



Daten ebenfalls verfügbar unter
[wirkungsmonitoring.gv.at](https://www.wirkungsmonitoring.gv.at)

2023

Bericht über die Wirkungsorientierte Folgenabschätzung 2022

gemäß § 68 Abs. 5 BHG 2013 iVm
§ 6 Wirkungscontrollingverordnung

Bundeskanzleramt



Impressum

Medieninhaberin, Verlegerin und Herausgeberin:
Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport (BMKÖS)
Sektion III – Öffentlicher Dienst und Verwaltungsinnovation
Sektionschef Mag. Christian Kemperle
Hohenstaufengasse 3, 1010 Wien
www.bmkoes.gv.at

Redaktion und Gesamtumsetzung: Mag. (FH) Stefan Lindeis, Abteilung III/C/10
Verlags- und Herstellungsort: Wien, Mai 2023
Grafiken: Iekton Grafik & Web development
Fotonachweis: BKA / Andy Wenzel (Cover, S. 3);
HBF / Minich (S. 7); BKA / Regina Aigner (Trennseiten)
Gestaltung: BKA Design & Grafik
Druck: Riedeldruck, Druck Fulfillment-Druck Service GmbH, 2214 Auersthal

Alle Rechte vorbehalten: Jede Verwertung (auch auszugsweise) ist ohne schriftliche Zustimmung der Medieninhaberin unzulässig. Dies gilt insbesondere für jede Art der Vervielfältigung, der Übersetzung, der Mikroverfilmung, der Wiedergabe in Fernsehen und Hörfunk sowie der Verarbeitung und Einspeicherung in elektronische Medien, wie z. B. Internet oder CD-Rom.

Diese Publikation steht unter oeffentlicherdienst.gv.at/publikationen zum Download zur Verfügung.

Rückmeldungen:
Ihre Überlegungen zu vorliegender Publikation übermitteln Sie bitte an: iii10@bmkoes.gv.at.
Bestellung von Druckexemplaren per Email an iii10@bmkoes.gv.at.

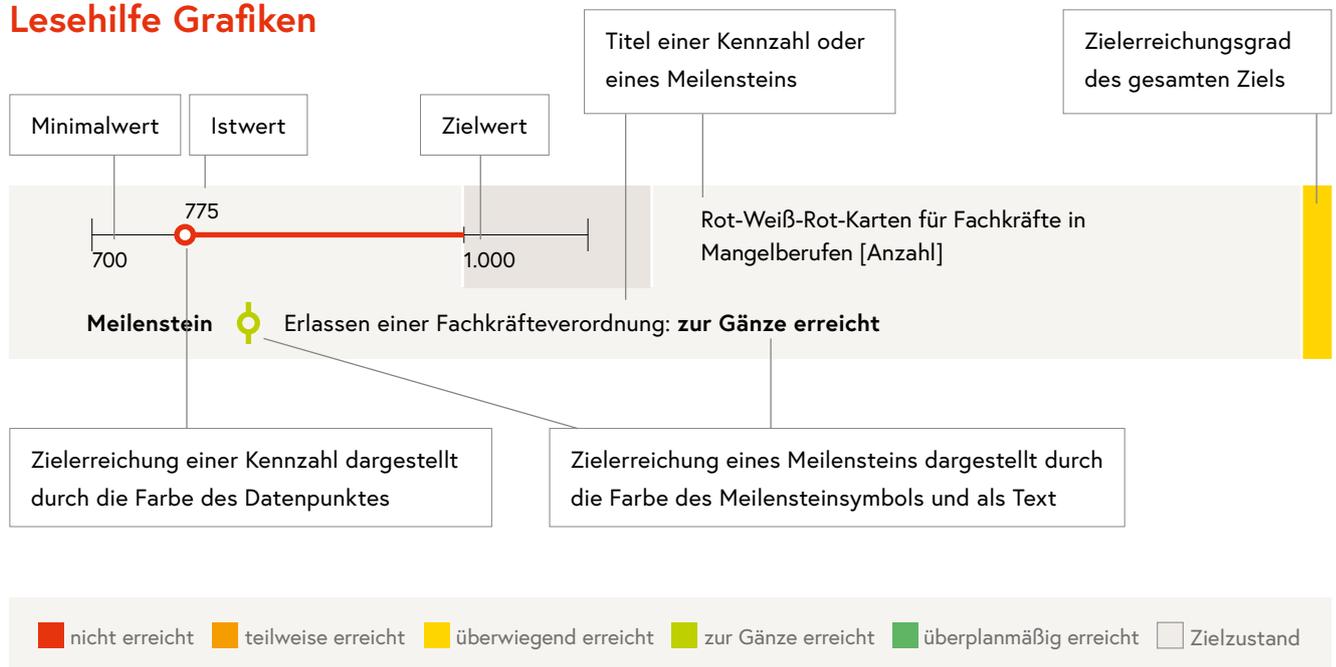
ISBN: 978-3-903097-49-0

Lesehilfe und Legende

Legende Symbolik

- Ⓢ Rechtssetzende Maßnahme
- ➔ Vorhaben
- 📁 Bündelung
- ■ ■ ■ ■ Gesamtbeurteilung des Erfolgs des Vorhabens
- Ⓢ Verwaltungskosten für Bürger:innen
- Ⓢ Verwaltungskosten für Unternehmen
- ♀♂ Tatsächliche Gleichstellung von Frauen und Männern
- 🛒 Konsumentenschutzpolitik
- 🤝 Soziales
- 👶 Kinder und Jugend
- 🌿 Umwelt
- 🏢 Unternehmen
- 📈 Gesamtwirtschaft

Lesehilfe Grafiken



Bundeskanzleramt

UG 10 – Bundeskanzleramt





„Netz- und Informationssystemssicherheitsgesetz (NISG): Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen“

Finanzjahr 2018

Vorhabensart  Bundesgesetz

Zuordnung zu mittel- und langfristigen Strategien

Das NISG setzt die RL (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 („NIS-RL“) um. Diese war die wichtigste Maßnahme der Cybersicherheitsstrategie der EU aus dem Jahr 2013 und der erste horizontale Unionsrechtsakt über Cybersicherheit. Am 16. Dezember 2020 stellte die EU-Kommission ein neues Cybersicherheitspaket vor, zu dessen Inhalt unter anderem eine neue EU-Cybersicherheitsstrategie zählt. Diese wurde in Form einer gemeinsamen Mitteilung der EK und des Hohen Vertreters der EU veröffentlicht und soll die Cybersicherheitsstrategie 2013 mit einem neuen strategischen Referenzrahmen für Cybersicherheit auf EU-Ebene ablösen. Die EU-Cybersicherheitsstrategie 2020 zielt darauf ab, das digitale Leben der Menschen in Europa sicher zu gestalten. Sichere und vertrauenswürdige digitale Instrumente sind für Wirtschaft, Demokratie und Gesellschaft gleichermaßen wichtig. Daher wurden folgende Vorschläge erarbeitet: 1) Steigerung der Resilienz von kritischer Infrastruktur und vernetzten Dingen; 2) Aus- und Aufbau von operativen Kapazitäten zur Vorbeugung, Abschreckung und Reaktion auf Cyberangriffe; 3) Zusammenarbeit mit internationalen Partnern für einen globalen, offenen, stabilen und sicheren Cyberraum, in welchem Völkerrecht, Menschenrechte, Grundfreiheiten und demokratische Werte gelten.

