Bundesministerium
Inneres

Datenschutz-Folgenabschätzung Entry/Exit System (EES) (inklusive Grenzkontrollsoftware und Adminkonsole)

Version 1.1.

Datenschutz-Folgenabschätzung
Entry/Exit System (EES)
(inklusive Grenzkontrollsoftware und Adminkonsole)

Inhaltsverzeichnis

1. Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten

In dieser Datenschutz-Folgenabschätzung (DS-FA) werden die Auswirkungen der Datenverarbeitung im Entry-Exit-System (im Folgenden als „EES“ bezeichnet) auf die Rechte und Freiheiten von natürlichen Personen untersucht. In Österreich beinhaltet die Umsetzung des EES verschiedene Bausteine, zentral sind hierbei die Grenzkontrollsoftware „GKS“ und die BMI-Webanwendung „Adminkonsole“ als Hauptbestandteile auf Softwareebene.

Als primäre Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten ist die *VERORDNUNG (EU) 2017/2226 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 30. November 2017 über ein* ***Einreise-/Ausreisesystem (EES)*** *zur Erfassung der Ein- und Ausreisedaten sowie der Einreiseverweigerungsdaten von Drittstaatsangehörigen an den Außengrenzen der Mitgliedstaaten und zur Festlegung der Bedingungen für den Zugang zum EES zu Gefahrenabwehr- und Strafverfolgungszwecken und zur Änderung des Übereinkommens zur Durchführung des Übereinkommens von Schengen sowie der Verordnungen (EG) Nr. 767/2008 und (EU) Nr. 1077/2011* (im Folgenden als „EES-VO“ bezeichnet) zu nennen.

Weitere Rechtsgrundlagen stellen die *VERORDNUNG (EU) 2016/399 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 9. März 2016 über einen Gemeinschaftskodex für das Überschreiten der Grenzen durch Personen* (im Folgenden als „Schengener Grenzkodex“ bezeichnet) sowie die Verordnung (EU) 2025/1534 über vorübergehende Abweichungen von bestimmten Bestimmungen der Verordnungen (EU) 2017/2226 und (EU) 2016/399 im Hinblick auf den schrittweisen Betriebsstart des Entry/Exit Systems (EES) (im Weiteren als „EES-Ergänzungs-VO“ bezeichnet) dar.

Mit der *VERORDNUNG (EU) 2017/2225 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 30. November 2017 zur Änderung der Verordnung (EU) 2016/399 in Bezug auf die Nutzung des Einreise-/Ausreisesystems* wird der Schengener Grenzkodex an die Inhalte der EES-VO angepasst.

Diese Rechtsgrundlagen gelten gemäß Art. 288 des Vertrags über die Arbeitsweise der Europäischen Union ohne weitere Umsetzungsmaßnahmen unmittelbar in den Mitgliedstaaten.

Weitere Dokumente, welche im Rahmen dieser DS-FA berücksichtigt wurden:

- 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)

- Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) vom 04.04.2017 (erarbeitet von der „Arbeitsgruppe für den Schutz der Rechte von Personen bei der Verarbeitung personenbezogener Daten“ eingesetzt nach den Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995

- 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

- RICHTLINIE (EU) 2016/680 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates

- Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz 2000 – DSG)

- CHARTA DER GRUNDRECHTE DER EUROPÄISCHEN UNION (2000/C 364/01)

- VERORDNUNG (EG) Nr. 767/2008 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 9. Juli 2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (VIS-Verordnung)

- VERORDNUNG (EU) 2019/817 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU)

2018/1726 und (EU) 2018/1861 des Europäischen Parlaments und des Rates, der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates

- VERORDNUNG (EU) 2019/818 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (polizeiliche und justizielle Zusammenarbeit, Asyl und Migration) und zur Änderung der Verordnungen (EU) 2018/1726, (EU) 2018/1862 und (EU) 2019/816

- Übereinkommen zur Durchführung des Übereinkommens von Schengen vom 14. Juni 1985 zwischen den Regierungen der Staaten der Benelux-Wirtschaftsunion, der Bundesrepublik Deutschland und der Französischen Republik betreffend den schrittweisen Abbau der Kontrollen an den gemeinsamen Grenzen vom 19. Juni 1990 (Schengener Durchführungsübereinkommen)

- Sämtliche Durchführungsrechtsakte der EU- Kommission zum EES gem. Art. 36 EES-VO und

- „EES CORE PROJECT – EES DATA PROTECTION IMPACT ASSESSMENT“: Datenschutz-Folgenabschätzung der eu-LISA zum zentralen EES vom 23.06.2021 (Beilage 1 zu diesem Dokument)

- Zusammenfassung der Stellungnahme des Europäischen Datenschutzbeauftragten zum zweiten Paket „Intelligente Grenzen“ der EU, C 463/14 (Beilage 2 zu diesem Dokument)

- Folgenabschätzungsbericht der Europäischen Kommission zum EES: COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Impact Assessment Report on the establishment of an EU Entry Exit System accompanying the document *Proposal for a regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011* and *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/xxx as regards the use of the Entry/Exit System (EES)*, Brussels, 6.4.2016 SWD(2016) 115 final (Teil 3), Beilage 3 zu diesem Dokument.

