WIEN / 29. April 2024

Stellungnahme zum NISG 2024

Ministerialentwurf betreffend Erlass eines Bundesgesetzes zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz 2024 – NISG 2024) und Änderung des Telekommunikationsgesetz 2021 und des Gesundheitstelematikgesetz 2012

Für epicenter.works
Sebastian Kneidinger
Thomas Lohninger

EPICENTER .WORKS
for digital rights

VORWORT UND KURZFASSUNG

Wir bedanken uns für die Möglichkeit, im Rahmen des Begutachtungsverfahrens[1] folgende Stellungnahme abgeben zu können. Wir haben uns dabei auf jene Punkte konzentriert, bei denen der österreichische Gesetzgeber auch den größten Umsetzungsspielraum im Rahmen der europarechtlichen Vorgaben hat und daher auch noch Möglichkeit zur Verbesserung im Zuge des nationalen Gesetzgebungsverfahrens besteht.

IT-Sicherheit ist eine staatliche Kernaufgabe in der Informationsgesellschaft. Kaum ein Gesellschaftsbereich ist heutzutage nicht abhängig von der Sicherheit vernetzter Systeme (Wirtschaft, Bildung, Demokratie, Medien, Verwaltung, etc.). Ausfälle und Manipulationen von Systemen hätten desaströse Konsequenzen für die Grundrechte der Betroffenen, den Wirtschaftsstandort und das Vertrauen in staatliches Handeln. Die hybriden Bedrohungslagen staatlicher und nicht-staatlicher Akteuere erfordern dringend mehr Investitionen in die Resilienz kritischer Systeme. Die derzeitige IT-Sicherheitssituation in Österreich lässt vor diesem Hintergrund vieles zu wünschen übrig.

Wir empfehlen die grundlegende Architektur des vorliegenden Entwurfes zu überdenken. Der vorliegende Entwurf des NIS2 Gesetzes enthält lediglich jene Verbesserungen, die europarechtlich vorgeschrieben sind. Da wo Umsetzungsspielraum besteht, wurde ein zentralistischer Ansatz gewählt, der alle Kompetenzen beim Innenministerium bündelt und jeden Kontrollmechanismus vermissen lässt. Die parlamentarische Kontrolle des Innenministeriums durch das Interpellationsrecht ist angesichts der Komplexität der Materie und der Vermischung der verschiedenen Aufgaben des Innenministeriums untauglich. Wir befürchten, dass dies dazu führt, dass die Kompetenzen im Rahmen der Cybersicherheit für allgemeine sicherheitspolizeiliche Aufgaben missbraucht werden und das eigentliche **Ziel des Gesetzes, nämlich die Erhöhung der Cybersicherheit, gerade nicht erreicht** wird. Angesichts der Tatsache, dass Österreich hier enormen Aufholbedarf hat - erinnert sei etwa an den Hackerangriff auf das Land Kärnten, den Angriff auf das Außenministerium oder die zahlreichen Angriffe auf österreichische Unternehmen[2] - sehen wir im vorliegenden Entwurf so kurz vor dem Ende der Legislaturperiode ein massives Versäumnis der österreichischen Bundesregierung und der an den Verhandlungen beteiligten Nationalratsabgeordneten.

Inhaltsverzeichnis

1 https://www.parlament.gv.at/gegenstand/XXVII/ME/326
2 https://www.wko.at/wien/news/zahl-der-cyberangriffe-stieg-um-89-prozent

