheitsvorfälle an die Behörde

bzw. das *CSIRT* zu melden, die 'erhebliche Auswirkungen auf die Bereitstellung eines der in Anhang III genannten [...] Dienste' haben [51, Art. 16 (3)]. [51, Art. 16)]
Als solche Dienste werden im genannten Anhang *Online-Marktplätze*, *Online-Suchmaschinen* und *Cloud-Computing-Dienste* definiert. [51, Anh. III]
Ebenso werden Parameter zur Einschätzung, ob Auswirkungen den erheblich seien, angeführt. Hier spielen etwa Dauer und geografische Ausbreitung des Vorfalls, sowie Auswirkungen auf die Bereiche Wirtschaft und Gesellschaft maßgebliche Rollen. [51, Art. 16 (4)]
Die Bestimmungen dieses Kapitels sind der Kommission nach nicht für Klein- und Kleinstunternehmen mit weniger als 50 Mitarbeitern gültig. [51, Art. 16 (11)]
Wie in Kapitel IV werden auch in Kapitel V Kapazitäten verankert, die der Mitgliedstaat seiner jeweiligen Behörde zur Ausübung ihrer Tätigkeit im Bereich der im Kapitel behandelten Anbieter zur Verfügung stellen muss. Falls Anbieter in mehreren Mitgliedstaaten tätig sind, sind die Behörden zur Kooperation verpflichtet. [51, Art. 17 (1) (2)]
Anbieter digitaler Dienste unterlegen der gerichtlichen Zuständigkeit jenes Unionsstaats, in dem sich ihre Hauptniederlassung befindet. Falls der Anbieter nicht im Gebiet der EU niedergelassen ist, aber Anhang III-Dienste, also *Online-Marktplätze*, *Online-Suchmaschinen* oder *Cloud-Computing-Dienste* zur Verfügung steht, ist, ähnlich wie in den Regelungen der DSGVO vorgesehen, einen Vertreter zu benennen. Dieser muss in einem Mitgliedstaat niedergelassen sein. [51, Anh. III] [51, Art. 18]

4.3.2.6 Kapitel VI: Normung und freiwillige Meldung

Kapitel VI regelt die Bereiche Normung und freiwillige Meldung. Normung bezieht sich darauf, dass die Mitgliedstaaten, um einheitliche Anwendungen konkreter Teile der NIS-Richtlinie zu gewährleisten, die Anwendung europäischer bzw. internationaler Sicherheitsnormen für Netz- bzw. Informationssysteme fördern. Es wird auf die ENISA Bezug genommen, die Leitlinien erlässt und Beratungsdienstleistungen für Mitgliedstaaten anbietet. [51, Art. 19]
Artikel 20 verankert die Möglichkeit der *freiwilligen Meldung*. Betreiber von Diensten, die nicht als wesentlich eingestuft wurden oder nicht digital sind, können freiwillig Vorfälle mit erheblichen Auswirkungen auf von ihnen angebotene Dienste melden. Diese werden von der zuständigen Behörde entsprechend Artikel 14 im Kapitel IV für Betreiber wesentlicher Dienste behandelt und die Behörde wird wie in Artikel 14 geregelt tätig, sofern die Bearbeitung keinen unverhältnismäßigen Aufwand bedeutet. [51, Art. 20]

4.3.2.7 Kapitel VII: Schlussbestimmungen

Innerhalb der Schlussbestimmungen sind etwa Sanktionen geregelt, die bei Verstößen gegen die NIS-Richtlinie verhängt werden. Diese müssen laut Richtlinie 'wirksam, angemessen und abschreckend' [51, Art. 21] sein und vonseiten der Mitgliedstaaten bis 9. Mai 2018 an die Kommission mitgeteilt werden. [51, Art. 21]
Weiters umfasst Kapitel VII Regelungen zum Ausschussverfahren, der Überprüfung, Übergangsmaßnahmen, die Umsetzung, das Inkrafttreten und die Adressaten. [51, Art. 22-27]
Die NIS-Richtlinie ist ab 10. Mai 2018 anzuwenden. [51, Art. 25]

4.3.3 Inhaltliche Analyse NIS-Richtlinie und nationale Umsetzung

Ebenso wie die Datenschutz-Grundverordnung ist die NIS-Richtlinie ab Mai 2018 von den Mitgliedstaaten anzuwenden. Die DSGVO gilt, wie bereits mehrfach im Rahmen dieser Arbeit erwähnt, grundsätzlich unmittelbar für die Mitgliedstaaten, allerdings sind über diverse Öffnungsklauseln und Regelungsspielräume nationale Regelungen möglich bzw. erforderlich, die in dieser Arbeit ausführlich behandelt werden.
Richtlinien hingegen, wie eben die NIS-Richtlinie, müssen durch nationale Gesetzgebung umgesetzt werden. Für Österreich ist dazu das *Bundesgesetz zur Cyber-Sicherheit* geplant, welches von mehreren Ministerien konzipiert wird. Begleitend unterstützt das *Kuratorium Sicheres Österreich* (KSÖ) hierbei mit seiner Expertise. [27]
Das CERT Österreich empfiehlt, im Zuge der Richtlinienumsetzung gut ablaufende Koordinierungsmechanismen zu schaffen, da durch die Regelungen zahlreiche Bereiche und Branchen berührt werden würden. Besonders wird auch auf die zu schaffende Vertrauensbasis für den Austausch zwischen den Mitgliedstaaten und den Notfallteams erwähnt. [1]
Bereits im Jänner 2017 berichtete der Standard über Verzögerungen hinsichtlich des Gesetzes. Der Artikel zitierte auch einen IT-Sicherheitsexperten, der eine steigende Nachfrage in der Cybersecurity-Branche prognostizierte und empfahl, 5-10 Prozent des gesamten IT-Budgets in den Bereich Cybersicherheit zu investieren. [11]
In Deutschland war bereits vor der NIS-Richtlinie ein IT-Sicherheitsgesetz verabschiedet worden, welches seit Juli 2015 Gültigkeit hat.

Die WKO begrüßte die Implementierung einer gemeinsamen, EU-weiten Richtlinie im Bereich Cybersecurity. Gerade durch die Abhängigkeit von Unternehmen und staatlichen Stellen vom Funktionieren digitaler Netze und Infrastrukturen und weil solche Netze oftmals nicht an nationalstaatlichen Grenzen Halt machen, könnten harmonisierte Regelungen zur Stabilität beitragen. Besonders betont wurde auch die Rolle der ENISA in der Umsetzungsphase. [38]

Das deutsche BSI begrüßte die NIS-Richtlinie ebenso ausdrücklich, da ein einheitlicher EU-Rechtsrahmen geschaffen werde. Das Bundesamt betonte, trotz einer Verbreiterung der Befugnisse für das BSI selbst, dass auch weiterhin die Herausforderungen im Bereich Cybersicherheit nur kooperativ von Wirtschaft und Staat gemeinsam gelöst werden könnten. BSI-Präsident Arno Schönebohm hob die Notwendigkeit eines hohen IT-Sicherheitsniveaus im Zusammenspiel von Staat, Wirtschaft und Gesellschaft für eine erfolgreiche Digitalisierung hervor. [59]

Der deutsche Jurist Thomas Feil, Fachanwalt für IT-Recht, führte außerdem an, dass aus Gründen des gemeinsamen Binnenmarktes eine Harmonisierung im Bereich Netz- und Informationssicherheit sinnvoll sei, auch weil von EU-Ebene aus die Robustheit dieser Netze als Garant für die Vollendung eines digitalen Binnenmarkts nützlich sein würde. [18]

5 Sicherheit und Datenschutz in der Cloud

Cloud Computing, also die Bereitstellung von Dienstleistungen wie IT-Services oder IT-Infrastruktur über das Internet, ist in den letzten Jahren von einem großen Trend zur angewandten Realität in heimischen Unternehmen und Behörden geworden. Die Gründe dafür, und damit die Vorteile von Cloud Computing, liegen auf der Hand: Rechenleistung, Speicherplatz oder beispielsweise ganze Anwendungen können *on demand* bestellt und eingesetzt werden. Dies ermöglicht den notwendigen Einsatz von IT-Lösungen flexibel an den betrieblichen Alltag anzupassen und somit ebenfalls Kosten zu sparen.
Dennoch bieten Cloudlösungen nicht ausschließlich Vorteile, sondern bergen auch eine Zahl an Risiken in sich. Gerade für den Bereich des Datenschutzes und der IT-Security können große Herausforderungen durch die Anwendung von Cloud Computing entstehen. So ist es oft auf den ersten Blick nicht ersichtlich, wo sich Daten, die auf Filesharing-Systemen wie z.B. Google Drive oder Dropbox abgelegt wurden, physisch tatsächlich befinden. Außerhalb des EU Raums unterliegen solche Anbieter oft kritisch zu bewertender Gesetzgebung, die keinesfalls europäischem Niveau entspricht. [28, S. 6]
Gerade in KMUs oder kleinen Behörden, die keine oder nur wenig Mitarbeiter mit Kenntnissen über die Materie beschäftigen können, herrscht oft nur wenig Bewusstsein über diese Problematik bzw. wird oft der vermeintliche 'Bequemlichkeitsfaktor' einer Nutzung solcher Clouddienste über Sicherheits- bzw. Datenschutzbedenken gestellt.
Und auch die sich möglicherweise ergebenden wirtschaftlichen und rechtlichen Konsequenzen werden oftmals verdrängt oder spielen bei den Entscheidungen der verantwortlichen Personen kaum eine Rolle.
Bevor auf zu setzende Rahmenbedingungen für eine sicherere europäische Cloud-Umgebung eingegangen wird, sollen kurz grundlegende Begrifflichkeiten und Charakteristika zu Cloud Computing erläutert werden.

5.1 Grundbegriffe Cloud Computing

Das US-amerikanische National Institute of Standards and Technology veröffentlichte 2011 eine Definition des Cloud Models, welches fünf Charakteristika, drei Servicemodelle und vier Einsatzmodelle umfasst. [35]

5.1.1 Charakteristika

- **On-demand self-service**:
  Der Kunde kann einseitig von sich aus und ohne menschliche Interaktion Computing-Ressourcen, zum Beispiel Serverleistungen oder Speicher, in Anspruch nehmen. [35, S. 2]

- **Broad network access**:
  Cloud-Dienstleistungen werden über einen Netzwerkzugang über standardisierte Zugangsmechanismen zur Verfügung gestellt und können auf

unterschiedlichen Endgeräten, wie Smartphones, Laptops oder PCs benutzt werden. [35, S. 2]

- **Ressource pooling**:
  Die Computing-Ressourcen des Providers werden in einem *Pool* zusammengefasst und dynamisch den unterschiedlichen Kunden zugewiesen. Aufgrund dieser Zuweisung ergibt sich eine Ortsunabhängigkeit der zugewiesenen Ressourcen, deswegen hat der Nachfrager der Cloud-Ressource im Allgemeinen keine Kontrolle darüber, woher er die Leistung bezieht. Dennoch kann bei manchen nachgefragten Ressourcen bzw. Dienstleistungen zumindest ein etwas abstrakterer Begriff der Örtlichkeit angegeben werden (z.B.: ein konkretes Land oder der EU-Raum). [35, S. 2]
  Dies ist deshalb bedeutend, weil es große Auswirkung auf eventuelle (datenschutz-) rechtliche Bestimmungen über Daten, die auf Cloudspeichern abgelegt oder von Cloudservices verarbeitet werden, haben kann.

- **Rapid elasticity**:
  Ressourcen sind dynamisch an Bedürfnisse des Kunden skalierbar, dies kann manuell oder automatisch erfolgen. Der Kunde kann zu jeder Zeit eine an seine Bedürfnisse angepasste Serviceleistung nachfragen. [35, S. 2]

- **Measured service**:
  Cloud-Systeme messen und überwachen die Ressourcen bzw. Dienstleistungen, welche dem Kunden zur Verfügung gestellt werden. Dies dient einerseits zur Optimierung, andererseits wird dadurch eine transparente Grundlage zur Verrechnung ermöglicht. Diese kann beispielsweise auf Basis von *pay-per-use* oder *charge-per-use* erfolgen. [35, S. 2]

5.1.2 Servicemodelle

1. **Software as a Service** *(SaaS)*:
   Im Rahmen von *SaaS*-Modellen bekommt der Kunde die Möglichkeit, in der Cloudumgebung laufende Applikationen des Providers zu nutzen. Zugang zu diesen Applikationen bzw. Programmen erhält er durch ein *thin client interface*, wie beispielsweise einen Webbrowser oder durch ein spezielles Programm. Die Applikationen sind über unterschiedliche Geräte des Kunden aufrufbar, z.B. PCs, Smartphones, Tablet-PCs, etc. [35, S. 2]
   Die den Applikationen unterliegende Cloud-Infrastruktur, wie beispielsweise das Netzwerk, die Server, Betriebssysteme oder Speicher kontrolliert der Kunde nicht, er besitzt maximal geringe Konfigurationsmöglichkeiten innerhalb der Applikationen. [35, S. 2]

2. **Platform as a Service** *(PaaS)*:
   Bei Cloudlösungen der Kategorie *PaaS* wird dem Kunden eine Plattform als Infrastruktur zur Verfügung gestellt, auf der er eigene Applikationen betreiben kann. Hierfür werden beispielsweise Programmiersprachen, Bibliotheken, Services und Tools zur Unterstützung angeboten. Die zugrundeliegende Cloud-Infrastruktur wird dabei nicht vom Kunden, sondern

vom Provider verwaltet. Der Kunde hat aber Kontrolle über den Einsatz von Applikationen. [35, S. 2f]
Kompakt zusammengefasst handelt sich also um eine Softwareumgebung, die dem Kunden für Entwicklung und Betrieb eigener Applikationen zur Verfügung gestellt wird.

3. **Infrastructure as a Service** *(IaaS)*:
   Unter *IaaS* versteht man die Zurverfügungstellung von Ressourcen wie Rechenleistung, Speicher oder Netzen, die der Kunde nutzen kann, um frei wählbare Software - inklusive Betriebssysteme - auszuführen. Die unterliegende Cloud-Infrastruktur wird zur Verfügung gestellt und somit nicht vom Kunden verwaltet, wohl aber der Speicher, das Betriebssystem und auch die benutzten Anwendungen. [35, S. 3]

5.1.3 Einsatzmodelle

- **Private Cloud**:
  Die Cloudumgebung wird exklusiv für eine Organisation, die mehrere Mitarbeiter umfasst, zur Verfügung gestellt, beispielsweise eine Abteilung eines Unternehmens. Dabei kann sie sowohl von der Organisation selbst, oder aber auch von einer anderen Partei zur Verfügung gestellt und betrieben werden. [35, S. 3]

- **Community Cloud**:
  Hier wird die Cloud einer begrenzten Gruppe an Nutzern zur Verfügung gestellt, die unterschiedlichen Organisationen gehören, welche gemeinsame Interessen verfolgen. Dies können verschiedene Unternehmen, Behörden oder beispielsweise ebenso Universitäten sein. [35, S. 3]

- **Public Cloud**:
  Die Dienstleistungen bzw. Ressourcen der *Public Cloud* stehen laut NIST-Definition einer breiten Öffentlichkeit zur Verfügung, wiederum kommen als Anbieter Unternehmen, Behörden, akademische Einrichtungen oder Kombinationen daraus in Frage. [35, S. 3]

- **Hybrid Cloud**:
  Als *hybride Cloud* bezeichnet man eine Mischform der obigen Einsatzmodelle. [35, S. 3]

5.2 Datenschutz- und IT-Security-Anforderungen an Cloud Computing

Über Cloud Computing zugängliche Services weisen wie eingangs bereits erwähnt zahlreiche Vorteile für die Benutzer auf. Wesentlichen Punkten wie Skalierbarkeit oder Verfügbarkeit *On Demand* stehen allerdings Risiken in Datensicherheit und -schutz gegenüber.
Bereits 2010 erwähnten Christmann et. al. in einem Artikel in der Fachzeitschrift HMD Herausforderungen im Bereich Technik und Recht, für die sie Maßnahmen wie Monitoring und Verschlüsselung bzw. EU-Standardvertragsklauseln und *Safe Harbor*-Principles empfahlen. [10]
Dass die Prinzipen von *Safe Harbor* wohl mindestens teilweise von den USA nicht sichergestellt wurden bzw. nicht dem europäischem Niveau entsprachen, ist einige Jahre später klar; nichtsdestotrotz ist der Zugang, entsprechende technische und rechtliche Maßnahmen zu treffen, wohl vielversprechend.
Dass das Thema durchaus Aufmerksamkeit auf sich zieht und österreichische Dienste mit dem heimischen Standort punkten wollen, zeigte die im Juli 2017 medial stark beachtete Ankündigung des Zertifikats *Austrian Cloud* der Wirtschaftskammer Wien. Diese wies darauf hin, dass mehr als zwei Drittel der heimischen Unternehmer nicht über den Ort ihrer gespeicherten Daten in der Cloud Bescheid wissen würden, obwohl es mit knapp 90 Prozent beinahe jedem ein Anliegen sei. Vertreter der Fachgruppe UBIT forderten einheitliche Standards und nannten 100 zertifizierte Unternehmen bis Ende 2017 als Ziel. [66]
Eine breite Übersicht über den konkreten Einsatz und aktuelle Trends von Cloudlösungen im Unternehmensbereich bietet der seit 2011 jährlich publizierte Cloud-Monitor von KPMG für den deutschen Markt. [68]
Grundsätzlich kommt der Bericht zu der Erkenntnis, dass 65 Prozent - also knapp zwei Drittel - aller deutschen Unternehmen Cloud Computing-Lösungen nützen und weitere 18 Prozent den Einsatz planen. Die Hälfte aller Unternehmen mit mehr als 2000 Mitarbeitern nutzen dabei Public Cloud Dienste, allerdings nur 29 Prozent der KMUs. Knapp 80 Prozent der Cloud-Kunden erwarten einen Hauptsitz des Cloud-Anbieters innerhalb der Union und zwei Drittel der befragten Unternehmen sorgen sich um die Compliance-Tauglichkeit von Cloud Computing-Technologien. [68, S. 5]
Damit ist die Etablierung der Technologie eindrucksvoll aufgezeigt, aber auch das Problembewusstsein scheint auf den ersten Blick vorhanden.
Stattliche 91 Prozent aller Cloud Anwender verwenden laut dem Monitor spezielle Sicherheitsservices, um die Cloud-Dienste abzusichern. Allerdings haben mit 53 Prozent mehr als die Hälfte aller Unternehmen keine Strategie zum Einsatz von Cloud Computing. [68, S. 5]
Hier gilt: je größer das Unternehmen, desto wahrscheinlicher das Verfolgen einer Strategie. Im Umkehrschluss bedeutet dies aber auch, dass beispielsweise in Betrieben mit weniger als 100 Mitarbeitern nur knapp 40 Prozent Cloud-Lösungen anhand einer eigenen Strategie einsetzen. [68, S. 8]
Dabei ist eine Cloud-Strategie kein abstrakter Luxus, sondern kann laut Empfehlungen der Studie zu einem maßgeblichen Wettbewerbsvorteil führen. Nicht nur das

WAS, auch das *WIE* ist im Bereich der Cloud entscheidend, hier führt kaum ein Weg über eine ganzheitliche Strategie vorbei, die Bereiche wie Sicherheit, Recht und Einsatzbereiche umfasst. [68, S. 11]
Besonders betont wird das Wachstumspotenzial des Bereichs der Public Cloud-Dienste, die - wie eingangs erwähnt - von jedem zweiten deutschen Betrieb mit mehr als 2000 Mitarbeitern eingesetzt werden. Gefragt sind vor allem Office-Lösungen, aber bereits knapp dahinter auf Platz zwei folgen IT-Sicherheitslösungen aus der Cloud - sprich *Security as a Service*. Dahinter folgen Groupware-Funktionen, wie Mail- und Kalenderlösungen, sowie ebenso stark ansteigend ERP-Lösungen. [68, S. 14]
Insgesamt bewerteten die befragten Unternehmen die Public Cloud-Effekte als sehr positiv, wobei naturgemäß der mobile Zugriff auf Ressourcen und die rasche Skalierbarkeit im Einsatz als stark positive Argumente erwähnt werden. Aber auch die Datensicherheit wuchs in den Umfragen als Pro-Faktor für Public Cloud-Dienste. [68, S. 15]
Datensicherheit - speziell die Sorge um den unberechtigten Zugriff auf sensible Daten - blieb jedoch ebenso das größte Bedenken gegen den Einsatz von Public Cloud-Diensten. Hier empfiehlt die Studie ein Mehr an Transparenz und Information zu Lösungen und Aspekten in den Bereich Security und Datenschutz, um mehr Kunden für die Public Cloud zu gewinnen. Gerade die kleinen Unternehmen, so folgert KPMG, sollten den Übergang zur Public Cloud nicht verpassen. [68, S. 16f]
Eine eigene Cloud-Strategie sucht man in der Mehrzahl der deutschen Unternehmen - wie bereits erwähnt - vergebens. Hier merkt die Studie an, dass in den allermeisten Fällen die IT-Abteilung Verantwortung für die Cloud-Sicherheit trägt, seltener befasst sich damit die Geschäftsführung oder ein externer Experte, noch rarer gesät sind mit 6 Prozent eigene Sicherheitsverantwortliche bzw. -abteilungen. Solch ein *Chief Information Security Officer* existiert in jedem vierten Unternehmen mit mehr als 2000 Mitarbeitern, in KMUs meist gar nicht. [68, S. 24]
Analog verhält es sich mit der Einsatzstrategie für Cloud-Dienste, die in Betrieben mit mehr als 500 Mitarbeitern mehrheitlich, in entsprechend kleineren Unternehmen mehrheitlich nicht vorhanden ist. Dass in Firmen mit weniger als 100 Angestellten die Geschäftsführung direkt für Cloud-Sicherheit verantwortlich ist bedeutet nicht, dass automatisch besonders strategisch vorgegangen wird. [68, S. 25]
Dies zeigt, dass dem Thema auf oberster Managementebene wohl oft nicht gebührend Aufmerksamkeit geschenkt wird, sei es aus Zeitgründen, sei es aufgrund mangelnder Prioritätensetzung.
Auch das Faktum, dass Sicherheitsverantwortliche bzw. - abteilungen in zwei Drittel der Fälle nicht in die Wahl des Cloud-Providers miteinbezogen werden, beweist, dass maßgeblich Luft nach oben besteht. [68, S. 26]
Bemerkenswertes Ergebnis der KPMG-Studie ist zudem, dass Datenschutz in der Public Cloud 'gefühlt' schwieriger als in internen Netzwerken zu bewerkstelligen sei, im Gegensatz dazu allerdings weniger Sicherheitsvorfälle in ebenjenen Public Clouds als intern passieren würden. [68, S. 28f]

Tatsächlich scheinen Public Cloud-Lösungen also besser als ihr Ruf und oftmals auch sicherer als interne Firmenspeicher bzw. -netzwerke zu sein.
Die bereits angesprochenen 91 Prozent Verbreitungsrate von Security Services für Cloud-Dienste setzen sich vor allem aus Zugriffsanmeldungen, Gerätemonitoring (im Rahmen des Datenzugriffs) bzw. Datenverschlüsselungen und Monitoring der Cloud-Dienste zusammen. [68, S. 31]
Abschließend fasst der KPMG-Monitor zusammen, dass Cloud-Dienste sich immer mehr im Unternehmensbereich etabliert haben. Für die zukünftige Marktentwicklung werden vor allem die Themen Datensicherheit und Vereinbarung mit Compliance-Anforderungen erwähnt, hier herrscht laut Studienersteller erheblicher Bedarf an Aufklärung und Beratung. Die Public Cloud wird aus Sicht der Studie mit Datensicherheit als grundsätzlich vereinbar und internen IT-Lösungen in Security als nicht nachstehend beurteilt. [68, S. 33f]
Konkrete Empfehlungen für (potentielle) Cloud-Anwender umfassen etwa die Erstellung einer Cloud-Strategie, die Befassung mit Argumenten pro und contra der unterschiedlichen Cloud-Typen sowie ein umfassendes IT Security-Management zur Gewährleistung der Datensicherheit, unabhängig davon, ob sensible Daten überhaupt mittels eines Cloud-Dienstes gespeichert werden. [68, S. 36]
Anbietern von Cloud-Lösungen wird empfohlen, den Kunden ein strategisches Vorgehen zur Einbettung ihrer angebotenen Dienste nahezulegen, den Standort Deutschland/Europa als Vertrauensvorschuss - und somit Wettbewerbsvorteil - zu nutzen und zu Complianceanforderungen aufzuklären bzw. zu beraten. [68, S. 36]

5.3 Fazit Cloud Computing

Cloud Computing ist kein Trend mehr, sondern in der privaten und betrieblichen Realität voll im Einsatz. Ob *Plattform*, *Infrastructure* oder *Software as a Service*, ob *Public*, *Private* oder *Hybrid Cloud*, die Nutzung von cloud-basierten Services befindet sich eindeutig auf dem Vormarsch.
Beeindruckende Wachstumsraten in Unternehmen attestiert der KPMG Cloud-Monitor 2017. Waren Cloud-Services im Jahr 2013 erst in 40 Prozent der Unternehmen (in Deutschland) im Einsatz und in 29 Prozent in Planung, nutzten 2016 bereits 65 Prozent der Betriebe Cloud-Computing und 18 Prozent planten einen Einsatz. [68, S. 7] Die Cloud ist also endgültig in der betrieblichen Realität angekommen. Wo jedoch noch Nachholbedarf herrscht, ist eine Strategie und ein wohlüberlegtes Einsatzkonzept für Cloudtechnologien.
Vor allem kleine Unternehmen mit weniger als 100 Mitarbeitern, so zeigt die KMPG-Studie für Deutschland, verfolgen nur in knapp 40 Prozent der befragten Verantwortlichen eine Strategie für den Einsatz von Cloud Computing. Hier gibt es einen eklatanten Unterschied zu großen Unternehmen mit über 2000 Mitarbeitern, wo eine Cloud-Strategie in 77 Prozent der Fälle vorhanden ist. [68, S. 8]
Es bedarf also eindeutig einer Bewusstseinssteigerung der Notwendigkeit von Cloud-Strategien, gerade im Bereich von KMUs.
Die Frage des Einsatzes von Cloud Computing in Unternehmen ist oft auch eine

Sache des Vertrauens. Die Frage des Speicherortes der Daten in Cloudspeichern oder die Sicherheit von vertrauenswürdigen Unternehmens- bzw. personenbezogenen Daten sind hier nur zwei wesentliche Fragestellungen.
Wie bereits in dieser Arbeit erwähnt wurde, ergibt die KMPG-Studie ebenso, dass das Vertrauen von Unternehmen in die Sicherheit und den Schutz von Daten in internen Netzwerken höher als in Public Clouds ist. Dem steht entgegen, dass in der Public Cloud weniger Sicherheitsvorfälle passieren, als innerhalb unternehmensinterner Netzwerke. [68, S. 28f]
Gerade für kleine und mittlere Unternehmen, die wenig finanzielle, zeitliche und personelle Ressourcen für den Aufbau einer komplexen IT-Infrastruktur besitzen, können Public Cloud-Lösungen also ein Mehr an Sicherheit für kritische Daten bedeuten. Dabei ist die Erstellung einer eigenen Cloud-Strategie mit einer Abwägung, in welchen Unternehmensbereichen Cloud-Technologien eingesetzt werden sollen und welche rechtlichen und technologischen Rahmenbedingungen zu beachten sind, wesentlich.
Ebenso betonte Sichao Wang 2015 in einem von der Cloud Security Alliance - einer Non-Profit-Organisation zur Stärkung von Wissensvermittlung im Bereich Cloudservices - angeführten Artikel, dass Anbieter von Cloud Services besonderen Fokus auf den Bereich von *Service Level Agreements* (*SLAs*) setzen sollten. Cloud Provider müssten laut Wang ein aussagekräftiges Performance Management System implementieren, um nachzuweisen, dass die Cloud Infrastruktur und die Cloud Services die vertraglichen Vereinbarungen einhalten würden. Generell müssten Cloud Service Provider Standards und Vorgangsweisen in Bereichen wie Datensicherheit, Datenschutz und Wiederherstellung von Services nach Ausfällen, also im Bereich *Business Continuity*, einführen bzw. maßgeblich erweitern, um das Vertrauen in die Cloud zu stärken. [63]
Kurz zusammengefasst kann die Cloud also nicht nur Vorteile im Bereich der Planung, des Einsatzes und der Kosten von Informationstechnologie, sondern sogar einen echten Mehrwert für die Sicherheit kritischer Daten von Unternehmen bringen. Dabei ist eine wohlüberlegte Strategie für den Einsatz von Cloud-Services unumgänglich. Diese Cloud-Strategie sollte, wie wesentliche IT-Sicherheits- und Datenschutzthemen generell, direkt an das Top-Management bzw. die Geschäftsführung berichtet und von dieser entschieden werden. Das darf aber nicht bedeuten, keine eigenen personellen Ressourcen für diese Bereiche abzustellen und das Thema zwar dem Vorstand zuzuordnen, ihm aber dort nicht gebührend Aufmerksamkeit zu schenken.
Abschließend kann festgehalten werden, dass Vertrauen in die Cloud gestärkt werden muss, wie Wang und die KPMG Studie fordern. Aufklärung und Beratung sind wesentlich und gerade Österreich und die Europäische Union können hier mit eigenen Cloud-Initiativen Standortvorteile, wie hohe Rechtssicherheit und ein gutes Datenschutzniveau, einbringen.

6 Identifikation zentraler Datenschutz- & IT-Security-Rahmenbedingungen zur Schaffung von Wettbewerbsvorteilen

Die Ist-Situation von Datenschutz und IT-Security wurde in den vorangegangenen Kapiteln ausführlich durchleuchtet und behandelt. Eine aktuelle Bewertung des Datenschutzes international und von drei nationalen Cybersicherheitsstrategien waren ebenso wie aktuelle und kommende Regulatorien, wie beispielsweise die Datenschutz-Grundverordnung und die NIS-Richtlinie, Teil der Betrachtung. Diese wurden inhaltlich zusammengefasst und bewertet.
Nun stellt sich allerdings die Frage, welche Schlüsse aus diesen Analysen in Kombination mit den Expertengesprächen, die im Rahmen dieser Arbeit geführt wurden, gezogen werden können und wie Österreich und die Europäische Union Datenschutz und Cybersecurity als Standortvorteil nutzen können.

