ÖSTERREICHISCHES ROTES KREUZ

Aus Liebe zum Menschen.

Büro für strategische Netz- und
Informationssystemsicherheit, Bundeskanzleramt
BKA - I/6 (Rechts- und Vergabeangelegenheiten)
Ballhausplatz 2
1010 Wien

per E-Mail an nis@bka.gv.at und
begutachtungsverfahren@parlament.gv.at
Betreff: Stellungnahme des ÖRK zum NISG

GENERALSEKRETARIAT
Geschäftsleitung

GL/133/ME
Wien, 17. Oktober 2018

Stellungnahme zum Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)

GZ: BKA-180.310/0234-I/6/2018

Sehr geehrte Damen und Herren,

das Österreichische Rote Kreuz (ÖRK) möchte anlässlich des oben genannten Entwurfes des Netz- und Informationssystemsicherheitsgesetzes (NISG) binnen offener Frist Stellung nehmen:

Allgemeine Anmerkungen

Als gemeinnütziger Verein gibt das ÖRK zu bedenken, dass bereits in jüngster Vergangenheit zur Umsetzung der und Anpassung an die EU-Datenschutz-Grundverordnung erhebliche Ressourcen zum Datenschutz und zur Datensicherheit aufgewendet wurden. Durch den erhöhten Verwaltungs- und Kostenaufwand, der zur Erfüllung der Pflichten des NISG notwendig wäre, bestünde für das ÖRK als gemeinnütziger Verein die Gefahr, dass noch weitaus mehr Spendengelder zur Erfüllung staatlicher Aufgaben zweckentfremdet würden.

Das ÖRK ersucht daher, für unter das NISG fallende gemeinnützige Vereine und Organisationen eine Finanzierung der durch das NISG notwendigen Maßnahmen durch die öffentliche Hand vorzusehen, damit Spendengelder nicht für staatliche Aufgaben zweckentfremdet werden. Falls eine Finanzierung durch die öffentliche Hand nicht möglich sein sollte, ersucht das ÖRK um Ausnahme vom Anwendungsbereich des NISG.

MENSCHLICHKEIT ▪ UNPARTEILICHKEIT ▪ NEUTRALITÄT ▪ UNABHÄNGIGKEIT ▪ FREIWILLIGKEIT ▪ EINHEIT ▪ UNIVERSALITÄT
Österreichisches Rotes Kreuz, Generalsekretariat, Wiedner Hauptstraße 32, 1041 Wien, Telefon: +43/1/589 00-0, Fax: +43/1/589 00-199,
E-Mail: office@roteskreuz.at, www.roteskreuz.at, Bankverbindungen: SPENDEN: Erste Bank, IBAN AT57 2011 1400 1440 0144, BIC GIBAATWWXXX;
ZAHLUNGSVERKEHR: Erste Bank, IBAN AT93 2011 1000 2345 6000, BIC GIBAATWWXXX, UID-Nr.: ATU16370905, DVR-Nr.: 0416061,
FA-Registrierungsnr.: SO 1131, ZVR-Zahl: 432857691

ÖSTERREICHISCHES ROTES KREUZ

Aus Liebe zum Menschen.

Zu § 3 des Gesetzesentwurfes

In §3 Z 1 lit c sind „Netz- und Informationssysteme" ua als „digitale Daten, die von den – in lit a und b genannten – Elementen zum Zweck ihres Betriebs, ihrer Nutzung, [...] verarbeitet werden" definiert. Das ÖRK versteht „digitale Daten" iSd lit c als den in lit a und lit b aufgezählten Elementen zugehörige Wartungs- und Sicherheits-Software. Allerdings ist die lit c sprachlich unklar, weshalb das ÖRK eine Präzisierung anregt.