ALLGEMEINER TEIL

Grundsätzlich begrüßt epicenter.works viele Regelungen des vorliegenden Gesetzesentwurfs, wie z.B. die zusätzlichen Anforderungen im Bereich der Risikomanagementmaßnahmen oder auch die Ausweitung der betroffenen Einrichtungen. Es ist jedoch anzumerken, dass jene Teile des Entwurfes, die tatsächlich eine Erhöhung der Cybersicherheit bewirken können, bereits durch die NIS2-Richtlinie abschließend geregelt wurden. Dort, wo der österreichische Gesetzgeber nun tätig geworden ist, gibt es einige problematische Punkte, die im Zuge des Gesetzgebungsprozesses dringend nachgebessert werden müssen. Im vorliegenden Entwurf überwiegen aus unserer Sicht die Verschlechterungen für die IT-Sicherheit eindeutig etwaige Verbesserungen. Zu diesen dringend verbesserungsbedürftigen Stellen zählen wir insbesondere die zu weitreichenden Kompetenzen des Bundesministers für Inneres (§ 8 Abs. 2), die vom Innenministerium bereitgestellten Informations- und Kommunikationstechnologien (IKT-Lösungen) mit kritischer Datenschutzgefahr (§ 17) und die zu weiten Ermächtigungen für Datenverarbeitungen und Datenübermittlungen (§§ 42 und 43) des vorliegenden Gesetzesentwurfes.

SPEZIFISCHER TEIL

Zu § 4: Konstruktionsfehler der nationalen Cybersicherheitsbehörde

Mit § 4 wird nunmehr der Bundesminister für Inneres als zuständige Behörde für Cyber-Sicherheit ausgestattet und übernimmt sowohl auf operativer als auch auf strategischer Ebene die zentrale Verantwortung für Cyber-Sicherheit in Österreich. Zuvor waren diese Agenden auf den Bundeskanzler und den Bundesminister für Inneres aufgeteilt.

Wir begrüßen zwar grundsätzlich die Aufhebung der bisherigen Aufteilung der Zuständigkeitsbereiche auf zwei Ministerien, halten aber die Bündelung der Zuständigkeiten und Aufgaben beim Bundesminister für Inneres insbesondere aus folgenden Gründen für verfehlt:

1. **Zielkonflikt:** Häufig verfolgen Cybersicherheit und polizeiliche Überwachungsaufgaben, etwa bei der Frage des Umgangs mit IT-Schwachstellen, gänzlich unterschiedliche Zielvorgaben. Wie aus der Debatte in Deutschland inzwischen bekannt sein sollte[3], führt dies zu einem Vertrauensverlust für Cybersicherheitsbehörden. Aufgrund der bisherigen Erfahrungen befürchten wir, dass die Cybersicherheit gegenüber der Strafverfolgung bzw. der damit verbundenen Überwachung ins Hintertreffen gerät. Dabei ist zu berücksichtigen, dass eine Cybersicherheitsbehörde mit umfangreichen Einschaubefugnissen ausgestattet bzw. auch zu einem sehr weitreichenden Einsatz von IKT-Lösungen in fremden Systemen ermächtigt ist.

3 Vgl Seite 14, „Cybersicherheit- Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland“ von Ammar Alkassar im Rahmen der öffentlichen Anhärung des Bundestagsauschuss für Digitales vom 25.01.2023; abrufbar unter: https://www.bundestag.de/resource/blob/931120/58bfd597f1f0c6f07bd9ea18d056435c/Stellungnahme-Alkassar-data.pdf

2. **Mangelnde Einbindung von Wissenschaft und Zivilgesellschaft:** Immer wieder kommen Forderungen aus der Politik, die nicht „state of the art" sind oder grundrechtlichen Anforderungen nicht genügen, wie z.B. ein „Verschlüsselungsverbot"[4]. Wir befürchten, dass dies durch die Ansiedlung aller Kompetenzen im Innenministerium zu einem abschreckenden Effekt für den Austausch zwischen politischen Entscheidungsträger:innen mit Wissenschaft, Zivilgesellschaft und IT-Sicherheitscommunity führen wird. In der Konsequenz gerät Österreich hier weiter ins Hintertreffen.