6.1 Subsidiarität in Datenschutz und IT-Security

Klar ist, dass Datenschutz und IT-Security Akteure aller Ebenen angehen. Der **Staat** muss einerseits im Rahmen seiner Schutzfunktion 'seinen' Cyberspace, seinen Wirtschaftsraum und seine Behörden und öffentlichen Stellen sowie insgesamt seine Bürger bestmöglich vor Bedrohungsbildern und Cyberkriminalität schützen. Andererseits darf der Staat allerdings nicht zur 'Datenkrake' mutieren. Gerade in Zeiten von extremer Steigerung der Generierung personenbezogener Daten und immer fortschrittlicheren Überwachungs- und Auswertungsmechanismen muss das Gleichgewicht zwischen Freiheit und Sicherheit wohlüberlegt ausbalanciert werden. Klare Strategien im Bereich der Cybersecurity und Datenschutz sind für die Zukunft gefragt, die ENISA kann hier von europäischer Ebene aus Know-how und konkrete Unterstützung für einzelne Mitgliedstaaten der Union liefern.
Die einzelnen Akteursebenen im Staat, wie beispielsweise Bund und Länder, kooperieren in enger Abstimmung miteinander, um größtmögliche Synergieeffekte zu erzielen, wie das beispielsweise im Rahmen der deutschen NCSS vorgesehen ist. [26, S. 36]

Auf **Unternehmensebene** müssen die Betriebe Datenschutz und IT-Security als Agenda für das oberste Management erkennen. Der Einsatz von (neuen) Technologien darf nicht nach dem 'Prinzip Zufall' geschehen, sondern muss einer klaren Direktive unterliegen. Ein konkretes Beispiel dafür sind Cloud Services, die zwar vom Großteil aller Unternehmen genutzt werden, wo es aber gerade im KMU-Bereich oft noch an einer Einsatzstrategie mangelt. Doch gerade die Public Cloud kann manchmal bessere Sicherheitslösungen bieten, als ein Klein- oder Mittelunternehmen im Rahmen der eigenen IT-Infrastruktur implementieren kann.
Solche Sicherheitslösungen müssen, so die aktuelle britische Cybersecurity-

Strategie, stets *business driven* sein, um den Bedürfnissen des jeweiligen Betriebs bestmöglich zu entsprechen. [7, S. 12] Die Europäische Union ist, das ist aus dieser Arbeit eindeutig hervorgegangen, internationaler Vorreiter im Datenschutz. Weder die Vereinigten Staaten, noch eine neue 'Digitalmacht' wie China haben, in letzterem Fall schon allein aufgrund der politischen Struktur, auch nur ansatzweise die Möglichkeit, mit einem ähnlichen Datenschutzniveau zu punkten. Datenschutz als Wettbewerbs- bzw. Standortvorteil für Unternehmen stellt also eine riesige Chance für Österreich und Europa dar.
Zudem kommen den Unternehmen weitere, wichtig Aufgaben zuteil. So erwähnt die britische NCSS für den Teilbereich DEVELOP etwa, dass für die Stärkung von Cybersecurity-Fähigkeiten zwar Förderungen der Regierung nötig sein werden, die Aufgabe aber schlussendlich nur der private Sektor erfüllen kann. Eine florierende Szene von Start-up-Unternehmen im Bereich IT-Security kann hier Nachwuchskräfte in diesem Bereich entwickeln. [7, S. 55f]

Schlussendlich benötigt ein funktionierender Datenschutz und eine wirksame IT-Sicherheitspolitik den mündigen **Bürger**. Nicht nur in seinem beruflichen, auch im privaten Kontext muss er auf seiner Ebene sein Handeln von wesentlichen Prinzipen des Datenschutzes und der Cybersecurity leiten lassen, natürlich stets in einem angemessenen Verhältnis von Kosten und Nutzen.
Zu einer ähnlichen Rollenverteilung kommt beispielsweise auch die britische Cybersicherheitsstrategie. [7, S. 26f] Man kann und darf also keinesfalls erwarten, dass sich jeder Bürger oder auch jedes KMU quasi zu einem IT-Hochsicherheitszentrum aufrüstet, allerdings ist es genauso wenig zielführend, sämtliche Verantwortung auf den Staat abzuwälzen, dies erwähnt etwa auch die österreichische Strategie für Cyber Sicherheit. [5, S. 7]. Schon mit wenigen konkreten Maßnahmen, wie einer effizienten Passwortvergabe, der Nutzung ausgewählter Clouddienste und der kritischen Hinterfragung bei der Weitergabe von relevanten IT-Informationen - Stichwort *Social Engineering* - könnten zahlreiche Cyberkriminalitätsattacken scheitern bzw. deutlich weniger Schaden anrichten.

Summa summarum bedarf es also eines **subsidiären Datenschutzes** und einer **subsidiären IT-Security**. Damit ist gemeint, dass weder Datenschutz, noch IT-Sicherheit 'von oben' verordnet oder von einer einzigen Akteursebene ganzheitlich bewältigt werden kann. Ganz im Sinne der Subsidiarität sollen Individuen und 'kleinere Einheiten' ermutigt werden, eigenverantwortlich im Rahmen ihrer Möglichkeiten Maßnahmen im Bereich des Datenschutzes und von IT-Security zu treffen. Für die individuelle Ebene kann subsidiärer Datenschutz beispielsweise bedeuten, sich mit der Thematik erstmals ernsthaft auseinanderzusetzen und bewusst Produkte und Lösungen, evtl. 'Made in Europe', mit entsprechend hohem Niveau an Datenschutz und IT-Security auszuwählen.
Auf der Unternehmensebene kann das Prinzip bedeuten, dass ein KMU sich erstmalig Gedanken über seine IT-Infrastruktur und gespeicherte personenbezogene Daten macht und dann für eine Datenschutzlösung und Sicherheitsstrategie, etwa auch mit Produkten aus der Cloud, entscheidet. Größere Unternehmen mit entsprechend mehr Ressourcen sollten Datenschutz und IT-Security entsprechend

eigenen Organisationseinheiten zuweisen und diese in alle relevanten Entscheidungsprozesse einbinden, diese Themen allerdings trotzdem auf oberster Managementebene strategisch behandeln.
Ein konkretes Beispiel einer staatlichen Aufgabe im Rahmen der Aufgabenverteilung des subsidiären Datenschutz bzw. der subsidiären IT-Sicherheit ist, wie eingangs bereits erwähnt, die Erstellung einer NCSS und ihre tatsächliche Implementierung, Evaluierung und Anpassung.
Nur wenn alle Stakeholder die Aufgaben in ihrem Bereich bestmöglich bewältigen, gibt es kein schwächstes Glied der Kette und der Standort kann von einer intakten Cybersecurity und einem gelebten Datenschutz profitieren. So kann man die Angst von Teilen der Bevölkerung vor der Nutzung neuer Technologien nehmen, die Wirtschaft fördern und einen **Return on Investment** (ROI) auf Datenschutz und IT-Sicherheit zu generieren. Österreich und Europa hätten die besten Voraussetzungen dafür.

6.2 Datenschutz und IT-Security als Wettbewerbsvorteil - Identifikation zentraler Rahmenbedingungen

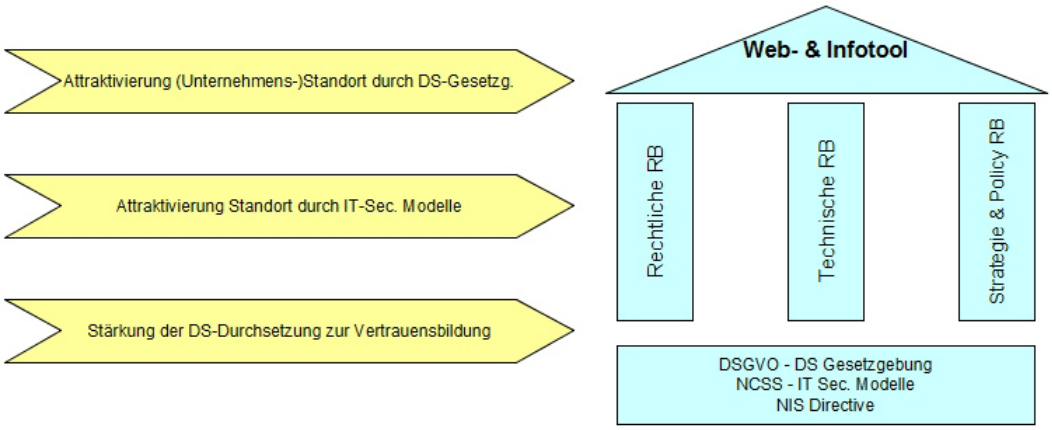
Abgeleitet aus einem subsidiären Datenschutz und einer subsidiären IT-Sicherheit liegt es also am Staat, geeignete Rahmenbedingungen zu setzen, um einen **ROI** für diese Bereiche zu ermöglichen. Es bedarf Initiativen in mehreren Bereichen, um diese Rahmenbedingungen so zu gestalten, dass sie sich in stimmiges Gesamtbild einbetten.
Der Standort Österreich und der Standort Europa haben, wie bereits mehrfach erwähnt, viele günstige Voraussetzungen, um in diesem Feld als starker Standort zu reüssieren. Ein global gesehen gutes Datenschutzniveau, innovative Unternehmen und eine Gesellschaft großteils mündiger Bürger mit einem starken Maß an Rechtssicherheit stellen gute Anknüpfungspunkte dar. Allerdings stehen auch große Herausforderungen im Wettbewerb an. Viele wichtige Unternehmen der Schlüsselindustrien im Bereich Informations- und Kommunikationstechnologien haben ihre Hauptquartiere nicht (mehr) in Europa. Gerade große Datenverarbeiter wie Facebook oder Google sind US-amerikanische Unternehmen, durch die DSGVO zwar demnächst innerhalb der EU an deren datenschutzrechtliche Vorgaben gebunden, aber dennoch keine originär europäischen Betriebe, die den hiesigen Standort stärken.
Ebenso nimmt die Bedeutung des europäischen Standorts global gesehen ab. Durch die demografischen Veränderungen, aber auch durch das steigende Wohlstandsniveau, etwa in Asien oder Südamerika, muss sich Europa immer mehr im globalen Wettbewerb behaupten.
Um auch im Zeitalter der Digitalisierung der schwindenden Bedeutung entgegenzuwirken wird es umso wichtiger, auf seine eigenen Stärken und Fähigkeiten zu setzen. Über den Faktor Quantität und Produktkosten wird dies kaum gelingen, über Qualität erfolgreich zu bleiben, wie eben etwa ein hohes Maß an Datensicherheit und Datenschutz, scheint dabei schon ein vielversprechenderer Ansatz zu sein.

Von diesen Überlegungen abgeleitet wurde das unten beigefügte grafische Modell entwickelt. Die links eingezeichneten gelben Pfeile stellen Maßnahmen dar, die es zu setzen gilt, um den Standort, der als Haus rechts dargestellt wird, zu stärken. Dazu zählt:

- Die Attraktivierung des (Unternehmens-)Standorts durch Datenschutzgesetzgebung.
- Die Attraktivierung des (Unternehmens-)Standorts durch IT-Security-Strategiemodelle.
- Die Stärkung der Datenschutzdurchsetzung zur Vertrauensbildung in der Wirtschaft und in der Bevölkerung.

So soll ein attraktiver Standort Österreich bzw. Europa ermöglicht werden, dessen Fundament (rechts als Rechteck dargestellt) schlanke, aber effiziente und effektive Regulatorien und Strategien sind, von denen sich (als 'Säulen') die entsprechenden weiteren Rahmenbedingungen ableiten, die subsidiär zu gestalten sind.
Das sind:

- Rechtliche Rahmenbedingungen.
- Technische Rahmenbedingungen.
- Strategische Rahmenbedingungen und Policies.



6.2.1 Rechtliche Rahmenbedingungen

Auch wenn die Datenschutz-Grundverordnung und ihre Auswirkungen von unterschiedlichen Seiten sehr verschieden bewertet werden, ist es jedoch allgemeiner Konsens, dass Europa bzw. die EU wohl weltweit zu den führenden Regionen in Sachen Datenschutzniveau gehören, wozu die Gesetzgebung den ihren Teil dazu beiträgt.
Dieser Eindruck verhärtete sich auch in den im Rahmen dieser Arbeit geführten Expertengespräche. So bemerkte etwa Henry Krasemann vom ULD im Rahmen einer Frage nach Datenschutzzertifizierungen an, dass die Idee der positiven Datenschutzstellung als Qualitätsmerkmal nach außen zwar nicht exklusiv europäisch sei, hierzulande aber mehr pfründe, da Datenschutz beispielsweise in den USA grundlegend anders gesehen werden würde.
Auch ULD-Chefin Marit Hansen merkte die 'Europäischen Werte' im Zusammenhang mit Datenschutz als Wettbewerbsvorteil an. [34]
Dabei sind effiziente und effektive rechtliche Rahmenbedingungen für Europa nur auf Ebene der Union zu lösen. Dazu bedarf es jedoch, ganz im Sinne des subsidiären Datenschutzes, auch einer aktiven Rolle der einzelnen Mitgliedstaaten, die durch die Öffnungsklauseln und Regelungsspielräume der DS-GVO als durchaus gegeben erscheint. Dabei kommt der internationalen Kooperation und dem Erfahrungsaustausch große Bedeutung bei, die europäische Datenschutz-Grundverordnung etwa widmet der internationalen Zusammenarbeit und Kohärenz ein eigenes Kapitel. [62, Kap. VII] Im Rahmen dieses Abschnitts soll nun auf zu setzende rechtliche Rahmenbedingungen eingegangen werden, um Datenschutz und IT-Sicherheit als europäischen Standortvorteil etablieren

zu können.

6.2.1.1 Geeignete Datenschutzgesetzgebung

Wie bereits mehrfach im Rahmen dieser Arbeit erwähnt, ist Datenschutzgesetzgebung ein Feld, in dem mannigfaltige Interessen aufeinandertreffen. Insofern ist die Frage nach einer 'idealen' Datenschutzgesetzgebung grundsätzlich nur sehr schwierig zu beantworten und sollte, je nach Perspektive des Betrachters, unterschiedliche Schwerpunkte und Gewichtungen vornehmen. Es ist also zutiefst unwahrscheinlich, dass Gesetze und Regulierungen im Bereich des Datenschutzes jemals auf ungeteilte Zustimmung aller betroffenen Seiten stößt, wie übrigens die meisten anderen Rechtsvorschriften ebenso wenig.
Ein treffendes Beispiel ist die vielzitierte Datenschutz-Grundverordnung, deren Analyse sehr unterschiedlich ausfällt. Im Rahmen der für diese Arbeit geführten Expertengespräche fiel die Bewertung grundsätzlich positiv aus, auch wenn beispielsweise Dr. Bäumler den sehr langsamen Fortschritt der Gesetzgebung im Vergleich zur technologischen Entwicklung anmerkte. Viele Punkte, die das ULD unter Bäumlers Leitung bereits vor Jahren bis Jahrzehnten aufgezeigt hatte und auf lokaler Ebene in Schleswig-Holstein bereits regelte, würden erst jetzt auf europäischer Ebene behandelt werden. [22]
Weitere positive Stimmen kamen etwa von EU-Justizkommissarin Jurova oder vom ehemaligen Staatssekretärs im deutschen Bundeswirtschaftsministerium, Rainer Sontowski. [36] [64]
Es existieren jedoch auch zahlreiche negative Stimmen, die ebenfalls bereits in dieser Arbeit im entsprechenden Kapitel zur DSGVO ausführlich zitiert wurden. Ein prominentes Beispiel eines harten Kritikers der Grundverordnung ist mit Prof. Dr. Alexander Roßnagel der Leiter der Projektgruppe *Verfassungsverträgliche Technikgestaltung* an der Universität Kassel. Hauptkritikpunkte waren unter anderem die Vielzahl an Öffnungsklauseln und der sich daraus ergebende geringe Grad an Harmonisierung innerhalb der Union, sowie der hohe Abstraktionsgrad und die Technikneutralität der Regelungen, die Anwendungen durch Behörden erschweren und Risiken nicht gebührend berücksichtigen würden. [29]
Dennoch: Die DSGVO kann grundsätzlich als legislative Basis dienen, Datenschutz als europäischen Wettbewerbsvorteil zu implementieren. Dies betonte etwa die deutsche Bundesdatenschutzbeauftragte Andrea Voßhoff, Datenschutz 'könne auch als Standortvorteil genutzt werden' [64].
Alleine schon die Existenz einer europaweiten Datenschutzregelung und die Debatte darüber, so gegensätzlich die Positionen auch sein mögen, ist ein wesentlicher Vorsprung gegenüber anderen Regionen dieser Welt.
Wichtig zu erkennen ist, dass im Bereich des Datenschutzes die zugrundeliegende Gesetzgebung natürlich einen großen Stellenwert hat, aber ein immer höherer Detailgrad der Regelungen nicht automatisch eine 'bessere' Regelung bedeutet. Dr. Bäumler bezeichnete es als 'deutschen Fehlweg', dass man geglaubt habe, dass 'das Heil nur in der Gesetzgebung liegt'. [22]
Dies habe zu immer ausufernden Gesetzen geführt, die nicht unbedingt zum höheren Verständnis beitrugen. Bäumler sprach sich also nicht für eine hohe

Regelungsdichte in allen Bereichen des Datenschutzes aus, sondern für eine Mischung aus Generalklauseln, genauen Vorschriften in ausgewählten Bereichen und flankierenden Maßnahmen, wie etwa Beratungspflichten sowie Gütesiegel und andere Zertifizierungen. [22]
Insofern ist Datenschutzgesetzgebung also als wichtig und notwendig anzusehen, sollte allerdings nicht als 'Allheilmittel' zur Erreichung eines angemessenen Schutzniveaus gesehen werden. Gerade bei allgemeinen, generalklauselartigen Gesetzestexten, die ob der Komplexität der Materie oft zielführend sind, erhält die tatsächliche Anwendung durch Behörden hohe Bedeutung. Auch Maßnahmen wie Gütesiegel und weitere Zertifizierungen, auf die in diesem Kapitel noch detailliert eingegangen wird, können im Verbund mit einer effizienten und effektiven Gesetzgebung dazu beitragen, das Datenschutzniveau zu erhöhen, ohne in sehr komplexe Regelungen und Belastungen auszuarten. So kann geeignete Datenschutzgesetzgebung dazu beitragen, Datenschutz als Standortvorteil möglich zu machen. In einigen Anwendungsfällen, wie beispielsweise manchen Cloud-Services, ist dies eben aufgrund der hohen Rechtssicherheit bereits heute der Fall.

6.2.1.2 Effiziente Datenschutzbehörde mit Beratungskompetenz

Auch im Zuge der Datenschutz-Folgeabschätzung gemäß DSGVO ist eine Beratungskomponente angeordnet. Wenn nämlich aus der Folgeabschätzung ein potentiell hohes Risiko ersichtlich wird, muss der Verantwortliche die Behörde kontaktieren, die ihm schriftliche Empfehlungen zur Verfügung stellt, falls die Verarbeitungsvorgänge nicht der DSGVO entsprechen. [62, Art. 36]
In vielen Fällen kann das ULD, das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein, als Vorbild für die Gestaltung einer innovativen Datenschutzbehörde herangezogen werden.
Besonders erwähnenswert erscheint hier die Pionierrolle des ULD. Das 2002 erschienene Buch 'Datenschutz als Wettbewerbsvorteil' von Dr. Helmut Bäumler, dem damaligen Datenschutzbeauftragen des Landes Schleswig-Holstein, zeigte bereits vor mehr als fünfzehn Jahren marktwirtschaftliche Konzepte und Herausforderungen an den Datenschutz auf. [2]
Als Chef der Behörde konnte Bäumler wesentliche Maßnahmen vorantreiben, die andernorts erst viel später oder noch überhaupt nicht getroffen wurden.
Einen konkreten Punkt, den Dr. Bäumler im Interview im Rahmen dieser Arbeit ansprach, stellt die Personalzusammensetzung einer Datenschutzbehörde dar. Einerseits seien laut ihm die Kapazitäten einer DSB im Verhältnis zu jenen der Sicherheitsbehörden geradezu lächerlich gering, andererseits wäre es von enormer Bedeutung, in diesen Behörden junge, engagierte Techniker zu engagieren, die einen praktischen Zugang zur Materie besitzen würden. Für kaum eine andere Gesetzesmaterie sei Kenntnis der Technik so entscheidend, wie im Datenschutz. [22]
Die 'ideale' Datenschutzbehörde vereint also technische Kompetenz und praktische Erfahrung von IT-Experten mit rechtlichem Fachwissen. Vertrauen der politischen Gremien und Exekutivorgane in diese Behörde muss ebenfalls gegeben

sein.
Zu welchen positiven Entwicklungen eine Kombination dieser Faktoren führen kann, zeigen die Leistungen des ULD. [22]
Unter diesen gesetzten Rahmenbedingungen sollte sich die DSB schließlich in erster Linie nicht als Stelle für Abmahnungen und Strafen verstehen, sondern partnerschaftlich die Wirtschaft beraten. Unternehmen und Bürger sollen durch rechtsverbindliche Auskünfte und klare Beratungen praktisch anwendbare Information und Hilfestellungen erhalten.
Bei Kontrollen ist aber sicherzustellen, dass trotz der partnerschaftlichen Augenhöhe von Behörde, Bevölkerung und Wirtschaft nichtsdestotrotz unvoreingenommene und dem Standard entsprechende Überprüfungen vorgenommen werden.
Diesen Ansatz verfolgte und verfolgt auch das ULD, Dr. Bäumler berichtete im Gespräch von der guten Kooperation seiner damaligen Behörde mit der Industrie- und Handelskammer. Mit diesem Ansatz würde man in der Wirtschaft entsprechend Gesprächspartner finden. Den Vorwurf von Behördenkollegen, man würde sich mit den später zu kontrollierenden Unternehmen gemein machen, entgegnete Dr. Bäumler deutlich, dass von Seiten des ULD meist schärfer und unnachgiebiger kontrolliert worden war, als dies vergleichsweise andere Behörden taten. [22]
Kritik an den aktuellen Regelungen zu Datenschutzbehörden kam von Abg. z. NR Eva-Maria Himmelbauer, die anmerkte, dass die DSB gleichzeitig als Kontroll- und als Strafbehörde fungieren soll. [16] Eine saubere Trennung dieser Kompetenzen einer DSB erscheint als absolut notwendig.
Die 'ideale' Behörde sollte zudem nicht durch das 'Prinzip Zufall' entstehen. Im Falle des ULD kamen, wie von Dr. Bäumler angeführt, einige Rahmenbedingungen wie 'positives Desinteresse' [22] der Politik, motivierte Techniker und engagierte verantwortliche Beamte zusammen. [22]
Solche Faktoren sollten in Zukunft bei Aufbau und Strukturierung von Datenschutzbehörden und dafür zu setzenden Rahmenbedingungen aber jedenfalls aktiv angestrebt werden. Weiters muss eine effiziente Datenschutzbehörde partnerschaftlich mit der Wirtschaft und der Gesellschaft kooperieren, bei Anfragen rechtsverbindliche Auskünfte erteilen und generell ein breites Beratungsangebot für Unternehmen und Bürger bereitstellen. Im Bereich der Überprüfungstätigkeit hat die DSB die festgelegten Kriterien und Vorschriften deutlich und gewissenhaft zu überprüfen. Dass diese Kombination aus partnerschaftlicher Beratung und konsequenter Überprüfung kein Gegensatz ist, sondern sich sehr gut ergänzt, zeigt das Beispiel des ULD für Schleswig-Holstein.

6.2.1.3 Geeignete europäische IT-Sicherheitsvorschriften

Geeignete rechtliche Rahmenbedingungen sind nicht nur für Datenschutzregelungen, sondern auch für IT-Sicherheitsvorschriften wesentlich, um diese beiden Faktoren zu einem Standortvorteil werden zu lassen. Vonseiten der Europäischen Union wurde hier die NIS-Richtlinie vorgelegt, die bis Mai 2018 umzusetzen ist.

[51]
Die Richtlinie wird von zahlreichen Seiten begrüßt und als geeignete Maßnahme zur Stärkung von IT-Security in der Union, und damit auch zur Steigerung des Standortvorteils IT-Sicherheit, gesehen.
So begrüßte etwa die WKO den europäischen Ansatz ausdrücklich, da digitale Netzwerke und kritische Infrastruktur meist über nationalstaatliche Grenzen hinausgehen würden. [38]
Auch das deutsche BSI bewertete die Richtlinie sehr positiv und betonte die notwendige Kooperation von Staat, Wirtschaft und Gesellschaft, um die Herausforderungen der Digitalisierung zu meistern. [59]
Die Voraussetzungen sind also gegeben, um durch europäische Harmonisierung ein einheitlich hohes Sicherheitsniveau und so einen Standortvorteil zu schaffen.

6.2.1.4 Gütesiegel & Zertifizierungen

Im Abschnitt zur Datenschutzgesetzgebung in diesem Kapitel wurde bereits erwähnt, dass Gütesiegel und Zertifizierungen einen wesentlichen Teil für die Verankerung eines hohen Datenschutzniveaus in Kombination mit Praktikabilität darstellen können.
Zwei bereits bewährte Möglichkeiten von Zertifizierungsverfahren sind die vom ULD in Schleswig-Holstein vergebenen Behördenaudits und Datenschutz-Gütesiegel. Die Audits beziehen sich auf Verfahren in Behörden, beispielsweise in Gemeinden des Bundeslands. Im Rahmen eines zweistufigen Verfahrens erfolgt zuerst eine Beratung bzw. ein Vorab-Audit, anschließend prüft das unabhängige Landeszentrum für Datenschutz selbst. [23]
Im Unterschied dazu bezieht sich das Datenschutz-Gütesiegel laut ULD-Verantwortlichem Henry Krasemann auf Produkte, die im öffentlichen Dienst in Schleswig-Holstein eingesetzt werden. Auch hier erfolgt das Zertifizierungsverfahren zweistufig. Zuerst analysieren vom ULD anerkannte Sachverständige das Produkt technisch und rechtlich. Anschließend wird das erstellte Gutachten beim ULD eingereicht und von der Behörde geprüft, die sich das Produkt im Bedarfsfall auch noch vorführen lassen kann. Das Siegel darf allerdings auch von privaten Stellen für Produkte geführt werden, die eventuell für den Einsatz im Landesdienst gar nicht vorgesehen sind. [23]
Außerdem könnten solche Siegel Krasemann zufolge wichtige Rechtssicherheit herstellen. Geschäftsführer und andere Verantwortliche könnten mit der Benutzung eines entsprechend zertifizierten Produktes sicher sein, der DSGVO und anderen Datenschutzgesetzen zu entsprechen, dies würde internen Prüfungsaufwand dieses Produktes und somit Bürokratie innerhalb eines Unternehmens oder einer Organisation maßgeblich reduzieren. Laut Krasemann müssten solche Zertifizierungen freiwillig erfolgen, da es sonst zu einem gewaltigen Aufwand für Behörden kommen würde. [23]
Datenschutzsiegel und -zertifizierungen sind auch in Kapitel IV der DSGVO verankert, die laut Verordnung zum Nachweis der Konformität von Verarbeitungstätigkeiten mit der DSGVO dienen sollen. Sie müssen über freiwillige und transparente Verfahren zugänglich sein und mindern nicht die Verantwor-

tung, etwa der Verantwortlichen, für die Einhaltung der DSGVO. Die in der Grundverordnung verankerte Zertifizierungsdauer wird für maximal drei Jahre erteilt und kann gegebenenfalls verlängert oder auch widerrufen werden. Solche Zertifizierungen sollen von einer entsprechenden Stelle, wie beispielsweise der Aufsichtsbehörde, vergeben werden. Diese Stellen selbst sollen für jeweils fünf Jahre akkreditiert werden. [62, Art. 42]
Krasemann kommentierte dazu, dass die DSGVO neue Möglichkeiten eröffne, aber noch einige Eckpunkte abzuklären wären. [23]
Auch der ehemalige ULD-Chef und Pionier des marktwirtschaftlichen Datenschutzes, Helmut Bäumler, bekräftigte im Interview im Rahmen dieser Arbeit die Wichtigkeit von Gütesiegeln und Zertifizierungen als flankierende Maßnahmen zu effizienter Datenschutzgesetzgebung. Marktwirtschaftlicher Datenschutz bedürfe eben der Bewerbung eines Produktes mit dem Faktor Datenschutz, dies könne etwa durch ein vertrauenswürdiges System von Zertifizierungen objektiv bekräftigt werden. Das Gütesiegel und die Zertifizierungsvorgänge des ULD, die ja bereits 1997 eingeführt wurden, bezeichnete Bäumler als damals ihrer Zeit weit voraus. [2, S.157] [22]
Auch Abg. z. NR Himmelbauer bezeichnete Gütesiegel als geeignetes Mittel, um Bewusstsein für einen Teil der Bevölkerung zu schaffen. [16]
Datenschutzgütesiegel und Zertifizierungen können also mehrere Nutzen besitzen, falls sie richtig implementiert werden.
Unternehmen und Behörden können damit ohne immensen internen Prüfungsaufwand sicherstellen, dass ein eingesetztes Soft- oder Hardwareprodukt den Standards der europäischen und nationalen Rechtsvorschriften erfüllt. Somit erhöht sich der Stellenwert des Datenschutzes bei der Produktauswahl, auch bei Privatpersonen, die mit einem Gütesiegel ausgezeichnete Produkte erkennen können. Der Effekt ist aber im Unternehmens- und Behördenbereich stärker zu erwarten, als im privaten Umfeld, da Geschäftsführer, Behördenleiter und weitere Verantwortliche ein veritables Interesse besitzen, sämtliche Rechtsvorschriften vor allem günstig und unbürokratisch zu erfüllen. Im Privatbereich ist diese Motivation naturgemäß schwieriger zu erreichen, hier ist auf Eigeninitiative der Bürger und durchaus auch auf Informationskampagnen zu setzen. Da viele, eher komplizierte, technologische Sachverhalte aber schwerlich in Kurzform transportiert bzw. dargestellt werden können, gewinnt der Bildungsaspekt an Bedeutung, der in diesem Kapitel noch behandelt wird.
Freiwillige Siegel und Zertifizierungen können also einen gewichtigen Teil zur Steigerung von Datenschutz und auch IT-Security als Wettbewerbsvorteil haben. Klar zertifizierte und mit einem Gütesiegel ausgezeichnete Produkte und Services unterstützen Unternehmen und Organisationen bei der Auswahl von Hard- und Software sowie IT-Services, da sie Rechtssicherheit durch die Zertifizierung erhalten und sich nicht intern mit Prüfungen zur Datenschutzkonformität herumzuschlagen brauchen.
Auch Privatpersonen können von solchen Siegeln, falls der Bekanntheitsgrad entsprechend groß und die Awareness gegeben ist, profitieren und somit tendenziell mehr 'datenschutzfreundliche' Produkte nachfragen, auch wenn der Effekt im Vergleich zu Unternehmen, Behörden und Organisationen, die hierbei stärker

in der Pflicht stehen, vermutlich geringer ausfallen wird. Der Standort Österreich bzw. Europa kann durch hier niedergelassene Unternehmen, die solch zertifizierte Produkte und Services anbieten, profitieren.

6.2.1.5 Fazit - Rechtliche Rahmenbedingungen

Rechtliche Rahmenbedingungen, um Datenschutz und IT-Security als Standortvorteil zu nutzen, umfassen also:

- **Geeignete Datenschutzgesetzgebung**, die nicht als 'Allheilmittel' zur Sicherung des Datenschutzes angesehen wird, sondern effizient und flankiert von weiteren Maßnahmen, wie etwa Zertifizierungen, klare und verständliche Regelungen schafft.

- **Effiziente Datenschutzbehörden**, welche nicht nur Juristen, sondern vor allem auch Techniker beschäftigen und sich mit einer starken Beratungskomponente der Wirtschaft und der Gesellschaft gegenüber auszeichnen.
  Verbindliche Auskünfte und veröffentlichte 'Best Practice'-Modelle sollen Unternehmen Rechtssicherheit und Anleitungen zum Thema Datenschutz geben. Nichtsdestotrotz müssen behördliche Überprüfungen konsequent und in gebotener Strenge durchgeführt werden.

- Entsprechende **europäische IT-Sicherheitsvorschriften**, die Cybersecurity, ausgehend von der Unionsebene, implementieren und Bewusstsein für die Priorität des Themas auf allen Akteursebenen schaffen.

- **Datenschutzgütesiegel & Zertifizierungen**, die als flankierende Maßnahmen zur Legistik dienen. Diese sollen die Sichtbarkeit von Datenschutz erhöhen und Unternehmen Rechtssicherheit geben, dass die zertifizierten Produkte allen erforderlichen Regelungen entsprechen. Damit kann wiederum die europäische IT-Branche gefördert werden. Siegel und Zertifizierungen sollen aber auch Awareness bei Privatpersonen schaffen und diese dazu animieren, bei der Auswahl von Produkten und Services vermehrt auf den Faktor Datenschutz zu achten.