Am 16. Dezember 2020 wurde als Teil des Cybersicherheitspaket neben der neuen EU-Cybersicherheitsstrategie auch der Vorschlag für einer neuen Richtlinie über Maßnahmen für ein hohes gemeinsames Maß an Cybersicherheit in der gesamten Union (NIS-2-Richtlinie, kurz „NIS-2-RL“). Die NIS-2-RL soll die NIS-RL aus dem Jahr 2016 ersetzen und substantiell verbessern. Die verfolgten Ziele sind grundsätzlich dieselben und werden fortgeschrieben. Konkret sollen die Cybersicherheitskapazitäten in der EU verbessert werden, eine intensivere

Zusammenarbeit zwischen den Mitgliedstaaten stattfinden sowie eine Verbesserung der Cyberresilienz öffentlicher und privater Einrichtungen erreicht werden. Insgesamt soll das Cybersicherheitsniveau in der EU weiter erhöht werden. Dieses hohe gemeinsame Niveau an Cybersicherheit innerhalb der EU wird durch folgende Maßnahmen gefördert:

- 1) Die Mitgliedstaaten haben nationale Cybersicherheitsstrategien zu verabschieden sowie zuständige Behörden, zentrale Anlaufstellen und CSIRTs (Computer Security Incident Response Teams in Europe) zu benennen.
- 2) Die Cyberresilienz von Unternehmen soll gestärkt werden und alle relevanten Sektoren umfassen. Alle öffentlichen und privaten Einrichtungen im gesamten Binnenmarkt, die wichtige Funktionen für die Wirtschaft und die Gesellschaft als Ganzes erfüllen, sollen als sogenannte wesentliche und wichtige Einrichtungen verpflichtet werden, angemessene Cybersicherheitsmaßnahmen zu ergreifen (insbesondere durch die Einrichtung eines Cybersicherheitsrisikomanagements sowie durch die Meldepflicht von Sicherheitsvorfällen).
- 3) Bei den Sektoren im Binnenmarkt, die bereits unter die Richtlinie fallen, sollen resillienzsteigernde Maßnahmen gefördert werden. Dies wird durch die stetige Angleichung des De-facto-Anwendungsbereichs, der Sicherheitsanforderungen und Meldepflichten bei IT-Sicherheitsvorfällen, der Bestimmungen für die nationale Aufsicht und Durchsetzung sowie der Kapazitäten der zuständigen Behörden in den Mitgliedstaaten erreicht.
- 4) Die gemeinsame Lageerfassung sowie die kollektive Vorsorge und Reaktionsfähigkeit soll verbessert werden, indem Maßnahmen zur Stärkung des Vertrauens zwischen den zuständigen Behörden gesetzt und der Informationsaustausch gestärkt wird.
- 5) Darüber hinaus werden Regeln und Verfahren für den Fall großflächiger Sicherheitsvorfälle oder Krisen festgelegt (Cybersicherheitskrisenmanagement): Die NIS-2-RL2 enthält erstmals die Pflicht zur Festlegung eines nationalen Rahmens für das Cybersicherheitskrisenmanagement und sieht die Einrichtung

eines europäischen Netzwerks der Verbindungsorganisationen für Cyberkrisen (European Cyber Crises Liaison Organisation Network [EU-CyCLONe]) vor. Dieses soll die koordinierte Bewältigung großer Cybersicherheitsvorfälle und -krisen unterstützen und den regelmäßigen Informationsaustausch zwischen Mitgliedstaaten und EU-Organen gewährleisten. Die NIS-2-RL wurde am 27. Dezember 2022 im Amtsblatt der Europäischen Union veröffentlicht (data.europa.eu/eli/dir/2022/2555/oj) und ist am 16. Jänner 2023 in Kraft getreten. Sie ist anschließend innerhalb von 21 Monaten national umzusetzen.

Zuordnung zu Wirkungszielen (Bundesvoranschlag)

2018-BMI-UG 11-W1:

Ausbau des hohen Niveaus der öffentlichen Ruhe, Ordnung und Sicherheit in Österreich, insbesondere durch bedarfsorientierte polizeiliche Präsenz, Verkehrsüberwachung, Schutz kritischer Infrastrukturen und sinnvolle internationale Kooperation

2018-BKA-UG 10-W3:

Das Bundeskanzleramt als inhaltlicher Impulsgeber, Koordinator und Brückenbauer. Angestrebte Wirkung: hoher Nutzen der Koordinationsleistungen des Bundeskanzleramts im Rahmen der Regierungs- und Europapolitik

Zuordnung zu Globalbudget-Maßnahmen (Bundesvoranschlag)

2018-BMI-GB11.02-M2:

Stärkung der Cyber-Sicherheit und des Schutzes kritischer Infrastrukturen

2018-BKA-GB10.01-M3:

Einrichtung der Behörde für strategische Netz- und Informationssystem-Sicherheit (NIS)

Problemdefinition

Netz- und Informationssysteme mit den zugehörigen Diensten spielen eine zentrale Rolle in der heutigen Gesellschaft. Für wirtschaftliche und gesellschaftliche Tätigkeiten ist es daher von entscheidender Bedeutung, dass sie verlässlich und sicher sind. Mit diesem Bundesgesetz werden daher Maßnahmen festgelegt, mit denen ein hohes Sicherheitsniveau von Netz- und Informationssystemen der in den Anwendungsbereich fallenden Einrichtungen erreicht werden soll.