Die Definition des „Sicherheitsvorfalls" in § 3 Z 6 knüpft an andere Kriterien an als Art 4 Z 7 iVm Art 4 Z 2 der Richtlinie (EU) 2016/1148. Dadurch ist unklar, ob Ereignisse, bei denen kein Angriff oder Einwirken Dritter auf die Netz- und Informationssysteme vorliegt, wie beispielsweise reine Hardware-Defekte oder Stromausfälle, bereits vom Begriff des „Sicherheitsvorfalls" umfasst sind. **Das ÖRK regt eine diesbezügliche Klarstellung an.**

In § 3 Z 6 sind außerdem nicht alle der in Art 6 Abs 1 RL (EU) 2016/1148 aufgezählten Faktoren, die bei der Bestimmung des Ausmaßes einer Störung gemäß Art 5 Abs 2 lit c RL (EU) 2016/1148 mindestens zu berücksichtigen sind, aufgezählt. Insbesondere fehlt die Aufzählung des Marktanteils der Einrichtung (Art 6 Abs 1 lit d RL (EU) 2016/1148). Zwar sind diese Faktoren in § 14 Abs 2 NISG aufgezählt, doch fehlt auch dort die klare Festlegung, dass diese Faktoren für die Bestimmung der Erheblichkeit einer Störung berücksichtigt werden müssen. **Das ÖRK regt eine Klarstellung und Angleichung an die Regelung der Richtlinie an.**

In § 3 Z 7 fehlt bei der Definition des „Risikos" die in der zugrundeliegenden Bestimmung Art 4 Z 9 RL (EU) 2016/1148 angeführte Bedingung, dass die das Risiko begründenden Umstände oder Ereignisse „mit vernünftigem Aufwand feststellbar" sein müssen. Dadurch wird in § 3 Z 7 NISG der Aufwand für die Ermittlung, ob ein Risiko besteht, nicht berücksichtigt, was zu enormen Aufwänden in der Risikoanalyse führen würde. **Das ÖRK regt daher an, die Regelung des Art 4 Z 9 RL (EU) 2016/1148 wortgleich zu übernehmen.**

§ 3 Z 14 definiert „Cloud-Computing-Dienst" als „einen digitalen Dienst, der den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglicht". Der Begriff Rechenressourcen deutet auf Rechnen hin und umfasst nicht die Speicherung oder Übertragung von Daten. Das ÖRK regt an, den Begriff „Rechenressourcen" durch „digitale Ressourcen" zu ersetzen.

MENSCHLICHKEIT ▪ UNPARTEILICHKEIT ▪ NEUTRALITÄT ▪ UNABHÄNGIGKEIT ▪ FREIWILLIGKEIT ▪ EINHEIT ▪ UNIVERSALITÄT
Österreichisches Rotes Kreuz, Generalsekretariat, Wiedner Hauptstraße 32, 1041 Wien, Telefon: +43/1/589 00-0, Fax: +43/1/589 00-199,
E-Mail: office@roteskreuz.at, www.roteskreuz.at, Bankverbindungen: SPENDEN: Erste Bank, IBAN AT57 2011 1400 1440 0144, BIC GIBAATWWXXX;
ZAHLUNGSVERKEHR: Erste Bank, IBAN AT93 2011 1000 2345 6000, BIC GIBAATWWXXX, UID-Nr.: ATU16370905, DVR-Nr.: 0416061,
FA-Registrierungsnr.: SO 1131, ZVR-Zahl: 432857691

ÖSTERREICHISCHES ROTES KREUZ

Aus Liebe zum Menschen.

Zu § 10 des Gesetzesentwurfes

§ 10 Abs 2 sieht vor, dass der Bundesminister für Inneres zur Erfüllung seiner Aufgaben gemäß § 5 Z 4 und 5 eine Aufstellung der vorhandenen Sicherheitsvorkehrungen sowie der aufgedeckten Sicherheitsmängel verarbeiten darf. Hierzu geben wir zu bedenken, dass mit der Speicherung der Aufstellung der vorhandenen Sicherheitsvorkehrungen eine zusätzliche potentielle Sicherheitslücke geschaffen wird. Zudem wird diese Aufstellung nicht den nötigen Grad der Aktualität besitzen, um hier seine Aufgaben zu erfüllen.