6.2.2 Technische Rahmenbedingungen

Ein wesentliches Erkenntnis im Umgang mit Datenschutz und IT-Sicherheit ist, dass diese Themenkomplexe nicht rein rechtlich gelöst werden können. So merkte etwa Dr. Bäumler dazu an: 'Für kaum eine andere Gesetzesmaterie ist die praktische Arbeit mit und die Kenntnis der Technik so wichtig wie beim Datenschutz' [22].
ULD-Leiterin Hansen betonte, dass technische Lösungen den Lösungsraum erweitern könnten und somit Möglichkeiten auftun würden, die der Gesetzgeber bei der Erstellung der Rechtsvorschriften eventuell gar nicht bedacht hatte. [34]
Es bedarf also entsprechender technischer Rahmenbedingungen, um Datenschutz und Cybersicherheit als europäischen Standortvorteil zu stärken. Von diesen

werden einige in diesem Abschnitt angeführt, die aber auch in den Bereichen *Rechtliche Rahmenbedingungen* und *Strategische Rahmenbedingungen und Policies* eine gewichtige Rolle spielen. Schließlich erfolgt die Verarbeitung personenbezogener Daten durch Technik und technologischer Fortschritt ermöglicht die Generierung und die Analyse von zunehmend mehr personenbezogenen Daten.

6.2.2.1 Technologien als Chance begreifen

Um ein höheres Maß an Datenschutz und IT-Sicherheit sicherzustellen und diese Themen schließlich als Standortvorteil nutzen zu können, dürfen neue technologische Entwicklungen nicht ausschließlich als Bedrohung angesehen, sondern sollten auch als mögliche Chance begriffen werden.
Eine dieser Möglichkeiten, Informationstechnologie bzw. -systeme sicherer zu gestalten, ist die Verwendung von Blockchain-Technologien. In der Zeitschrift Forbes schrieb Jonathan Chester, Gründer des auf Bitcoin spezialisierten Zahlungsabwicklungsunternehmens Bitwage, im März 2017, dass die Blockchain ganz neue Möglichkeiten im Identity Management eröffnen könnte. Blockchains könnten *Security* bzw. *Privacy by default* insofern realisieren, als dass die Identifizierung aufgrund der kryptografischen Hashfunktion stattfinden würde und nicht aufgrund eines Abgleichs mit tatsächlichen Identifikationsdaten. Diese müssten auch nicht mehr zentral gespeichert werden und könnten in einem Cyberangriffsfall gar nie gestohlen werden, ganz einfach, weil sie von vornherein nie abgelegt würden. [9]
Die Blockchain ermöglicht also auch die Realisierung des Grundsatzes der Datenminimierung, der in der DSGVO verankert ist [62, Art. 5] und stellt eine vielversprechende neue Technologie für Security-Anwendungen dar.
Dem in der Datenschutz-Grundverordnung enthaltenen 'Recht auf Löschung' bzw. 'Recht auf Vergessenwerden' [62, Art. 17] könnte man durch solch eine Datenminimierung gänzlich zuvorkommen. Es wäre im Optimalfall also gar nicht mehr nötig oder möglich, personenbezogene Daten zu löschen, wenn diese gar nie abgespeichert worden wären.
Die DSGVO greift auch grundsätzlich das Thema 'Privacy by default' auf, Datenschutz soll durch sichere Technikgestaltung und entsprechende Voreinstellung realisiert werden, hier werden v.a. Verantwortliche im Sinne der Datenschutz-Grundverordnung in die Pflicht genommen. Der Grundsatz *Privacy by default* kann auch explizit durch genehmigte Zertifizierungsverfahren bestätigt werden. [62, Art. 25]
Im nachfolgenden Abschnitt werden diese Themen *Privacy & Security by Design* bzw. *by Default* detaillierter beleuchtet.

6.2.2.2 Privacy & Security by Design bzw. by Default

Datenschutz und IT-Security sind keineswegs als rein rechtliche Themen zu begreifen. Entsprechende Technikgestaltung ist ein maßgeblicher Teil, um ein hohes Niveau an Datenschutz und IT-Sicherheit zu erreichen. Dr. Helmut Bäumler verortete im Interview das Problem darin, dass man früher dem eigenen

Datenschutz quasi hinterherlaufen und ihn nachträglich einprogrammieren haben müsse. Die Idee von *Privacy by Default* sei, dass man diesen Vorgang umdrehen und entsprechend datenschutzfreundliche Voreinstellungen implementieren würde. [22]
Die aktuelle ULD-Vorsitzende Marit Hansen bezeichnete *Privacy by Design* als Möglichkeit, viele Probleme bereits im Vorfeld zu beseitigen. Man könne mit Technikgestaltung oft viel erreichen, der Lösungsraum würde mit technischen Realisierungen also erweitert und so würden Möglichkeiten entstehen, die sogar über die ursprüngliche Relevanz des Gesetzgebers hinausgehen würden. [34]
Das zeigt deutlich auf, dass Technik und Technologie zu einem besseren Datenschutzniveau beitragen können und Möglichkeiten schaffen, die im Zuge der Gestaltung von Rechtsvorschriften gar nicht angedacht oder vielleicht auch noch nicht möglich waren.
Ein von Hansen erwähntes Beispiel von Technikgestaltung, das schon existiert, betrifft den Bereich der *Attribute-based Credentials*, also attributbasierte Berechtigungsnachweise. So besitzt etwa der deutsche Personalausweis die Möglichkeit, mittels mathematischer Funktionsausführung gewisse Parameter zu beantworten, beispielsweise Volljährigkeit. Es ist also möglich, technisch abzuprüfen, ob eine Person mindestens 18 Jahre alt ist, ohne dass diese gleich den gesamten Ausweis vorzeigen müsste. Das entspricht ganz dem Prinzip der Datenminimierung. [34]
Wie bereits mehrfach erwähnt wurde, ist dieses Prinzip auch in der DSGVO verankert. Ein eigener Abschnitt 'Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen' ist Teil des Kapitels IV. Zur Zielerreichung wird das Prinzip der Datenminimierung, etwa durch Pseudonymisierung, genannt. Außerdem sind durch organisatorische und technische Maßnahmen entsprechende datenschutzfreundliche Voreinstellungen zu treffen. [62, Art. 27]

Nicht nur Datenschutz, auch IT-Sicherheit ist ein Punkt, der bei Technikgestaltung von Anfang an bedacht werden sollte. Die deutsche Cybersicherheits-Strategie erwähnt etwa das Prinzip *Security by Design*. Damit wird in der Strategie die Berücksichtigung von Sicherheitsaspekten an Beginn der IT-Produktentwicklung bezeichnet und eingefordert. [26, S. 18]
Die britische NCSS erwähnt im Abschnitt *Building a more secure Internet* die Priorität, dass Onlineprodukte *secure by default* sein müssten. Hard- und Softwarekomponenten sollten also standardmäßig integrierte Security-Maßnahmen besitzen. Konkret wird die Entwicklung von *Secure Internet Services* durch die Regierung und öffentliche Stellen geplant. Diese Services müssen sich nicht darauf verlassen, dass das Internet andernfürsich sicher ist, sondern bringen eigene Security-Mechanismen mit ein. Konkret benannt werden zu fördernde Identifizierungsstandards wie *FIDO* (*Fast Identity Online*), die innovative Authentifizierungsmaßnahmen anstatt Passwörtern zur Useridentifikation verwenden. [7, S. 36f]
Der Bereich Cloud Computing ist oft besonders von Bedenken und teilweise Vorurteilen in den Bereichen Datenschutz und IT-Sicherheit geprägt. Dabei können Cloud-Services, wie im entsprechenden Kapitel erwähnt, auch *Security as a Service* bieten. Entsprechende Lösungen weisen nämlich oft viel bessere

Sicherheitsperformanz auf, als etwa eigens aufgebaute IT-Lösungen von Klein- und Mittelunternehmen. [68, S. 14]
Zusammengefasst können also die Prinzipien *Privacy* bzw. *Security by Design* wesentlich dazu beitragen, als Wettbewerbsvorteil für Österreich und die Europäische Union zu dienen. Besonders deutlich wird das im Bereich des Cloud Computing, in dem schon etliche Initiativen existieren, die mit einem Standortvorteil in Österreich oder Europa werben. Hier ist die Vertrauensbildung in die Cloud besonders wichtig, da, richtig ausgewählt und angewandt, solche Services nicht nur einen echten Mehrwert für Funktionalität und Kostenoptimierung, sondern auch im Bereich Sicherheit bieten können.

6.2.2.3 Fazit - Technische Rahmenbedingungen

Technische Rahmenbedingungen, um Datenschutz und IT-Security als Standortvorteil zu stärken, umfassen also:

- Generell die Erkenntnis, dass **Datenschutz und IT-Sicherheit** nicht nur **rechtlicher**, sondern auch **technischer Rahmenbedingungen** bedürfen, um diese erfolgreich zu gestalten und zum europäischen Standortvorteil werden zu lassen.
- **Konkrete Erkennung und Verwendung neuer Schlüsseltechnologien**, wie beispielsweise der Blockchain, die für innovative Datenschutz- und Securitylösungen genutzt werden können.
- ***Privacy & Security by Design and by Default* begreifen und implementieren.** Einerseits müssen durch *Privacy by Default* datenschutzfreundliche Voreinstellungen realisiert werden, andererseits sollen Prinzipien des Datenschutzes und der IT-Sicherheit bereits im Planungs- und Entwicklungsstadium von Soft- und Hardwareprodukten und Services gebührend berücksichtigt werden, ganz gemäß der Prinzipien *Privacy by Design* und *Security by Design*

6.2.3 Strategische Rahmenbedingungen und Policies

'Zurück aus der Zukunft in die Realitäten des Datenschutzes im Jahre 2002. Der marktwirtschaftliche Datenschutz steckt noch in den Kinderschuhen.' [2, S. 6]. Mit diesem Zitat beschrieb Bäumler die aktuelle Realität des Jahres 2002 in seinem Buch 'Datenschutz als Wettbewerbsvorteil'. Im Jahr 2017, 15 Jahre später, erscheint das Zitat in vielen Lebensbereichen nach wie vor zuzutreffen.
Wie in den beiden vorhergegangenen Abschnitten *Rechtliche Rahmenbedingungen* und *Technische Rahmenbedingungen* bereits erwähnt, sind freilich einige positive Entwicklungen in den letzten Jahren geschehen. Zeitgleich haben aber auch rasante technische Entwicklungen stattgefunden, deren Funktionsweisen und Möglichkeiten weite Teile der Bevölkerung nicht immer in ihrer ganzen Tragweite begreifen.
Daher muss die Awareness für Datenschutz und IT-Security in Gesellschaft,

Wirtschaft und Politik gesteigert werden und die Themen weniger als regulatorische Hindernisse, sondern als echte Chancen für den Standort Österreich und generell Europa begriffen werden.
Strategische Rahmenbedingungen und Policies umfassen also Maßnahmen, um den Stellenwert von Privacy und IT-Security auf den oben angeführten Ebenen zu stärken, aber etwa auch die Gestaltung von Strategien zur IT-Sicherheit auf nationaler und europäischer Ebene.

6.2.3.1 Nationale IT-Sicherheitsstrategien und -politik gestalten

Subsidiäre IT-Security bedeutet, dass der Staat durch entsprechende Strategien eine Politik verfolgt, die seine Wirtschaft und Gesellschaft vor Bedrohungen aus dem Cyberspace schützt. Diese Rolle bedarf einer entsprechenden Planung, derer drei wurden im Rahmen dieser Arbeit genauer analysiert.
Weswegen das Verfolgen solch eines Plans überhaupt so bedeutend ist, betonte die britische NCSS in einem Vergleich der aktuellen Strategie 2016-2021 mit ihrem Vorgänger. In der neuen Version wurde der Regierung und ihren Behörden ein höherer Stellenwert im Bereich der IT-Security eingeräumt. Damit war nicht gemeint, dass der Markt keinen Platz in der Rollenverteilung habe, aber trotz vielen Erfolgen gebe er dem Thema Cybersicherheit einen zu geringen Stellenwert. Eine aktivere IT-Sicherheitspolitik sei also notwendig. [7, S. 27]
Die Eckpfeiler DEFEND, DETER und DEVELOP umrahmen die Priorität einer aktiven Verteidigungs- und Sicherheitspolitik für den Cyberspace. [7]
In der deutschen NCSS wird ein Fokus auf Schutz der Unternehmen gegenüber Cyberkriminalität, wie beispielsweise Wirtschaftsspionage, verfolgt. Auch sollen im Rahmen der Strategie IT-Schlüsseltechnologien identifiziert und Betriebe in diesem Bereich gefördert werden, um die Wettbewerbsfähigkeit zu steigern. [26, S. 18] [26, S. 23]
Ein hohes Schutzniveau und damit ein echter europäischer Standortvorteil aus IT-Sicherheit kann also nur generiert werden, wenn die Mitgliedstaaten der Union, genauso wie das Großbritannien als Zielsetzung formuliert, als Angriffsziele eingeschätzt werden, die entsprechend dem Grundsatz *High Cost - High Risk* keine lohnende Destinationen für Cyberattacken darstellen. Nationale Cybersecurity-Strategien sind längst kein Luxus, den sich Staaten leisten können, sondern absolut notwendig und innerhalb der Union demnächst sogar verpflichtend. Der Entstehungs- und Anpassungsprozess einer solchen Strategie bedarf also ausreichend finanzieller und personeller Ressourcen und sollte, wie von der ENISA empfohlen, im Rahmen eines **NCSS-Lifecycles** erfolgen. [17, S. 7]
Dieser umfasst die beiden Schlüsselphasen *Entwicklung und Ausführung* sowie *Evaluierung und Anpassung*, welche die jeweilige Strategie durchlaufen muss. Am Ende der zweiten Phase hat die Strategie dabei im Lifecycle-Modell nicht ausgedient oder wird hinfällig, sondern das Evaluierungsergebnis wird genutzt, um die NCSS neu anzupassen. [17, S. 7]
Mit gutem Beispiel voran geht hier die bereits erwähnte britische NCSS. Neben dem Kapitel *beyond 2021*, in dem man auf etwaige langfristige Entwicklungen Bezug nimmt, wurde mit *Effective Horizon Scanning* eine Methode zur Trend-

beobachtung der Cyber- und technologischen sowie geopolitischen Landschaft in die Strategie aufgenommen. [7, S. 60f]
Sich immer wieder erneuernde nationale Cybersicherheitsstrategien passen ihren Fokus somit neuen Bedrohungen, aber auch neuen Chancen stetig an. Diese neuen Herausforderungen und Möglichkeiten liegen mitunter nicht nur in technologischen, sondern auch in wirtschaftlichen, politischen oder gesellschaftlichen Neuentwicklungen.
Die 'ideale' Strategie kann so ein echter Eckpfeiler zur Implementierung eines Standortvorteils Cybersecurity werden. Expertise dafür kann und sollte vonseiten der Mitgliedstaaten bei der ENISA eingeholt werden.

6.2.3.2 Stellenwert von Datenschutz und IT-Security in der Bildung verankern

Der Stellenwert von Datenschutz und IT-Sicherheit in Politik, Wirtschaft und Gesellschaft, so sind sich die im Rahmen dieser Arbeit befragten Experten einig, muss gestärkt werden. Während auf die einzelnen Ebenen, wie eben beispielsweise die Wirtschaft, in eigenen Abschnitten noch gesondert eingegangen wird, ist es wesentlich zu erkennen, dass eine Verankerung dieser Themen nicht 'vom Himmel fallen' kann. Deswegen bedarf es verstärkter Anstrengungen im Bildungsbereich, um das Bewusstsein und die Kompetenz für Datenschutz und Cybersecurity langfristig gesehen zu erhöhen.
Abg. z. NR. Eva-Maria Himmelbauer sprach im Zuge des Interviews im Rahmen dieser Arbeit etwa davon, Schülern nicht nur Fertigkeiten im Umgang mit Programmen wie Word und Excel, sondern vor allem von technologischem Grundverständnis und digitalem Humanismus zu vermitteln. [16].
In die gleiche Richtung gehen die Ideen von Henry Krasemann vom ULD, der Grundverständnis im Bereich IKT als Voraussetzung sieht, Produkte und in Folge dessen etwaige Zertifizierungen und Gütesiegel erst richtig einschätzen zu können. [23]
Auch die deutsche nationale Cybersecuritystrategie setzt einen Fokus auf Bildung, um 'digitaler Sorglosigkeit entgegenzuwirken' [26, S. 14] und 'digitale Kompetenzen bei allen Anwendern zu fördern' [26, S.14]. Dies umfasst die Vermittlung solcher Kompetenzen innerhalb der Schule, der dualen Ausbildung, der Universität sowie der Erwachsenenbildung allgemein. [26, S. 14]
Ebenso legt die britische NCSS großen Wert auf Bildungs- und Schulungsangebote, um Großbritannien zur 'World Leading Digital Nation' [7, S. 37] zu machen.
Es sollte allerdings nicht nur das Grundverständnis der Bevölkerung verstärkt werden, um in Zukunft reüssieren zu können, muss die Ausbildung von IT-Fachkräften und -Akademikern forciert werden, da hier in vielen europäischen Ländern ein eklatanter Mangel herrscht. Dies fordert auch Abgeordnete Himmelbauer im Interview zu dieser Arbeit. [16]
Das bereits zitierte, für den Datenschutz wesentliche 'Volkszählungsurteil' 1983 in Deutschland spricht davon, dass freie Entfaltung für der Persönlichkeit unter modernen Datenverarbeitungsmöglichkeiten voraussetzt, den Einzelnen vor unbegrenzter Erhebung, Verarbeitung, Weitergabe und Speicherung zu schützen.

Außerdem müsse der Einzelne immer grundsätzlich über Preisgabe und Verwendung seiner personenbezogenen Daten bestimmen können. [6, S. 45f]
Das setzt allerdings einen mündigen User voraus, der sich der Möglichkeiten, aber auch der Risiken von modernen Informationstechnologien bewusst ist. Ein entsprechendes Bildungsangebot, verankert in unterschiedlichen Ausbildungsabschnitten und -instituten, soll keine Angst vor dem 'gläsernen Bürger' oder scheinbar allwissenden 'Datenkraken' schüren, sondern einen selbstbewussten, eigenverantwortlichen Umgang mit modernen Technologien ermöglichen und ermutigen.

6.2.3.3 Stellenwert von Datenschutz und IT-Security in der Wirtschaft stärken

Datenschutz darf in Unternehmen und Organisationen jedweder Größe kein Thema für 'Einzelkämpfer' sein, sondern muss die oberste Managementebene angehen. Dort soll die Zuständigkeit aber auch nicht 'geparkt' werden, nur, weil sich sonst niemand dafür verantwortlich fühlt. Klar definierte Verantwortliche, die etwa in Unternehmensstrategien hinsichtlich IT eingebunden werden bzw. diese mitentwickeln, sind dafür unabdingbar. Das ein Großunternehmen dafür mehr Ressourcen aufwenden kann und sollte, als ein KMU, ist klar und verständlich, nur dürfen auch kleine und mittlere Unternehmen die wichtigen Bereiche IT-Security und Datenschutz nicht ignorieren. Hier können qualitativ hochwertige Sicherheitslösungen von außen zugekauft werden, beispielsweise Dienste aus der Cloud als *Security as a Service*. Dadurch, so zeigte der bereits im Rahmen dieser Arbeit mehrfach erwähnte KPMG-Cloudmonitor, kann in vielen Fällen ein höherer Grad an Sicherheit gewährleistet werden, als durch firmen- bzw. organisationsinterne Netzwerke und Maßnahmen. [68, S. 28f]
Der Stellenwert der beiden Themen könnte, wie bereits im eigenen oberen Abschnitt zum Thema erwähnt, durch entsprechende Gütesiegel und Zertifizierungen erhöht werden. Den Unternehmen würde dadurch Rechtssicherheit und deutliche Vereinfachung in der Auswahl und internen Überprüfung von Hard- und Software geboten werden. Der vergleichsweise einfache Zugang zu sicheren und qualitativ hochwertigen IKT-Lösungen kann das Sicherheits- und Schutzniveau für Europa und Österreich heben und somit zum Standortvorteil beitragen.
Schließlich bietet IT-Security, das erwähnt die britische NCSS, echte betriebswirtschaftliche Vorteile. Eine geplante Maßnahme umfasst deshalb die Kampagne 'Cyber Aware', im Rahmen die Notwendigkeit von Investitionen in Cybersecurity durch potentiellen Kosten im Schadens- bzw. Angriffsfall erklärt werden. [7, S. 43] Auch Entscheidungsträger in Klein- und Mittelunternehmen müssen die Bedeutung erkennen, die IT-Sicherheit für ihren Betrieb hat. Kein Unternehmen kann es sich leisten, dieses Thema zu ignorieren. Bereits mit vergleichsweise geringen Investitionen können wichtige Maßnahmen getroffen werden. Eine konkrete Expertenmeinung empfiehlt beispielsweise, 5-10 Prozent des gesamten IT-Budgets in den Bereich Cybersicherheit zu investieren. [11]

6.2.3.4 Stellenwert von Datenschutz und IT-Security in der Gesellschaft heben

Dieser Abschnitt ergänzt sich naturgemäß mit dem vorherigen Themenpunkt *Stellenwert von Datenschutz und IT-Security in der Bildung verankern*, denn über Bildungsmaßnahmen kann die Priorität von Datenschutz und die Wichtigkeit von IT-Security mittel- bzw. langfristig in der Gesellschaft Einzug halten.
Schon 2002 erwähnte Helmut Bäumler einleitend in seinem Buch 'Datenschutz als Standortvorteil' den Verbraucherwunsch als Maß der Dinge. Er führte vor bereits fünfzehn Jahren an, dass in Deutschland nur wenige Verbraucher positive Erfahrungen mit dem Thema Datenschutz gemacht hätten. [2, S. 2f]
Fast könnte man meinen, dass sich eineinhalb Jahrzehnte später daran nur wenig geändert hätte. Vielerorts wird Datenschutz im privaten Umfeld eher als Randthema wahrgenommen. Marit Hansen merkte an, dass der Datenschutz im persönlichen Umfeld oft erst eine Rolle spielen würde, wenn er etwa durch Missbrauch nicht mehr gegeben sei und nannte dies *Privacy by Disaster*. [34]
Auch Henry Krasemann erwähnte dieses fehlende Bürgerinteresse bis zum Unglücksfall. [23]
Positiv in die Zukunft blickte Eva-Maria Himmelbauer, die Datenschutz im Gespräch im Rahmen dieser Arbeit als Generationenfrage bezeichnete. Diese würde für manch ältere Generation zuweilen eine 'Black Box' darstellen, technikaffine Schüler, die immer wieder bei der Abgeordneten im Parlament zu Gast seien, würden aber genau über die Privatsphäreneinstellungen der von ihnen genutzten Services Bescheid wissen. [16]
Helmut Bäumler kritisierte im Gespräch im Rahmen dieser Arbeit die langsame Entwicklung des gesellschaftlichen Interesses und bezeichnete Datenschutz in der Gesellschaft als absolutes Gewinner- und Zukunftsthema, er sei nur ungeduldig, wann diese Zukunft denn endlich anfinge. Es würden sich nämlich Menschen täglich millionenfach gegen Datenschutz und für vermeintlich günstige oder kostenfreie Produkte und Services entscheiden. [22]
Es scheint also unausweichlich, vor allem den gesellschaftlichen Stand des Datenschutzes zu stärken. Es sind seit dem Erscheinen des Buches von Helmut Bäumler im Jahr 2002 natürlich Fortschritte in der Schaffung von Awareness für Datenschutz erzielt worden, auch Vorfälle wie die Enthüllungen von Edward Snowden oder der Rechtsstreit von Maximilian Schrems gegen Facebook haben viele Bürger für das Thema sensibilisiert.
Dennoch ist das Ziel der Reise nicht erreicht: Es gilt, vor allem durch Maßnahmen im Bereich der Bildung, den Datenschutz und auch die IT-Sicherheit als wesentliche Zukunftsthemen in der Gesellschaft zu verankern.

6.2.3.5 IT-Schlüsselindustrien in Europa halten und ausbauen

Ein grundlegendes Problem für den europäischen Standort stellt das Faktum dar, dass sehr viele globale Player im Bereich der IT nicht (mehr) in Europa ansässig sind. Regelmäßig wird ein 'brain drain' in das Silicon Valley beklagt, im Rahmen dessen einzelne Experten oder ganze Unternehmen Europa verlassen würden.

Tatsächlich wird es für die EU und Österreich entscheidend sein, Schlüsselindustrien zu halten, zu stärken und neu aufzubauen. Nur wenn Entwicklung im eigenen Land bzw. in der Union stattfindet, gibt es überhaupt die Möglichkeit zu gestalten.
Dr. Helmut Bäumler bezeichnete dies als 'Anbietervielfalt'. [22]
Auch ULD-Leiterin Hansen wies im Gespräch auf das Problem fehlender europäischer Anbieter in der IT-Branche hin. Es sei eine 'gewisse Hoheit über die Entwicklung' notwendig. [34]
Abg. z. NR Himmelbauer betonte ebenso, dass es mehr europäischer Unternehmen und Services im Bereich Informationstechnologien bedürfe. [16]
Eine wesentliche Aufzählung der notwendigen Rahmenbedingungen, um vermehrt IKT-Unternehmen nach Europa zu locken bzw. deren Gründung und Aufbau zu initiieren, würde den Rahmen dieser Arbeit freilich sprengen. Nichtsdestotrotz können die Punkte dieses Modells, wie etwa effiziente Gesetzgebung, ein wirksames System an Gütesiegeln und Zertifizierungen, eine kooperative Datenschutzbehörde und viele weitere dazu beitragen, den Standortvorteil Europas und Österreichs herauszustreichen und somit dazu beizutragen, viele 'Silicon Valleys' mitten in der Union entstehen zu lassen.

6.2.3.6 Fazit - Strategische Rahmenbedingungen und Policies

Strategische Rahmenbedingungen und Policies, um Datenschutz und IT-Security als Standortvorteil zu nutzen, umfassen also:

- **Nationale IT-Sicherheitsstrategien und -politik gestalten.** Diese Strategien sollten gemäß des *NCSS-Lifecycles* entwickelt werden, um in der zweiten Schlüsselphase durch Evaluierung und Methoden wie *Effective Horizon Scanning* neuen Bedrohungen entgegenzutreten und neue Chancen erkennen zu können.

- **Stellenwert von Datenschutz und IT-Security in der Bildung verankern.** Durch Bildungsmaßnahmen soll die Wichtigkeit von Datenschutz und IT-Security langfristig verankert werden und sozusagen in die breite Bevölkerung und somit alle Akteursebenen 'einsickern'. Ebenso muss die Ausbildung von IT-Fachkräften und Akademikern gefördert werden, um genügend Experten zur Verfügung zu haben, damit Österreich und Europa im internationalen Wettbewerb überhaupt reüssieren können.

- **Stellenwert von Datenschutz und IT-Security in der Wirtschaft stärken.** Datenschutz darf in Unternehmen kein Thema für 'Einzelkämpfer' darstellen, sondern die Priorität muss von oberster Managementebene erkannt werden. Diese muss klare Zuständigkeiten benennen und wesentliche Entscheidungen selbst treffen. Auch IT-Sicherheit geht bereits Klein- und Mittelunternehmen an, hier muss die Awareness geschaffen und etwaige Möglichkeiten, etwa auch hochwertige Securitylösungen aus der Cloud, aufgezeigt werden. Ein grober Richtwert ist, 5-10 Prozent des gesamten IT-Budgets in den Bereich Cybersicherheit zu investieren.

- **Stellenwert von Datenschutz und IT-Security in der Gesellschaft heben.** Fehlendes Interesse an Datenschutz attestierte Helmut Bäumler den deutschen Verbrauchern bereits im Jahr 2002. In den vergangenen Jahren hat sich diese Awareness, teilweise durch negative Enthüllungen wie den Fall Snowden, verstärkt. Nichtsdestotrotz spielt Datenschutz (und auch IT-Sicherheit) im privaten Umfeld heutzutage eher erst nach negativen Erfahrungen eine Rolle, dem sogenannten *Privacy by Disaster*. Insofern muss, eben auch durch die erwähnten Bildungsmaßnahmen, der Stellenwert von Datenschutz und IT-Security, auch und besonders für die ältere Generation, gehoben werden.

- **IT-Schlüsselindustrien in Europa halten und ausbauen.** Viele globale Marktführer im IT-Bereich sind nicht (mehr) in Europa angesiedelt und viele innovative Menschen und Unternehmen wandern in Gebiete wie das Silicon Valley ab. Um diesen 'brain drain' aufzuhalten, müssen wichtige Schlüsselindustrien in Europa gehalten bzw. neu aufgebaut werden. Dazu ist eine Vielzahl von Rahmenbedingungen zu setzen, die Maßnahmen im Rahmen des Modells dieser Arbeit können einen Teil dazu beitragen.

6.2.4 Verzahnung Datenschutz & IT-Sicherheit

Die beiden großen Themenkomplexe dieser Arbeit, *Datenschutz* und *IT-Security*, wurden zu Beginn jeweils in einem eigenständigen Kapitel behandelt. Die hier angeführten Rahmenbedingungen verzichten in weiten Teilen aber auf eine Aufteilung in zwei Themengebiete und gliedert sich nach Bereichen, etwa technischer oder rechtlicher Art.
IT-Sicherheit und Datenschutz fallen beide unter das Dach der *Informationssicherheit* und sind teils eng ineinander verzahnt. So erwähnt die ENISA in ihrem 'Practical Guide' zur Entwicklung nationaler Cybersicherheitsstrategien als 18. Aktionspunkt Sicherheit mit Datenschutz in Einklang zu bringen. [17, S. 14]
Dr. Bäumler merkte bezüglich dem Verhältnis Datenschutz und IT-Sicherheit folgendes an: 'Die schönsten Datenschutz-Prinzipien, die nicht technisch nachvollziehbar, also datensicher, umgesetzt werden können, nützen nichts.' [22]
ULD-Zertifizierungsverantwortlicher Henry Krasemann bezeichnete Datensicherheit auch als Teil des Datenschutzes und brachte ein Beispiel zur Anonymisierung von Daten. Falls diese frühzeitig erfolgen würde, könnten weniger strenge Sicherheitsbestimmungen angewandt werden. Krasemann bezeichnete Datenschutz und Datensicherheit als durchaus eng miteinander zusammenhängend. [23]
Datenschutz und IT-Sicherheit sollten also keinesfalls als komplett deckungsgleiche Themen angesehen werden. Dennoch gibt es große Interdependenzen zwischen den beiden Bereichen, die in dieser Arbeit und im Modell aufgezeigt werden. Rahmenbedingungen zur Verbesserung des Datenschutzes als
Standortvorteil können nicht isoliert hinsichtlich der Maßnahmen für IT-Sicherheit zur selben Zielsetzung betrachtet werden, es bedarf also eines ganzheitlichen Ansatzes, um diese zwei Themen in Politik, Wirtschaft und Gesellschaft zu

verankern und die Standorte Europa bzw. Österreich zu stärken.