Mit der 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 (im Folgenden: NIS-RL), die am 8. August 2016 in Kraft getreten ist, soll dies auch EU-weit erreicht werden. Vor diesem Hintergrund sollen die Mitgliedstaaten eine nationale NIS-Strategie zur Bestimmung der Ziele und der damit verbundenen Regulierungsmaßnahmen erarbeiten, nationale (strategische und operative) Behörden und Computer-Notfallteams benennen und bestimmte, für das Gemeinwohl wichtige private und öffentliche Anbieter (Betreiber wesentlicher Dienste und digitale Diensteanbieter) zu angemessenen Sicherheitsmaßnahmen und Meldung erheblicher Störfälle verpflichten. Die von der NIS-RL vorgesehenen Maßnahmen zielen darauf ab, die Zusammenarbeit zwischen den Mitgliedstaaten in strategischer und operationeller Hinsicht zu stärken.

Betreiber eines wesentlichen Dienstes stellen einen Dienst der in Anhang II der NIS-RL genannten und im Folgenden aufgelisteten Sektoren zur Verfügung: Energie (Elektrizität, Erdöl, Erdgas), Verkehr (Luftverkehr, Schienenverkehr, Schifffahrt, Straßenverkehr), Bankwesen (Kreditinstitute), Finanzmarktinfrastrukturen (Betreiber von Handelsplätzen, zentrale Gegenparteien), Gesundheitswesen (Einrichtungen der medizinischen Versorgung, einschließlich Krankenhäuser und Privatkliniken), Trinkwasserlieferung und -versorgung (Lieferanten von und Unternehmen der Versorgung mit „Wasser für den menschlichen Gebrauch“), Digitale Infrastruktur (Internet Exchange Points, DNS-Diensteanbieter, TLD-Name-Register). Ferner sollen Einrichtungen des Bundes und der Länder im Rahmen der österreichischen Umsetzung berücksichtigt werden.

Digitale Diensteanbieter sind – ab einer gewissen Größe – sämtliche Anbieter eines Online-Marktplatzes, einer Online-Suchmaschine oder eines Cloud-Computing Dienstes.

Mit dem vorliegenden Gesetzesvorhaben wird die NIS-RL umgesetzt und darüber hinaus ein Regelwerk zu den in Österreich bereits seit vielen Jahren bestehenden Koordinationsstrukturen im Bereich der Sicherheit von Netz- und Informationssystemen geschaffen.

Ziele

Ziel 1: ■ Schaffung der Voraussetzungen für die Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen

Meilenstein 🕒 Schaffung von Sicherheitsvorkehrungen: **überwiegend erreicht**

Meilenstein 🕒 Schaffung neuer Koordinierungsstrukturen: **zur Gänze erreicht**

Maßnahmen

1. Weiterentwicklung und Koordination einer neuen Strategie für die Sicherheit von Netz- und Informationssysteme	Beitrag zu Ziel 1	■
2. Einrichtung von nationalen Koordinierungsstrukturen zur Prävention sowie zur Bewältigung von Sicherheitsvorfällen	Beitrag zu Ziel 1	■
3. Einrichtung von Computer-Notfallteams zur Unterstützung der BwD bei der Bewältigung von Risiken und Sicherheitsvorfällen	Beitrag zu Ziel 1	■
4. Ermittlung der Betreiber wesentlicher Dienste	Beitrag zu Ziel 1	■
5. Pflicht zur Setzung geeigneter Sicherheitsvorkehrungen; Informations- und Meldepflichten	Beitrag zu Ziel 1	■
6. Einrichtung und Betrieb einer Meldesammelstelle und einer zentralen Anlaufstelle	Beitrag zu Ziel 1	■
7. Betrieb und Nutzung von IKT-Lösungen	Beitrag zu Ziel 1	■

■ nicht erreicht ■ teilweise erreicht ■ überwiegend erreicht ■ zur Gänze erreicht ■ überplanmäßig erreicht □ Zielzustand

Finanzielle Auswirkungen

in Tsd. €	2018	2019	2020	2021	2022	Gesamt
Erträge	0	0	0	0	0	0
Plan	0	0	0	0	0	0
Aufwendungen gesamt	0	127	573	688	1.023	2.411
Plan	0	5.044	5.524	5.832	6.321	22.721
Nettoergebnis	0	-127	-573	-688	-1.023	-2.411
Plan	0	-5.044	-5.524	-5.832	-6.321	-22.721

Erläuterungen

Im Vergleich zu den in der WFA ersichtlichen geplanten Personalaufwänden fielen die tatsächlichen Personalaufwände wie folgt aus (in Tausend €):

2019: Personalaufwand 127 (davon 127 im BKA)

2020: Personalaufwand 573 (davon 129 im BKA)

2021: Personalaufwand 688 (davon 131 im BKA)

2022: Personalaufwand 1023 (davon 134 im BKA)

In Bezug auf den Personalaufwand, ist die Plan-Ist-Abweichung darauf zurückzuführen, dass die ursprünglich vorgesehenen Planstellen des BKA nicht besetzt werden konnten.

In Bezug auf die Sachaufwände (betrieblicher Sachaufwand und Werkleistungen) waren in der WFA Aufwendungen im BMI für den Aufbau und den Betrieb von IKT-Lösungen zur Vorbeugung von Sicherheitsvorfällen (§ 13 NISG), wie in der WFA ersichtlich, vorgesehen. Der angestrebte Betrieb der IKT-Lösungen zur Vorbeugung von Sicherheitsvorfällen konnte zum Zeitpunkt der Evaluierung jedoch noch nicht in Betrieb genommen werden. Zusätzlich wird darauf hingewiesen, dass in den Jahren 2020 bis 2022 folgende Investitionen (in Tsd. €) angefallen sind: 2020: 1.841, 2021: 4.581, 2022: 1.278.

Konnte die Bedeckung (der Struktur nach), wie in der WFA dargestellt, durchgeführt werden? Nein

Ad BKA: Die finanziellen Auswirkungen des Vorhabens zulasten der UG 10 konnten innerhalb der Auszahlungsobergrenzen des Bundesfinanzrahmens 2019–2022 bedeckt werden (Detailbudget 10.01.02).

Ad BMI: Die Abweichungen zwischen Plan und Ist, insbesondere in den Jahren 2018 und 2019 begründen sich dadurch, dass erst mit Ende 2019 die Zustimmung des BMF zur Umsetzung erfolgt ist und dadurch mit den Beauftragungen der Projekte gestartet werden konnte.

Weiters wird angemerkt, dass es aufgrund der Pandemie zu Lieferverzögerungen gekommen ist bzw. dass komplexe Ausschreibungen (z. B. Sensornetzwerk) auch zu den Abweichungen Plan-Ist geführt haben.