Die Erläuterungen zu § 10 Abs 2 (Erläuterungen Seite 12, 1. Absatz) sehen vor, dass vom Bundesminister für Inneres ua Zugangsdaten verarbeitet werden dürfen. Zugangsdaten können Kennwörter sein. Die Weitergabe von Kennwörtern ist nach den Prinzipien des Datenschutzes nicht gestattet. Wir regen daher die Streichung der „Zugangsdaten" in der Aufzählung an.

Gemäß § 10 Abs 3 ist vorgesehen, dass jedes NIS-Büro jene Auskünfte verlangen darf, die es als wesentliche Voraussetzung zur Erfüllung seiner Aufgaben benötigt. Es wird in diesem Zusammenhang nicht dargelegt, was unter diesen „wesentlichen Voraussetzungen" zu verstehen ist. Nach dem Wortlaut liegt dies im alleinigen Ermessen der NIS-Büros, weshalb das ÖRK eine Einschränkung bzw. Präzisierung des Wortlautes anregt. Darüber hinaus sind gemäß Gesetzestext „die ersuchten Stellen verpflichtet, unverzüglich Auskunft zu erteilen". Das ÖRK beurteilt diesen Wortlaut als zu unkonkret und regt eine genaue Darlegung jener Informationen an, die von dieser Auskunft umfasst sein dürfen. Das ÖRK regt in Bezug auf die auskunftspflichtigen Informationen an, dass dies nur solche sein dürfen, die unmittelbar mit der Netz- und Informationssystemsicherheit der Dienste des jeweiligen Betreibers – beschränkt auf die jeweils eigene Domain – in Zusammenhang stehen. **Das ÖRK ersucht um dementsprechende Ausformulierung bzw. Anpassung des Gesetzeswortlautes.**

MENSCHLICHKEIT ▪ UNPARTEILICHKEIT ▪ NEUTRALITÄT ▪ UNABHÄNGIGKEIT ▪ FREIWILLIGKEIT ▪ EINHEIT ▪ UNIVERSALITÄT
Österreichisches Rotes Kreuz, Generalsekretariat, Wiedner Hauptstraße 32, 1041 Wien, Telefon: +43/1/589 00-0, Fax: +43/1/589 00-199,
E-Mail: office@roteskreuz.at, www.roteskreuz.at, Bankverbindungen: SPENDEN: Erste Bank, IBAN AT57 2011 1400 1440 0144, BIC GIBAATWWXXX;
ZAHLUNGSVERKEHR: Erste Bank, IBAN AT93 2011 1000 23456000, BIC GIBAATWWXXX, UID-Nr.: ATU16370905, DVR-Nr.: 0416061,
FA-Registrierungsnr.: SO 1131, ZVR-Zahl: 432857691

ÖSTERREICHISCHES ROTES KREUZ

Aus Liebe zum Menschen.

Zum 5. Abschnitt des Gesetzesentwurfes: Verpflichtungen für Betreiber wesentlicher Dienste, Anbieter digitaler Dienste und Einrichtungen des Bundes

Gemäß § 15 Abs 1 haben die Betreiber wesentlicher Dienste „geeignete, dem Stand der Technik entsprechende Sicherheitsvorkehrungen" zu treffen. Art 14 Abs 1 RL (EU) 2016/1148 spricht hingegen von „geeigneten und **verhältnismäßigen** technischen und organisatorischen Maßnahmen". Gleiches gilt sinngemäß für die Pflichten der Anbieter digitaler Dienste in § 18 Abs 1 NISG im Vergleich zum zugrundeliegenden Art 16 Abs 1 RL (EU) 2016/1148. **Im Sinne der Vermeidung der Übererfüllung bei der Umsetzung der Richtlinie sollte auch im NISG die Verhältnismäßigkeit der Maßnahmen, die Betreiber wesentlicher Dienste bzw. Anbieter digitaler Dienste zu setzen haben, berücksichtigt werden.**