6.3 Fazit Erkenntnisableitung & europäische Perspektive

Im Rahmen dieses Kapitels wurde versucht, einen kurzen Aufriss über zu setzende Rahmenbedingungen zu geben, um Datenschutz und IT-Security weniger als regulatorische Hindernisse, sondern als echte Chancen für Österreich und Europa begreifen zu können.
Europa hat in vielen Bereichen grundsätzlich sehr gute Voraussetzungen, um einen Standortvorteil aus diesen Themen generieren zu können. Dazu zählt etwa ein hoher Stellenwert von Rechtssicherheit und deren guter Ruf, der grundsätzliche europäische Wertekanon und das Bewusstsein, dass Datenschutz und IT-Sicherheit Themen sind, die die gesamte Europäische Union betreffen, wie die DSGVO und die NIS-Richtlinie zeigen, so unterschiedlich diese auch bewertet werden. Diesen guten Ruf und die Vertrauenswürdigkeit zu nutzen, betont etwa auch die deutsche Cybersicherheitsstrategie. [26, S. 23]
Auch ULD-Leiterin Marit Hansen wies im Expertengespräch im Rahmen dieser Arbeit auf dieses potentielle Alleinstellungsmerkmal gegenüber außereuropäischen Regionen hin. [34]
Allerdings sind noch zahlreiche Herausforderungen zu bewältigen, bis aus den beiden Themen ein wirklicher, umfassender Wettbewerbsvorteil generiert werden kann. Dies beginnt im Bereich des mangelnden Datenschutzbewusstseins in weiten Teilen der Bevölkerung. Auch die Notwendigkeit für IT-Security muss, gerade bei privaten Personen und Klein- bzw. Mittelunternehmen in weiten Teilen stärker transportiert werden.
Ein weiteres Problem besteht darin, dass viele große IT-Unternehmen fernab des Standorts Europas sitzen. Um hier überhaupt Handlungsfähigkeit zu behalten, müssen IT-Schlüsselindustrien in Europa gehalten, gefördert und neu angesiedelt werden. Auch dieser Herausforderung wird man nur subsidiär begegnen können, um Anbietervielfalt in Europa zu ermöglichen.
Im Rahmen der Erkenntnisableitung wurden Teilbereiche identifiziert, in denen Rahmenbedingungen gestaltet werden müssen, um Datenschutz und Cybersecurity als Positiva darzustellen und als Standortvorteil nutzen zu können. Dazu zählen technische und rechtliche Bedingungen sowie strategische Faktoren, die sich in einen ganzheitlichen Ansatz einfügen. Dieser spiegelt sich grafisch im unten angeführten Modell wider. So können Datenschutz und IT-Security als Wettbewerbsvorteil für Europa begriffen und genutzt werden.
Ein politisches Ziel, das beispielsweise Eva-Maria Himmelbauer erwähnte, ist hierbei der *Digitale Binnenmarkt* für Europa. Hier könnte die Chance genutzt werden, den europäischen Markt als breiten Standort zur Verfügung zu haben, um hochqualitative IT-Services und Produkte anbieten zu können, die auch 'Europe based' über Europa hinaus global reüssieren können. [16]

7 Modell & Schulungstool Datenschutz & IT-Security als Standortvorteil

7.1 Beschreibung des Modells - Template

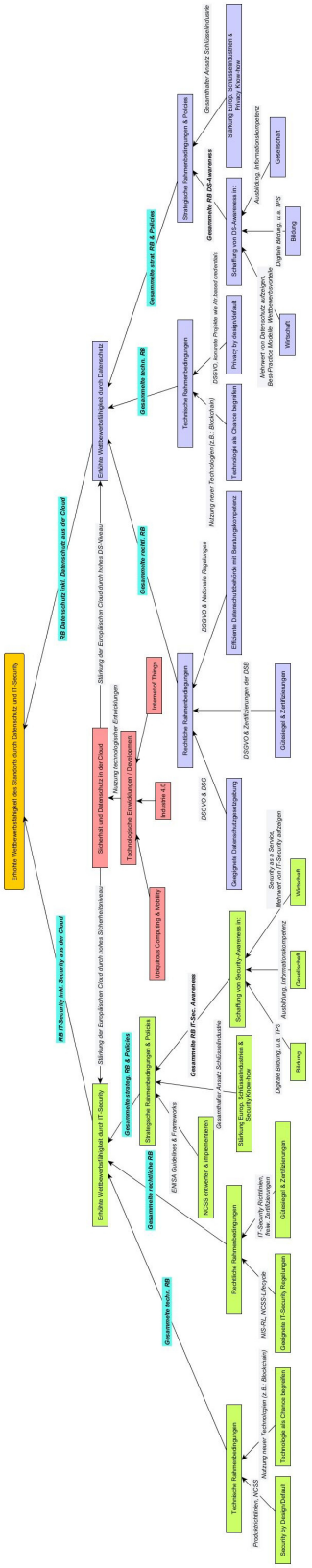
Im vorherigen Kapitel wurden zentrale Rahmenbedingungen aus den Bereichen Datenschutz und IT-Security identifiziert, die maßgeblich zu besseren Standort- und Wettbewerbsbedingungen für Österreich und Europa beitragen können. Daraus wird im Rahmen dieses Kapitels ein Modell entwickelt, welches die im Rahmen dieser Arbeit gewonnenen Erkenntnisse zusammenfassen und optisch aufbereiten soll.
Diesem Modell liegt eine subsidiäre Aufgaben- und Verantwortungsverteilung zugrunde, wie sie ausführlich im letzten Kapitel beschrieben wurde. Dies bedeutet, dass die Verantwortlichkeit für IT-Security und Datenschutz nicht 'von oben herab', also top-down bestehen, sondern dass jede Akteursebene, seien es etwa Behörden, Unternehmen oder Privatpersonen, die mit ihren technischen, zeitlichen und organisatorischen Fähigkeiten bewältigbaren Herausforderungen selbst begegnen sollen. Die quasi 'übergeordnete Stelle' soll und muss dann eingreifen, wenn die Kapazitäten der jeweiligen Akteursebene nicht ausreichen.
Das Modell ist grundsätzlich *bottom-up* gestaltet, da dies die Umstände der Realität grundsätzlich am besten widerspiegeln. Das bedeutet, dass die unterschiedlichen Rahmenbedingungen, die in den verschiedenen Bereichen zu setzen sind, sich gegenseitig ergänzen, quasi 'gebündelt' werden, und so auf das höhere Ziel hinwirken. Dies entspricht auch dem subsidiären Ansatz, aus den jeweiligen 'kleinen' Einheiten bzw. Akteuersebenen heraus Vorteile für den gesamten Standort zu generieren.
Die einzelnen Rahmenbedingungen wurden im letzten Kapitel ausführlich behandelt. In diesem Modell sind sie als **farbige Rechtecke** dargestellt und, um die optische Übersichtlichkeit zu steigern, farbig nach Themenbereichen aufgeschlüsselt.
Grün entspricht den zu setzenden Wettbewerbsfähigkeiten aus dem Bereich IT-Security, **blau** markiert sind zu setzende Eckpfeiler aus dem Bereich Datenschutz. Als 'Querschnittsmaterie' sind die Sicherheits- und Datenschutzrahmenbedingungen **rot** eingefärbt, das grundsätzlich zu erreichende Ziel erhöhter Wettbewerbsfähigkeit des Standorts entsprich dem **goldenen Rechteck**.

Um diese Rahmenbedingungen erreichen zu können, bedarf es etlicher zu setzender Maßnahmen, die ebenfalls im Rahmen der Identifikation im letzten Kapitel beschrieben wurden. Konkrete Tools, Ansätze, Strategien und Maßnahmen, die daraus identifiziert worden sind, sind im Modell als **bläulich hinterlegte, kursive Kantenbeschriftungen** dargestellt. Die bereits angesprochenen 'gebündelten' Maßnahmen, also beispielsweise die Kante von *Rechtliche Rahmenbedingungen* zur *Erhöhten Wettbewerbsfähigkeit durch Datenschutz* sind an den Kanten **türkis hinterlegt und fett-kursiv** markiert. Diese sollen die Maßnahmen, Tools, Strategien etc. der niedrigeren Ebenen sozusagen als

'Bündelung' darstellen.

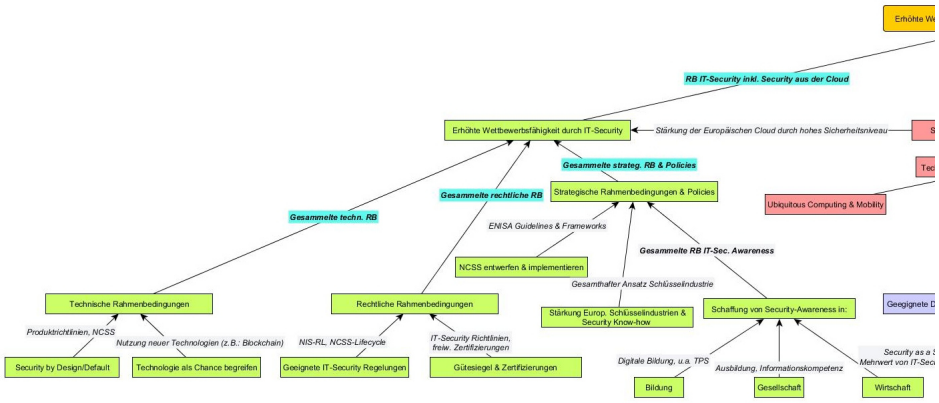
Auf der folgenden Seite ist das gesamte Modell dargestellt. Aus Gründen der Übersichtlichkeit werden auf den darauffolgenden Seiten die einzelnen Teilbereiche dargestellt und beschrieben.

7.1.1 Grafische Darstellungen des Modells



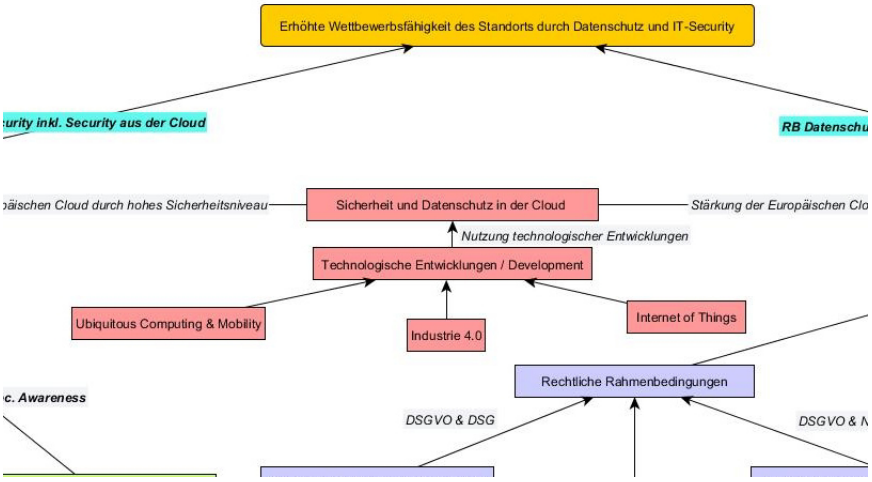
7.1.1.1 Bereich IT-Security - grün

Der 'grüne Ast' des Modells umfasst die Maßnahmen und Rahmenbedingungen aus dem Bereich der **IT-Security**. Diese werden, ebenso wie aufseiten des Datenschutzes, in *Technische Rahmenbedingungen*, *Rechtliche Rahmenbedingungen* sowie *Strategische Rahmenbedingungen und Policies* eingeteilt. Auf die Rahmenbedingungen und deren Bedeutung wurde im Detail bereits im vorherigen Kapitel eingegangen, wesentliche Maßnahmen, Tools, Strategien und Regelungen, um diese Eckpfeiler zu realisieren, umfassen etwa wohl durchdachte NCSS nach NCSS-Lifecycle, die Nutzung neuer Technologien für Security oder einen gesamthaften Ansatz zur Haltung und zum Ausbau von Schlüsselindustrien in Europa. Auch Tools wie das TPS können und müssen eine wesentliche Rolle beim Wissensaufbau und bei der Schaffung von Awareness spielen.



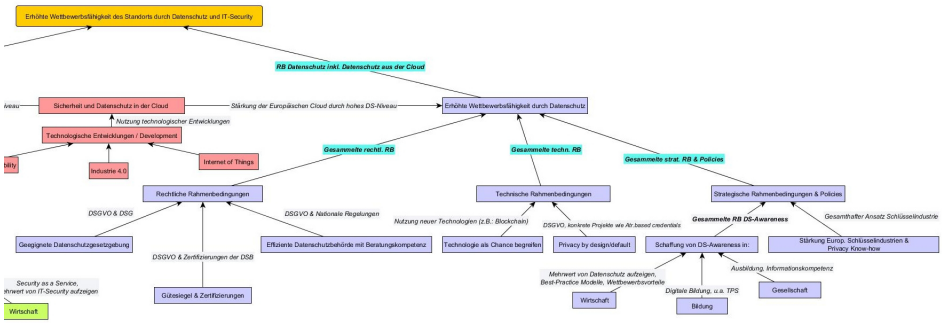
7.1.1.2 Bereich Cloud - rot

Der 'rote Bereich' des Modells repräsentiert den Einfluss der Cloud Computing-Technologien. Sehr viele Rahmenbedingungen und Maßnahmen zu Datenschutz und IT-Security wirken ebenso auf die Cloud bzw. beinhalten Maßnahmen Cloud-Technologien betreffend .
Dennoch sollen, ob des hohen Stellenwerts des Themas, Maßnahmen zur Stärkung der europäischen Cloud prominent und beide Themenbereiche, also Datenschutz und IT-Security betreffend, dargestellt werden. Dieser Teilbereich ist besonders stark von technologischen Entwicklungen, wie etwa Ubiquitous Computing, geprägt. Dies wird im Modell auch dargestellt.



7.1.1.3 Bereich Datenschutz - blau

Bläulich gefärbt sind die Maßnahmen aus dem Gebiet des Datenschutzes. Diese werden, ebenso wie aufseiten der IT-Security, in *Technische Rahmenbedingungen*, *Rechtliche Rahmenbedingungen* sowie *Strategische Rahmenbedingungen und Policies* eingeteilt. Auf die Rahmenbedingungen und deren Bedeutung wurde im Detail bereits im vorherigen Kapitel eingegangen, wesentliche Maßnahmen, Tools, Strategien und Regelungen, um diese Eckpfeiler zu realisieren, umfassen etwa die geeignete Datenschutzgesetzgebungen, diese Rolle kann die DSGVO durchaus einnehmen, die Etablierung von Datenschutzbehörden mit entsprechender Beratungskompetenz oder das Aufzeigen von Mehrwert durch Datenschutz in der Wirtschaft. Bei der für den Datenschutz im Vergleich zu IT-Security beinahe noch wichtigeren Schaffung von Awareness können und müssen Lerntools und Wissenssammlungen, wie beispielsweise das TPS, eine entsprechende Rolle einnehmen.



7.2 TPS - Tool for Privacy and Security as Competitive Advantage

Die im Rahmen dieser Arbeit gewonnenen Erkenntnisse und verfassten Zusammenfassungen von Information zu IT-Security, Datenschutz und deren Eignungen, als Wettbewerbsvorteil zu dienen, wurden ebenso in einem Webtool aufbereitet. Das **Tool for Privacy and Security as Competitve Advantage**, kurz **TPS**, verfolgt dabei folgende **Zielsetzungen**

- Generelle Aufbereitung von Information zu den Themen Datenschutz, IT-Security und Sicherheit bzw. Datenschutz in der Cloud zum Einstieg in die Materie. Ein Schwerpunkt wird auf aktuelle Richtlinien und Verordnungen, beispielsweise die NIS-RL und die DSGVO, gelegt.

- Selbstständiger und/oder angeleiteter Wissenserwerb im Rahmen der inhaltlichen Aufbereitungen und der Maßnahmen des Lerntools.

- Anreiz zur inhaltlichen Auseinandersetzungen und Diskussion über Datenschutz- und IT-Sicherheitsrahmenbedingungen im Standort Europa und Österreich

Dabei werden v.a. folgende **Zielgruppen** adressiert:

- *Anfänger ohne Vorwissen*: Personen, die sich bis dato nicht oder nur kaum mit Datenschutz und IT-Security beschäftigt haben, sollen mit den einsteigerfreundlichen Aufbereitungen ersten Kenntnisse erwerben. Ebenso soll Awareness für die Priorität der beiden Themen geschaffen werden und so der spezifische Nutzen von Datenschutz bzw. IT-Security für die breite Bevölkerung erklärt werden.

- *Erfahrenere User*: Personengruppen, die sich bereits mit IT-Sicherheit bzw. Datenschutz auseinandergesetzt haben, können mittels des Webtools ihre Kenntnisse vertiefen. Ebenso sollen sie dazu angeregt werden, die Möglichkeit, dass Datenschutz und IT-Sicherheit Wettbewerbsvorteile und weniger regulatorische Hindernisse darstellen können, (erstmalig) in Betracht zu ziehen. Zu dieser Zielgruppe können beispielsweise Hochschüler oder (Young) Professionals aus den Bereichen IT, Recht und Betriebswirtschaft zählen.

- *Vereins- bzw. Unternehmensverantwortliche*: Gerade in Bezug auf die DSGVO herrscht zurzeit oft Unklarheit für viele Unternehmer, Vereinsvorstände und andere Betroffene. Das Lerntool TPS und diese Arbeit sind naturgemäß nicht in der Lage, eine Rechtsberatung auch nur annähernd zu ersetzen, dennoch soll die Angst vor der Materie durch Wissensaufbau genommen werden. Auch diese Zielgruppe soll dazu angeregt werden, die Möglichkeit, dass Datenschutz und IT-Sicherheit Wettbewerbsvorteile und weniger regulatorische Hindernisse darstellen können, (erstmalig) in Betracht zu ziehen.

7.3 Anforderungsanalyse & Ziele/Nicht-Ziele nach IEEE-Standard

Um die im vorherigen Abschnitt bereits anvisierten Zielstellungen und adressierte Zielgruppen zu erreichen, ist eine Anforderungsanalyse im Rahmen der Toolentwicklung unabdingbar. Dafür müssen funktionale und nicht-funktionale Anforderungen, Beispiele von Anwendungsfällen sowie Ziele und Nicht-Ziele definiert werden.

7.3.0.1 Funktionale Anforderungen

Funktionale Anforderungen umfassen konkrete Funktionen, die das System leisten können muss. Solch funktionale Anforderungen umfassen etwa:

- TPS muss Eingaben des Users im Rahmen der interaktiven Komponenten, etwa der Tests, entgegennehmen und verarbeiten können.
- Neue Fragen für den interaktiven Bereich müssen einfach, etwa per .csv-Datei, in das Tool eingespielt werden können, um eine einfache Erweiterbarkeit zu gewährleisten.
- Das Tool muss entsprechende übersichtliche Darstellungsmöglichkeiten besitzen, um dem User fachliche Information zu den behandelten Themen zur Verfügung zu stellen.
- Das System muss dem User eine fachliche Einführung in die Materie, sowie einen umfangreichen Glossar mit entsprechenden Darstellungsoptionen zur Verfügung stellen.

7.3.0.2 Nicht-funktionale Anforderungen

Nicht-funktionale Anforderungen umfassen, im Unterschied zu den funktionalen Anforderungen, keine konkreten Use Cases sondern den Bereich, wie das System die Leistungen realisieren sollen muss.
Nicht-funktionale Anforderungen an das TPS umfassen:

- *Benutzbarkeit, Usability und Accessability*: Das Tool muss von einer Vielzahl von Benutzern von unterschiedlichen Endgeräten aus zugänglich und bedienbar sein.
- *Performanz*: Das TPS muss auch auf weniger leistungsfähigen Systemen gut bedienbar bleiben, um möglichst viele potentielle User erreichen zu können.
- *Robustheit und Fehleranfälligkeit*: Das TPS soll mittels bewährter, robuster Technologien entwickelt werden, um einen möglichst hohen Grad an Verfügbarkeit zu gewährleisten.

- *Änderbarkeit und Wartbarkeit*: TPS muss vonseiten des Administrators bzw. Seitenbetreibers leicht mit neuem Content bespielt werden können. Die Ebene der Darstellung soll, entsprechend dem Model View Controller-Muster, von der Ebene des Inhalts modular getrennt sein, um eine entsprechende Änderung in einem Bereich ohne gravierende Änderung auf die jeweils anderen zu ermöglichen.

7.3.0.3 Ziele und Nicht-Ziele

Im Zuge der Systementwicklung ist es im IT-Projektmanagement üblich, Ziele und Nicht-Ziele zu definieren.
Ziele des Systems umfassen:

- TPS soll dem User, anfangend vom Einsteiger in das Themengebiet bis zum fortgeschrittenen Kenner der Materie, übersichtlich und strukturiert Information zu IT-Security, Datenschutz und Cloud-Technologien und deren Potentiale als Wettbewerbsvorteil zur Verfügung stellen.
- Das Tool soll dem Benutzer im Rahmen eines Glossars eine kompakte und übersichtliche Information zu Fachbegriffen aus Datenschutz, IT-Security und Cloud Computing zur Verfügung stellen.
- Im Rahmen eines interaktiven Elements sollen User in mehreren, aufeinander aufbauenden Lernphasen Wissen zu den behandelten Themengebieten erwerben und testen können.
- Das Tool soll interessierten Benutzern darüber hinausgehend eine umfangreiche Link- und Informationssammlung mit weiterführenden Informationen zur Verfügung stellen.
- Außerdem soll TPS Verantwortliche in Unternehmen, Vereine und Organisationen bzw. interessierten Individuen v.a. hinsichtlich der DSGVO und ihre sich daraus ergebenden Rechte und Pflichten informieren.

Nicht-Ziele des Systems sind:

- TPS kann und soll keine Rechtsberatung zum Thema Datenschutz und IT-Security ersetzen.
- Das Tool soll nicht eins-zu-eins Gesetzestexte, Richtlinien oder Verordnungen wiedergeben.
- Das System soll keinen extrem hohen Detailgrad an Information bezüglich IT-Security und Datenschutz aufweisen.
- TPS soll kein moderiertes Forum, Gästebuch o.ä. umfassen.

7.4 Systemkonzeption & Entwicklung

Anhand dieser funktionalen und nicht-funktionalen Anforderungen sowie der Ziele und Nicht-Ziele wurde das TPS entwickelt. Aufgrund der Anforderungen im Bereich Benutzbarkeit, Performanz und Änderbarkeit bzw. Wartbarkeit wurde beschlossen, das TPS als Webservice zu implementieren.
Argumente dafür waren u.a. die einfache und schnelle Verfügbarkeit von unterschiedlichen Endgeräten aus, die robusten, plattformunabhängigen Technologien dahinter und die einfachere Wartbarkeit.
Als Auszeichnungs-, Skript- und als Stylesheet-Sprache wurden HTML, PHP und CSS ausgewählt. Ziel war, das TPS komplett neu zu konzipieren, ohne auf bestehende Vorlagen, Frameworks oder Style-Vorlagen zurückzugreifen. Grund dafür war u.a., dass dadurch das System maßgeschneidert an Anforderungen und Ziele bzw. Nicht-Ziele angepasst werden konnte. HTML für den Bereich des Contents, PHP als Skriptsprache und CSS für die Stylesheets stellt außerdem eine vielfach bewährte Technologiekombination dar.
Die Fragen zur Wissensüberprüfung werden mittels CSV-Dateien eingelesen und können so einfach erweitert bzw. abgeändert werden.
Parallel zur Entstehung des inhaltlichen Teils der Arbeit wurde, nachdem die Anforderungen und Ziele bereits definiert waren, sukzessive und in mehreren Iterationen das Tool TPS entwickelt. Nach Abschluss der Kapitel zu Datenschutz, IT-Security und Cloud Computing wurden die Inhalte für das TPS aufbereitet und in das System eingespielt.
Für die Entwicklung wurden die Tools *Brackets* und *notepad++* als Editoren sowie *xampp* als Apache-Webserver verwendet. Getestet wurde das Tool mittels den Browsern *Firefox*, *Chrome* sowie *Internet Explorer*.

7.5 Test

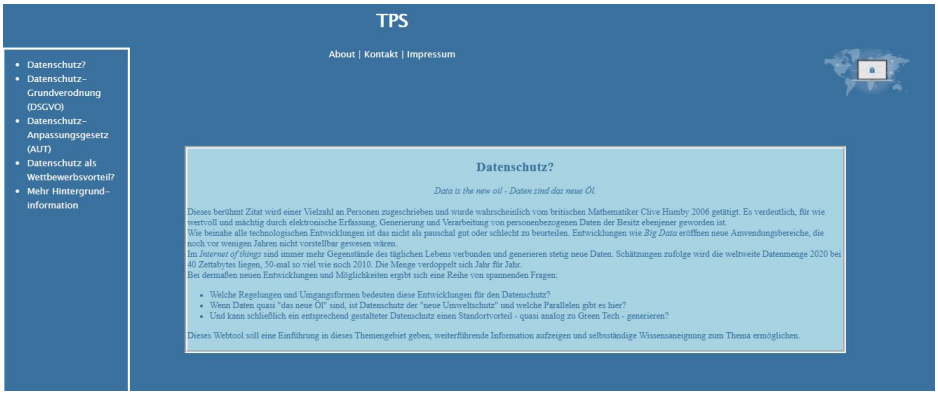
Das Tool wurde, wie bereits beschrieben, während der Entwicklung iterativ in mehreren Schritten überarbeitet. Die Systemkonzeption ist bereits oben angeführt, um die HTML- bzw. CSS-Darstellung zu überprüfen, wurde das *Brackets*-interne Feature der Livevorschau genutzt.
Da dieses Feature allerdings auf sich alleine gestellt keine PHP-Funktionalitäten testen kann, wurde mittels *xampp* ein Apache-Webserver gestartet und die Livevorschau von *Brackets* mit diesem verknüpft.
So konnte in den Browsern *Firefox*, *Chrome* sowie *Internet Explorer* eine Testung der PHP-Features erfolgen.
TPS lief auf all diesen Browsern problemlos und mit guter Performanz, die möglichst simple Darstellung war schließlich auch ein Entwicklungsziel.
Insgesamt lief das Tool bei der Testung auf drei verschiedenen PC-Systemen mit den drei oben angeführten Browsern in jeweils unterschiedlichen Versionen stabil und war voll funktionsfähig.

7.6 Tutorial

Das *Tool for Privacy and Security as a Competitive Advantage* bietet eine Vielzahl von Features.
Auf der Startseite gibt es (neben Menüpunkten wie About, Kontakt und Impressum) vier Menüpunkte:

Die Menüpunkte *Datenschutz und DSGVO*, *IT Security und NIS-Richtlinie* sowie *Sicherheit und Datenschutz in der Cloud* sind als Einführungskapitel in die jeweilige Materie zu betrachten und können unabhängig von anderen Features des Webtools betrachtet und studiert werden, fließen aber auch in die Wissenserwerbsphase des Lerntools ein.

Exemplarisch soll an dieser Stelle ein Screenshot eines solchen Kapitels gezeigt werden. Immer vorhanden ist auf der linken Seite eine Sidebar mit Übersichts-Links zu den Themen der Seite:

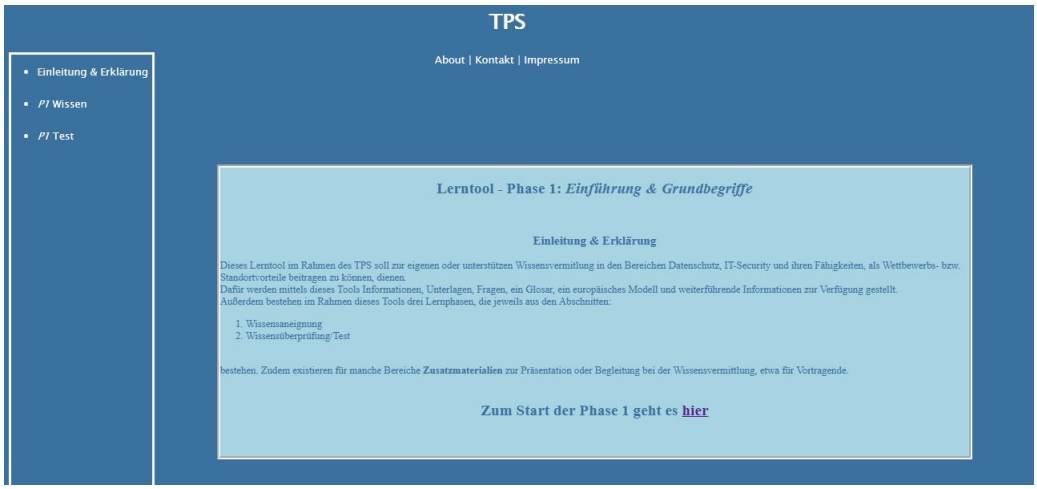


Ein zentrales Feature von TPS ist der Menüpunkt *Lerntool und Europäisches Standortmodell*, welches folgende Unterpunkte beinhaltet:

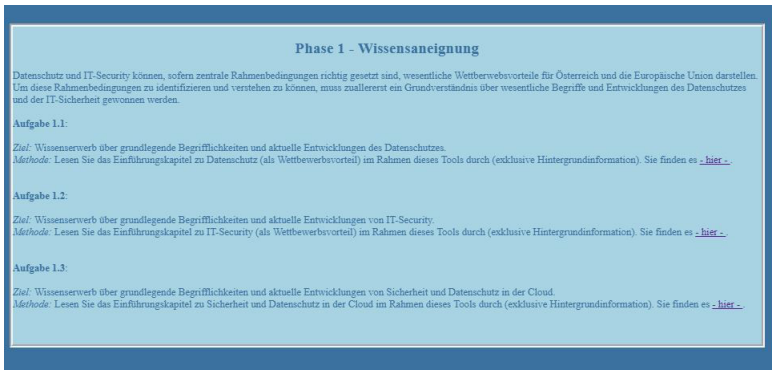
- Europäisches Modell: Datenschutz und IT Sicherheit als Standortvorteil
- Das **Lerntool** mit seinen drei Lernphasen *P1 - Einführung und Grundbegriffe*, *P2 - Europäische Grundlagen*, *P3 - Rahmenbedingungen für Standortvorteile* und schließlich der *Case Study*.
- *DSGVO - was ist neu?* - Quickchecks für Unternehmer, User und Vereinsverantwortliche.
- Ein umfangreiches *Glossar*
- Weiterführende Information mittels *Linksammlung und Literaturempfehlung*

An dieser Stelle sei exemplarisch die Phase 1 des **Lerntools** gezeigt. Eine Phase besteht immer aus dem Wissenserwerb und der anschließenden Wissensüberprüfung mittels eines Quiz.