3. **Personalausstattung:** Laut dem letzten Rechnungshofbericht zur Koordination der Cybersicherheit in Österreich[5] waren weder das Bundeskanzleramt noch das Innenministerium in der Lage, die zur Verfügung gestellten Planstellen zu besetzen. Dies stellt ein massives Risiko für die Cyber-Sicherheit dar. Wir bezweifeln, dass die derzeit vorgeschlagene Konstruktion geeignet ist, dieses Problem zu lösen. **Die vorgeschlagene Regelung kann den Personalnotstand nicht lösen**, da geeignete Fachkräfte im IT-Sicherheitsbereich weitaus mehr in der Privatwirtschaft verdienen als nach den Bestimmungen des Besoldungsrechts möglich wäre. Lediglich eine Auslagerung auf eine GmbH wäre hier eine tragbare Lösung. Diesbezüglich sei auf die kolportierten enormen Kosten für die Notfallhilfe im Fall des Cybersicherheitsvorfalls der Kärntner Landesregierung verwiesen. Ähnliche Notfälle werden folgen und bis heute fehlt es an ausreichend professionellem Personal für die öffentliche Hand um auf solche Angriffe zu reagieren, geschweige denn staatliche Infrastruktur davor zu schützen.

Vor diesem Hintergrund regen wir, wie bereits in unserer Stellungnahme zum ersten NISG[6], die Einrichtung eines Bundesamtes für Netz- und Informationssicherheit an, wie es derzeit etwa auch in Deutschland besteht Dieses sollte aus den genannten Gründen nicht im Ressortbereich des Innenministeriums[7] angesiedelt sein und weiters mit einer entsprechenden Unabhängigkeit ausgestattet sein. Ebenfalls die Konstruktion ähnlich der RTR GmbH und TKK würde sich für diesen Bereich anbieten. In einem solchen Bundesamt könnten die Präventionskapazitäten im NIS-Bereich effektiv und effizient gebündelt, vorhandene Expertise eingebracht und weitere Expertise aufgebaut werden.

In der hybriden Bedrohungslage des 21. Jahrhunderts drohen mit der vorliegenden Konstruktion auch weitaus höhere Kosten für die Steuerzahler:innen. Wenn weiterhin in jedem gravierenden IT-Sicherheitsvorfall teure Fachkräfte aus der Privatwirtschaft zugezogen werden müssen, ist dies weitaus teurer als eine Bündelung von spezialisiertem Personal in einer GmbH, das für die Reaktion auf solche Vorfälle zur Verfügung stünde.

Zu § 8 Abs 2: Alleinige Ernennung des nationalen CSIRT durch BMI

Der Bundesminister für Inneres hat bei Vorliegen der Voraussetzungen gemäß § 9 NISG 2024 eine Einrichtung zur Wahrnehmung der Aufgaben des nationalen CSIRT zu ermächtigen. Das nationale CSIRT ist eine Schlüsseleinrichtung für die Cyber-Sicherheit im Allgemeinen und für die Umsetzung des NISG 2024 mit den dazugehörigen massiven Einsichtsrechten im Besonderen. Aufgrund dieser enormen Relevanz sehen wir es als äußerst kritisch an, dass der Bundesminister für Inneres eine derart wichtige Entscheidung im Alleingang treffen kann und keine nachgelagerte Kontrolle vorgesehen ist. Wir schlagen daher vor, diese Ermächtigung dem „Inneren Kreis der operativen

4 https://www.derstandard.at/story/2000010739866/staatliche-hintertueren-12-antworten-zum-verschluesselungsverbot und https://netzpolitik.org/2023/eu-beraet-ueber-going-dark-hinter-verschlossenen-tueren/

5 Seite 93, abrufbar unter: https://www.rechnungshof.gv.at/rh/home/home/2022-13_Koordination_Cyber-Sicherheit.pdf

6 Abrufbar unter: http://epicenter.works/content/stellungnahme-zum-netz-und-informationssystemsicherheitsgesetz-nisg

7 Litauen siedelte zB ihr National Cyber Security Centre beim Verteidigungsministerium an

Koordinierungsstruktur“ (IKDOK), bestehend aus Vertretern des Bundeskanzlers, des Bundesministers für Inneres, des Bundesministers für Landesverteidigung und des Bundesministers für europäische und internationale Angelegenheiten , zu übertragen. Dies sollte auch für die Kompetenz zum Widerruf der Ermächtigung gelten (vgl § 10 Abs 7) .

