Formelle Kommentare des EDSB zum Durchführungsbeschluss der Kommission zur Festlegung eines Musters für einen Sicherheitsplan, eines Musters für die Aufrechterhaltung des Geschäftsbetriebs und eines Notfallplans zur Aufrechterhaltung und Wiederherstellung des Betriebs gemäß Artikel 59 Absatz 4 der Verordnung (EU) 2018/1240

1. Einleitung und Hintergrund

Das Europäische Reiseinformations- und -genehmigungssystem (ETIAS) wurde durch die Verordnung (EU) 2018/1240[1] geschaffen und verpflichtet alle von der Visumpflicht befreiten Drittstaatsangehörigen, vor dem Datum ihrer Ausreise in den Schengen-Raum online eine Reisegenehmigung zu beantragen.

Gemäß Artikel 59 Absatz 4 der Verordnung (EU) 2018/1240 wurde der Europäischen Kommission die Befugnis übertragen, im Wege von Durchführungsrechtsakten ein Muster eines Sicherheitsplans sowie eines Notfallplans zur Aufrechterhaltung und Wiederherstellung des Betriebs anzunehmen. Die von der Kommission angenommenen Musterpläne dienen dem Verwaltungsrat der eu-LiSA, dem Verwaltungsrat der Europäischen Agentur für die Grenz- und Küstenwache sowie den Mitgliedstaaten als Grundlage – ggf. in angepasster Form – für die Annahme ihrer eigenen Sicherheits- und Notfallpläne, um die Sicherheit des ETIAS-Informationssystems zu gewährleisten.

Die vorliegenden formellen Kommentare des EDSB ergehen in Beantwortung der legislativen Konsultation durch die Europäische Kommission vom 15. April 2021 gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725.[2] Diesbezüglich begrüßt der EDSB, dass auf diese Konsultation in Erwägungsgrund 9 des Entwurfs des Durchführungsbeschlusses verwiesen wird.

Der EDSB möchte betonen, dass diese formellen Kommentare künftige zusätzliche Kommentare des EDSB nicht ausschließen, insbesondere wenn weitere Fragen aufgeworfen oder neue Informationen verfügbar werden, beispielsweise infolge des Erlasses anderer damit zusammenhängender Durchführungs- oder

[1] Verordnung (EU) 2018/1240 des Europäischen Parlaments und des Rates vom 12. September 2018 über die Einrichtung
eines Europäischen Reiseinformations- und -genehmigungssystems (ETIAS) und zur Änderung der Verordnungen (EU) Nr. 1077/2011, (EU) Nr. 515/2014, (EU) 2016/399, (EU) 2016/1624 und (EU) 2017/2226, ABl. L 236 vom 19.9.2018, S. 1.

[2] Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG, ABl. L 295 vom 21.11.2018, S. 39 (Verordnung (EU) 2018/1725).

delegierter Rechtsakte gemäß der Verordnung (EU) 2018/1240. Darüber hinaus greifen diese formellen Kommentare etwaigen künftigen Maßnahmen des EDSB in Ausübung seiner Befugnisse gemäß Artikel 58 der Verordnung (EU) 2018/1725 nicht vor.

2. Kommentare

Der EDSB stellt fest, dass der Entwurf der Anlage zum Durchführungsbeschluss der Kommission einen Leitfaden zur Methodik der Abfassung eines Musters eines Sicherheitsplans sowie eines Notfallplans zur Aufrechterhaltung und Wiederherstellung des Betriebs enthält. Dennoch gilt nur Anhang 10 der Anlage zum Entwurf des Durchführungsbeschlusses der Kommission als vollwertiger „Musterplan".

Der EDSB erinnert daran, dass „unbeschadet des Artikels 22 der Verordnung (EG) Nr. 45/2001", der anschließend durch Artikel 33 der Verordnung (EE) 2018/1725 ersetzt wurde, und unbeschadet der Verordnung (EU) 2016/679, Artikel 59 Absätze 2 und 3 der Verordnung (EU) 2018/1240 Sicherheitsmaßnahmen regelt[3]. Dies bedeutet, dass die Anforderungen an die Einrichtung von Sicherheitsmaßnahmen im Entwurf des Durchführungsbeschlusses der Kommission nicht nur auf die Angaben in Artikel 59 der Verordnung (EU) 2018/1240 beschränkt sind, sondern auch sämtliche Anforderungen der Verordnung (EU) 2018/1725 und der Verordnung (EU) 2016/679 erfüllen müssen.