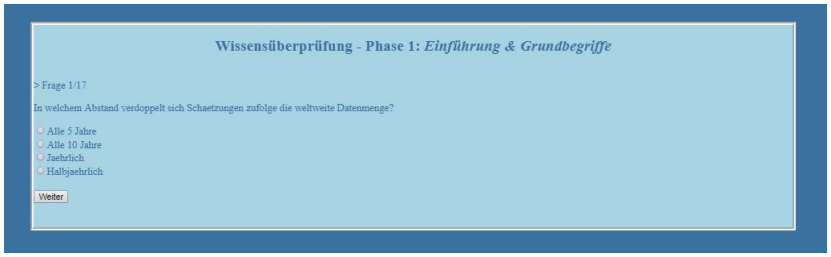
Dies sieht für die Phase 1 etwa so aus:



Die Aufgaben einer Phase sehen beispielhaft wie folgt aus, es sind jeweils für den Wissenserwerb aufbereitete Lernunterlagen verlinkt:

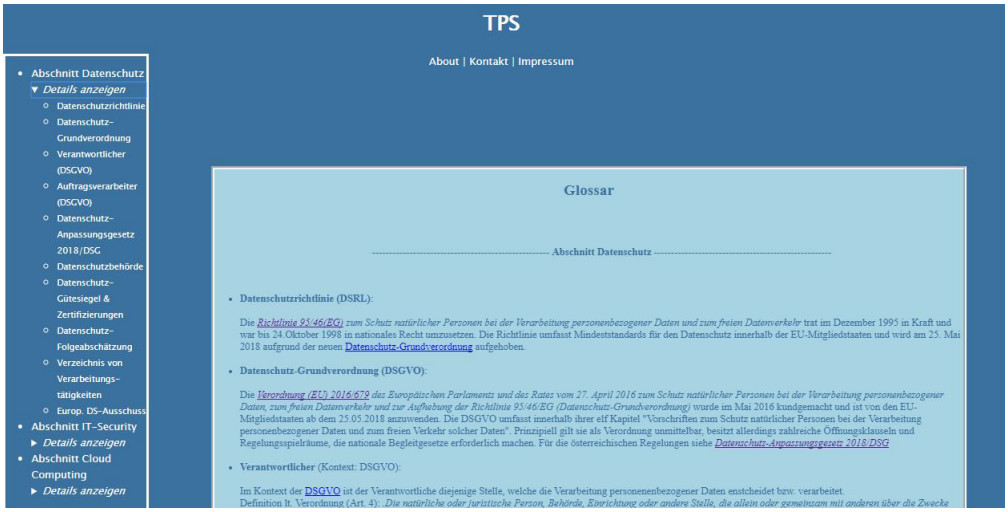


Anschließend kann mit mit Klick auf *Start Quiz* die Wissensüberprüfung beginnen, im Rahmen derer Single-Choice-Fragen zum erworbenen Wissen abgeprüft werden:



Phase 3 und Case Study unterscheiden sich insofern von der ersten beiden Phasen, als dass keine richtig/falsch Fragen existieren, sondern offene Fragen und Handlungsanweisungen mit Lösungsansätzen, die zur kritischen Beschäftigung mit der Materie einladen sollen.
Weitere, bereits erwähnte Features neben den Phasen mit ihren eigens aufbereiteten Unterlagen und Tests sind der Quickcheck (DSGVO - was tun?), das Modell, eine Link- bzw. Literatursammlung sowie ein Glossar, die alle mit intuitiven Sidebar-Elementen überblickt werden können.

Anbei ist exemplarisch ein Teil des Glossars dargestellt:



Grundsätzlich wurde versucht, das TPS mit einem möglichst hohen Maß an Usability und Accessability zu gestalten.

8 Zusammenfassung

Im Rahmen dieser Arbeit wurde eine breite und detaillierte Übersicht über die Themenfelder Datenschutz und IT-Security gegeben, aktuelle Entwicklungen in den beiden Feldern miteinbezogen und ihre Fähigkeit, einen Standortvorteil darstellen zu können, beleuchtet.
Das erste große Kapitel beschäftigte sich dabei mit dem Datenschutz als Wettbewerbs- und Standortvorteil. Nach einem kurzen historischen Überblick wurde dabei vor allem auf die hochaktuelle Datenschutz-Grundverordnung der Europäischen Union eingegangen und diese inhaltlich zusammengefasst sowie analysiert.
Die begleitenden nationalen Gesetzesregelungen, das Maßnahmenpaket 'Datenschutz-Anpassungsgesetz 2018', fanden mit Zusammenfassung und Analyse ebenso Einzug in die Arbeit. Um eine globale Perspektive zu ermöglichen, beendete eine Betrachtung der Situation des Datenschutzes in den USA und anderen Regionen der Welt das Kapitel.
Das zweite inhaltliche Hauptkapitel befasste sich mit IT-Security als Wettbewerbsvorteil. Dabei wurden drei aktuelle nationale Cybersicherheitsstrategien zusammengefasst und verglichen, und zwar jene von Österreich, Deutschland und Großbritannien. Zuvor wurden Richtlinien und strategische Hilfestellungen der zuständigen Behörde der EU, der ENISA, für die Erstellung einer solchen NCSS kompakt zusammengefasst.
Die für die IT-Sicherheit sehr relevante und aktuelle NIS-Richtlinie der Union fand mit Zusammenfassung und Analyse ebenso Eingang in dieses Kapitel.
Anschließend folgte das Kapitel 'Datenschutz und Sicherheit in der Cloud'. Innerhalb dessen wurden, nach einer kurzen thematischen Einführung zur Erklärung von Funktionsweisen und Grundbegriffen, Datenschutz- und Sicherheitsanforderungen an Cloud Computing formuliert.
Aus den daraus gewonnenen Erkenntnissen und den vier im Rahmen dieser Arbeit geführten Experteninterviews wurden zu setzende Rahmenbedingungen für einen Standortvorteil für Datenschutz bzw. IT-Security in Österreich und Europa definiert. Diese gliederten sich in rechtliche, technische und strategische Rahmenbedingungen, welche jeweils ausformuliert und am Ende des Abschnitts zusammengefasst wurden.
Aus diesen Rahmenbedingungen wurde das (grafische) Modell entwickelt, welches *bottom up* die zu setzenden Schritte und Tools bzw. Maßnahmen in einer baumartigen Struktur beinhaltet.
Zusätzlich wurde das Webtool TPS zur Wissensaneignung, Überprüfung und weiteren Beschäftigung mit den Themen Datenschutz, IT-Security und Cloud Computing Technologien allgemein und deren mögliche Wirkung als Standortvorteile realisiert.
Im Rahmen dieser Masterarbeit wurde außerdem das *Tool for Privacy and Security as Competitive Advantage*, kurz **TPS** entwickelt. Mittels dieses Tools ist ein selbstständiger Wissens- und Kompetenzerwerb im Rahmen der Themenfelder Datenschutz, IT-Security und deren Fähigkeit, einen Wettbewerbsvorteil darzustellen, möglich.

Das Tool und dessen Entwicklung und Features wurde ebenso in dieser Arbeit beschrieben und ein bebildertes Tutorial zur Verfügung gestellt.

9 Conclusio

Datenschutz und IT-Security als Standortvorteile für Europa?
Das Ziel dieser Arbeit war es zu untersuchen, ob diese beiden Themenkomplexe weniger als regulatorische Hindernisse, denn als reelle *USPs* und Vorteile für den Standort Österreich bzw. Europa dienen können.
Nach Recherche und empirischer Arbeit fällt das Urteil darüber positiv aus.
Zuerst zum Thema Datenschutz:
Wie bereits mehrmals im Rahmen dieser Masterarbeit geschrieben ist gerade der Datenschutz ein Themengebiet, bei dem mannigfaltige Interessen zusammenprallen. Das zeigt sich bereits eindrucksvoll bei den höchst unterschiedlichen Stellungnahmen und Meinungen zur Datenschutz-Grundverordnung, deren Bandbreite von 'sehr gelungen' bis 'katastrophal' reicht. Im globalen Vergleich kann man allerdings festhalten, dass sich die Europäische Union immerhin mit dem Thema auf großer Bühne beschäftigt und sicherlich einige interessante Konzepte aufgegriffen hat. Ob das große Ziel der EU-weiten Harmonisierung des Datenschutzrechts aufgrund der zahlreichen Öffnungsklauseln und Regelungsspielräume näher rückt, darf bezweifelt werden. Dem gegenüber steht allerdings das valide Argument, dass ein gewisses Maß an Flexibilität nationalstaatliche Besonderheiten bzw. Schwerpunkte besser abbilden kann und so das Prinzip der Subsidiarität - mehr dazu später in dieser Conclusio - zumindest teilweise realisiert.
Im Vergleich zu ähnlich großen Wirtschaftsräumen, wie den USA oder der Volksrepublik China, kann Datenschutz aber definitiv ein Positivum für den Standort Europa darstellen, gerade aufgrund der hohen Rechtssicherheit, des guten Rufs und der demokratischen Strukturen.

Auch IT-Security gewinnt in Zeiten eines stetig steigenden Grades an Vernetzung immer mehr an Bedeutung. Die staatliche Ebene ist laut der ab Mai 2018 umzusetzenden NIS-Richtlinie verpflichtet, neben der Benennung von Betreibern *wesentlicher Dienste* eine nationale Strategie zum Schutz von Netz- und Informationssystemen vorzulegen.
Solch nationale Cybersecurity-Strategien (NCSS) sind bereits in vielen Mitgliedstaaten der Union in unterschiedlichen Iterationsstufen vorhanden und können einen wesentlichen Beitrag dazu liefern, durch eine ganzheitliche Betrachtung die 'Pflicht zur Cybersecurity' in einen echten Standortvorteil umzuwandeln.
Eine Vorbildrolle in Sachen NCSS kann von den untersuchten Ländern jedenfalls Großbritannien attestiert werden, das *world's leading digital nation* werden will. Gerade die Vermarktung von Cybersecurity-Lösungen und der Anspruch, bestmögliche Rahmenbedingungen für wirtschaftliche Tätigkeiten im Cyberspace bieten zu wollen, zeigt, dass ein hoher Grad an IT-Security durchaus - zumindest in planerischer Hinsicht - als Standortvorteil angestrebt wird.
Insofern wird auch die NIS-Richtlinie größtenteils sehr positiv rezipiert, ein vorgegebenes einheitlich hohes Schutzniveau an Netz- und Informationssicherheit in den EU-Mitgliedsstaaten wirkt sich auch auf die Fähigkeit aus, im (globalen) Vergleich IT-Security als Standortvorteil realisieren zu können.

Bei näherer Beschäftigung mit den Themen Datenschutz bzw. IT-Sicherheit darf eine Betrachtung der Auswirkungen von Cloud Computing-Technologien auf diese beiden Bereiche ebenso nicht fehlen. Durch massive Wachstumsraten, im privaten und unternehmerischen Sektor, ist die 'Cloud' in unseren Alltag mehr integriert, als je zuvor.
Der unbestrittenen Praktikabilität stehen dabei oft Datenschutz- und Sicherheitsbedenken entgegen. Hier gilt es festzuhalten, dass Cloud-Technologien nicht per se schlecht für Datenschutz oder Cybersecurity sind, oft ist sogar das Gegenteil der Fall. Sicherheitslösungen aus der Cloud können in vielen Fällen quasi *Security as a Service* anbieten. Gerade viele KMUs können durch die Nutzung der Cloud einen höheren Sicherheitsgrad für personenbezogene Daten und Geschäftsinterna gewinnen, als durch die bescheidenen Aufbaumöglichkeiten einer eigenen IT-Infrastruktur. Der Einsatz sollte jedoch stets mittels einer ganzheitlichen Cloud-Strategie durchgeführt werden, an der es aktuell gerade bei KMUs noch fehlt.
Cloud Computing steht der These von Datenschutz und IT-Sicherheit als Wettbewerbsvorteil also nicht entgegen, ganz im Gegenteil. Charakteristika wie ein hohes Niveau an Datenschutz, ein exzellenter Ruf und starke Cybersecurity können für viele Privat- und Unternehmenskunden einen Anreiz bieten, Dienste und Ressourcen der 'Europäischen Cloud' in Anspruch nehmen zu wollen.
Initiativen wie *Cloud Made In Austria* beweisen, dass dieser Standortvorteil bereits im Marketing angekommen ist.
Der empirische Teil dieser Arbeit umfasst unter anderem vier Expertengespräche, etwa mit Dr. Helmut Bäumler, Abg. z. NR. Eva-Maria Himmelbauer oder Dipl.-Inf. Marit Hansen. Der dabei gewonnene Einblick auf Datenschützerseite zeigt die wichtige Erkenntnis, wie eine innovative Behörde, im konkreten Fall das ULD Schleswig-Holstein, eine Pionierrolle der Datenschutzgesetzgebung spielen und trotz strenger Prüfungen eine ausgezeichnete Kommunikationsbasis zur Wirtschaft aufbauen konnte. Marktwirtschaftliche Datenschutz, so Dr. Bäumler der Pionier auf diesem Gebiet, würde mit dem Interesse der Verbraucher stehen und fallen. Interesse und die Awareness für das Thema seien aber nie wirklich in der breiten Bevölkerung angekommen.
Abg. z. NR. Eva-Maria Himmelbauer, ÖVP-Verhandlerin für das österreichische Datenschutz-Anpassungsgesetz 2018, verortete die Awareness als Generationenfrage. Bei HTL-Schülern sei etwa schon sehr viel an Wissen zu Datenschutz und Informationssicherheit vorhanden. Ebenso betonte sie die Bedeutung von IT-Schwerpunkten in der Bildung, die über Skills wie Programmieren hinausgehen auch beispielsweise IT-Ethik umfassen müssten.

Aus all diesen Erkenntnissen ergaben sich zu setzende rechtliche, technische und strategische Rahmenbedingungen und ein subsidiärer Ansatz für Datenschutz und IT-Security. Das bedeutet, dass Datenschutz bzw. IT-Sicherheit nicht ausschließlich 'von oben herab' verordnet werden kann, sondern Verantwortlichkeiten auf den unterschiedlichsten Akteursebenen, wie Staat, Unternehmen und Bürger verankert sind.
Natürlich sind die Möglichkeiten der jeweiligen Akteursebene, beispielsweise

des Individuums, meist begrenzt. In diesem Falle müssen - ganz im Sinne der Subsidiarität - 'höhere' Ebenen, zum Beispiel der Staat bzw. seine Behörden unterstützend eingreifen, wie z.B. bei einer Cyberattacke auf ein KMU. Dennoch ist es wichtig zu begreifen, dass alle Stakeholder die Aufgaben in ihrem Bereich bestmöglich bewältigen, damit schlicht kein schwächstes Glied der Kette existiert. So kann man die Angst vor der Nutzung neuer Technologien nehmen, personenbezogene Daten adäquat schützen, innovative Wirtschaftszweige fördern und damit einen **ROI** auf Datenschutz und IT-Sicherheit erzielen.

Geleitet von diesem subsidiären Grundsatz bilden die rechtlichen, technischen und strategischen Rahmenbedingungen bzw. Policies die Eckpfeiler, um solch einen Standortvorteil für Österreich bzw. die EU erreichen zu können. Exemplarische Beispiele für solche Bedingungen sind effiziente Datenschutzbehörden mit Beratungskompetenz, der geeignete Einsatz von Datenschutzgütesiegeln und -zertifizierungen, das Verfolgen eines *Privacy by Design bzw. Default*-Ansatzes oder der Ausbau von IT-Schlüsselindustrien in Europa.
Aus diesen Bedingungen ergibt sich das grafisch dargestellte europäische Modell, dass vor allem eines zeigt:
Datenschutz und IT-Security sind keine isoliert zu betrachtenden Themen. Um einen echten Standortvorteil aus diesen Faktoren zu generieren, dürfen sie nicht ausschließlich etwa bloß als technische oder nur als rechtliche Bereiche oder nur den Staat angehend betrachtet werden.
Datenschutz und IT-Sicherheit sind auch keine Themen, die von einer staatlichen Instanz einfach kurzfristig verordnet werden können, um hier einen Wettbewerbsvorteil generieren zu können.
Denn schon das grafische Modell zeigt: Um diese beiden Faktoren als Standortvorteile nutzen zu können, ist ein *bottum-up* Ansatz notwendig. Viele Stakeholder und Akteure müssen zahlreiche Maßnahmen treffen, um schlussendlich im Zusammenwirken echte Vorteile entstehen lassen zu können.
Europa und Österreich haben in vielen Bereichen sehr gute Voraussetzungen, als Region mit hoher Rechtssicherheit, gutem Ruf und exzellent ausgebildeten Fachkräften ein hohes Niveau an Datenschutz und IT-Sicherheit als USP zu etablieren.
Zweifellos existieren auch große Herausforderungen, etwa bei der Ansiedlung von IT-Schlüsselindustrien oder der Awareness in Bevölkerung und Wirtschaft für diese Themen. Diese erscheinen bei näherer Betrachtung allerdings nicht unüberwindbar.
Es gilt allerdings noch viel zu tun, um eine entsprechend breite Awareness zu schaffen, damit schlussendlich ein **Return On Investment** auf Datenschutz und IT-Security generiert werden kann. Handlungen in diesen Feldern sind sowieso zu setzen, es gilt nun, diese auch entsprechend den obigen Zielvorgaben zu gestalten.
Diese Arbeit soll in Verbindung mit dem Webtool TPS, das speziell für dieses Themenfeld aufbereitete Information enthält, einen kleinen Teil zur Verbesserung der Situation beitragen.

10 Quellenangabe

References

[1] Computer Emergency Response Team Austria. *NIS-Richtlinie: Umsetzung aus österreichischer Sicht*. Jan. 23, 2017. URL: https://cert.at/reports/report_2016_chap04/content.html (visited on 09/01/2017).

[2] Helmut Bäumler. *Datenschutz als Wettbewerbsvorteil. Privacy sells: Mit modernen Datenschutzkomponenten Erfolg beim Kunden*. Ed. by Albert von Mutius. Vol. 1st. Friedr. Vieweg & Sohn Verlagsgesellschaft mbH, 2002. 248 pp. ISBN: 978-3-322-90278-8.

[3] *Bericht Cyber Sicherheit 2017*. Tech. rep. Cyber Sicherheit Steuerungsgruppe / BKA, May 1, 2017.

[4] Danny Boyle and Ben Farmer. "HMS Queen Elizabeth is 'running outdated Windows XP', raising cyber attack fears". In: *The Telegraph* (June 27, 2017). URL: http://www.telegraph.co.uk/news/2017/06/27/hms-queen-elizabeth-running-outdated-windows-xp-software-raising/ (visited on 10/01/2017).

[5] Abt. IV/6 Bundeskanzleramt Österreich. *Österreichische Strategie für Cyber Sicherheit*. Tech. rep. Erarbeitet in Kooperation von: Bundeskanzleramt Österreich; Bundesministerium für europäische und internationale Angelegenheiten; Bundesministerium für Inneres; Bundesministerium für Landesverteidigung und Sport. Wien: Bundeskanzleramt Österreich, Sektion IV - Koordination, Abteilung IV/6 - Sicherheitspolitische Angelegenheiten, 2013.

[6] Bundesverfassungsgericht. *Urteil vom 15.12.1983, 1 BvR 209/83 u. a. - Volkszählungsurteil*. Dec. 15, 1983.

[7] National security Cabinet Office and The Rt Hon Philip Hammond MP intelligence HM Treasury. *National Cyber Security Strategy 2016-2021*. Tech. rep. Cabinet Office, National security and intelligence, HM Treasury, The Rt Hon Philip Hammond MP, Nov. 1, 2016.

[8] National security Cabinet Office and The Rt Hon Philip Hammond MP intelligence HM Treasury. *Policy paper National Cyber Security Strategy 2016 to 2021*. Ed. by National security Cabinet Office and The Rt Hon Philip Hammond MP intelligence HM Treasury. Nov. 1, 2016. URL: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 (visited on 04/30/2016).

[9] Jonathan Chester. "How The Blockchain Will Secure Your Online Identity". In: *Forbes* (Mar. 3, 2017). URL: https://www.forbes.com/sites/jonathanchester/2017/03/03/how-the-blockchain-will-secure-your-online-identity/#7206856e5523 (visited on 10/03/2017).

[10] Stefan Christmann et al. “Datensicherheit und Datenschutz im Cloud Computing — Risiken und Kriterien zur Anbieterauswahl”. In: *HMD Praxis der Wirtschaftsinformatik* 47 (5 Oct. 1, 2010), pp. 62–70.

[11] “Cybersicherheitsgesetz verzögert sich, Begutachtung im 2. Halbjahr”. In: *derStandard.at* (Jan. 13, 2017).

[12] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, ed. *Wir über uns*. URL: https://www.datenschutzzentrum.de/ueber-uns (visited on 05/17/2017).

[13] Die Bundesbeauftragte für Datenschutz und Informationsfreiheit, ed. *EU-US Privacy Shield und Datenübermittlungen in die USA*. URL: https://www.bfdi.bund.de/DE/Europa_International/International/Artikel/EU-US_PrivacyShield_Daten%C3%BCbermittlungenUSA.html?nn=5217132 (visited on 05/01/2017).

[14] Die Bundesbeauftragte für Datenschutz und Informationsfreiheit, ed. *Safe Harbor und Schrems-Urteil des EuGH*. URL: https://www.bfdi.bund.de/DE/Europa_International/International/Artikel/SafeHarbor.html?nn=5217132#Start (visited on 05/01/2017).

[15] ENISA, ed. *About ENISA*. URL: https://www.enisa.europa.eu/about-enisa (visited on 04/30/2017).

[16] Paul Rockenbauer Eva-Maria Himmelbauer. *Interview mit Abg. z. NR Eva-Maria Himmelbauer, BSc*. Angeführt im Anhang dieser Masterarbeit. 2017.

[17] Nicole Fallessi et al. *National Cyber Security Strategies. Practical Guide on Development and Execution*. Tech. rep. ENISA, Dec. 1, 2012.

[18] Thomas Feil. *NIS-Richtlinie und IT-Sicherheitsgesetz: Ein Vergleich*. Jan. 5, 2016. URL: https://www.recht-freundlich.de/nis-richtlinie/nis-richtlinie-und-it-sicherheitsgesetz-ein-vergleich#Zusammenfassung (visited on 07/31/2017).

[19] Futurezone GmbH, ed. *Österreichisches Hacker-Nationalteam ist Europameister*. Oct. 23, 2015. URL: https://futurezone.at/digital-life/oesterreichisches-hacker-nationalteam-ist-europameister/160.048.827 (visited on 10/08/2017).

[20] *Guide to the EU-U.S. Privacy Shield*. Tech. rep. European Commission, 2016. DOI: 10.2838/199012.

[21] Dagmar Hartge. *Geschichte des Datenschutzes und der Dienststelle*. Land Brandenburg - Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht. 2017. URL: http://www.lda.brandenburg.de/cms/detail.php/bb1.c.251507.de.

[22] Paul Rockenbauer Helmut Bäumler. *Interview mit Dr. Helmut Bäumler*. Angeführt im Anhang dieser Masterarbeit. 2017.

[23] Paul Rockenbauer Henry Krasemann. *Interview mit Henry Krasemann*. Angeführt im Anhang dieser Masterarbeit. 2017.

[24] Papst Johannes Paul II., ed. *Codex Iuris Canonici*. 1983.

[25] Bundesministerium des Innern. *Chancen und Potentiale der Digitalisierung ausschöpfen. Bundeskabinett beschließt "Cyber-Sicherheitsstrategie für Deutschland 2016"*. Ed. by Bundesministerium des Innern. Nov. 9, 2016. URL: http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2016/11/cybersicherheitsstrategie-vorstellung.html (visited on 04/27/2017).

[26] Bundesministerum des Innern. *Cyber-Sicherheitsstrategie für Deutschland. 2016*. Tech. rep. Berlin: Bundesministerum des Innern, Nov. 1, 2016.

[27] Alexander Janda. *Digitale Sicherheit: Enquete des KSÖ zum Cyber-Gesetz. Digitale Sicherheit als Standortfaktor, der erhalten und ausgebaut werden muss*. Ed. by Kuratorium Sicheres Österreich (KSÖ). OTS. June 13, 2016.

[28] Stefan Fenz und Johannes Goellner und Gerald Quirchmayr et.al. *Cloud Sicherheit - Leitfaden für Behörden und Klein- und Mittelbetriebe*. Ed. by Johannes Goellner und Stefan Fenz und Gerald Quirchmayr. Sept. 1, 2014. ISBN: 978-3-902944-44-3.

[29] Universität Kassel. *Studie: EU-Datenschutz-Grundverordnung verfehlt alle Ziele – Kasseler Juristen entwirren Rechtslage*. Sept. 27, 2016. URL: https://www.uni-kassel.de/uni/nc/universitaet/nachrichten/article/studie-eu-datenschutz-grundverordnung-verfehlt-alle-ziele-kasseler-juristen-entwirren-rechtslag.html (visited on 08/20/2017).

[30] Europäische Kommission. *2000/520/EG. Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des "sicheren Hafens" und der diesbezüglichen "Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA*. Ed. by Europäische Kommission. July 26, 2000.

[31] Arthur D. Little and Wirtschaftskammer Österreich. *Digitale Transformation von KMUs in Österreich - 2017. Erhebung des Digitalisierungsstatus*. Tech. rep. Sept. 1, 2017.

[32] Dimitra Liveri and Anna Sarri. *An evaluation Framework for National Cyber Security Strategies*. Tech. rep. ENISA, Nov. 1, 2014. DOI: 10.2824/3903.

[33] Dimitra Liveri and Anna Sarri. *Annex A: Mapping of cybersecurity strategies*. Tech. rep. Annex of: An evaluation Framework for National Cyber Security Strategies. ENISA, Nov. 1, 2014. DOI: 10.2824/3903.

[34] Paul Rockenbauer Marit Hansen. *Interview mit Dipl.-Inf. Marit Hansen*. Angeführt im Anhang dieser Masterarbeit. 2017.

[35] Peter Mell, Tim Grance, et al. "The NIST definition of cloud computing". In: (2011).

[36] orf.at, ed. *Wie gut sind die neuen Regeln?* Dec. 16, 2015. URL: http://orf.at/stories/2314998/2314987 (visited on 08/19/2017).

[37] Republik Österreich, ed. *Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird. Datenschutz-Anpassungsgesetz 2018.* Titel des Gesetztes lautet 'Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG)'. 2017.

[38] Wirtschaftskamme Österreich, ed. *NIS-Richtlinie der EU in Kraft getreten – was bedeutet sie für KMU?* Oct. 10, 2016. URL: https://www.wko.at/Content.Node/blogs/it-safe/NIS-Richtlinie-der-EU.html (visited on 07/10/2017).

[39] "Österreichische Firmen haben beim Datenschutz Nachholbedarf". In: *derStandard.at* (Apr. 18, 2017). URL: http://derstandard.at/2000056120158/Oesterreichische-Firmen-haben-beim-Datenschutz-Nachholbedarf (visited on 09/15/2017).

[40] "Österreichs Unternehmen sind bei IT-Sicherheit Nachzügler". In: *derStandard.at* (May 26, 2017). URL: http://derstandard.at/2000058280565/Oesterreichs-Unternehmen-sind-bei-IT-Sicherheit-Nachzuegler (visited on 08/20/2017).

[41] Parlamentsdirektion. *Nationalrat verabschiedet umfangreiche Novelle zum Datenschutzgesetz. (PK-Nr. 829).* 2017. URL: https://www.parlament.gv.at/PAKT/PR/JAHR_2017/PK0829/ (visited on 06/29/2017).

[42] Parlamentsdirektion. *Parlamentarisches Verfahren - Datenschutz-Anpassungsgesetz 2018. (1664 d.B.)* 2017. URL: https://www.parlament.gv.at/PAKT/VHG/XXV/I/I_01664/index.shtml#tab-ParlamentarischesVerfahren (visited on 07/16/2017).

[43] Parlamentsdirektion. *Stellungnahmen zum Ministerialentwurf 322 - Datenschutz-Anpassungsgesetz 2018. (322/ME).* 2017. URL: https://www.parlament.gv.at/PAKT/VHG/XXV/ME/ME_00322/index.shtml (visited on 06/23/2017).

[44] Parlamentsdirektion. *Übersicht - Ausschussbericht - Datenschutz-Anpassungsgesetz 2018. 1761 d.B.* 2017. URL: https://www.parlament.gv.at/PAKT/VHG/XXV/I/I_01761/index.shtml (visited on 07/16/2017).

[45] Parlamentsdirektion. *Übersicht - Datenschutz-Anpassungsgesetz 2018. (1664 d.B.)* 2017. URL: https://www.parlament.gv.at/PAKT/VHG/XXV/I/I_01664/index.shtml#tab-Uebersicht (visited on 07/16/2017).

[46] Article 29 Data Protection Working Party. *WP 238. Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision.* Tech. rep. Apr. 13, 2016.

[47] Hans Zeger und Philipp Hochstöger. *Stellungnahme zum Entwurf eines Bundesgesetzes, mit dem das Bundes-Verfassungsgesetz geändert, das Datenschutzgesetz erlassen unds das Datenschutzgesetz 2000 aufgehoben wird (Datenschutz-Anpassungsgesetz 2018, DSG 2018).* Ed. by ARGE DATEN - Österreichische Gesellschaft für Datenschutz. June 23, 2017.

[48] Michael Rath. “Massenhaft Nutzer – mangelhafter Datenschutz”. In: *Computerwoche* (Aug. 19, 2012).

[49] *Richtlinie 95/46/EG*. Oct. 24, 1995.

[50] *Richtlinie (EU) 2015/153. Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft*. 2015.

[51] *Richtlinie (EU) 2016/1148. Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union*. 2016.

[52] Claudia Rosenmayr-Clemenz. Ed. by Wirtschaftskammer Österreich. June 29, 2017. URL: `https://news.wko.at/news/oesterreich/Datenschutz-Anpassungsgesetz-2018-vom-Nationalrat-beschlo.html` (visited on 08/04/2017).

[53] Alexander Roßnagel, ed. *Europäische Datenschutz-Grundverordnung: Vorrang des Unionsrechts - Anwendbarkeit des nationalen Rechts*. Vol. 1. Nomos, 2016. 342 pp. ISBN: 978-3848730742.

[54] Fabian Schmid. *'Husch-Pfusch': Kritik an neuem Datenschutzgesetz*. Ed. by derstandard.at. June 23, 2017. URL: `http://derstandard.at/2000059695288/Husch-Pfusch-Kritik-an-neuem-Datenschutzgesetz` (visited on 07/20/2017).

[55] Matthias Schmidl. *Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung Leitfaden*. Tech. rep. Republik Österreich - Datenschutzbehörde, 2017.

[56] Mark Scott and Natasha Singer, eds. *How Europe Protects Your Online Data Differently Than the U.S.* (Jan. 31, 2016): *The New York Times*.

[57] Annika Selzer. “Datenschutz in Europa und den USA. Grenzüberschreitender Datenverkehr nach dem Safe Harbour Aus”. In: Menschenrechte im 'Cyberraum' (Dec. 4, 2015). Ed. by Fraunhofer-Institut für Sichere Informationstechnologie. Schader Stiftung. Darmstadt, Dec. 5, 2015.

[58] Kristin Shi-Kupfer and George C. Chen. “Massenhaft Nutzer – mangelhafter Datenschutz”. In: *Zeit Online* (Aug. 20, 2017).

[59] Bundesamt für Sicherheit in der Informationstechnik, ed. *Gesetz zur Umsetzung der NIS-Richtlinie. Mehr Aufgaben und Befugnisse für das BSI*. 2017. URL: `https://www.bsi.bund.de/DE/DasBSI/NIS-Richtlinie/NIS-Richtlinie.html` (visited on 09/05/2017).

[60] Wirtschaftskammer Steiermark. *EU-Datenschutz-Grundverordnung (DS-GVO). Kurzüberblick und Zeitplan*. Wirtschaftskammer Österreich. Sept. 28, 2017. URL: `https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung.html` (visited on 09/14/2017).

[61] Wirtschaftskammer Steiermark, ed. *EU-Datenschutz-Grundverordnung (DSGVO): Dokumentationspflicht - Verzeichnis von Verarbeitungstätigkeiten. Pflicht und Umfang von Verzeichnissen von Verarbeitungstätigkeiten*. Aug. 28, 2017. URL: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Dokumentationspflicht.html (visited on 09/06/2017).

[62] *Verordnung (EU) 2016/679*. 2016.

[63] Sichao Wang. "Are enterprises really ready to move into the cloud". In: ().

[64] Andreas Wilkens. *Datenschützer bewerten EU-Grundverordnung als 'Meilenstein'*. Ed. by heise online. Apr. 21, 2016. URL: https://www.heise.de/newsticker/meldung/Datenschuetzer-bewerten-EU-Grundverordnung-als-Meilenstein-3179872.html (visited on 08/04/2017).

[65] Andreas Wilkens and Stefan Krempel. *Rechtsexperte: Datenschutz-Grundverordnung als 'größte Katastrophe des 21. Jahrhunderts'*. Ed. by heise online. Apr. 27, 2016. URL: https://www.heise.de/newsticker/meldung/Rechtsexperte-Datenschutz-Grundverordnung-als-groesste-Katastrophe-des-21-Jahrhunderts-3190299.html (visited on 08/07/2017).