In diesem Zusammenhang möchten wir zum Ausdruck bringen, dass wir die Arbeit von CERT.at als bisheriges nationales CSIRT außerordentlich schätzen und hoffen, dass diese Konstellation auch weiterhin erhalten bleibt. Wir kennen keine Einrichtung in Österreich, die eine vergleichbare Kompetenz oder ein ähnliches Vertrauen der relevanten Stakeholder genießt.

Zu § 10: Aufsicht von CSIRTs, Weisungsrecht und anonyme Meldungen

§ 10 sieht vor, dass die CSIRTs hinsichtlich ihrer Tätigkeit der Aufsicht des Bundesministers für Inneres unterliegen, wozu gemäß Abs. 4 auch die Verpflichtung der CSIRTs gehört, alle zur Ausübung des Aufsichtsrechts erforderlichen Auskünfte zu erteilen und die dafür notwendigen Unterlagen zu übermitteln.

Wir erachten die derzeitige Aufsichtskompetenz als zu umfassend bzw. zu ungenau formuliert. So sieht Abs. 2 vor, dass der Bundesminister für Inneres den CSIRTs in Ausübung seines Aufsichtsrechts Weisungen erteilen kann, insbesondere zur Wahrung „sicherheitspolitischer Interessen“. Dies sollte dahingehend präzisiert werden, dass dieses **Weisungsrecht nur der Vollziehung der Gesetze im Kontext der Cyber-Sicherheit dient**, für die die CSIRTs auch eingerichtet wurden, und nicht etwa der Verfolgung anderer Zwecke.

Weiters weisen wir darauf hin, dass es zu den Aufgaben der CSIRTs gehört, freiwillige Meldungen im Sinne des § 37 entgegenzunehmen, die auch anonym erfolgen können müssen. In der Praxis ist es jedoch denkbar, dass Einrichtungen, die eine freiwillige Meldung abgeben, im direkten Austausch mit dem CSIRT keine anonyme Meldung abgeben können oder wollen, aber gegenüber dem Bundesministerium für Inneres ihre Anonymität gewahrt wissen wollen. Bei kritischen Meldungen gibt es sehr oft die Notwendigkeit nachzufragen, und ein produktiver Austausch über die Bedrohungslage hilft schnell adäquat zu reagieren. Wir empfehlen daher, den Passus entsprechend zu ergänzen, um eine solche Meldung zu ermöglichen und damit auch die tatsächliche Nutzung der freiwilligen Meldung zu fördern. **Sollte die Anonymität gegenüber dem Innenministerium nicht gewahrt sein, ist mit einem Ausbleiben von Meldungen zu rechnen.**

Aus unserer Sicht wäre es empfehlenswert Aufsichts- und Weiseungskompetenzen auf jenes Maß zu begrenzen, welches absolut notwendig ist. Aus unserer Praxiserfahrung wissen wir, dass wesentliche Akteure aus dem Bereich der Wissenschaft und der Zivilgesellschaft, durchaus berechtigte, Vorbehalte gegenüber dem Innenministerium haben. Ohne einer solchen Zusammenarbeit aller für die IT-Sicherheit engagierten Kräfte in Österreich wird es aber wohl kaum zu Verbesserungen im hochkomplexen und stark vernetzten Themenbereich der Cybersicherheit kommen.

Zu § 11: Koordinierte Offenlegung von Schwachstellen

Der vorliegende Gesetzesentwurf sieht vor, dass das nationale CSIRT für die Koordinierung der Meldungen von Schwachstellen zuständig ist. Abs. 2 sieht weiters vor, dass natürliche und juristische Personen auf Wunsch eine Schwachstelle anonym an das nationale CSIRT melden können und die Anonymität auch in weiterer Folge zu wahren ist.