Wirkungsdimensionen

📌 Verwaltungskosten für Unternehmen

Zu diesem Zeitpunkt liegen keine Informationen vor, die eine Beurteilung der tatsächlich eingetretenen Verwaltungskosten für Unternehmen ermöglichen. Im Bericht „NIS Investments 2022“ der Agentur der Europäischen Union für Cybersicherheit (ENISA) wurden jedoch Daten darüber gesammelt, wie die

in der RL (EU) 2016/1148 genannten Betreiber wesentlicher Dienste und Anbieter digitaler Dienste ihre Cybersicherheitsbudgets investieren und wie diese Investitionen durch die RL (EU) 2016/1148 beeinflusst wurden. Der Bericht ist abrufbar unter: www.enisa.europa.eu/publications/nis-investments-2022

Gesamtbeurteilung des Erfolgs des Vorhabens

Die erwarteten Wirkungen des Gesamtvorhabens sind überwiegend eingetreten.

Das NISG ist ein wesentlicher Faktor zur Erhöhung des Cybersicherheitsniveaus in Österreich und stellt somit einen Erfolg dar. Mit dem NISG wurde erstmals in Österreich ein eigenes Gesetz zur Regulierung der Sicherheit von Netz- und Informationssystemen erlassen. Ferner wurden erstmals zuständige Behörden und Computer-Notfallteams formell eingerichtet und mit dezidierten Aufgaben und Befugnissen ausgestattet. Des Weiteren wurden die Strukturen, insbesondere im operativen Bereich, verrechtlicht und damit solide Grundlagen zur Kooperation und Bewältigung von Cyberfällen geschaffen. Dies hat sich im Besonderen bei der grundsätzlich erfolgreichen Bewältigung des Cyber-Angriffs auf das Bundesministerium für europäische und internationale Angelegenheiten der Republik Österreich (BMEIA) Anfang 2020 gezeigt.

Von entschiedenem Erfolg war auch die Ermittlung der Betreiber wesentlicher Dienste, weil auf diese Weise erstmals in rechtlich verbindlicher Weise für die Daseinsvorsorge relevante kritische Infrastrukturen identifiziert wurden, die aufgrund einer Risikobewertung Sicherheitsvorkehrungen implementieren müssen, wodurch die Cyber-Resilienz Österreichs maßgeblich gesteigert werden konnte. Das Aufsichtssystem, welches auf Überprüfungen durch unabhängige Dritte („qualifizierte Stellen“) beruht, stellt ein wirkungsvolles Mittel zur Erhöhung der Netz- und Informationssystemsicherheit bei den Betreibern wesentlicher Dienste dar. Die qualifizierten Stellen nehmen dabei eine zentrale Rolle ein, da sie als Prüfstellen für Betreiber wesentlicher Dienste fungieren und von diesen auch heranzuziehen sind. Einzelheiten über die qualifizierte Stellen werden in der Verordnung des BMI über qualifizierte Stellen (QuaStEV) festgelegt, wobei unterstützend ein Leitfaden publiziert wurde („NIS Fact Sheet 7/2019“).

Das NISG konnte sohin in den Hauptgesichtspunkten (vgl. ERIRV 369 BlgNR XXVI. GP, 1) und im Besonderen im Bereich der kritischen Infrastruktur der Daseinsvorsorge seine erwarteten Wirkungen erfüllen.

Im Bereich der Einrichtungen der öffentlichen Verwaltung wurde der Ansatz der freiwilligen Selbstkontrolle gewählt, wodurch der Erfolg nicht zentral messbar ist. Doch wurde zur Unterstützung der Einrichtungen des Bundes vom BKA ein Umsetzungsleitfaden publiziert (NIS Fact Sheet 9/2019).

Im Zusammenhang mit nationaler Netz- und Informationssicherheit fand 2022 die EU-Cybersicherheitsübung statt. An der innerstaatlich vom Bundeskanzleramt koordinierten EU-Cybersicherheitsübung nahmen 12 Einrichtungen teil, was zu einer gesamtstaatlichen Resilienz bei Cybervorfällen beigetragen hat. Die Bewertung der Cybersicherheitsübung durch die teilnehmenden Einrichtungen erfolgte nach dem Schulnotensystem. Die teilnehmenden Einrichtungen bewerteten die Übung im Durchschnitt mit Gut (2).

Im Rahmen einer WFA Evaluierung werden zukünftige Regelungsvorhaben zur nationalen Umsetzung der NIS-2-RL evaluiert, nicht aber das NISG und die NISV in der derzeit geltenden Fassung.

Haben sich Verbesserungspotentiale ergeben? Ja

Die in der WFA zur Umsetzung des NISG und damit zur Aufrechterhaltung der Cybersicherheit als notwendig definierten Personalressourcen konnten nicht bereitgestellt werden (insbesondere im BKA).

Das Aufsichtssystem über die Anbieter digitaler Dienste hat gemäß der RL (EU) 2016/1148 ex-post ausgestaltet zu sein und war vollharmonisiert. Infolgedessen ist es nicht möglich zu beurteilen, ob das NISG zu einer Erhöhung der Netz- und Informationssystemsicherheit der Anbieter digitaler Dienste geführt hat. Verbesserungspotenzial ergibt sich daher in diesem kritischen Bereich, da auch Cloud-Dienste-Anbieter darunter fallen. Infolge der Vollharmonisierung wird die Verbesserung erst durch die Umsetzung der diesbezüglichen Änderung des unionsrechtlichen Rahmen durch die NIS-2-RL erfolgen können, indem wesentliche Anbieter digitaler Dienste einem strengeren Aufsichtssystem unterworfen werden.

Die Länder haben keine Regelungen auf landesgesetzlicher Ebene getroffen, um die Pflichten zu Sicherheitsvorkehrungen bei wichtigen Diensten und zur Meldung von Sicherheitsvorfällen entsprechend den öffentlichen Einrichtungen des Bundes

zu übernehmen. Infolgedessen konnte das NISG keine rechtlichen Wirkungen zur Erhöhung der Netz- und Informationssystemsicherheit auf Landesebene entfalten.

Die Netz- und Informationssystemsicherheit der Einrichtungen des Bundes kann nicht zentral beurteilt werden, da eine vergleichbare Überprüfungs- und Nachweispflicht wie bei den Betreibern wesentlicher Dienste nicht vorgesehen ist. Der Mangel an konkreten und vorgegebenen Meldeschwellenwerten macht eine gemeinsame Lageerfassung bei Vorfällen, die mehrere Einrichtungen des Bundes betreffen, herausfordernd.