[66] "Wirtschaftskammer startet 'Austrian Cloud'". In: *derStandard.at* (July 6, 2017). URL: http://derstandard.at/2000060882598/Nach-Cyber-Attacke-Wirtschaftskammer-startet-Austrian-Cloud (visited on 09/03/2017).

[67] KPMG AG Wirtschaftsprüfungsgesellschaft, ed. *3 von 4 Unternehmen in Österreich von Cyberattacken betroffen*. Sept. 13, 2017. URL: https://home.kpmg.com/at/de/home/media/press-releases/2017/09/kpmg-cyber-security-in-oesterreich-2017.html (visited on 09/25/2017).

[68] KPMG AG Wirtschaftsprüfungsgesellschaft and Bitkom Research GmbH. *KPMG Cloud-Monitor 2017. Cyber Security im Fokus: DIe Mehrheit vertraut der Cloud*. Tech. rep. 2017.

11 Glossar - Abkürzungsverzeichnis

- Abg. z. NR - Abgeordnete(r) zum Nationalrat (Österreich)
- ACD - Active Cyber Defense
- AGB - Allgemeine Geschäftsbedingungen
- AK - Kammer für Arbeiter und Angestellte/Arbeiterkammer (Ö)
- APCIP - Austrian Program for Critical Infrastructure Protection (Österreich)
- BDSG - Bundesdatenschutzgesetz (D) - nationale deutsche Umsetzung der DSRL Datenschutzrichtlinie 'alt' - (Richtlinie 95/46/EG)
- BND - Bundesnachrichtendienst (D)
- BMEIA - Bundesministerium für Europa, Integration und Äußeres (Ö)
- BKA - Bundeskanzleramt
- BRD - Bundesrepublik Deutschland
- BRZ-CERT - Computer Emergency Response Team des Bundesrechenzentrums (Ö)
- BSI - Bundesamt für Sicherheit in der Informationstechnik (D)
- C4 - Cyber Crime Competence Cefnter der österreichischen Bundesregierung
- CERT - Computer Emergency Response Team
- CNI - Critical National Infrastructure - Nationale kritische Infrastruktur (UK)
- CSIRTs-Netzwerk - Computer Security Incident Response Teams Network
- Cyber-AZ - Nationales Cyber-Abwehrzentrum (D)
- DOS - Denial of Service
- DDOS - Distributed Denial of Service
- DSB - Datenschutzbehörde
- DSG - Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten - Datenschutzgesetz (Österreich)
- DSG 2000 - Datenschutzgesetz 2000 (Österreich)
- DSGVO - Datenschutz-Grundverordnung (Verordnung (EU) 2016/679)
- DSRL - Datenschutzrichtlinie 'alt' - (Richtlinie 95/46/EG)

- ENISA - European Union Network and Information Security Agency
- EU - Europäische Union
- EuGH - Europäischer Gerichtshof
- FMA - Finanzmarktaufsicht (Ö)
- FPÖ - Freiheitliche Partei Österreichs
- GovCERT - Staatliche(s) Computer Emergency Response Team
- H1 bis H7 - Handlungsfelder 1 bis 7 der österreichischen Strategie für Cyber Sicherheit 2013
- HF1 bis HF4 - Handlungsfelder 1 bis 4 der deutschen Strategie für Cyber Sicherheit 2016
- HTL - Höhere Technische Lehranstalt (Ö)
- IKT - Informations- und Kommunikationstechnologie(n)
- IIot - Industrial Internet of Things
- IoT - Internet of Things
- KIRAS - Förderungsprogramm für Sicherheitsforschung (Ö)
- KMU / KMUs - Klein- und Mittelunternehmen
- KSÖ - Kuratorium Sicheres Österreich
- MAD - Militärischer Abschirmdienst (D)
- MilCERT - Militärisches Computer Emergency Response Team
- MIRTs - Mobile Incident Response Teams (des BSI)
- NATO - North Atlantic Treaty Organisation / Organisation des Nordatlantikvertrags
- NCSC - National Cyber Security Center (UK)
- NCSS - National Cyber Security Strategy / Nationale Cybersecurity Strategie
- NOCP - National Offensive Cyber Programme (UK)
- NSA - National Security Agency (USA)
- OECD - Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
- OSZE - Organisation für Sicherheit und Zusammenarbeit in Europa
- ÖSCS - Österreichische Strategie für Cyber Sicherheit

- ÖVP - Österreichische Volkspartei
- QRF - Quick Reaction Force, Schnellermittlungseinheit des Bundeskriminalamtes (D)
- ROI - Return on Investment
- SKKM - Staatliches Krisen- und Katastrophenmanagement (Österreich)
- SLA - Service Level Agreement
- SME - Small and Medium Enterprises / Klein- und Mittelunternehmen
- SPÖ - Sozialdemokratische Partei Österreichs
- UBIT - Unternehmensberatung, Buchhaltung und Informationstechnologie - Fachgruppe bzw. Sparte der Wirtschaftskammer Österreich
- USP - unique selling proposition / Alleinstellungsmerkmal
- VN - Vereinte Nationen
- WKO - Wirtschaftskammer Österreich
- ZITiS - Zentrale Stelle für Informationstechnik im Sicherheitsbereich (D)

12 Anhang

12.1 Interview Hansen

Die Expertin

Marit Hansen ist Landesbeauftragte für Datenschutz Schleswig-Holstein und somit Leiterin des Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD). Sie ist Diplom-Informatikerin und seit 1995 im ULD tätig, zuerst als Referentin, seit 2008 als stellvertretende Leiterin und ist seit 2015 mit der Leitung beauftragt.
Ihre zahlreichen Publikationen umfassen u.a. die Themengebiete Privacy by Design, Datenschutz im Cloud Computing, die Datenschutzgestaltung für vernetzte Fahrzeuge oder die Herausforderung für Verbraucherdatenschutz in der digitalen Welt. [12]

Das Gespräch

Rockenbauer: Vielen Dank für die Interviewmöglichkeit, mit Herrn Krasemann aus dem ULD werde ich über das Gütesiegel sprechen, mit Ihnen würde ich gerne eher Datenschutzthemen einer höheren Ebene ansprechen. Die Idee der Masterarbeit ist, das Feld der IT-Security und Privacy als Standortvorteil zu beforschen. Als ULD Schleswig-Holstein beraten Sie ja Unternehmen, Behörden und Bürger in Datenschutzangelegenheiten, wie sieht Ihr Arbeitsalltag diesbezüglich aus, welche der drei Gruppen fragen hier mehr nach Ihrer Expertise an?

Hansen: Wir haben ja nicht nur viel an Beratung, sondern auch an aufsichtsbehördlicher Tätigkeit und Projektzusammenarbeiten, insgesamt reden wir sogar von sieben Säulen im ULD.
Bei der Beratung machen Unternehmen eher einen geringen Teil aus, behördlich wird zurzeit mehr nachgefragt. Bei den Bürgern wollen sich die einen beraten lassen, die anderen wollen eher Beschwerden vorbringen. Das wirkt sich dann wieder auf Unternehmen und andere Privatpersonen aus und daraus resultieren dann häufig wieder Beratungsleistungen. Dadurch spielt manchmal wiederum das Bewusstsein für Datenschutzfragen eher eine Rolle und zukünftige Gestaltungsfragen werden gestellt.
Einiges versuchen wir auch im Vorfeld zu lösen, etwa durch Veranstaltungen, zu denen viele Unternehmer oder auch Rechtsanwälte, die in diesem Bereich tätig sind, kommen. Keine Firma hätte ja Interesse, beim Datenschutz etwas falsch zu machen, es sei denn, ihr Geschäftsmodell basiert darauf. Wir versuchen also gemeinsam den Lösungsraum zu erweitern um zu einer besseren Systemgestaltung zu kommen. Dann kommt man zu einem Ergebnis, das wir auf Konferenzen und auch unseren Abgeordneten gegenüber verbreiten.
Unser tägliches Doing ist also sehr vielfältig und umfasst sowohl Beratung,

als auch Beschwerdeannahme, zusätzlich eigene Ideeneinbringung, was man besser machen kann.

Rockenbauer: Über Dr. Bäumlers Buch 'Datenschutz als Wettbewerbsvorteil' bin ich ja auf das ULD Schleswig-Holstein aufmerksam geworden.

Hansen: Falls Sie Interesse haben, kann ich Ihr Mail gerne an ihn weiterleiten, er äußert sich immer wieder noch über Datenschutzthemen.

Rockenbauer: Sehr gerne, herzlichen Dank!

Hansen: Viele Inhalte des Buches haben wir mittlerweile hier bearbeitet und viele Dinge, die er gefordert hat, kommen mittlerweile z.B. über die Datenschutzgrundverordnung. Das ist sicherlich auch ihm zuzuschreiben.

Rockenbauer: Um zum übergeordneten Thema und zur großen Frage zu kommen: Glauben Sie, dass Datenschutz - auch für Unternehmen - überhaupt einen Standortvorteil darstellen kann?

Hansen: Wir befinden uns in einer globalisierten Welt und haben mit dem Europäischen Wirtschaftsraum ja etwas, wo auch gemeinsame Werte eine Rolle spielen. Spätestens mit Trump, China oder anderen globalpolitischen Entwicklungen - also spätestens seit kurzem - ist vielen bewusst geworden, dass dieses globale Zusammenspiel auch fragil sein kann. Daher auch die Rückbesinnung auf Werte und auch Standortvorteile wie zum Beispiel 'Wo sind denn die Daten?'. Spätestens seit Snowden kann man sagen, dass es eine Rolle spielt, wer an welche Daten herankommt und wo z.B. amerikanische Firmen an Daten kommen. Nicht, weil die Firmen sie selbst missbrauchen, sondern weil die Behördenzugriffe dann durchstoßen können. Cloud Computing beispielsweise kann ja für flexibles Arbeiten eine tolle Sache sein, beherbergt gleichzeitig aber ein Risiko. Hier trifft der Standort - das Territorium - über die Rolle der Zugriffsrechte eine Aussage. Solche Überlegungen sind in letzter Zeit essentiell geworden. Deswegen sind politische Instabilitäten bzw. Machtspiele mancher Regierungen doch ein Faktor, wo man froh ist, dass die Daten an einem sicheren Standort sind.
Bei Safe Harbor zum Beispiel war das genau nicht der Fall, auch Privacy Shield hat einige Lücken. Damit bin ich nicht zufrieden. Das bedeutet aber, dass Europa gegenüber außereuropäischen Gebieten als Standortvorteil gesehen werden kann, alleine deswegen, weil die Daten da sind. Das interessiert vielleicht auch die Unternehmen in Sachen Risikoeinschätzung, wo die eigenen Daten gelagert werden. Ansonsten liegt es am Territorium und

der Rechtsdurchsetzung.
Differenzieren kann man auch noch zwischen Unternehmen, die sich einfach an die Richtlinien halten und Betrieben, die ihr Businessmodell auf besonders hohem Datenschutz und besonders hoher Security aufbaut. Nicht jeder wird sehr hohe Summen in IT-Sicherheit bzw. Datenschutz investieren wollen oder können, aber wenn solche Dienstleister existieren und Vertrauenswürdigkeit unter Beweis stellen, dann ist das für den Gesamtbereich ein Vorteil. Auch da baut sich immer mehr auf. Aber von der anderen Seite betrachtet, was sind denn Standortnachteile? Mittlerweile haben wir ein Problem mit vielen Abhängigkeiten. Wenn viele Betriebssysteme, Soft- oder Hardware schon so gestaltet wird, dass man mit allen Schutzmöglichkeiten nicht gewisse Datenabflüssen unterbinden kann, weil es zum Beispiel gar keine europäischen Hersteller mehr gibt, kann es insgesamt zu einem Nachteil werden.
Solche Entwicklungen können dann wiederum zum Aufbau von eigenen Kapazitäten führen.
Ein konkretes Beispiel sind im Bereich Automobile die Smart Cars. Der Markt ist ziemlich aufgeteilt zwischen Apple, Microsoft und Google mit ihren autonomen Fahrzeugen. Die deutschen Automobilhersteller gelten hier im Vergleich als relativ vertrauenswürdig, aber doch auch hochpreisiger. Hier wird das Businessmodell, dass das Produkt möglichst billig sein muss, umgedreht. Das 'Hardwareprodukt' Auto darf etwas kosten, es bringt einen Mehrwert.
Auf der anderen Seite steht ein Auto, welches den Fahrer ausspioniert, gegen den Fahrer arbeitet und Informationen an beispielsweise den Hersteller übermittelt, die man gar nicht übermittelt haben möchte. Und auf einmal bekommen wir einen anderen 'Drive' in dieses Thema. Das funktioniert aber nur noch, wenn eine gewisse Hoheit über die Entwicklung besteht und da sind wir wieder beim Standortvorteil.

Rockenbauer: Gerade die Aufzeichnung und Verwendung der aufgezeichneten Daten bei neuen Autoherstellern, wie zum Beispiel Tesla, ist sicherlich ein interessantes Gebiet.

Hansen: Genau, viele Themen, die im Buch von Dr. Bäumler aufgezeigt wurden, haben sich weiter radikalisiert. Siehe eben die Causa Snowden, die aufzeigt, worauf Geheimdienste zugreifen.
Die Idee vom dezentralen Internet und dem Selbstdatenschutz funktioniert also gar nicht so gut, wenn auf einmal alles wieder zurückzentralisiert wird und in der Cloud stattfindet. Erst durch das Bewusstsein für solche Probleme ergibt sich, das etwa die deutsche Cloud oder europäische Anbieter zum Vorteil werden können. Das österreichische Klassenbuch wird beispielsweise bei uns in den Schulen eingesetzt, weil es sich in der internationalen Ausschreibung durchgesetzt hat. Ein amerikanischer Anbieter

hätte beispielsweise keine Chance gehabt.

Rockenbauer: Sie haben ja im Themenkomplex 'Privacy by Design' einiges publiziert. Ist es Ihrer Meinung nach möglich, das bereits so zu verankern und wo sehen Sie die Herausforderungen in diesem Bereich?

Hansen: Ich sehe viele Möglichkeiten, Probleme bereits im Vorfeld auszuschließen. Beispielsweise hatte ich bereits mit einer Datenbank im polizeilichen Bereich zu tun. Diese Datenbank sollte eigentlich gar keine personenbezogenen Daten enthalten, tat sie dann aber durch Fehlverständnis und falsche Anordnungen doch. Weil sie nicht personenbezogen sein sollte, existierten auch keine automatisierten Löschroutinen, die Daten waren viel zu lange gespeichert. Außerdem existierten Freitextfelder, in diese wurden - obwohl für statistische Auswertungen gedacht - viele personenbezogene Daten eingetragen. Freitextfelder und keine Löschroutine im Polizeibereich sind dann schon Alarmglocken für uns. Und da sprechen wir über ganz simple Dinge und noch gar nicht über die hohe Kunst des 'Privacy by Design'.
Hier kann man durch wenig Technik relativ viel erreichen. Bei komplexeren Systemen bringt uns ein Mehr an Technik oft auch ein Mehr an Möglichkeiten. Exemplarisch dafür ist das Vorzeigen von Ausweisen an verschiedenen Stellen zu nennen. Wenn ich Ihnen und Ihrem Chef beispielsweise meinen Führerschein zeige, können Sie ihr Wissen kombinieren und haben relativ viele Daten über mich erfahren. Im digitalen Bereich muss das hingegen nicht sein, hier haben wir Projekte mit attributbasierten Berechtigungsnachweisen - sogenannten 'Attribute-based Credentials'- durchgeführt.
Um beim vorhin genannten Beispiel zu bleiben, könnten Sie und Ihr Chef beide überprüfen, ob ich einen Führerschein besitze, allerdings nicht die Information bekommen, dass es sich um mich bzw. dieselbe Person handelt. Wir erweitern also den Lösungsraum mit technischen Lösungen und haben so Möglichkeiten, die eventuell sogar über die ursprüngliche Vorstellungsmöglichkeit des Gesetzgebers hinausgehen. Diese Initiativen hatten in den letzten Jahren allerdings zu wenige Anreize und man muss die Frage stellen, warum sich das nicht noch viel eher durchgesetzt hat. Vielleicht, weil diese Lösungen technisch komplexer sind, wenig in Usability investiert wurde und die datengetriebenen Geschäftsmodelle - wie beispielsweise soziale Netzwerke - viel mehr Bemühungen in Design und Bedienbarkeit umgesetzt haben.
Ohne eine geeignete Anschubfinanzierung ist es viel schwieriger. Jetzt haben wir mit der Datenschutzgrundverordnung die Möglichkeit, dass diese eingebauten technischen Möglichkeiten sogar zur Pflicht werden. Wenn es bessere Möglichkeiten gibt, die den steinigen Weg zum 'State of the Art' gegangen sind, gibt es danach keine Ausrede mehr, etwas Schlechteres einzusetzen.

Diese Wendung ist mir total wichtig, hier ist es entscheidend, dass Unternehmen und Aufsichtsbehörden über die Möglichkeiten der Technik Bescheid wissen. Darum ist die Kommunikation ein entscheidendes Thema und Personen mit gutem Rechts- und gutem Technikverständnis sind gefragt.
Ein Beispiel: In Deutschland besitzt der Personalausweis die Möglichkeit, mittels einer mathematischen Funktionsausführung die Frage nach der Volljährigkeit zu beantworten, man muss also nicht mehr den gesamten Ausweis mit allen Informationen vorweisen. Von dieser Funktion weiß allerdings kaum jemand was und sie wird dementsprechend sehr wenig genutzt.
Wenn nun einige den Weg gehen und wir zeigen, dass es geht und bauen Systeme so auf, dann wird 'Privacy by Design' immer noch kein Automatismus sein, aber es gibt zumindest vorzeigbare Lösungen, die bei Ausschreibungen auch berücksichtigt werden können. Dadurch lassen sich Hebelwirkungen erzielen.
Die behördlichen und betrieblichen Datenschutzbeauftragten werden übrigens selten in Ausschreibungen miteinbezogen, dann kommen solche Kriterien leider nicht zum Zug. Aber wenn diese Eigenschaften bei Ausschreibungen mehr Würdigung erfahren, dann zwingt man die Anbieter zum Nachdenken. Wenn die Nachfrage da ist, wird es - Henne-Ei - auch vermehrt angeboten werden. Jene, die sich darum kümmern, generieren einen Vorteil daraus.
Bei Ausschreibungen müssen laut Datenschutzgrundverordnung solche Dinge ja berücksichtigt werden. In Schleswig-Holstein haben wir das Gütesiegel, Produkte die mit dem Datenschutzrecht besonders vereinbar sind, müssen vorgezogen werden. Gut getestete Produkte sparen also Arbeit, denn laut schleswig-holsteinischem Landesgesetz und nun auch der Datenschutz-Grundverordnung existiert ja die Verantwortung. Wer jetzt Tools bzw. Software einsetzen will, der muss die Dokumentation im Griff haben, der muss das bei uns testen und freigeben lassen. Wer das ohne Unterstützung macht hat viel Arbeit, beispielsweise bei einem Windows 10, das sehr wenig dokumentiert und wo Datenabflüsse nur schwer zu verhindern sind. Das kann zum Beispiel dazu führen, dass so ein Einsatz in der Verwaltung gar nicht erlaubt ist.
Eine Kritik aber gleich noch an der Grundverordnung: Man hätte die Hersteller stärker in die Pflicht nehmen sollen. Erwartungen an die Hersteller hätte man besser adressieren können. Da hätte man schon im Rahmen der Grundverordnung mehr verlangen können. Denn wenn keine bessere Lösung da ist, hat man als Kunde ja keine Wahlmöglichkeit. Aber es gibt in dem Bereich durchaus Unternehmen, die ihr Geschäftsmodell auf höherem Datenschutz aufbauen.

Rockenbauer: Und vielleicht generiert man dann so auch Kundeninteresse an Produkten mit hochwertiger Privacy, auch wenn diese etwas teurer sind. Nun sind wir ohnehin schon tief im Thema Datenschutz-Grundverordnung. Generell

herrscht bei Ihnen ein positiver Grundtenor bei der Verordnung mit einigem Optimierungsbedarf - etwa bei der Verpflichtung der Hersteller - vor?

Hansen: Ja, genau.

Rockenbauer: Was ist ihre Meinung zum neuen Strafausmaß von bis zu 4 Prozent des Unternehmensumsatzes? Hier sind einige Unternehmer ja ziemlich beunruhigt.

Hansen: Ich bin da eher positiver gestimmt, kenne aber natürlich auch andere Meinungen, die sagen, dass man eine kleine Firma so an den Rande des Abgrunds bringen kann. Aber es wird faktisch so sein, dass die Höchststrafe praktisch nie verhängt werden wird. Man will für die 'harten Fälle' noch etwas Luft nach oben lassen. Verhältnismäßigkeit und Eigenschaften wie die Größe der Firma, Motivation etc. werden mit einfließen. Wenn es sich anders entwickelt, wird die andere Seite vor Gericht ziehen, wenn das Unternehmen aus seiner Sicht wirtschaftlich stark und unbegründet beschädigt wird. Da kommt es dann meistens zu einem Kompromiss.
Aber solche Möglichkeiten, wie diese 4 Prozent Strafe, sind wichtig, damit man überhaupt ernst genommen wird. Bei harten Verstößen muss es auch harte Sanktionsmöglichkeit geben, die in den nächsten zehn Jahren aber wahrscheinlich gar nie ausgeschöpft werden.
Gerade die KMU müssen da gar keine Angst haben, bei dem Artikel wird ja auch angeführt, welche Parameter dabei berücksichtigt werden müssen. Ohne Strafen passiert allerdings fast nie etwas, wir brauchen also diese Möglichkeit der Aufmerksamkeit.

Rockenbauer: Also trifft es Ihrer Meinung nach dann eher nicht die Klein- und Mittelunternehmer mit voller Härte, sondern die, die kriminelle Machenschaften quasi im eigenen Geschäftsmodell verankert haben?

Hansen: Ja, genau. Außerdem kann man sich ja immer vertrauensvoll an die Aufsichtsbehörde wenden und kann im Falle der Unsicherheit anfragen und in den Kontakt kommen. Alle Personen und Unternehmen, die einen besseren Datenschutz wollen, können schnell in Kontakt kommen. Wenn man umgekehrt gleich immer den Konfrontationskurs nimmt, haben beide Seiten verloren, also Firmen und Aufsichtsbehörden.
Wer sich eben traut mit uns zusammenzuarbeiten, gibt zwar Einblicke preis, erhält aber auch welche in die Behörde und versteht eventuell die Situation. Dies gilt nicht nur im Firmenbereich, sondern beispielsweise auch in Zusammenarbeit mit der Polizei, für die wir regelmäßig Datenschutzbeauftragte ausbilden.

Rockenbauer: Als Abschlussfrage und um eine Zukunftsperspektive zu erhalten: Glauben Sie, dass Datenschutz für Bürger und Unternehmen als Positivum darstellbar sein wird oder wird das eher noch schwieriger, weil viele der 'Digital Natives' gar nicht wissen, wo und wie sie ihre Daten mutwillig preisgeben? Ist diese Awarenessschaffung möglich?

Hansen: Ja, absolut. Ich kann natürlich an gar nichts anderes glauben und arbeite selbst an der Umsetzung und Etablierung. Viele 'Digital Natives' - wie beispielsweise meine Kinder - besitzen bereits sehr viel Bewusstsein für diesen Bereich. Auch von Hollywood werden ja immer mehr düstere Zukunftsvisionen im Bereich Datenschutz gezeichnet wo man merkt, dass das gar nicht mehr so zukünftig ist.
Wir haben also eine digitalisierte Welt, die nicht mehr nur im Sinne der Menschen arbeitet, sondern vielleicht sogar dagegen. Konzerne wie Google und Facebook besitzen einfach eine immense Macht, die sich eventuell auch auf Grundrechte auswirken kann. Und da ist Datenschutz kein kleines Thema, sondern für die gesellschaftliche Weiterentwicklung essentiell. Wir werden aus gewissen Risiken hinauskommen müssen, um keine Außenseiter zu generieren. Von den 'Digital Natives' waren einige sehr bequem, aber ich glaube gerade die nächste Generation ist nicht mehr unpolitisch.
Es ist natürlich schwierig, das Thema zu begreifen, aber es wird immer mehr greifbare Effekte geben. Einer ist zum Beispiel die Preisdiskriminierung, also wenn Personen aufgrund ihrer Profile ungerecht in Sachen Preisgestaltung behandelt fühlen.

Rockenbauer: Also zum Beispiel wenn eine Versicherung viele Daten über den Kunden besitzt, meint, dass er zu ungesund lebt und die Prämie deutlich erhöht?

Hansen: Genau, oder bei Flugbuchungen oder im Supermarkt, die ja teilweise schon digitale Preisschilder besitzen. Wenn die Person hinter mir einen anderen Preis zahlen muss, fühlt sie sich wahrscheinlich ungerecht behandelt. Manche Personengruppen werden dann wahrscheinlich mehr diskriminiert als andere, beispielsweise die mit geringer Kreditwürdigkeit. Aus solchen Schubladen kann man dann wahrscheinlich nur schwer entkommen.

Rockenbauer: Oftmals hört man ja in Bezug auf die eigenen Daten Aussagen wie 'Ich habe eh nichts zu verbergen'. Wobei jeder dann wahrscheinlich etwas hat, was er nicht in aller Öffentlichkeit publiziert haben will.

Hansen: Ich glaube auch, dass das persönliche Verhalten doch zeigt, dass es in gewissen Lebenssituationen eben schon wichtig ist, dass eben nicht jeder Bescheid weiß, beispielsweise beim Tod eines nahen Verwandten oder wenn man einen Fehler gemacht hat, der einem selbst peinlich ist.

Auch im Bereich Mobbing ist es ein hoher Anteil, der dies in der Schule oder im dienstlichen Kontext erfahren hat. Wenn wir einen großen Teil an Leuten haben, die sich nicht mehr zugehörig fühlen, haben wir Probleme, dass wir diese verlieren oder auch Terroristen heranbilden.
Dieses Bewusstsein zur steigenden Bedeutung von Datenschutz wird glaube ich durchaus mehr.
Das Spannende am Datenschutz ist ja, dass es nicht nur um Technikgestaltung, sondern schon auch um unsere Zukunft geht. Da spielt auch Meinungsfreiheit und Informationsfreiheit mit. Die Grundrechte sind zum Glück über die Jahrzehnte stabil geblieben und nun muss man sie weiter mit Leben füllen. Hier tun wir unser Möglichstes und ich bin sehr optimistisch. Manche Dinge werden erst dann bewusst, wenn man selbst einen Unglücksfall hat, das nenne ich 'Privacy by Disaster' und das gehört verhindert. Wenn es aber dann doch eintritt, ist der Wake-up Call umso deutlicher.

Rockenbauer: Die Grundrechte müssen also auch in die digitale Welt hinausgetragen und dort verteidigt werden.

Hansen: Genau, wobei verteidigen klingt etwas defensiv. Wir bauen sie ein, wir unterstützen und schützen sie gegen diejenigen, die sie zerstören wollen.

Rockenbauer: Datenschutz also nicht nur als technische, sondern auch als gesellschaftliche Komponente. Vielen Dank für das interessante Gespräch!

12.2 Interview Bäumler

Der Experte

Dr. Helmut Bäumler ist deutscher Jurist und Datenschutzexperte. Er war von 1980 bis 1989 Referent beim Bundesbeauftragten für Datenschutz mit Schwerpunkt in der Kontrolle von Geheimdiensten und Polizeibehörden.
Von 1992 bis 2004 war er Landesdatenschutzbeauftragter von Schleswig-Holstein und maßgeblich für die Modernisierung des Landesdatenschutzrechts und Bildung des Unabhängigen Landeszentrums für Datenschutz (ULD) verantwortlich.
Bäumlers Verdienst war u.a. die Ersetzung einer eher technikfeindlichen Perspektive auf den Datenschutz durch die Erreichung von mehr Datenschutz mittels innovativen, technischen Konzepten. Das ULD ist heute in Datenschutzfragen und - konzepten für seine Vorreiterrolle international bekannt.

Das Gespräch

Rockenbauer: Zuerst herzlichen Dank für die Interviewmöglichkeit, Herr Dr. Bäumler! Eingangs zum Thema Datenschutz als Wettbewerbsvorteil, welche Entwicklungen hat in Ihrer 'aktiven Zeit' im Gebiet, also seit Anfang der 1980er bis Anfang der 2000er, der Datenschutz durchgemacht? Auch in der öffentlichen Wahrnehmung, etwa von Unternehmen und Bürgern?

Bäumler: Ich habe 1980 beim damaligen Bundesbeauftragen für Datenschutz, Prof. Bull, begonnen zu arbeiten. Damals war ich zuständig für die Kontrollen bei den Geheimdiensten und beim Bundeskriminalamt - eine besonders konfliktreiche Thematik. Ich habe den Datenschutz von Anfang an so erlebt, dass ich ihn persönlich als wichtig, notwendig und realisierungsbedürftig gesehen habe, dass er in der breiten Bevölkerung aber nicht wirklich angekommen ist.
In Deutschland ist die Gesetzgebung im Wesentlichen auf ein paar engagierte Abgeordnete zurückzuführen. Bei den Liberalen war es meiner Meinung nach eher aus Überzeugung, bei CDU/CSU- und SPD-Abgeordneten war es, das ist natürlich eine subjektive Einschätzung, eher ein bisschen aus Angst vor der Technik.
Diese Mischung - Implementierung von oben und angstbegleitet - hat dazu geführt, dass die Bürger in der Breite damit nie wirklich warm geworden sind. Datenschutz war im Zuge der scharfen Terrorismusbekämpfung auf eine Konfrontation mit der Polizei ausgelegt und es gab Interesse daran, den Datenschutz öffentlich zu diskreditieren, etwa als 'Fahndungsverhinderer'.
Das waren natürlich keine besonders glücklichen Startbedingungen.
Auch wenn man noch so überzeugt vom Datenschutz ist, muss man - denke ich - doch immer die Frage stellen, was die sagen, deren Interessen wir ja in Wirklichkeit schützen. Und da gibt es im Rückblick auf meine über 20jährige Tätigkeit im Datenschutz doch viele Enttäuschungen, etwa dass

viele Bürger nicht interessiert waren und dass ihnen nicht vermittelt wurde, eigene Interessen im Datenschutz zu erkennen.
Das war rückblickend ein großer Fehler. Es ist uns einfach nicht gelungen, bei der Bevölkerung so anzukommen, wie es für den Datenschutz nötig gewesen wäre. Wenn wir später auf den marktwirtschaftlichen Datenschutz zu sprechen kommen, hat das große Auswirkungen.
Insgesamt ist Datenschutz also eine gute Sache, dummerweise haben diejenigen, für die er gemacht worden ist, nicht wirklich angebissen. Daran krankte das Thema von Anfang an, es war eben eher ein Elitenthema.

Rockenbauer: In Ihrem Interview aus dem Jahr 2009, das auf der ULD-Seite online gestellt wurde, bezeichnen Sie Datenschützer ja als stete Warner vor dem Gewitter, welches dann nie wirklich kommt. So verlieren die Datenschützer ihre Glaubwürdigkeit.