Auch die Pflichten, die sich aus § 15 Abs 3 NISG ergeben, sind nach Meinung des ÖRK zu unkonkret festgelegt. Auch hier spricht sich das ÖRK dafür aus, dass diese Pflichten auf die Netz- und Informationssysteme der jeweils eigenen Domain des Betreibers bzw. Anbieters beschränkt sein müssen, da nur hier ein Gestaltungsspielraum für die Betreiber bzw. Anbieter besteht. Zudem gilt, wie auch zu § 10 Abs 3 NISG bereits angemerkt, dass nur in solche Informationen Einschau genommen werden darf, die unmittelbar mit der Netz- und Informationssystemsicherheit der Dienste des jeweiligen Betreibers in Zusammenhang stehen. **Das ÖRK ersucht um entsprechende Anpassung des Gesetzeswortlautes.**

In § 15 Abs 3 ist festgelegt, dass der Nachweis über die Erfüllung der Anforderungen nach § 15 Abs 1 „ein Jahr nach Zustellung des Bescheids gemäß § 14 Abs 5 Z 1 jederzeit verlangt werden kann". Da die Erfüllung der Anforderungen nach Einschätzung des ÖRK länger als ein Jahr dauern würde, **spricht sich das ÖRK für eine Verlängerung der Frist um ein weiteres Jahr aus.**

Gemäß § 16 Abs 1 muss die Meldung eines Sicherheitsvorfalls „unverzüglich" erfolgen und hat gemäß § 16 Abs 3 sämtliche Angaben zu enthalten, „die im Zeitpunkt der Meldung bekannt sind". In der demonstrativen Aufzählung dieser Angaben befindet sich auch die „vermutete oder tatsächliche Ursache" des Sicherheitsvorfalls. Das ÖRK weist darauf hin, dass die konkrete Ursache zum Zeitpunkt der (unverzüglichen) Meldung im Regelfall noch nicht bekannt sein wird, da es einer eingehenden Analyse („Root Cause Analysis") bedarf, um die Ursache zu ermitteln.

MENSCHLICHKEIT ▪ UNPARTEILICHKEIT ▪ NEUTRALITÄT ▪ UNABHÄNGIGKEIT ▪ FREIWILLIGKEIT ▪ EINHEIT ▪ UNIVERSALITÄT
Österreichisches Rotes Kreuz, Generalsekretariat, Wiedner Hauptstraße 32, 1041 Wien, Telefon: +43/1/589 00-0, Fax: +43/1/589 00-199,
E-Mail: office@roteskreuz.at, www.roteskreuz.at, Bankverbindungen: SPENDEN: Erste Bank, IBAN AT57 2011 1400 1440 0144, BIC GIBAATWWXXX;
ZAHLUNGSVERKEHR: Erste Bank, IBAN AT93 2011 1000 2345 6000, BIC GIBAATWWXXX, UID-Nr.: ATU16370905, DVR-Nr.: 0416061,
FA-Registrierungsnr.: SO 1131, ZVR-Zahl: 432857691

ÖSTERREICHISCHES ROTES KREUZ

Aus Liebe zum Menschen.

Gemäß § 16 Abs 4 haben Betreiber wesentlicher Dienste bei Inanspruchnahme von Diensten eines Anbieters digitaler Dienste „jede erhebliche Auswirkung auf die Verfügbarkeit der wesentlichen Dienste, die von einem den Anbieter digitaler Dienste beeinträchtigenden Sicherheitsvorfall verursacht wurde, […] zu melden." Eine Meldepflicht des Betreibers wesentlicher Dienste sollte nach Meinung des ÖRK nur dann bestehen, wenn diesem der Sicherheitsvorfall bekannt ist. Der Betreiber wesentlicher Dienste, der unter Umständen erst verspätet Servicerückmeldungen vom Anbieter digitaler Dienste bekommt, steht nach dem derzeitigen Gesetzesentwurf in der Verantwortung, obwohl er die technischen Rahmenbedingungen und potentiellen Ursachen des Sicherheitsvorfalls beim Anbieter digitaler Dienste nicht klar bestimmen und daher auch nicht zureichend melden kann. **Das ÖRK ersucht um entsprechende Anpassung des Gesetzestextes.**