Mit § 11 wird zwar dem Wortlaut nach den Vorgaben der NIS 2 Richtlinie entsprochen, dem Ziel und Zweck der Bestimmung, nämlich die koordinierte Offenlegung von Schwachstellen zu erleichtern, wird diese **Minimalvariante** der Umsetzung jedoch **nicht gerecht**. Wie sich aus Erwägungsgrund 60 der NIS 2-Richtlinie ergibt, soll nicht nur eine anonyme Meldung ermöglicht werden, sondern es sollen auch mögliche **straf- und zivilrechtliche Fragen** geregelt werden, die sich im Zusammenhang mit der koordinierten Offenlegung von Schwachstellen ergeben können. Die Nichtberücksichtigung dieser Aspekte im vorliegenden Gesetz stellt aus unserer Sicht ein massives Versäumnis dar. Österreich kennt sowohl strafrechtliche (§ 118a StGB) als auch datenschutzrechtliche (§ 62 DSG 2018) Bestimmungen, die eine massive Hürde für die Offenlegung von Schwachstellen darstellen. Wenn Sicherheitsforscher:innen mit Freiheitsstrafen von bis zu 3 Jahren oder Verwaltungsstrafen von bis zu 50.000 konfrontiert werden, ist dies kaum geeignet, die Offenlegung von Schwachstellen zu erleichtern. Auch wenn in der Praxis in Österreich bisher keine Verurteilungen in diesem Zusammenhang bekannt geworden sind, reicht allein die Strafandrohung bzw. der mögliche Aufwand im Zuge eines Ermittlungsverfahrens aus, um Sicherheitsforscher:innen von der Offenlegung von Sicherheitslücken abzuhalten.

Damit positioniert sich **Österreich gegen die Empfehlungen der Europäischen Agentur für Cybersicherheit („ENISA“)**, die zu diesem Thema einen umfassenden Bericht erstellt hat, aus dem die Forderung nach einem sicheren Rechtsrahmen für die Offenlegung von Schwachstellen klar hervorgeht.[8]

Derzeit haben einige europäische Mitgliedsstaaten bereits einen robusten Rechtsrahmen für die Offenlegung von Schwachstellen geschaffen (z.B. Belgien) oder sind dabei, dies zu tun (z.B. Spanien). Ein weiterer Vorreiter in dieser Hinsicht ist beispielsweise Litauen. Hier wurde insbesondere unter Federführung des Verteidigungsministeriums ein sicherer Rechtsrahmen für Sicherheitsforschung und den Umgang mit Sicherheitslücken geschaffen. Dabei spielten für Litauen besonders Überlegungen zu hybriden Bedrohungsszenarien aus Russland eine wichtige Rolle, was auch für Österreich keine unrealistischen Szenarien sind. Nach Anpassung der rechtlichen Rahmenbedingungen konnte so bereits im ersten Jahr nach Einführung eine Verdoppelung der gemeldeten Sicherheitslücken beim nationalen Cybersicherheitszentrum festgestellt werden.[9]

Wir fordern daher eine Neufassung des § 118a StGB sowie des § 62 DSG 2018, so dass ein **verantwortungsvoller Umgang mit Wissen über IT-Sicherheitslücken den handelnden Personen nicht mehr zum Nachteil ausgelegt** werden kann.

Darüber hinaus regen wir eine entsprechende Einbindung von Wissenschaft und Zivilgesellschaft bei etwaigen weiteren Aktivitäten in diesem Bereich an (Erstellung von Bug Bounty Programmen, Vertrauensaufbau mit der Community und Verbesserung der Kommunikation).

Gerne möchten wir in diesem Zusammenhang auf unsere ausführliche Stellungnahme zu dieser Thematik vom 19. April 2023 verweisen[10] und auf medial diskutierte Fälle, in denen dieses Problem sehr reale Konsequenzen für Sicherheitsforscher:innen hatte[11].