Bäumler: Das Gewitter ist - wenn ich das so sagen darf - schon gekommen, teilweise sogar noch schlimmer, als ich es je befürchtet habe. Die Enthüllungen von Snowden haben mich schon vom Hocker gehauen. Auch, dass die europäischen Regierungen flügellahm darauf reagiert haben, war ein GAU für den Datenschutz, mehr als ein Gewitter.
Aber der Gedanke vorher ist natürlich nicht falsch, dass man bei diesem Thema wohldosiert vorgehen muss und das Publikum nicht mit ständigen Weltuntergangsprophezeiungen überfordern darf. Aber wenn wir vorher gewusst hätten, dass eines Tages ein Snowden mit diesen Informationen kommt, hätte man manchmal noch viel drastischer reagieren müssen.

Rockenbauer: In meinem Gespräch mit Frau Hansen hat sie erwähnt, dass viele Dinge, die Sie prognostiziert haben, eigentlich noch viel dramatischer eingetreten sind. Nehmen wir beispielsweise das Themenfeld Cloud Computing. Cloudbasierte Dienste sind heutzutage im privaten und unternehmerischen Umfeld absoluter Usus. Sehen Sie da noch größere Herausforderungen auf den Datenschutz zukommen, als noch vor einigen Jahren angenommen?

Bäumler: Ja, das spricht einen zweiten wichtigen Aspekt an. Ich bin prinzipiell ein sehr optimistischer Mensch und halte wenig von Weltuntergangsszenarien. Aber zwei, drei Dinge muss man kritisch zu den Grundlagen der Datenschutzarbeit anmerken. Die eine Sache habe ich schon erwähnt, die mangelnde Verankerung in der Bevölkerung. Die zweite sprechen Sie jetzt an: die unglaubliche Dynamik der Technik.
Man hat sich kaum auf irgendwas eingestellt, schon kommt eine technische Neuerung, bei der man schnell etwas, nicht zwangsläufig immer dagegen, sondern zumindest begleitend, beratend unternehmen müsste. Das führt zu einem dritten Mangel, dann möchte ich schon mit den Mängeln aufhören, aber man muss es realistisch beschreiben. Das dritte Problem ist die Ausstattung der Datenschutzbehörden.
Der Staat hat zu den Bürgern quasi zugesagt, dass die Thematik des Datenschutzes durch Installierung einer Kontrollbehörde beachtet wird.

Und wenn man sich die Datenschutzbehörden qualitativ ansieht, bestanden diese zumeist aus einer Mischung von einigen Enthusiasten, zu denen ich mich auch zähle, und vielen völlig normalen Beamten, die ihre Laufbahn dorthin verschlagen hat. Diese haben ihre Arbeit so gut wie immer gemacht, haben aber für das Thema nicht so sehr gebrannt, wie die Enthusiasten. Es war im Grunde eine ganz kleine Gruppe, die am Werk war. Im Prinzip hat sich an diesen Größenverhältnissen nie wirklich etwas geändert.
Wenn ich das mit den Sicherheitsbehörden vergleiche, sind es ganz andere Dimensionen. Ich weiß nicht, wie viele Stellen aktuell der Bundesbeauftrage für Datenschutz hat, eventuell 70 oder 80. Das ist im Vergleich mit Polizei und Geheimdiensten einfach nur lächerlich. Man gaukelt dem Publikum vor, dass es jemanden gibt, der alles kontrollieren kann, das ist aber in der Größe und - jetzt kommt der zweite Punkt - in der personellen Zusammensetzung völlig unmöglich.
Eigentlich müssten in den Datenschutzbehörden überwiegend junge, engagierte und in den allerneuesten Entwicklungen versierte Techniker tätig sein, die das Thema von der technischen Seite und praktisch angehen.
Es ist schon auch wichtig, Juristen für eine Datenschutzgesetzgebung zu haben, aber für kaum eine andere Gesetzesmaterie ist die praktische Arbeit mit und die Kenntnis der Technik so wichtig wie beim Datenschutz. Da hapert es bis heute. Das ULD ist da eine ganz kleine Ausnahme, insofern dort überdurchschnittlich viele Techniker tätig sind. Aber die Größenordnung stimmt auf Deutschland bezogen nicht.
Darum wäre es viel ehrlicher gewesen, von Seiten der Politik und der Datenschutzbeauftragten schon viel früher deutlich zu kommunizieren: Liebe Bürger, glaubt ja gar nicht, dass wir das alles im Griff haben, ihr müsst euch mindestens in gleichem Maß selbst darum kümmern. Ohne Druck der Bürger auf die Politik wird der Datenschutz seine Feigenblattfunktion kaum überwinden können
Man kann ja politisch entscheiden, dass es nicht so wichtig ist, in diesem Bereich Kontrollkapazitäten aufzubauen, dann muss man das aber, möglichst vor den Wahlen, den Bürgern deutlich sagen . Aber so zu tun, als ob, und die Bürger in Sicherheit zu wiegen, ist problematisch.

Rockenbauer: Gerade der Aspekt der Techniker im Bereich des Datenschutzes ist für mich natürlich sehr interessant, da ich ja meine Arbeit im Studium der Wirtschaftsinformatik verfasse. Mein Betreuer, Univ.-Prof. Dipl.-Ing- Dr. Dr. Quirchmayr, ist ja sowohl Informatiker, als auch Jurist.
Vielleicht zu einem Thema, welches in Schleswig-Holstein unter ihrer Führungsrolle stark implementiert wurde, nämlich Datenschutzaudit und Gütesiegel. Hier durfte ich bereits mit dem zuständigen Referatsleiter im ULD, Herrn Krasemann, reden. Meine Frage dazu: Haben Sie das Datenschutz-Gütesiegel als Instrument eines marktwirtschaftlichen Datenschutzes gesehen, welches einen werbewirksamen Wettbewerbsvorteil erzeugen kann oder war es eher als ein Kontrollsiegel für Behörden gedacht?

Bäumler: Die Intention war ganz eindeutig, einen Baustein für den marktwirtschaftlichen

Datenschutz zu versuchen. Marktwirtschaftlicher Datenschutz bedeutet ja, auf dem Markt geeignete Produkte mit der Eigenschaft eines guten Datenschutzes zu bewerben. Das muss aber von irgendjemand vertrauenswürdigem bestätigt werden, also benötigt man schon so etwas wie ein Gütesiegelsystem. Unser Gütesiegel war seiner Zeit allerdings weit voraus, das war generell ein Nachteil vieler Dinge, die wir in Schleswig-Holstein gemacht haben. Da standen wir vor der Wahl, den Bundesgesetzgeber aufzufordern etwas zu tun und zu warten, oder in unserem Bereich selber etwas zu machen.
Wir haben uns für Letzteres entschieden und haben, so denke ich, gezeigt, dass es funktioniert. Es gibt ja auch Firmen, die mit unserem Gütesiegel Werbung machen, aber im Vergleich ist das leider verschwindend gering. Ich hätte mir schon erwartet und gehofft, dass die Initialzündung mehr Wirkung erzielt. Es ist zwar in der Datenschutz-Grundverordnung der EU auch angesprochen und man liest von Versuchen mit Datenschutz-Gütesiegeln, aber es ist alles langsam und mühselig. Da Sie sich selbst mit Informationstechnologie befassen wissen Sie ja, wie unglaublich dynamisch sich die Dinge hier entwickeln.
Da liegt jedenfalls noch ein großes Potential. Marktwirtschaftlicher Datenschutz steht und fällt aber damit, was die Verbraucher dazu sagen. Für die Unternehmer ist natürlich enorm wichtig, ob die Kunden Datenschutz nachfragen. Und da gibt es momentan wohl nur ein kaum messbares Datenschutzbewusstsein.
In Fußballerkreisen sagt man, wenn jemand große Töne spricht, dass die Wahrheit auf dem Platz liegt. Das habe ich für uns gelegentlich so adaptiert: Die Wahrheit liegt im Computerladen um die Ecke. Geht da ein Kunde hinein und fragt, ob es das gleiche Produkt auch“ in datenschutzgerecht“ gibt?
So ein Fall kommt vielleicht ab und zu vor, aber vergleichsweise wahrscheinlich doch eher selten. Damit fehlt es an Nachfrage und wir sind wieder beim ersten Thema, bei der fehlenden Grundverankerung des Datenschutzes in der Gesellschaft.
Seit meinem Ausscheiden stoße ich gelegentlich auf ein positives Beispiel: Mein Mailanbieter web.de wirbt immer wieder mit deutschem Datenschutzniveau und deutschem Datenschutzstandard. Ein Gütesiegel hab ich dort noch nicht gesehen, aber immerhin spricht das mal jemand als Aspekt an. Achten Sie beim Kauf eines IT-Artikels auf Datenschutzstandards?

Rockenbauer: Ich kenne die Thematik von meinem Mailanbieter GMX ebenso, der ja mit Datenschutz und Servern in Deutschland wirbt.
Erschreckend finde ich hingegen das fehlende Bewusstsein in meiner Generation, letztens hat ein Freund, ebenso Mitte 20, ebenso Bachelor-Absolvent einer Universität auf die Thematik Datenschutz repliziert, dass er ohnehin nichts zu verbergen hätte.

Bäumler: Natürlich hat jede Person etwas zu verbergen. Im Gespräch mit solchen Leuten kommt man auch ganz schnell auf Themengebiete, bei denen sie

betonen, dass sie niemanden etwas angingen.
Es geht ja nicht nur um negative Aspekte, der Datenschutz greift ja viel früher. Es geht darum, dass es schließlich meine persönliche Sache ist, wem ich etwas über mich erzähle.

Rockenbauer: Wir haben vorhin über die Datenschutz-Grundverordnung gesprochen, die bis nächstes Jahr umzusetzen ist. Frau Hansen und Herr Krasemann haben in den jeweiligen Gesprächen gemeint, dass das Vehikel der Datenschutz-Grundverordnung durchaus verwendet werden kann, um auch über den Bereich Ausschreibungen das Gütesiegel zu stärken. Im Landesrecht von Schleswig-Holstein werden Produkte mit Gütesiegel ja bereits bei öffentlichen Ausschreibungen bevorzugt. Auf europäischer Ebene ist da doch noch einiges unklar. Darum meine Frage an Sie ist, wie das damals auf der Ebene Schleswig-Holstein so rasch umgesetzt werden konnte.
War das Interesse der Politik größer?

Bäumler: In Schleswig-Holstein war es eine merkwürdige Mischung aus zwei sich vermeintlich widersprechenden Bedingungen.
Die eine Bedingung war, dass es am Anfang schon einige engagierte Abgeordnete zu dem Thema gab. Aber es gab auch breites Desinteresse, das allerdings ein 'positives' Desinteresse war. Der Grundtenor lautete häufig: Die beim ULD machen das schon ganz gut, lasst die mal ruhig arbeiten.
Es kamen auch immer wieder positive Rückmeldungen nach Schleswig-Holstein bzgl. des ULD, worauf man dann in der Politik auch stolz war. Dass das Land Schleswig-Holstein wegen der Projekte des ULD einen Innovationspreis der EU bekam, wurde wohlwollend zur Kenntnis genommen. Mit den Berichterstattern der Fraktionen haben wir in der Regel gut kooperiert. Die Stimmung war im Parlament allgemein so, dass man dem ULD Freiheit gelassen und dafür auch erträgliche Bedingungen geschaffen hat.
Außerdem haben wir die Wirtschaft nicht als Feind angesehen, sondern mit der Industrie- und Handelskammer gut zusammengearbeitet und mit dieser Seite Dinge zuvor besprochen, ohne dass das unsere kritische Haltung im Kontrollbereich aufgeweicht hat. Wir haben nach meinem Dafürhalten sogar schärfer kontrolliert und härter kritisiert als andere Datenschutzbehörden. Aber wir hatten eben auch das zweite Gesicht. Wir sind proaktiv auf die Unternehmen zugegangen und haben betont, dass wir nicht nur die Kontrollbehörde sind, sondern eben auch Berater.
Da haben viele Datenschutzbeauftragte zuerst gemeint, dass man nicht mehr unabhängig sei. Das fand ich aber nicht wirklich überzeugend. Man muss Rat geben, wenn jemand Rat will. Dieser muss dann aber auch verbindlich sein, da muss man sich als Bürger oder Firma drauf verlassen können.
Mit dieser Haltung findet man in der Wirtschaft dann natürlich Gesprächspartner. Darum hat das Beratungsgebiet eine große Bedeutung gehabt, auch, wenn uns Kollegen manchmal kritisiert und behauptet haben, dass wir uns mit den später zu kontrollierenden Betrieben gemein machen

würden. In der Kontrollpraxis waren unsere Prüfungen dann aber eher schärfer und unnachgiebiger.

Rockenbauer: Sozusagen eine Beratungskomponente, anstatt gleich zu bestrafen.

Bäumler: Ja genau, wenn jemand wirklich Beratung will, geht man in den Betrieb und sieht sich die Lage an. Es geht ja um die Sache, also dass dort ein gutes Datenschutzniveau herrscht.
Das steht wie gesagt konsequenten Kontrollen nicht im Weg. Wir haben bei Kontrollen die 'Opfer' oft nach dem Losverfahren ausgewählt und dann objektiv kontrolliert. Beratung ist gut und Kontrolle muss auch sein.

Rockenbauer: Was sind - glauben Sie - erfolgreiche Parameter für eine hochwertige Datenschutzgesetzgebung? Möglichst generelle oder möglichst spezifische Gesetzestexte, oder braucht es ganz andere Mechanismen wie Gütesiegel und Audit, um Datenschutz als Positivum darzustellen?

Bäumler: Ich glaube der deutsche Fehlweg liegt darin, dass man gemeint hat, dass das Heil nur in der Gesetzgebung liegt. Bei immer mehr Datenverarbeitung hat das immer genauere und ausufernde Gesetze bedeutet.
Das hat zu einer Gesetzgebung geführt, die viele nicht mehr verstanden haben. Ich bin also nicht für diese ganz detaillierte Gesetzgebung in allen Nebensächlichkeiten. Man muss ein Gespür dafür entwickeln, wo es wirklich wichtig ist, genau zu regeln und wo man generalklauselartig vorgehen kann, ergänzt durch flankierende Maßnahmen, wie etwa einem Gütesiegel, einem Audit oder Beratungspflichten.
Sozusagen ein Mix von Generalklauseln und präziser Unnachgiebigkeit dort, wo es wirklich drauf ankommt, etwa im Gesundheitsbereich.
Damit könnte man den Wust an Datenschutzgesetzgebung etwas schlanker gestalten.

Rockenbauer: Es fällt immer wieder der Begriff 'Privacy by Default'. Bei Ihnen habe ich schon herausgelesen, dass das quasi Teil der Lösung beziehungsweise eine Conditio sine qua non ist.

Bäumler: Ja! Grundsätzlich musste man früher seinem Datenschutz hinterherlaufen und hinterherprogrammieren. Die gute Idee hier ist, dass es umgedreht wird, also entsprechende datenschutzfreundliche Voreinstellungen existieren.
Das ist, glaube ich, in der Datenschutz-Grundverordnung enthalten, wie sie auch einige weitere Dinge aus Schleswig-Holstein regelrecht wörtlich übernommen hat. Dies könnte ja ein Hoffnungsschimmer sein.
Es gibt aber natürlich noch große Unterschiede, wie zum Beispiel im Fall Facebook der irische und im Vergleich der deutsche Datenschutz agiert.

Rockenbauer: Der prominenteste Fall, Europe vs. Facebook, hat ja in Österreich seinen Ausgang genommen, wo ein damaliger Jus-Student Daten aus dem Netzwerk angefordert hat, um zu bemerken, dass vermeintlich gelöschte Daten noch gespeichert waren.

Bäumler: Darum ist die Kontrollkomponente auch so wichtig. Wo Menschen tätig sind, werden Fehler gemacht, oder man agiert zu blauäugig. Deswegen muss man eben auch in die Unternehmen gehen und vor Ort nachprüfen.

Rockenbauer: Bei der Frage nach Optimierungsbedarf im Rahmen der Datenschutz-Grundverordnung hat Frau Hansen gemeint, dass die Hersteller oft zu wenig in die Pflicht genommen würden. Auf der anderen Seite steht, dass man die europäischen Hersteller und Unternehmen, die oftmals ohnehin nur eine untergeordnete Rolle spielen, nicht noch über die Maßen belastet. Glauben Sie, dass die Erhaltung eines europäischen IT-Sektors wichtig ist, um überhaupt europäische IT-Produkte und Dienstleistungen zur Auswahl zu haben oder spielt das eher keine Rolle?

Bäumler: Ja, es sei denn es gelänge, für den europäischen Markt verbindliche Anforderungen an den Datenschutz zu formulieren, sodass auch außereuropäische Unternehmen gezwungen wären, sich an die Anforderungen für den europäischen Markt anzupassen.
Oft traut man sich aber nicht an die großen Anbieter heran. Klar, die Lobbyarbeit im Vorfeld der Datenschutz-Grundverordnung war dem Vernehmen nach intensiv und ich kann mir schon vorstellen, dass europäische Hersteller mit dem von Ihnen zitierten Argument aufgetreten sind. Es wäre schon nicht schlecht, wenn es Anbietervielfalt gäbe - auch europäische Anbieter. Aber hätte, wäre, wenn - in dieser Liga, wer als Anbieter am IT-Markt auftritt, spielen wir Datenschützer nicht mit, da können wir keinen Einfluss nehmen.

Rockenbauer: Es führt also kein Weg daran vorbei, den Kunden Awareness zu vermitteln und ihr Interesse zu wecken?

Bäumler: Ja, da sehen Sie auch die Enttäuschung nach den Snowden-Enthüllungen. Da gab es ab und zu aufmüpfige Bemerkungen von Regierungsmitgliedern, aber eigentlich merkte man, wie bei der Zerrissenheit der entscheidenden Politiker zwischen Loyalität gegenüber den USA und Loyalität gegenüber den eigenen Bürgern sich eindeutig erstere durchgesetzt hat.
Hätte man bei der Gelegenheit die USA kritisiert und die Bürger aufmerksam gemacht, hätte das schon eine Chance für europäische Hersteller sein können. Danach kam aber keinerlei die Überwachung einschränkende Gesetzgebung, eher im Gegenteil. Im Rahmen der Terrorismusbekämpfung wird auch in Deutschland seit Jahren permanent, fast zwanghaft, ein Gesetz nach dem anderen verschärft. Snowden als Chance eines Bewusstseinswandels ist verpasst worden, indem man abgewiegelt und die Problematik verniedlicht hat. Mehr noch: Man versucht eher den USA in Sachen Überwachung nachzueifern.

Rockenbauer: Die zweite Säule meiner Arbeit befasst sich ja mit IT-Sicherheit als Wettbewerbsvorteil. Ich habe die Erfahrung gemacht, dass viele Laien die Notwendigkeit für IT-Sicherheit eher verstehen. Fruchtende Argumente wären, dass man zum Beispiel Produktionsprozesse, Betriebsgeheimnisse

oder Know-how schützen muss. Datenschutz ist da vielen schon weniger wichtig.
Inwieweit sehen sie diese Bereiche verzahnt? Sind es zwei Teile eines ganzen Bildes?

Bäumler: Für mich persönlich sind es nicht komplett zwei Teile ein und derselben Sache. Die schönsten Datenschutz-Prinzipien, die nicht technisch nachvollziehbar, also datensicher, umgesetzt werden können, nützen nichts.
In der Praxis es ist es eher so, dass die Datensicherheit leichter zu vermitteln ist. Hier geraten wir in ein schwieriges Konfliktfeld.
Wenn ich Behörden vorschreibe, wie sie ihre Datenverarbeitung noch sicherer gestalten sollen, dann ist diese eventuell vor dem Bürger noch verborgener. Da ergeben sich komplizierte Fragen der Transparenz. Also muss man fragen: Datensicherheit in wessen Interesse?
Die US-Geheimdienste würde nach Snowden wahrscheinlich sagen, dass man die Datensicherheit verbessern müsse, obwohl man sich von unserer Seite vielleicht wünschen würde, dass man doch öfter durch Personen wie Snowden von solchen Dingen erfahren würde.
Datensicherheit ist also ein ambivalentes Instrument. Es kann also ein Mittel der 'Datenherren' sein, um Praktiken abzuschotten. Aber trotzdem, aufgrund der anderen Seite der Datensicherheit, bleibe ich dabei: Jedwede Regelung was und wie man etwas elektronisch verarbeiten darf wäre obsolet, wenn ihre Einhaltung nicht auch durch eine solide, datensichere Konstruktion gewährleistet ist. Datensicherheit und Datenschutz gehören also meiner Meinung nach untrennbar zusammen.
Auch durch den Trump-Wahlkampf entsteht jetzt mehr und mehr ein Bewusstsein dafür, dass man die IT-Infrastruktur vehementer absichern muss, auch in Deutschland, wo man eine riesige Behörde dafür geschaffen hat. Für Datenschutz wird aber leider, wie ich eingangs erwähnt habe, eher wenig getan. Man sieht immerhin, wozu die Politik fähig wäre, wenn man ein Thema als wichtig erkennt.

Rockenbauer: Vielleicht noch kurz zu ihrer Vorreiterrolle in Schleswig-Holstein, sowohl was sie als Person, als auch das ULD als Behörde betrifft. Hatten Sie in Ihrer aktiven Zeit das Gefühl, dass man - etwa in der Zusammenarbeit mit anderen deutschen und internationalen Behörden - einen Stein ins Rollen bringen konnte? Oder war es sozusagen noch zu früh für den Rest der Welt?

Bäumler: Alleine standen wir nicht und wir waren auch nicht für alle Maßnahmen alleine verantwortlich. Wir hatten gute Gesprächspartner, etwa bei der niederländischen oder der kanadischen Datenschutzbehörde, mit denen wir intensiv zusammengearbeitet haben.
Auch in Deutschland haben uns viele Kollegen die Daumen gedrückt und die Vorgänge in Schleswig-Holstein als richtig erachtet. Sie hatten aber in ihren Ländern einfach nicht die gleichen Bedingungen, den Weg ebenso sofort zu gehen.

Ich war etwas enttäuscht und habe gedacht, dass der Funke schneller überspringt. Mich hat vor einiger Zeit eine Journalistin nach Verabschiedung der Datenschutz-Grundverordnung angerufen und gefragt, ob ich mich denn nicht freue, da ja viele Konzepte aus Schleswig-Holstein enthalten wären. Meine Antwort war, dass das leider 20 Jahre gebraucht hätte - in der EDV ein Jahrhundert. Diese Prozesse müssen viel, viel schneller gehen. Man freut sich schon über aufgegriffene Dinge, es fehlt aber die Dynamik, es ist bis heute viel zu bürokratisch.

Rockenbauer: Sie schreiben ja in ihrem Buch 'Datenschutz als Wettbewerbsvorteil' aus dem Jahr 2002 von Mechanismen, die jetzt über die Datenschutz-Grundverordnung langsam eingeführt werden, sechzehn Jahre später. Inzwischen gibt es aber 'neue' Herausforderungsfelder wie soziale Netzwerke, in denen unzählige Datenmengen freiwillig preisgegeben werden, oder auch der Bereich der Smart Cars, die immer mehr Daten mit aufzeichnen. Hier ist das Bewusstsein ja eher spärlich ausgeprägt.

Bäumler: Gut, dass sie das nochmal sagen. Zu Beginn habe ich ja bereits erwähnt, dass marktwirtschaftlicher Datenschutz ein entsprechendes Kundenbewusstsein voraussetzt und eines der Probleme ist, dass Millionen Bürger die Warnungen der Datenschützer vor der Benutzung solcher Angebote abwägen, aber sich für diese Dienste entscheiden, weil die Vorteile in ihren Augen anscheinend überwiegen.
Da fragt man sich natürlich, ob die Leute das gar nicht wollen, ob es ihnen nicht wichtig genug ist. Liegt es an den fehlenden Alternativen der Datenschützer oder ist die Marktmacht der Konzerne zu groß? Darin liegen viele ungelöste Fragen.

Rockenbauer: Oftmals spielt eventuell eine Rolle, dass Personen für digitale Inhalte nicht zahlen wollen, wenn es eine - wenn auch aus Datenschutzsicht bedenkliche - kostenlose Alternative gibt.

Bäumler: Ganz genau, da herrscht natürlich eine Kultur der kostenlosen Benutzung, die dann aber sicherlich die Daten kostet. Da habe ich leider auch keine Lösung parat. Millionenfach entscheiden sich Menschen heute Tag für Tag gegen Datenschutz. Wenn man für so eine Sache wie den Datenschutz eintritt, also eine gute Sache für den Bürger, dann erwartet man sich gelegentlich Bestätigung. Dem ist aber nicht so. Datenschutz kommt leider oft als sperriges Thema rüber - vor allem im politischen Bereich - und zu wenig als das, was es ist: Ein Gewinner-Thema, mit dem man durchaus etwas werden kann.

Rockenbauer: Es soll schließlich ja auch ein Wettbewerbsvorteil und eine Win-Win-Win Situation für Bürger, Unternehmer und die Politik werden. Meine Fragen sind alle bestens beantwortet, ich bedanke mich herzlich für das Gespräch!

Bäumler: Sehr gerne. Das ist ein absolutes Zukunftsthema. Ich bin nur ungeduldig, wann die Zukunft endlich anfängt.

12.3 Interview Krasemann

Der Experte

Hermann Henry Krasemann ist als Jurist beim Unabhängigen Landeszentrum für Datenschutz in Schleswig-Holstein (ULD) tätig. Dort leitet er das Referat Zertifizierung.

Das Gespräch

Rockenbauer: Zuallererst vielen Dank für die Interview-Möglichkeit. Mit Frau Hansen habe ich bereits über Datenschutz als Wettbewerbschance generell gesprochen, im Rahmen dieses Gesprächs würde ich gerne auf das IT-Gütesiegel bzw. Audits speziell eingehen. Wie laufen denn Verfahren für diese beiden Zertifizierungen bei Ihnen ab, inwiefern unterscheiden sie sich?

Krasemann: Das ist bei beiden sehr unterschiedlich. Der Behördenaudit ist ein Audit, das sich auf Verfahren bezieht. Unser Datenschutz-Gütesiegel bezieht sich aber auf Produkte. Das Target of Evaluation, das zertifiziert wird, ist also schon ganz unterschiedlich, ebenso die Rechtsnormen, auf die die Vorgänge beruhen. Für das Gütesiegel haben wir eine Rechtsnorm im schleswig-holsteinischen Landesrecht, die extra dafür geschaffen wurde. Den Audit machen wir sozusagen im Rahmen unserer normalen Tätigkeit. Das Verfahrensaudit können wir also nur für Stellen aus dem öffentlichen Bereich in Schleswig-Holstein durchführen, also zum Beispiel Gemeinden, dem Landesnetz etc. Dafür prüfen wir selbst und sind auch selbst vor Ort. Üblicherweise ist das zweistufig aufgebaut, mit einer Beratung bzw. einem 'Vorab-Audit' davor. Dieses Verfahren führen wir vom ULD durch. Anders ist die Situation beim Gütesiegel. Da geht es um Produkte, die nur im öffentlichen Dienst in Schleswig-Holstein einsetzbar sein müssen, die Hersteller sind also vorwiegend Private. Diese Zertifizierung basiert ebenso auf einem zweistufigen Verfahren, wobei zuerst von uns anerkannte Sachverständige zum Zug kommen. Diese Sachverständigen analysieren das Produkt technisch und rechtlich und reichen das Gutachten bei uns ein, welches wir im Rahmen der zweiten Stufe prüfen. Im Bedarfsfall können wir uns dann noch selbst das Produkt vorführen lassen, generell überprüfen wir aber das Gutachten. Schließlich verleihen wir das Datenschutzgütesiegel Schleswig-Holstein, welches von den privaten Stellen geführt werden darf. Der rechtliche Kniff ist also sozusagen die 'Vorprüfung' für den eventuellen Einsatz im Landesbereich, sonst würde es ja gar nicht unter Landesrecht fallen.

Rockenbauer: Die herstellenden Unternehmen bekommen über den Beschaffungsaspekt also einen Anreiz, Produkte mit besonders hoher Berücksichtigung des Datenschutz anzubieten?

Krasemann: Genau, es darf ja auch mit dem Siegel geworben werden. Bei vielen ist das durchaus der Hauptantriebspunkt, das Siegel kann dann auf der Webseite oder am Produkt direkt abgebildet werden.

Rockenbauer: Da es ja im Rahmen meiner Arbeit ja nicht nur der Einsatz in und von öffentlichen Stellen, sondern auch die Nutzung von Privatpersonen zentral ist: Haben Sie das Gefühl, dass das in der Werbung ankommt? Werben Unternehmer damit offensiv oder könnte man diesen Aspekt noch ausbauen? Welche Erfahrungen haben Sie damit gemacht?

Krasemann: Sehr unterschiedliche. Die Zielrichtung ist auch sehr unterschiedlich. Einige Hersteller von Produkten, die primär gerade für den öffentlichen Dienst gedacht sind, nutzen das Siegel für Ausschreibungen. Andere haben es für Werbezwecke, gar nicht nur nach außen, aber auch um intern Absicherung zu haben, um es sozusagen als interne Revision zu nutzen. Aber der Großteil nutzt es, damit das Gütesiegel am Produkt abgebildet ist. Wieweit das dann nachgefragt wird, wissen wir nur bedingt. Ein bisschen daraus ablesen können wir es, dass das Produkt nach zwei Jahren rezertifiziert werden muss, was relativ häufig gemacht wird. Das zeigt also meines Erachtens schon, dass das Siegel gültig gehalten werden soll. Und wir merken in bestimmten Branchen, z.B. Schredder, dass das Siegel von einsetzenden Stellen im Privatbereich nachgefragt wird. Da die Endconsumer-Produkte bei unserer Zertifizierung bis dato nahezu nicht vorkommen, ist die Idee, dass ein Kunde in einem Fachgeschäft auch darauf achtet, dass ein gewisses Produkt das Gütesiegel hat, bisher noch nicht eingetreten. Das finden wir also eher im B2B Bereich, wo das Siegel es werbend genutzt wird.

Rockenbauer: Besonders in Branchen mit einem hohen Aufkommen an vertraulichen Daten bzw. besonderem Bedürfnis nach Integrität?

Krasemann: Ja, zum Beispiel im Medizinbereich. Hier existieren ja viele Vorschriften, die die Anwender vor allem auch einfach erfüllen möchten, da wissen sie bei einem nach Gütesiegel zertifiziertem Produkt natürlich, dass das möglich ist und sie erhalten die Dokumentation so, dass es entsprechend umsetzbar ist.

Rockenbauer: Wie sieht es da im deutschen bzw. europäischen Vergleich aus? Im Rahmen einer kurzen Recherche habe ich so ein Gütesiegel nur im Bundesland Mecklenburg-Vorpommern gefunden. Hat Schleswig-Holstein hier eine Vorreiterrolle inne, sind sie da sozusagen Pionier?

Krasemann: Ja, wobei man unterscheiden muss. Von öffentlichen Stellen verliehene Datenschutz-Gütesiegel gibt es eigentlich nur noch eines, das von Ihnen erwähnte von Mecklenburg-Vorpommern. Meines Wissens nach ist dort das Verfahren existent, aber noch kein Siegel verliehen worden. Von zahlreichen privaten Anbietern existieren aber solche Datenschutzsiegel oder vor allem auch Datensicherheitssiegel. Aber für den Datenschutzbereich sind wir in Deutschland im öffentlichen Bereich tatsächlich Pioniere. Das kann sich

allerdings alles mit der Datenschutz-Grundverordnung ändern, wo sich ganz neue Möglichkeiten, auch für die Zertifizierung, auftun. Aber das ist noch schwierig für uns einzuschätzen, da ist eine Reihe von Fragen offen. Vieles ist noch leider ungeklärt.

Rockenbauer: Wo wir schon bei der Datenschutz-Grundverordnung sind: Wird diese bessere Rahmenbedingungen für Zertifizierungen, wie Audits, bieten oder ist es noch zu früh, da etwas zu prognostizieren?