In diesem Zusammenhang ist auszuführen, dass die Anbieter digitaler Dienste einen Sicherheitsvorfall gemäß § 18 Abs 2 dann zu melden haben, wenn der Anbieter Zugang zu Informationen hat, die benötigt werden, um die Auswirkung eines Sicherheitsvorfalls zu bewerten. Der Gesetzgeber hat nicht darauf Bedacht genommen, hier auch die Meldepflicht des digitalen Anbieters an jene Betreiber der wesentlichen Dienste zu regeln, die die Dienste des digitalen Anbieters in Anspruch nehmen. Der Betreiber wesentlicher Dienste ist in der Erbringung seiner Dienstleistung vom Anbieter digitaler Dienste abhängig. Wir regen daher an, die Regelung des § 16 Abs 4 sinngemäß auch den Anbietern digitaler Dienste aufzuerlegen und eine Meldepflicht von Anbietern digitaler Dienste an jene Betreiber der wesentlichen Dienste einzuführen, die die Dienste dieser digitalen Anbieter in Anspruch nehmen.

Darüber hinaus regt das ÖRK an, für alle Einrichtungen, die im Rahmen des NISG Einsicht in Unterlagen und Netz- und Informationssysteme der Betreiber wesentlicher Dienste oder der Anbieter digitaler Dienste nehmen, eine zu § 22 Abs 3 DSG vergleichbare Regelung zur Verschwiegenheit zu treffen.

MENSCHLICHKEIT ▪ UNPARTEILICHKEIT ▪ NEUTRALITÄT ▪ UNABHÄNGIGKEIT ▪ FREIWILLIGKEIT ▪ EINHEIT ▪ UNIVERSALITÄT
Österreichisches Rotes Kreuz, Generalsekretariat, Wiedner Hauptstraße 32, 1041 Wien, Telefon: +43/1/589 00-0, Fax: +43/1/589 00-199,
E-Mail: office@roteskreuz.at, www.roteskreuz.at, Bankverbindungen: SPENDEN: Erste Bank, IBAN AT57 2011 1400 1440 0144, BIC GIBAATWWXXX;
ZAHLUNGSVERKEHR: Erste Bank, IBAN AT93 2011 1000 2345 6000, BIC GIBAATWWXXX, UID-Nr.: ATU16370905, DVR-Nr.: 0416061,
FA-Registrierungsnr.: SO 1131, ZVR-Zahl: 432857691

ÖSTERREICHISCHES ROTES KREUZ

Aus Liebe zum Menschen.

Zur Darstellung der Berechnung der Verwaltungskosten für Unternehmen

Im Anhang der Wirkungsorientierten Folgenabschätzung (Seite 18) ist der Stundensatz für externe Gutachten mit EUR 53,- angeführt. Diese Bemessung erachtet das ÖRK als völlig unrealistisch. Angebracht wäre an dieser Stelle ein Stundensatz von mindestens EUR 150,-. Werden Zertifizierungen, wie beispielsweise jene nach ISO 2700x gefordert, steigen die Kosten noch deutlich höher an, da diese mit Sicherheit nicht innerhalb von 40 Stunden, wie in der WFA angeführt, umgesetzt werden können. Die Kosten für allfällige technische Anpassungen und organisatorische Maßnahmen, um das geforderte Schutzniveau zu erreichen, scheinen ebenfalls nicht auf. Auch die Gebühren für das Frühwarnsystem (Seite 16 der WFA) werden nicht berücksichtigt. Die Kosten, die für Unternehmen durch Umsetzung des NISG entstehen würden, sind mit Sicherheit deutlich höher als in den WFA angegeben. **Das ÖRK ersucht um transparente und realistische Berechnung der entstehenden Verwaltungskosten und wiederholt im Zusammenhang mit dem hohen Kostenaufwand seine Forderung nach Finanzierung der durch das NISG notwendigen Maßnahmen durch die öffentliche Hand.**

Wir ersuchen um Berücksichtigung unserer Anliegen

und verbleiben mit freundlichen Grüßen!

Dr. Werner Kerschbaum
Generalsekretär

Mag. Michael Opriesnig
Stv. Generalsekretär

Ansprechpartnerin
Mag.ª Magdalena Ebenbauer
Tel +43/1/589 00-115
E-Mail magdalena.ebenbauer@roteskreuz.at