Im Bereich der öffentlichen Verwaltung wird es jedoch sowohl auf Bundes- als auch Landesebene zu Verbesserungen durch die Umsetzung der diesbezüglichen Änderungen des unionsrechtlichen Rahmens (NIS-2-RL) kommen. Da die NIS-2-RL bei Einrichtungen der öffentlichen Verwaltung einen größeren nationalen Gestaltungsspielraum zulässt, müssen einzelne Umsetzungsmodelle erst bewertet und abgestimmt werden. Als Leitlinie solle dabei das Regierungsprogramm 2020–2024 „Aus Verantwortung für Österreich“ dienen, welches die „Umsetzung verbindlicher, überprüfbarer und durchsetzbarer Sicherheitsstandards im Rahmen der Richtlinie für Netz- und Informationssystemsicherheit (NIS) im öffentlichen Sektor“ angibt.

Weiterführende Informationen

NIS Fact Sheet 1/2019: Kontaktstellen von Betreibern wesentlicher Dienste (Version 2) (PDF)

www.nis.gv.at/dam/jcr:65dca834-9740-435b-b343-0100cba117c1/NIS_Fact_Sheet_2019_01_2_0.pdf

Bericht „NIS Investments 2022“

www.enisa.europa.eu/publications/nis-investments-2022

EU-Cybersicherheitsstrategie

digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

Umsetzungsleitfaden für Einrichtungen des Bundes NIS Fact Sheet 9/2019

www.nis.gv.at/dam/jcr:188f0654-393f-4bfd-96db-33f8577182dc/NIS_Fact_Sheet_2019_09_1_0.pdf

Qualifizierte Stellen NIS Fact Sheet 7/2019 – Version 2

www.nis.gv.at/dam/jcr:1a4e5df2-739d-4ac7-8e3d-175fa99a7f51/NIS_Fact_Sheet_2019_07_2_0.pdf



Netz- und Informationssystem-sicherheitsverordnung – NISV

Finanzjahr 2019

Vorhabensart  Verordnung

Zuordnung zu mittel- und langfristigen Strategien

Die NISV führt einzelne Bestimmungen des NISG näher aus und dient somit der Umsetzung der RL (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 („NIS-RL“). Die NIS-RL war die wichtigste Maßnahme der Cybersicherheitsstrategie der EU aus dem Jahr 2013 und der erste horizontale Unionsrechtsakt über Cybersicherheit.

Zuordnung zu Wirkungszielen (Bundesvoranschlag)

2019-BKA-UG 10-W3:

Das Bundeskanzleramt als inhaltlicher Impulsgeber, Koordinator und Brückenbauer. Angestrebte Wirkung: hoher Nutzen der Koordinationsleistungen des Bundeskanzleramts im Rahmen der Regierungs- und Europapolitik

Zuordnung zu Globalbudget-Maßnahmen (Bundesvoranschlag)

2019-BKA-GB10.01-M3:

Monitoring der bescheidmäßig erlassenen Sicherheitsvorkehrungen für BetreiberInnen wesentlicher Dienste durch die Behörde für strategische Netz- und Informationssystem-Sicherheit (NIS), damit entsprechend der EU-Richtlinie NIS bei sensiblen Infrastrukturen Österreichs (Wasser- und Energieversorgung, Bankwesen, digitale Dienste etc.) eine wirksame Widerstandskraft gegen Cyber-Bedrohungen aufgebaut werden kann.

Problemdefinition

Netz- und Informationssysteme mit den zugehörigen Diensten spielen eine zentrale Rolle in der heutigen Gesellschaft. Für wirtschaftliche und gesellschaftliche Tätigkeiten ist es daher von entscheidender Bedeutung, dass sie verlässlich und sicher sind. Mit dem Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystem-sicherheitsgesetz – NISG), BGBl. I Nr. 111/2018, werden Maßnahmen festgelegt, mit denen ein hohes Sicherheitsniveau von Netz- und Informationssystemen der in den Anwendungsbereich fallenden Einrichtungen erreicht werden soll.

Mit dem vorliegenden Verordnungsvorhaben wird gemäß § 4 Abs. 2 des Netz- und Informationssystem-sicherheitsgesetzes (NISG) ein Regelwerk für Kriterien für die Parameter zu Sicherheitsvorfällen gemäß § 3 Z 6 lit. a bis d NISG, nähere Regelungen zu den in § 2 NISG genannten Sektoren gemäß § 16 Abs. 2, die Sicherheitsvorkehrungen nach § 17 Abs. 1 NISG und die Ausnahmen von Verpflichtungen für Betreiber wesentlicher Dienste gemäß § 20 Abs. 1 NISG geschaffen.

Ziele

Ziel 1:  Umsetzung des NISG durch Festlegung von Sicherheitsvorkehrungen und näheren Regelungen zu den Sektoren

Meilenstein 

Betreiber wesentlicher Dienste, deren Sicherheitsvorfälle und Sicherheitsvorkehrungen sind rechtlich näher definiert: **zur Gänze erreicht**

Maßnahmen

1. Festlegung näherer Regelungen zu jedem in § 2 NISG genannten Sektor	Beitrag zu Ziel 1
2. Beschreibung der von Betreibern wesentlicher Dienste zu erbringenden Sicherheitsvorkehrungen	Beitrag zu Ziel 1

■ nicht erreicht
 ■ teilweise erreicht
 ■ überwiegend erreicht
 ■ zur Gänze erreicht
 ■ überplanmäßig erreicht
 Zielzustand

Finanzielle Auswirkungen

Erläuterungen

Finanzielle Auswirkungen im Zusammenhang mit der NISV sind in der WFA zum NISG abgeschätzt worden. Die Evaluierungsergebnisse zur WFA des NISG sind im vorliegenden Bericht enthalten.

ergebnisse zur WFA des NISG sind im vorliegenden Bericht enthalten.

Wirkungsdimensionen

Unternehmen

Durch die NISV werden keine Verwaltungskosten für die Betreiber wesentlicher Dienste verursacht. Die möglichen Auswirkungen sind bereits durch das NISG gegeben und wurden

in der WFA zum NISG berücksichtigt. Abschätzungen zu eingetretenen Auswirkungen entlang von Wirkungsdimensionen sind in der Evaluierung der WFA zum NISG enthalten und gehen somit aus diesem Evaluierungsbericht 2022 hervor.