8 Vgl Seite 74 Report „Coordinated Vulnerability Disclosure Policies in the EU“, ENISA, April 2022

9 Siehe Seite 11, „Key trends and statistics of the national cyber security status of Lihtuania 2021- Q1 2022“, Ministry of defence of the Republic of Lithuania , abrufbar unter: https://www.nksc.lt/doc/en/Key-trends-and-statistics-2021-q1-2022.pdf

10 Stellungnahme zu Verschärfungen Cyberkriminalität, Link: http://epicenter.works/fileadmin/import/epicenter.works_-_verschaerfungen_computerkriminalitaet_stgb2023.pdf

11 https://epicenter.works/content/massive-sicherheitsluecke-in-oesterreich-testetat-aufgedeckt-gesundheitsministerium

Zu § 15: Fehlende wissenschaftliche und zivilgesellschaftliche Einbindung bei der österreichischen Cybersicherheitsstrategie

§ 15 sieht vor, dass die Bundesregierung eine nationale Cyber-Sicherheitsstrategie verabschiedet. Wie bereits zu § 4 angemerkt, ist die Einbindung von Wissenschaft und Zivilgesellschaft in Fragen der Cybersicherheit durch staatliche Stellen derzeit unzureichend. Gerade bei einem so grundlegenden Dokument wie einer mehrjährigen nationalen Strategie ist dieser Umstand besonders kritisch zu betrachten. Wir regen daher an, gesetzlich Mechanismen vorzusehen, die eine entsprechende Einbindung sicherstellen.

Zu § 17: Zentrale IKT Lösungen mit kritischer Datenschutzgefahr

Wie bereits in der alten Fassung des NIS-Gesetzes findet sich im NISG 2024 eine gesetzliche Verpflichtung des Bundesministers für Inneres zum Betrieb von IKT-Lösungen zur Erfüllung seiner Aufgaben. In § 17 Abs. 2 findet sich darüber hinaus eine Ermächtigung des Bundesministers für Inneres, IKT-Lösungen zur Früherkennung von Risiken, Cyber-Bedrohungen oder Cyber-Sicherheitsvorfällen von Netz- und Informationssystemen zu betreiben, wobei wesentliche oder wichtige Einrichtungen an diesen IKT-Lösungen teilnehmen und dabei bestimmen können, welche Daten übermittelt werden.

Grundsätzlich begrüßen wir diesen Ansatz der Bereitstellung von Lösungen zur Verbesserung der IT-Sicherheit durch den Staat. Wir geben aber zu bedenken, dass derartige IKT-Lösungen häufig Daten in außerordentlich großem Umfang erfassen und weiterverarbeiten, was wiederum die Gefahr einer **anlasslosen Massenüberwachung** mit sich bringt und damit auch die datenschutzrechtliche Zulässigkeit fraglich erscheinen lässt. Daher sollte in jedem Fall eine Präzisierung der zulässigen Ausgestaltung bzw. der Zulässigkeit der Datenverarbeitung erfolgen. Aus datenschutzrechtlicher Sicht noch sinnvoller wäre die Bereitstellung einer Open-Source-Lösung durch das Bundesministerium für Inneres, die von den Einrichtungen selbst gehostet werden kann und nur im Anlassfall nach Prüfung der Verantwortlichen auch Meldungen an das BMI vornehmen kann.

Weiters regen wir an, die Zuständigkeit für den Betrieb derartiger IKT-Lösungen zur Vermeidung von Interessenskonflikten nicht beim Bundesministerium für Inneres, sondern bei einer anderen Stelle (z.B. dem nationalen CSIRT) anzusiedeln.

Wir erlauben uns darauf hinzuweisen, dass derartige IKT-Lösungen gem. Art. 25 DSGVO nach dem Grundsatz des Datenschutzes durch Technikgestaltung (Privacy by Design) zu gestalten sind. Angesichts der besonderen Gefahr derartiger Software in kritischen Einsatzbereichen, sollte gesetzlich verpflichtend vor der Inbetriebnahme eine Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO durchgeführt werden.

Zu § 42: Überschießende Datenverarbeitung

In § 42 wird normiert, wer Verantwortlicher für die Datenverarbeitung im Sinne der DSGVO ist und zu welchen Zwecken die Verarbeitung erfolgen darf.