Krasemann: Es erhöht natürlich zuerst die Sichtbarkeit und Internationalität dieses Siegels. Nach außen hat man mit einem Siegel aus Schleswig-Holstein ja ein gewisses 'Lokalitätsproblem'. Das könnte mit einem Siegel nach Datenschutz-Grundverordnung allein marketingtechnisch verändern, da das ganze größer klingt. So gesehen wäre ich dem erst mal positiv gegenüber. Das Problem existiert aber natürlich andersherum: Mittels welches Verfahrens die Zertifizierung EU-weit erfolgen soll, ist im Moment nur bedingt erkennbar. Durch das neue Bundesdatenschutzgesetz haben wir mal eine Idee, wie in Deutschland seine Akkreditierung solcher Zertifizierungsstellen passiert. Wir sind glühende Verfechter der Zweistufigkeit, also dass nach Gutachtern noch wir als Aufsichtsbehörde kontrollieren. Die Gefahr besteht ohne eine neutrale Qualitätskontrolle natürlich immer, dass das dementsprechend nach hinten losgehen kann, weil zu viele Zertifikate ohne ausreichend Überprüfung durch die Gegend kursieren können. In verschiedenen Ländern gibt es dann eventuell verschiedene Akkreditierungsverfahren von Zertifizierungsstellen, die dann am Ende des Tages doch ein einheitliches Gütesiegel nach Datenschutz-Grundverordnung ausstellen sollen. Und es existieren ja jetzt schon unterschiedliche Auffassungen innerhalb der EU, wie man mit Unternehmen wie beispielsweise Facebook umgeht. Wenn dann ein Mitgliedstaat einem Produkt ein Siegel erteilt, ein anderer aber zum Beispiel ein Bußgeld ausspricht und dies öfter passiert, ist die Idee des Siegels natürlich verbrannt. Diese Gefahr besteht meiner Meinung nach also durchaus noch. Aber erst mal bin ich positiv gestimmt, dass die Idee des offensiv nach außen Tragens einer guten Datenschutzeinstellung überwiegen kann. Dadurch könnte man andere, besonders sensible Kundenschichten mit so einem Siegel gewinnen. Da habe ich durchaus Hoffnung.

Rockenbauer: Also sozusagen einen Return on Investment aus Datenschutz generieren?

Krasemann: Genau.

Rockenbauer: Um eine etwas internationalere Perspektive auf das Thema zu bekommen: Haben Sie das Gefühl, dass Datenschutz in Europa am größten geschrieben wird, etwa im Vergleich zu Asien oder Amerika - auch im Bereich der Zertifizierung?

Krasemann: Zu Asien kann ich eher wenig sagen, aber gerade Amerika ist in Datenschutzangelegenheiten schon etwas anders aufgestellt. Wir haben ja gerade

das Problem der Verwendung von europäischen Daten in Amerika, weil sehr viele amerikanische Anbieter wie Microsoft, Google, Amazon oder Facebook hier auf dem Markt sind. Diese Anbieter werden aus Datenschützersicht zumindest teilweise kritisch gesehen. Sehr viele dieser Unternehmen verarbeiten Daten eben in den USA. Da könnte man sich mit einem Siegel schon abgrenzen. Diese Möglichkeit steht natürlich auch den Unternehmen dort offen, das Siegel ist nicht auf Europäer beschränkt. Die Idee, Datenschutz nach außen darzustellen ist also nicht nur europäisch, es pfründet hier allerdings eher, als in den USA, weil man dort Datenschutz anders bewertet und sieht.

Rockenbauer: Um nochmal auf die Datenschutz-Grundverordnung zurückzukommen: Frau Hansen hat in unserem Gespräch gemeint, dass die Hersteller von IT-Produkten im Rahmen der Datenschutz-Grundverordnung zu wenig in die Pflicht genommen wurden. Auf der anderen Seite steht, dass die europäische Industrie mit Regulativen nicht zu sehr belastet werden soll. Glauben Sie, dass man die Hersteller von Hardware- und Softwareprodukten bzw. elektronischen Dienstleistungen durch Maßnahmen- wie beispielsweise ein Gütesiegel - von Seiten des Gesetzgebers mehr in die Pflicht nehmen müsste, oder ist eine freiwillige Zertifizierung die einzige Alternative, weil sonst die europäische Industrie den internationalen Anschluss verliert?

Krasemann: Ich glaube, etwas anderes als Freiwilligkeit funktioniert gar nicht. Alleine schon aus Praktikabilitätsgründen, wenn sich jeder ab einer gewissen Art von Datenverarbeitung zertifizieren lassen müsste, würde man eine wahnsinnig große Akkreditierungsmasse und somit einen riesigen Aufwand schaffen. Zum zweiten würde es auf starken Widerstand der Industrie stoßen. Es geht ja darum, einen Wettbewerbsvorteil zu generieren. Aus verschiedenen Erfahrungen weiß ich, dass in anderen Bundesländern, die ebenfalls so ein Siegel einführen wollten, der Widerstand der Industrie- und Handelskammern teils sehr groß war, aus Angst, ein Zwangssiegel mit verbundenen Kosten und Aufwand einzuführen das sich für manche Betriebe gar nicht auszahlen kann. Die Datenschutz-Grundverordnung hat natürlich auch Klein- und Mittelunternehmen im Blick, allerdings ist so ein Gütesiegel ab einem gewissen Niveau natürlich mit Aufwand verbunden. Aufwand für die prüfende Stelle, aber auch für das Unternehmen, welches geprüft wird. Man wird immer auf Dinge stoßen, wo nachzubessern ist. Oft fehlen Löschroutinen, Logging-Mechanismen sind zu weitgehend oder existieren gar nicht. Komplett richtig gemacht hat eigentlich noch niemand alles. Es entsteht also ein Aufwand, der zeitweise sehr groß sein kann, gerade in der Dokumentation. Wenn man so eine Zertifizierung also verpflichtend einführt, würde das einen kaum zu bewältigenden Aufwand generieren. Wobei allerdings zu beachten ist, dass viele dieser Pflichten für die Firmen auch losgelöst von einer Zertifizierung bestehen. Und schließlich geht es um einen Wettbewerbsvorteil, man kann sich ja hier gegenüber der Konkurrenz absetzen.

Rockenbauer: Im Gespräch mit Frau Hansen haben wir auch das Thema 'Attribute Based Credentials' behandelt. Es ist ja in Deutschland schon möglich, mittels mathematischer Funktion Parameter, wie zum Beispiel Volljährigkeit, auf einem Personalausweis abzufragen um das Herzeigen des Ausweises und die damit verbundene Preisgabe von unnötig viel Information zu verhindern. Dennoch nehmen diese Möglichkeit vergleichsweise wenige Personen wahr. Wie kann man, glauben Sie, die Awareness in diesem Bereich erhöhen?

Krasemann: Also generell halte ich es für eine gute Idee, ein Siegel bekannter zu machen. Stiftung Warentest zum Beispiel kennt und beachtet man etwa, unser Siegel schon weniger. Die Frage wird sein, wie das mit dem Datenschutz-Gütesiegel nach Datenschutz-Grundverordnung sein wird. Dass das trotzdem durch gute Wiedererkennbarkeit und entsprechende Öffentlichkeitswirksamkeit interessanter gestaltet werden kann, ist richtig. Dies Frage ist allerdings immer, inwieweit das den Bürger interessiert. Wir als Aufsichtsbehörde merken, dass vielen die Thematik eigentlich relativ egal ist. Diese Personen horchen erst dann auf, wenn sie zum Beispiel eine Rechnung bekommen, weil ihre Daten missbraucht werden oder wenn sie im Internet gestalkt werden, weil Daten herumgegangen sind. Ob solche Personengruppen vorher für eine Gütesiegel-Werbekampagne empfänglich sind, ist fraglich. Dieses grundsätzliche Problem versuchen wir daher schon in der Schule anzugehen, in dem wir versuchen, Schüler bzw. ganze Klassen für das Thema zu sensibilisieren und Verständnis zu wecken. Deswegen: Werbung ist immer gut, kann aber auch ziemlich stark verpuffen. Gerade bei einer sensiblen Thematik, wie zum Beispiel dem neuen Personalausweis mit den Identifikationsmöglichkeiten, sind das oft Dinge, die nicht in einem 30-Sekunden-Werbespot dargestellt werden können. Oft sind vielen Leuten maschinenlesbare Vorgänge etwas suspekt und dann würde man damit vielleicht sogar den gegenteiligen Effekt erzielen und Misstrauen für solche Attribute Based Credentials schaffen. Dem könnte man mit einem Siegel wiederum entgegenwirken, welches aussagt, dass man diesem Produkt vertrauen kann. Notwendig dafür ist meiner Meinung nach aber immer ein gewisses Grundverständnis, was überhaupt passiert. Da kommen die Schulen ins Spiel.

Rockenbauer: In welchen Bereichen ist die Awareness-Schaffung Ihrer Meinung nach schwieriger?

Krasemann: Schwierig ist es da, wo es am ehesten benötigt wird, also wo die Dinge kompliziert werden. Eben beim Personalausweis oder bei Cloud-Diensten. Gerade Letzteres ist etwas, bei denen man Fehler machen kann, wie etwa eine falsche Konfiguration. Im Businessbereich kann dem bei der Produktbenutzung noch eher entgegengetreten werden, in dem die Benutzer etwa durch vertragliche Regelungen etwas zur Kenntnis nehmen müssen. Beim Bürger bekommt man so etwas nur bedingt hin. Hier kann ich auch kein fertiges Rezept nennen. Die ursprüngliche Frage war ja, ob sich massiver Werbeeinsatz lohnt. Ich bin da etwas skeptisch, am besten

wäre hier die eigene Erfahrung des Users, der durch Anwendung merkt, welche Vorteile so ein Siegel mit sich bringt und es beim nächsten Kauf berücksichtigt. Sprich: Eigene Erfahrung ist meiner Meinung nach besser als Hochglanzwerbung.

Rockenbauer: Diese Awareness ist im betrieblichen Kontext also vielleicht leichter zu schaffen als im privaten Feld, wo das Preisargument ja oft entscheidend ist.

Krasemann: Ja genau. Die 1,99 Euro, die Threema als Alternative zu WhatsApp kostet, war für viele der Grund, nicht Threema zu verwenden sondern bei WhatsApp zu bleiben. Selbst bei Beträgen, die sich im Kaufpreis einer Kugel Eis befinden, wird dem datenschutzschlechteren Produkt da der Vorzug gegeben.

Rockenbauer: Um einen kurzen Ausblick in die Zukunft zu wagen: Gütesiegel werden im Rahmen der Datenschutz-Grundverordnung eine Rolle spielen, wie es dann implementiert und gelebt wird, steht aber alles andere als fest?

Krasemann: Richtig, genau.

Rockenbauer: Um vielleicht noch kurz zur zweiten Säule meiner Arbeit, IT-Security, zu kommen. Inwieweit sehen sie diese mit dem Datenschutz verzahnt? Viele betrachten diese zwei Thematiken ja eher getrennt voneinander. Sie haben ja schon die IT-Security-Siegel angesprochen, die vielfach existieren und eher auf breitere Nachfrage stoßen. Zusatzfrage: Kann man Unternehmen IT-Security einfacher verkaufen, als Datenschutz? Vielleicht auch mit der Argumentation des Schutzes eigener geheimer Geschäftsprozesse oder Produktpläne.

Krasemann: Ich glaube man kann das ganz gut kombinieren. Datensicherheit ist ja auch Teil des Datenschutzes. Wenn man Daten zum Beispiel frühzeitig anonymisiert und dann etwas laschere Datensicherheit auf diese anonymisierten Daten anwendet, kann das irgendwann relativ egal sein, wenn die anonymisierten Daten rauskommen. Wenn man also beispielsweise Kreditkartendaten frühzeitig wieder löscht und sich dann eine Sicherheitslücke auftut, werden jedenfalls keine Kreditkartendaten gestohlen, weil sie ja gar nicht mehr vorhanden sind. Datenschutz und Datensicherheit hängen da durchaus eng miteinander zusammen. Gerade Anonymisierung und frühzeitiges Löschen kann den Aufwand an die Datensicherheit verringern. Für viele Branchen geht das natürlich nicht, nichtsdestotrotz kann das manchmal eine interessante Überlegung sein. Gerade in Business-Bereichen, wie zum Beispiel dem Medizinsektor, ist man nicht nur auf Datensicherheit, sondern auch auf Datenschutz aus. Ein Leiter einer Klinik will seine Krankenakten natürlich nicht irgendwo frei im Internet veröffentlicht wissen, er will Datensicherheit und Datenschutz. Der eigene Leidensdruck ist in diesen Bereich natürlich gegeben. Sich also ausschließlich auf Datensicherheit zu konzentrieren ist auch nicht die richtige Lösung. Erst recht, weil mit der neuen Datenschutz-Grundverordnung die Möglichkeiten der Aufsichtsbehörden,

Bußgelder zu erhöhen, deutlich erweitert wurden. Verantwortliche Personen, wie zum Beispiel Geschäftsführer, können dann mit der Benutzung von Gütesiegel-Produkten, die ja aussagen, dass hier rechtskonform gehandelt wird, vielleicht etwas besser schlafen.

Rockenbauer: Genau, diese Bußgelder wie zum Beispiel die 4 Prozent-Strafe auf Basis des Umsatzes habe ich auch schon mit Frau Hansen besprochen, die gemeint hat, dass dies ein wichtiges Druckmittel darstellt. Für das kleine oder mittlere Unternehmen wird es laut ihr aus Fahrlässigkeit ja eher nicht zu dieser Höchststrafe kommen.

Krasemann: Ja, genau.

Rockenbauer: Ich bedanke mich für das interessante Gespräch!

Krasemann: Ich danke auch!

12.4 Interview Himmelbauer

Zur Person

Eva-Maria Himmelbauer ist Abgeordnete zum Nationalrat und gehört dem Parlamentsklub der Österreichischen Volkspartei an, für den sie als Bereichssprecherin für Innovation und Telekommunikation tätig ist.
Die studierte Wirtschaftsinformatikerin (Technische Universität Wien) war und ist im Familienunternehmen EDV-Himmelbauer tätig und verfügt über weitere Berufserfahrung, etwa bei IBM Österreich oder Siemens Intelligent Traffic Systems.
Zu ihren politischen Funktionen zählen unter anderem die der Bezirksvorsitzenden der Jungen Wirtschaft Hollabrunn.

Das Gespräch

Rockenbauer: Zuallererst vielen herzlichen Dank für die Interviewmöglichkeit! Als Bereichssprecherin für Innovation und Telekommunikation des ÖVP-Parlamentsklubs waren Sie maßgebliche Verhandlerin für das Datenschutz-Anpassungsgesetz 2018 bzw. die Novelle des Datenschutzgesetzes in Hinblick auf die Datenschutz-Grundverordnung der EU. Eventuell können Sie ein kurzes Resümee über den finalen Entwurf ziehen?

Himmelbauer: Die Datenschutz-Grundverordnung gibt ja schon klare Richtungen vor, die umzusetzen sind, da sie ab 25. Mai 2018 anzuwenden ist. Die DSGVO hat aber mehr als 40 Öffnungsklauseln, die für uns als Gesetzgeber in der Betrachtung relevant waren.
Meine Ausgangslage war, den Datenschutz betreffend, dem Einzelnen die Möglichkeit zu geben, sein Recht wahrzunehmen - hier sagt die Verordnung dezidiert aus, welche Rechte existieren. Gleichzeitig - wenn es um die Umsetzung geht - sprechen wir von sehr viel Arbeit für die Unternehmer. Hier galt es, diese Bürde und damit den bürokratischen Aufwand möglichst gering zu halten.
Das ist uns in vielerlei Hinsicht gelungen, einzelne Verbesserung konnten wir zum Beispiel bei der Öffnungsklausel hinsichtlich des Zustimmungsalters erreichen, das von 16 auf 14 Jahren herabgesenkt wurde. Das einfach deshalb, weil in Österreich mit 14 Jahren bereits geringfügige Geschäfte des täglichen Bedarfs durchgeführt werden dürfen und es die Lebensrealität widerspiegelt, wenn man mit 14 Jahren eine App im Appstore kaufen kann und dann sinnvollerweise auch der Datenschutzerklärung zustimmen darf. Das war in den Verhandlungen auch breiter Konsens.
Was andere Bereiche, zum Beispiel die Datenschutzbehörde, betrifft, war das etwas schwieriger. Sie fungiert ja gleichzeitig als Kontroll- und Strafbehörde. Eine Trennung hat hier nicht stattgefunden, aber mit dem Verweis an ein derzeit beim VwGH anhängiges Verfahren betreffend der FMA,

wo es genau darum geht, in welcher Höhe ein Kontrollorgan auch Strafen aussprechen kann. Dieses Verfahren wollen wir auch zur Kenntnis nehmen und es kann folgend noch zu Änderungen kommen.

Rockenbauer: Diese Nicht-Trennung wurde ja auch in mehreren außerparlamentarischen Stellungnahmen - zum Beispiel in jener der Industriellenvereinigung - kritisiert. Als Beispiel der Trennung wurden dort der Bereich Kartellrecht mit Kartellgericht und Bundeswettbewerbsbehörde benannt.
Grundsätzlich ist Ihrer Meinung das Anpassungsgesetz also eine gelungene Umsetzung?

Himmelbauer: Ja, den Prozess an sich kann man kritisieren, da das Gesetz Ende Mai in Begutachtung kam, Anfang Juni im Ministerrat war und dem Parlament überstellt wurde. So musste der Prozess zügig in Gang kommen, da die Umstellung zeitnah erfolgen muss, um den unternehmen Rechtssicherheit zu bieten. Wir hätten das natürlich auch im Herbst machen können, aber aufgrund der derzeitigen Lage und des Wahltermins 15. Oktober hätte es dazu führen können, dass das Gesetz gar nicht mehr in dieser Legislaturperiode zustande kommt. Das hätte dazu geführt, dass es vermutlich erst im nächsten Jahr beschlossen worden wäre und das wiederum hätte Rechtsunsicherheit zur Folge gehabt.

Rockenbauer: Um kurz zur Datenschutz-Grundverordnung zu kommen: Wie bewerten Sie die Verordnung andernfürsich?

Himmelbauer: Die Intention an sich kann ich gut verstehen, Daten sind ja das 'neue Öl' und für den Einzelnen ist es schwierig, in dieser technologischen Welt mit allen Diensten und Applikationen die Übersicht zu bewahren, welche Daten von ihm wo existieren und was mit ihnen geschieht.
Die Grundintention, verbindliche Rechte zu schaffen, die jeder einfordern kann, die somit auch Kontrolle über die Daten ermöglichen, finde ich richtig. Im Prozedere der Verordnungserstellung ist leider Gottes in diesen Verhandlungen viel zu Lasten der Wirtschaft passiert.
Auch Unternehmen mit weniger als 250 Mitarbeitern sind von hohem bürokratischem Aufwand, beispielsweise bei dem Verfahrensverzeichnis oder der Folgeabschätzung, betroffen. Diese hätte man beispielsweise davon verschonen können. Ich kenne das aus Klein- und Mittelunternehmen, die in Zukunft diese Tätigkeiten auslagern müssen. Die 'KMU-Klausel' *[Besagt, dass gewisse Artikel erst ab 250 MA im Unternehmen anzuwenden sind, Anm.]* wurde leider sehr verwaschen. Das führt dazu, dass doch jedes Unternehmen unter diese Regelungen fallen könnte. Hier steht nämlich dezidiert in der Verordnung, dass KMU nur nicht darunter fallen, wenn nicht regelmäßig eine Datenverarbeitung stattfindet. Die Frage ist, ob nicht bereits Personalverwaltung und Buchhaltung als regelmäßige Datenverarbeitung gelten und somit fast jeder Betrieb in die Regelung fällt.

Hier verstehe ich den Unmut und die Unsicherheit mancher Unternehmer. Auch etwa im Bereich des Strafausmaß'. Ich sehe ein, dass - wenn man sich an den großen Konzernen ausrichtet - eine Abschreckung gegeben sein muss. Für die Kleinunternehmen sind diese Strafausmaße aber unverhältnismäßig hoch.

Rockenbauer: In einem bereits stattgefundenen Gespräch mit Frau Hansen - der Leiterin der Datenschutzbehörde in Schleswig-Holstein - hat sie die Wichtigkeit dieser Strafhöhen betonte, um als Behörde tatsächlich ernst genommen zu werden. Auf die Frage der KMU entgegnete sie, dass dort natürlich andere Maßstäbe anzuwenden sind.
Wobei dies bei einer legistischen Verankerung hoher Strafen vermutlich schwierig zu garantieren ist.

Himmelbauer: Ganz genau.

Rockenbauer: Ganz grundsätzlich, weil Sie viel mit Datenschutzgesetzgebung zu tun haben und hatten: Kann Datenschutzrecht auch einen Wettbewerbsvorteil - ein Positivum darstellen - sofern richtig gestaltet? Besonders für Österreich bzw. Europa - Stichwort Austrian Cloud bzw. Services direkt in Österreich bzw. der EU?

Himmelbauer: Ich glaube durchaus, dass wir das als USP nutzen können.
Hier sind sowohl Persönlichkeits-, als auch Unternehmensrechte den Datenschutz betreffend gewahrt. Dass die eigenen Daten vertrauenswürdig behandelt werden, ist ein positives Merkmal.
Zum Wettbewerbsvorteil braucht es mehr als die Verordnung. Es bedarf mehr europäischer Unternehmen im Bereich Informationstechnologie und Internet, europäische Rechenzentren müssen entstehen und ihre Services anbieten.
Aktuell haben wir in diesem Bereich vor allem Rechenzentren, die sich in amerikanischer Hand befinden. Dabei existieren in vielen Bereichen ja schon Vorgaben, dass die Daten auf Servern in der EU gespeichert sein müssen. Da braucht es aber noch viel, viel mehr. Die Verordnung ist sicher ein guter Schritt um den Rechtsrahmen auch zu gestalten, das kann aber nur die eine Seite sein.

Rockenbauer: Von den großen IT-Unternehmen ist ja SAP einer der wenigen internationalen Spitzenreiter mit Hauptsitz in Europa. Besteht nicht auch die Gefahr, dass wir - als Europa - Kernkompetenzen verlieren, wenn es nur mehr 'externe' Hardware- und Softwarehersteller gibt?

Himmelbauer: Genau. Viele Unternehmen haben ja Standorte in Europa, sind aber nichtsdestotrotz aus den USA. Microsoft sitzt in Irland genauso wie Facebook, Google ja auch in Deutschland.

Rockenbauer: Zu den Datenschutzbehörden: Wie sehen sie die - auch zukünftige - Rolle der Behörde? Um Zuge meiner bisherigen Gespräche und Forschungsarbeit bin ich auf die Wichtigkeit der Beratungskomponente aufmerksam geworden. Ist das in Österreich möglich?

Himmelbauer: Zumindest ansatzweise haben wir das im Gesetzestext des Datenschutz-Anpassungsgesetz - das ja nicht beschlossen wurde, es kam ja eine Novelle des bestehenden Datenschutzgesetzes - hineingeschrieben, dass die Behörde eine beratende Tätigkeit haben soll und im Rahmen der Prüfung auch beraten vor strafen soll. Die Behörde steht aber hier natürlich auch vor großen Herausforderungen, sie kann nicht für jedes betroffene Unternehmen innerhalb eines Jahres das Verfahrensverzeichnis und die Folgeabschätzung erledigen. Wir haben hier zum Beispiel auch erreicht, dass alle Einwilligungen, die DSGVO-konform sind, weiterhin Gültigkeit behalten und nicht vor dem 25. Mai 2018 neu eingeholt werden müssen. Auch das wäre überbordende Bürokratie gewesen.
Die Behörde soll in Zukunft also auch beratend tätig sein, wird es aber nicht schaffen, die erforderlichen Aufgaben gänzlich für das Unternehmen zu erledigen.

Rockenbauer: In diesem Bereich hat man im ULD in Schleswig-Holstein ja auch schon zahlreiche positive Erfahrungen gemacht, wo Unternehmen etwa eine rechtssichere Antwort bei Anfrage an die Behörde bekommen, ob ein gewisses Vorgehen regelkonform ist.
Ein weiterer Bereich ist der der Datenschutzgütesiegel und -prüfzeichen, die ja durch die DSGVO ermöglicht werden. Die gab es bis dato in Deutschland sehr vereinzelt, großteils nur auf Landesebene.
Kann so ein Gütesiegel Awareness schaffen, oder wird hier eher nur auf den Preis für ein Produkt, eine Dienstleistung oder ein Service geschaut?

Himmelbauer: Wir reden in vielen Bereichen ja gar nicht über Preise. Ich kann Facebook ja nur nützen, wenn ich die AGBs und die Datenschutzbestimmungen akzeptiere, ich kann es also nur nutzen, oder eben nicht. Da gibt es keinen direkten Preis dafür, der Preis sind ja dann sozusagen die eigenen Daten, die man zur Verfügung stellt.
Solche Siegel können natürlich auch Bewusstsein für einen Teil der Bevölkerung schaffen. Viel wichtiger ist allerdings, dass die Verordnung solche Services von außerhalb der Union ja auf Einhaltung des europäischen Datenschutzstandards verpflichtet, falls sie innerhalb der EU benutzt werden sollen. So kann der User sich auf dieses Schutzniveau verlassen und sich seiner Rechte sicher sein.
Solche Gütesiegel und Prüfzeichen finde ich generell schon sinnvoll, allerdings dürfen sie nicht verpflichtend gemacht werden.

Rockenbauer: Kann man denn ihrer Meinung nach Datenschutz für die breite Bevölkerung greifbar machen oder ist es ein schwer vermittelbares Thema?

Himmelbauer: Ich halte das für eine Generationenfrage. Vor drei Wochen waren zwei HTL-Klassen auf Besuch hier im Parlament, die sich sehr mit dem Thema Datenschutz befassen. Die Schüler wissen ganz genau, wo die Privatsphäre-Einstellungen ihrer Services sind, was sie dort einstellen können und welche Gefahren dadurch entstehen. Sie sind sich auch dessen bewusst, was sie posten.
Es gibt aber natürlich auch andere Gruppen, auch ältere Generationen, die sich im späteren Lebensverlauf hineingelebt haben, für die das noch immer diese etwas schwer zu handhabende Black Box darstellt. Da benötigt es auch viel technisches Verständnis, etwa was ein Algorithmus überhaupt ist, oder wie Speicherung erfolgt. Das kann man natürlich nicht bei der gesamten Bevölkerung voraussetzen. Hier kann ein Gütesiegel - wie es vorhin erwähnt wurde - wahrscheinlich schon ein gewisses Maß an Sicherheit geben.
Aber wie gesagt ist die Thematik sicherlich eine Generationenfrage, wo mit Verlauf der Zeit immer mehr Bewusstsein entsteht. Ich glaube aber, dass in der Schule digitale Kompetenzen stärker gefördert werden müssen, wo etwa Themen wie Datenschutz oder Datensicherheit vermittelt werden.

Rockenbauer: Also grundsätzlich ein leichter Automatismus aufgrund der jungen Generationen, die mit dem Thema vertraut sind und zu setzende Maßnahmen und Unterstützungen bei denjenigen Bevölkerungsgruppen, die sich - etwa altersbedingt - in der Materie wenig oder gar nicht auskennen.

Himmelbauer: Ja genau. Das Thema haben wir ja nicht nur bei der Datenschutz-Grundverordnung über die wir sprechen, sondern auch in anderen Bereichen Bei ELGA im Gesundheitsbereich beispielsweise, wo sich der Patient die Frage stellt, was mit seinen Daten passiert.
Es sind manchmal dieselben Personen, die etwa ELGA nicht vertrauen aber trotzdem die Apple Watch tragen, die ihre Vitaldaten an einen amerikanischen Server schickt.

Rockenbauer: Stichwort 'Privacy by Default' - müssen zu den rechtlichen Rahmenbedingungen für Datenschutz auch technische Rahmenbedingungen gesetzt werden?

Himmelbauer: 'Privacy by Default' ist ja auch vorgesehen, es kommt dezidiert - soweit ich das aus dem Ausschuss im Europäischen Parlament mitbekommen habe - ja auch über die ePrivacy-Verordnung.
An sich eine sehr gute Maßnahme, es soll ja eine bewusste Entscheidung sein, was mit den eigenen Daten geschieht. Man kann sie beispielsweise auch für die Weiterleitung an Dritte freigeben, wenn es eigener Überlegung nach sinnvoll erscheint. Es soll nur eine bewusste Entscheidung sein.

Rockenbauer: Abschließend die Frage, welche Rahmenbedingungen Sie sich für einen österreichischen bzw. europäischen IT-Standort wünschen würden? Sind

das Maßnahmen im Bereich Datenschutz, IT-Security, Bildung oder gänzlich andere?

Himmelbauer: Prinzipiell würden wir mehr IT-Fachkräfte benötigen, diese Suche nach Informatikern und IT-versierten Kräften ist deutlich spürbar. Hier benötigt es Fachkompetenz, die aus den eigenen Reihen kommen muss. Sie kann teilweise aus dem Ausland abgedeckt werden, es wäre aber sinnvoll, unsere Schüler und Studenten in diesen Zukunftsbereichen ausbilden.
Wir können die Berufsbilder, die in zehn oder fünfzehn Jahren existieren werden, nicht vorhersagen, aber Fachkräfte im IT-Bereich werden wir benötigen. Vor fünfzehn Jahren war es auch nicht absehbar, dass nun besonders viele App-Entwickler gebraucht werden.
Das heißt für mich in der Schule anzusetzen und digitale Kompetenzen zu vermitteln. Nicht nur Anwendungen wie Word oder Excel zu erlernen, sondern prinzipielles Technologieverständnis an die Schüler weiterzugeben, es geht aber hin bis zum digitalen Humanismus mit Umgangsformen im Netz und ethischen Fragestellungen. Das ist ein Teil, den auch wir als Gesetzgeber gestalten können.
Darüber hinaus benötigen wir auch Maßnahmen im Gebiet der Infrastruktur - Breitbandausbau - vor allem im ländlichen Bereich.
Der Gesetzgeber darf sich auch nicht der Illusion hingeben, technischen Wandel aufhalten zu können, analog zu Beispielen aus früheren industriellen Revolutionen, wo der Zug nicht schneller als 30 km/h fahren durfte, da der Aberglaube herrschte, dass man eine schnellere Fahrt nicht überleben würde.
Hier müssen wir also Rahmenbedingungen setzen, dass Innovation in technischer Hinsicht passieren kann und dass wir eine Umwelt formen können, in der alle von den Chancen dieser Digitalisierung profitieren können.

Rockenbauer: Wie fällt ihre Prognose in dieser Hinsicht für den Österreich und Europa aus? Besteht eine Chance, einen zukunftsfähigen IT-Standort zu schaffen?

Himmelbauer: Ich hoffe schon, ich sehe auch die Möglichkeiten darin. Dafür benötigt es allerdings die Europäische Union.
Wenn sich ein Unternehmen etablieren will, ist natürlich nicht nur der österreichische, sondern auch der größere europäische Markt interessant. Das Internet kennt keine nationalstaatlichen Grenzen.
Wir müssen also auf europäischer Ebene harmonisieren - wie etwa jetzt durch die DSGVO - und auch vorantreiben, digitaler Binnenmarkt lautet hier das Stichwort. Es soll hier also die Chance genutzt werden können, einen breiten Markt für Services, Dienstleistungen und Produkte zur Verfügung zu haben und einen Standort zu haben, um auch über den Kontinent hinausgehen zu können.

Rockenbauer: 'Europe based' sozusagen.

Himmelbauer: Ganz genau.

Rockenbauer: Vielen Dank für das interessante Gespräch!