Gesamtbeurteilung des Erfolgs des Vorhabens

Die erwarteten Wirkungen des Gesamtvorhabens sind zur Gänze eingetreten.

Die erwarteten Wirkungen des Gesamtvorhabens konnten zur Gänze erreicht werden, da alle Punkte des Gegenstands der NISV (§ 1 NISV) festgelegt wurden und sich als vollzugstauglich erwiesen haben. Mit der NISV konnte basierend auf § 4 Abs. 2 NISG ein Regelwerk für Kriterien für die Parameter zu Sicherheitsvorfällen gemäß § 3 Z 6 lit. a bis d NISG, nähere Regelungen zu den in § 2 NISG genannten Sektoren gemäß § 16 Abs. 2, die Sicherheitsvorkehrungen nach § 17 Abs. 1 NISG und die Ausnahmen von Verpflichtungen für Betreiber wesentlicher Dienste gemäß § 20 Abs. 1 NISG geschaffen werden.

Die Parameter zu Sicherheitsvorfällen werden in den §§ 4 bis 10 NISV jeweils in den Abs 2 geregelt. Sie haben sich soweit als tauglich erwiesen, um die Information der Computer-Notfallteams und der zentralen Meldestelle im BMI bei schwerwiegenden Vorfällen zu gewährleisten.

Bei den näheren Regelungen zu den in § 2 NISG genannten Sektoren gemäß § 16 Abs. 2 NISG handelt es sich insbesondere um die wesentlichen Dienste, die in den §§ 4 bis 10 NISV jeweils in den Abs 1 festgelegt wurden und auf deren Basis die Betreiber wesentlicher Dienste ermittelt wurden. Es handelt sich dabei um die erstmalige rechtliche Festlegung von Schwellenwerten, um für die Daseinsvorsorge relevante Einrichtungen identifizieren zu können. Der Festlegung gingen umfangreiche Gespräche mit Sicherheits- und Branchenexperten sowie Regulatoren voraus. Die erfolgreiche Ermittlung der Betreiber wesentlicher Dienste (Stand Februar 2023: 99) und der Umstand, dass kein einziges Unternehmen ein Rechtsmittel gegen die Ermittlung erhoben hat, zeugen von der Akzeptanz und Tauglichkeit der festgelegten wesentlichen Diensten.

Die Sicherheitsvorkehrungen werden in § 11 iVm Anlage I NISV geregelt. Es handelt sich um Sicherheitsvorkehrungen, die nach dem Stand der Technik üblich sind und sich an internationalen und europäischen Standards orientieren. Insbesondere wurde

auf dem Leitfaden der EU Agentur für Cybersicherheit (ENISA) und der NIS-Kooperationsgruppe „Reference document on security measures for Operators of Essential Services“ aufgebaut, um eine EU-weit einheitliche Anwendung zu gewährleisten. Um Betreiber bei der Umsetzung der Sicherheitsvorkehrungen zu unterstützen, haben das BKA und BMI im sogenannten „NIS Fact Sheet 9/2022“ die Sicherheitsvorkehrungen näher erläutert und mit nationalen, europäischen und internationalen Informationssicherheitsstandards gemappt sowie im „NIS Fact Sheet 3/2021“ die Darstellung und Dokumentation von Überprüfungen näher erläutert.

Die Ausnahmen von Verpflichtungen für Betreiber wesentlicher Dienste gemäß § 20 Abs. 1 NISG sind Bestimmungen, um Doppelbelastungen zu vermeiden. Die §§ 17 oder 19 sind nicht anwendbar, wenn für die Erbringung eines wesentlichen Dienstes im Unionsrecht oder in Materiengesetzen, die auf unionsrechtlichen Bestimmungen beruhen, Vorschriften zu Sicherheitsvorkehrungen oder zur Meldepflicht bestehen, die zumindest ein gleichwertiges Sicherheitsniveau für Netz- und Informationssysteme gewährleisten, und der Bundeskanzler diese Vorschriften und deren Eignung mittels Verordnung im Einvernehmen mit dem Bundesminister für Inneres festlegt. Solche Bestimmungen wurden für die Sektoren Bankwesen (§ 6 Abs. 3 NISV), Finanzmarktinfrastrukturen (§ 7 Abs. 3 NISV) und Digitale Infrastruktur (für Telekomunternehmen; § 10 Abs. 3 NISV) eingeführt. Die unionsrechtliche Grundlage findet sich in Art 1 Abs 7 RL (EU) 2016/1148 und die Mitteilung der EU-Kommission COM(2017) 476 final.

Weiterführende Informationen zur Gesamtbeurteilung der NISV können der Evaluierung betreffend die WFA NISG entnommen werden. Diese Evaluierung ist im vorliegenden Evaluierungsbericht 2022 enthalten.

Haben sich Verbesserungspotentiale ergeben? Ja

Erste Erfahrungen in Zusammenhang mit dem Nachweis der Umsetzung der Sicherheitsvorkehrungen durch die Betreiber wesentlicher Dienste legen nahe, dass eine detailliertere Ausformulierung der Sicherheitsmaßnahmen in Anlage I die Umsetzung durch die Betreiber wesentlicher Dienste (zusammen mit den qualifizierten Stellen) und den Vollzug durch das BMI erleichtern könnte.

Weiterführende Informationen

NIS Fact Sheet 3/2021: Erläuterungen zur Aufstellung von Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste (Version 2) (PDF)

www.nis.gv.at/dam/jcr:bfc2c432-769d-4620-b0f7-33f13e286fed/NIS_Fact_Sheet_2021_03_2_0.pdf

CG Publication 01/2018 – Reference document on security measures for Operators of Essential Services
ec.europa.eu/digital-single-market/en/nis-cooperation-group

NIS Fact Sheet 9/2022: Sicherheitsmaßnahmen für Betreiber wesentlicher Dienste (PDF)

www.nis.gv.at/dam/jcr:bbe1c393-ba27-43b3-8d38-890610cfcc75/NIS_Factsheet_9_2022_1_0.pdf

Bundeskanzleramt

UG 25 – Familie und Jugend





Anpassung der Familienleistungen für im EU-Ausland/im EWR/in der Schweiz lebende Kinder an die dortigen Lebenshaltungskosten

Finanzjahr 2018

Vorhabensart (§) Bundesgesetz

Zuordnung zu Wirkungszielen (Bundesvoranschlag)

2018-BKA-UG 25-W1: Lasten- und Leistungsausgleich zwischen kinderlosen Personen und Eltern mit Unterhaltspflichten

Zuordnung zu mittel- und langfristigen Strategien

Das Regelungsvorhaben steht mit folgender Zielsetzung aus dem Regierungsprogramm 2017–2022 im Zusammenhang (siehe S. 102):

Europarechtskonforme Indexierung der Familienbeihilfe (Anpassung an die Lebenshaltungskosten im jeweiligen EU-Staat).