Diese Regelungen sind aus unserer Sicht nicht klar genug determiniert. Besonders kritisch sehen wir, dass die Verarbeitung personenbezogener Daten nicht nur zu Zwecken der Durchsetzung des vorliegenden NIS2-Gesetzes erfolgen soll, sondern darüber hinaus auch zum „*Schutz vor und zur Abwehr von Gefahren für die öffentliche Sicherheit*“. Die Datenverarbeitung soll also beispielsweise auch

zu sicherheitspolizeilichen Zwecken erfolgen. Damit wird der von uns zu § 4 dargestellte **Zielkonflikt** zwischen Cybersicherheit und polizeilichen Überwachungsbefugnissen nun auch auf datenschutzrechtlicher Ebene hergestellt. Wir befürchten, dass dies zu einer Zweckentfremdung der Cybersicherheitsbefugnisse und -maßnahmen für allgemeine sicherheitspolizeiliche Aufgaben führt.

Wir regen daher an, die entsprechende Passage zu streichen oder zu präzisieren. Wir geben zu bedenken, dass durch die Amtshilfe und die Bestimmung des § 78 StPO (Anzeigepflicht von Beamten und öffentlichen Dienststellen) ohnehin bereits ausreichende Mechanismen bestehen, die sicherstellen, dass relevante Vorfälle auch an die zuständigen Behörden weitergeleitet werden.

Zu § 43: Überschießende Datenübermittlung

In § 43 wird festgelegt, wer zu welchem Zweck Daten an welche Dritten übermitteln darf.

Aus unserer Sicht sind die Befugnisse zur Übermittlung personenbezogener Daten zu weit und zu ungenau gefasst, insbesondere die Befugnis zur Übermittlung personenbezogener Daten an „*andere in- und ausländische Behörden oder Stellen, soweit dies zur Aufgabenerfüllung erforderlich ist*" in Absatz 2.

Die Befugnis zur Übermittlung personenbezogener Daten an ausländische Behörden oder Stellen sollte auf den in der NIS-Richtlinie vorgesehenen Informationsaustausch beschränkt werden. Ansonsten besteht die Gefahr, dass Daten, die im Rahmen der Cybersicherheitsaufgaben erhoben wurden, leichtfertig für andere Zwecke an ausländische Sicherheitsbehörden übermittelt werden. Dies ist insbesondere dann gefährlich, wenn ausländische Sicherheitsbehörden Personen aufgrund ihrer Herkunft, ihrer politischen Einstellung, ihrer sexuellen Orientierung oder anderer Merkmale verfolgen. Alle diese Merkmale sind aus den Daten im Sinne des § 42 sehr leicht ableitbar, weshalb hier besondere Vorsicht geboten ist.

Zur Datenschutz-Folgenabschätzung

Die Erläuterungen zum Gesetzesentwurf enthalten auf den Seiten 47 bis 49 eine Datenschutz-Folgenabschätzung.

Wir halten die vorliegende Datenschutz-Folgenabschätzung (DSFA) für **unzureichend**, insbesondere sind wesentliche Überlegungen, die im Sinne der Empfehlungen des Europäischen Datenschutzausschusses (vormals „Working Party 29") anzustellen sind, nicht enthalten (z.B. die Thematik der Verhältnismäßigkeit).

Besonders kritisch ist daher, dass wohl sämtliche Verantwortliche, auch die Stellen, die mit einer allfälligen Cybersicherheitsbehörde in Kontakt stehen, selbst eine Datenschutz-Folgenabschätzung durchführen müssten, um allfällige Haftungsthemen im Sinne des Art. 83 DSGVO möglichst zu vermeiden. Wir gehen davon aus, dass aufgrund der Eingriffstiefe der vorgesehen Datenverarbeitungen voraussichtlich eine Konsultation der Datenschutzbehörde gemäß Art. 36 DSGVO erforderlich sein wird.

Der enormen Dringlichkeit und Relevanz des Themas IT-Sicherheit werden die DSFA – wie auch der vorliegende Entwurf insgesamt – leider nicht gerecht.