Außerdem erinnert der EDSB daran, dass gemäß Artikel 33 Absatz 1 der Verordnung (EU) 2018/1725 sowie Artikel 32 Absatz 1 der Verordnung (EU) 2016/679 eine verpflichtende Analyse des Risikos „für die Rechte und Freiheiten natürlicher Personen" in die Risikoanalyse des Verantwortlichen bzw. Verarbeiters aufzunehmen ist. Eine Orientierungshilfe zu dieser Anforderung gibt der EDSB in seinen Leitlinien zu Sicherheitsmaßnahmen für die Verarbeitung personenbezogener Daten (Guidelines on Security Measures for Personal Data Processing[4]).

Während die herkömmlichen oder allgemeinen Risikomanagementmaßnahmen im Bereich der Datensicherheit darauf abzielen, die Netz- und Informationssysteme der Organisation (und die darin enthaltenen Daten) zu schützen, zielen die genannten Artikel der Datenschutzvorschriften darauf ab, den Einzelnen und seine Rechte durch den Schutz seiner Daten zu schützen. Es gibt einen Unterschied zwischen den Gütern, die bei beiden Tätigkeiten geschützt werden sollen, was unter bestimmten Umständen zu unterschiedlichen Schlussfolgerungen führen könnte.

Der EDSB stellt fest, dass die Rechte und Freiheiten natürlicher Personen als ein zu schützendes Gut in den Musterplänen nicht hinreichend berücksichtigt wurden. So enthalten beispielsweise die Begriffsbestimmungen von „Folgenabschätzung für den Betrieb", „Folgenabschätzung", „Risikoanalyse" und „Sicherheitsplan" und andere keinen

[3] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119 vom 4.5.2016, S. 1-88.

[4] https://edps.europa.eu/data-protection/our-work/publications/guidelines/security-measures-personal-data-processing_en.

Verweis auf natürliche Personen als betroffene Personen und ihre Rechte. Ebenso bezieht sich Abschnitt „C6 SICHERHEITSKONTROLLEN UND VERFAHREN“ nicht auf die Risiken für die Rechte und Freiheiten natürlicher Personen.

Der EDSB empfiehlt, die Aspekte der Privatsphäre und des Datenschutzes in das Risikomanagement für die Datensicherheit einzubeziehen, um einen ganzheitlichen Ansatz zu gewährleisten und Synergien beim Management der Datensicherheit und des Schutzes der verarbeiteten Informationen ohne unnötigen Mehraufwand zu ermöglichen, und fordert die Kommission auf, den Entwurf des Durchführungsbeschlusses entsprechend zu ändern.

Der EDSB stellt ferner fest, dass in dem Dokument wiederholt auf die US-Norm NIST 800-54 rev.4 und nicht auf die neueste Fassung rev.5 Bezug genommen wird, die auch „Datenschutzrisiken“ enthält. Zum Beispiel enthält die neueste Norm NIST 800-53 rev.5 in der Risikobewertung (Seite 240) die „Wahrscheinlichkeit und Auswirkung nachteiliger Effekte auf den Einzelnen durch die Verarbeitung personenbezogener Daten“, was in der älteren rev.4 der gleichen Norm nicht der Fall ist (Seite 152). In mehreren anderen nationalen Normen, wie dem deutschen „BSI Grundschutz“ in seiner neuesten Fassung, werden auch die Rechte und Freiheiten natürlicher Personen in ihrer Methodik berücksichtigt.

Der EDSB empfiehlt der Kommission daher, bei der Bezugnahme auf eine US-Norm auf die neueste Norm NIST 800-53 rev.5 zu verweisen, die stärker an Artikel 32 Absatz 1 der Verordnung (EU) 2016/679 bzw. an Artikel 33 Absatz 1 der Verordnung (EU) 2016/679 angelehnt ist.

Brüssel, den 7. Juni 2021

Wojciech Rafał WIEWIÓROWSKI
(elektronisch unterzeichnet)