Dieses Regelungsvorhaben trägt nicht signifikant zur Erreichung von SDG-Zielen oder SDG-Unterzielen bei.

Zuordnung zu Globalbudget-Maßnahmen (Bundesvoranschlag)

2018-BKA-GB25.01-M1:

Bereitstellung von finanziellen Transferleistungen zum Ausgleich der Unterhaltslasten für noch nicht selbsterhaltungsfähige Kinder durch den Familienlastenausgleichsfonds (FLAF), dazu zählen u. a. die Familienbeihilfe, die Fahrtenbeihilfen, das Kinderbetreuungsgeld (mit dem das System des Lastenausgleichs zum Leistungsausgleich weiterentwickelt wurde) sowie die Aufrechterhaltung der Einnahmenseite des FLAF, wobei die Finanzierung der Leistungen aus dem FLAF nachhaltig sichergestellt werden soll

Problemdefinition

Auf Grund von EU-Koordinierungsregelungen werden die Familienbeihilfe und der Kinderabsetzbetrag auch für Kinder gewährt, die ständig in einem EU/EWR-Staat oder der Schweiz leben. Durch einen undifferenzierten Export von Familienbeihilfe

und Kinderabsetzbetrag entstehen Verzerrungen. Es wird von einem Personenkreis von 132.000 Kindern ausgegangen, die von der Maßnahme betroffen sind.

Ziele

Ziel 1: ■ Vermeidung von Verzerrungen beim Leistungsexport der Familienbeihilfe und des Kinderabsetzbetrages



Maßnahmen

1. Differenzierung bei Familienbeihilfe und Kinderabsetzbetrag beim Leistungsexport

Beitrag zu Ziel 1

■ nicht erreicht ■ teilweise erreicht ■ überwiegend erreicht ■ zur Gänze erreicht ■ überplanmäßig erreicht □ Zielzustand

Finanzielle Auswirkungen

in Tsd. €	2018	2019	2020	2021	2022	Gesamt
Erträge	0	0	0	0	0	0
Plan	0	0	0	0	0	0
Aufwendungen gesamt	0	115	0	0	1	116
Plan	0	-113.875	-114.000	-114.000	-114.000	-455.875
Nettoergebnis	0	-115	0	0	-1	-116
Plan	0	113.875	114.000	114.000	114.000	455.875

Erläuterungen

Der EuGH hat in seinem Urteil vom 16. Juni 2022, (C-328/20) ausgeführt, dass der Anpassungsmechanismus eine ungerechtfertigte mittelbare Diskriminierung aufgrund der Staatsangehörigkeit der Wanderarbeitnehmer/innen darstellt und daher nicht mit dem Unionsrecht vereinbar ist. Mit der Novelle des Familienlastenausgleichsgesetzes 1967 sowie des Einkommensteuergesetzes 1988 (BGBl. I Nr. 135/2022) wurden im Juli 2022 die nicht mehr anzuwendenden Indexierungsbestimmungen formell aufgehoben. Es wurde der europarechtskonforme Rechtszustand durch Nachzahlungen wiederhergestellt.

Für die Einführung und Aufhebung der Indexierung der Familienbeihilfe entstanden Kosten in der Gesamthöhe von € 116.622,57 (Kosten für die Umstellung auf die indexierten Beträge € 115.136,63 plus Abwicklungskosten zur Aufhebung der Indexierung € 1.485,94). Die ursprünglich vorgesehenen Kosten für Werkleistungen in der Höhe von € 125.000 für die Umstellung der indexierten Beträge fielen somit geringer aus als ursprünglich vorgesehen. Der Grund für die geringeren Kosten für Werkleistungen war eine tatsächlich weniger kostenintensivere technische Umsetzung.

In den Jahren 2019 bis 2021 kam es vorübergehend zu Minderauszahlungen bei den Transferleistungen. Infolge des EuGH Urteiles im Jahr 2022 mussten jedoch für 87.949 Fälle (143.705 Kinder) automationsunterstützte Nachzahlungen in der Höhe von € 337.250.976,10 für den Indexierungszeitraum

Jänner 2019 bis Juni 2022 geleistet werden (Familienbeihilfe € 53.133.706,59; Differenzzahlung € 184.370.263,64; Kinderabsetzbetrag € 99.747.005,87), weshalb sich die Auszahlungen auf einen späteren Zeitpunkt verschoben haben und die intendierte Einsparung nicht erreicht wurde (der Ist-Wert wird folglich in der Tabelle oberhalb mit € 0 dargestellt).

Konnte die Bedeckung (der Struktur nach), wie in der WFA dargestellt, durchgeführt werden? Nein

Wegen des EuGH-Urteiles betreffend die Indexierung der Familienbeihilfe wurde vom Gesetzgeber die Durchführung von automationsunterstützten Nachzahlungen für den Zeitraum Jänner 2019 bis Juni 2022 an den von der Indexierung nach unten betroffenen Personenkreis beschlossen (siehe BGBl. I Nr. 135/2022). Die ursprünglich geplanten Einsparungen bzw. Minderausgaben in der Höhe von jährlich € 114 Mio. traten daher nicht ein. Im Gegenzug mussten für 143.705 Kinder die Familienbeihilfen nachbezahlt werden.

Die infolge des EuGH-Urteiles geleisteten Nachzahlungen betreffend den Indexierungszeitraum Jänner 2019 bis Juni 2022 sowie die betraglich bereinigten Transferzahlungen ab Juli 2022 konnten über eine Budgetaufstockung bei der UG 25 im Rahmen der zweiten BFG-Novelle 2022 bedeckt werden.

Die Werkleistungen im Zusammenhang mit der Einführung (2019) und Aufhebung der Indexanpassung (2022) konnten im laufenden Budgetvollzug finanziell bedeckt werden.

Wirkungsdimensionen

Kinder und Jugend

Das Regelungsvorhaben führte zu keinen wesentlichen Auswirkungen in der Wirkungsdimension Kinder und Jugend, weil die mit dem Vorhaben angestrebte Anpassung der Familienbeihilfe und des Kinderabsetzbetrages entsprechend dem Niveau der Lebenserhaltungskosten in jedem einzelnen EU- und EWR-Staat

widerrufen wurde. Weiterführende Informationen dazu gehen aus der Gesamtbeurteilung des Vorhabens hervor. Es wurde von einem Personenkreis von 132.000 Kindern ausgegangen, der von der Maßnahme betroffen sei. In 87.949 Fällen wurden nun für 143.705 Kinder automationsunterstützte Nachzahlungen für den Zeitraum Jänner 2019 bis Juni 2022 durchgeführt.

Gesamtbeurteilung des Erfolgs des Vorhabens

Die erwarteten Wirkungen des Gesamtvorhabens sind nicht eingetreten.

Der Erfolg des Vorhabens wurde aufgrund des Feststellungsurteils des EuGHs, wonach die Indexierung der Familienleistungen gegen EU-Recht verstößt, nicht erreicht.

Auf Grund der Verordnung (EG) Nr. 883/2004 werden die Familienbeihilfe und der Kinderabsetzbetrag auch für Kinder gewährt, die sich ständig in einem EU/EWR-Staat oder der Schweiz aufhalten. Zur Vermeidung von Verzerrungen bei un-differenziertem Export wurden mit der FLAG Novelle (BGBl. I Nr. 83/2018) die Familienbeihilfe und der Kinderabsetzbetrag nach der Kaufkraft jenes Landes, in dem das Kind wohnt, ab Jänner 2019 indexiert. Die indexierten Beträge kamen ab Jänner 2019 zur Auszahlung.

Die Europäische Kommission reichte in weiterer Folge eine Vertragsverletzungsklage gegen die Republik Österreich ein, da nach Ansicht der Kommission eine Indexierung der Familienleistungen gegen das EU-Recht verstoße. Der EuGH-Generalanwalt teilte diese Ansicht in seinen Schlussfolgerungen vom 20. Jänner 2022.

Der EuGH hat am 16. Juni 2022 in seinem Urteil festgestellt, dass die Indexierung der Familienbeihilfe, des Kinderabsetzbetrages und weiterer steuerlicher Begünstigungen gegen die Verpflichtungen aus dem EU-Recht verstößt. Der EuGH gab daher der Vertragsverletzungsklage der Europäischen Kommission in vollem Umfang statt, da er beide Rügen der Kommission als begründet erachtete.

Der EuGH hat im Wesentlichen festgestellt, dass

- sowohl die Indexierung der Familienbeihilfe und des Kinderabsetzbetrages „nach oben“ als auch „nach unten“ nicht mit dem Unionsrecht vereinbar ist, da aufgrund der Koordinierungsverordnung die Familienleistung für in der EU, im EWR und in der Schweiz lebende Kinder exakt der für in Österreich lebende Kinder gewährten Leistung entsprechen muss;
- durch die Indexierungsbestimmungen Wanderarbeitnehmer/innen mittelbar diskriminiert wurden;
- ein Anpassungsmechanismus nach Maßgabe des Wohnsitzstaates der Kinder vom EuGH nicht gerechtfertigt ist und Wanderarbeitnehmer/innen in gleicher Weise wie inländische Arbeitnehmer/innen zu behandeln sind.

Das Urteil des EuGHs wurde von der Republik Österreich zur Kenntnis genommen. Vom Gesetzgeber wurde mit der FLAG-Novelle (BGBl. I Nr. 135/2022) die Indexierung der Familienbeihilfe und des Kinderabsetzbetrages bereinigt. Die notwendigen Umsetzungsmaßnahmen, wie zum Beispiel die Durchführung von Nachzahlungen und die Umstellung der indexierten Beträge auf österreichischen Beträge, wurden bereits von BKA und BMF getroffen.

Die Maßnahmen, die mit der Indexierung der Familienbeihilfe und des Kinderabsetzbetrags gesetzt wurden, führten nur vorübergehend zu einer jährlichen Ausgabenminderung für den FLAF. Die Kosten für die zu erbringenden Werkleistungen waren im Verhältnis zu der Ausgabenminderung wegen der Indexierung sehr gering. Wegen des EuGH-Urteils wurden Nachzahlungen für den Indexierungszeitraum getätigt, wodurch keine Ausgabenminderung eintrat.

Für den Indexierungszeitraum Jänner 2019 bis Juni 2022 wurden 362 Familien höhere Beträge an Familienbeihilfe und Kinderabsetzbetrag im Vergleich zu den österreichischen Beträgen für im EU-Ausland/im EWR/in der Schweiz lebende Kinder mit höheren Lebenserhaltungskosten gewährt. Es kam somit im Indexierungszeitraum auch zu einer Indexierung „nach oben“. Der EuGH hat neben den Indexierungsbestimmungen „nach unten“ auch jene „nach oben“ aufgehoben. Seit dem Anspruchsmonat Juli 2022 werden an diesen Personenkreis die österreichischen Beträge ausbezahlt. Mit der FLAG-Novelle (BGBl. I Nr. 135/2022) wurde vom Gesetzgeber beschlossen, dass von einer Rückforderung der ausbezahlten Mehrbeträge seitens der Republik Österreich Abstand genommen wird.

Verbesserungspotential für zukünftige Vorhaben im Bereich der Familienbeihilfe ergibt sich nicht, da die zum Zeitpunkt der Einführung der Indexierung vorgelegenen Informationen nicht auf eine Europarechtswidrigkeit der Bestimmungen hingewiesen haben. Beispielsweise hat die Europäische Kommission vor der Brexit-Abstimmung dem Vereinigten Königreich eine Zusage zur Indexierung von Familienleistungen (Berücksichtigung der unterschiedlichen Lebensstandards in Europa bei der Gewährung von Familienleistungen) erteilt. Weiters erhalten die Bediensteten der Europäischen Kommission indexierte familienbezogene Zuwendungen. Zudem wurde im Vorfeld die EU-Rechtskonformität einer solchen Gesetzesmaßnahme geprüft und von einem Gutachten bestätigt.

Das Vorhaben hat sich als unionsrechtswidrig herausgestellt, weshalb rückwirkend vom Gesetzgeber eine Bereinigung im Sinne einer Aufhebung der gesetzlichen Bestimmungen erfolgte. Da die Bereinigung der Indexierung aufgrund eines Initiativantrages beschlossen wurde, existiert hierfür keine evaluierungsbedürftige WFA.

Haben sich Verbesserungspotentiale ergeben? Nein

Weiterführende Informationen

Pressemitteilung EuGH

curia.europa.eu/jcms/upload/docs/application/pdf/2022-06/cp220102de.pdf