2. Ziele dieses Dokuments

- Beschreibung der wichtigsten Akteure bei Datenverarbeitungsvorgängen im Zusammenhang mit dem EES

- Beschreibung der Datenverarbeitungsvorgänge im EES

- Bewertung der Notwendigkeit und Verhältnismäßigkeit der Datenverarbeitung

- Analyse und Bewertung der mit der Datenverarbeitung im EES verbundenen Risiken für die Rechte und Freiheiten der betroffenen Personen inkl. Beschreibung von Maßnahmen und Mechanismen für die Risikominimierung

3. Gründe für die Erstellung dieses Dokuments

- Der Zweck des EES umfasst die innovative Nutzung oder Anwendung technologischer oder organisatorischer Lösungen, die neuartige Formen der Datenerhebung und -nutzung beinhalten können;

- Die Datenverarbeitung umfasst auch eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gem. Art. 35 Abs. 3 lit b DSGVO;

- Das EES wird eine große Menge an Daten unter Verwendung innovativer technischer Lösungen verwalten;

- Die Datenverarbeitung kann schutzbedürftige Personen wie Kinder betreffen.

Bundesministerium
Inneres

4. Verzeichnis von Verarbeitungstätigkeiten gem. Art. 30 DSGVO

Jeder Verantwortliche ist gem. Art. 30 DSGVO verpflichtet, ein Verzeichnis aller Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen, zu führen:

Tabelle 1 Verzeichnis der Verarbeitungstätigkeiten gem. Art. 30 DSGVO

1. Name und die Kontaktdaten des Verantwortlichen gem. Art. 30 Abs 1 lit a DSGVO und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten	In Österreich gelten als **„Verantwortliche“ gem. Art. 4 Z 7 i.V.m. Art. 26 DSGVO**: **Bundesminister für Inneres** Herrengasse 7 1010 Wien **Landespolizeidirektionen:** **LPD Burgenland** Telefon: 059133/10/0 Fax: 059133/10/1009 LPD-B@polizei.gv.at **LPD Kärnten** Telefon: 059133/20/0 Fax: 059133/20/7800 LPD-K@polizei.gv.a

	LPD Niederösterreich Telefon: 059133/30/0 Fax: 059133/30/7800 LPD-N@polizei.gv.at **LPD Oberösterreich** Telefon: 059133/40/0 Fax: 059133/40/7800 LPD-O@polizei.gv.at **LPD Salzburg** Telefon: 059133/50/0 Fax: 059133/50/7800 LPD-S@polizei.gv.at **LPD Steiermark** Telefon: 059133/60/0 Fax: 059133/60/1009 LPD-ST@polizei.gv.at **LPD Tirol** Telefon: 059133/70/0 Fax: +4359133 70 7888 LPD-T@polizei.gv.at

	LPD Vorarlberg Telefon: 059133/80/0 Fax: 059133/80/1009 LPD-V@polizei.gv.at **LPD Wien** Telefon: 01 31310-0 LPD-W@polizei.gv.at **Zuständige Ansprechstelle des Verantwortlichen gem. Art. 4 Z 17 DSGVO**: **Bundesministerium für Inneres** Abteilung V/B/6 Integrierte Grenzverwaltung BMI-V-B-6@bmi.gv.at **Anträge gem. Art. 15 bis 18 DSGVO werden ausnahmslos unter BMI-EES@bmi.gv.at entgegengenommen.** Als **„Datenschutzbeauftragte“** gelten: ▪ Datenschutzbeauftragte(r) des Bundesministers für Inneres (DSBa-BMI) bmi-datenschutzbeauftragter@bmi.gv.at ▪ Datenschutzbeauftragte(r) der Landespolizeidirektionen (DSBa-LPD) LPD-Datenschutzbeauftragter@polizei.gv.at

2. Zwecke der Verarbeitung gem. Art. 30 Abs 1 lit b DSGVO	Die Durchführung der Grenzkontrolle mittels der Grenzkontrollsoftware dient der Überprüfung der Voraussetzungen für die Ein- und Ausreise aller Reisenden, die sich der Grenzkontrolle stellen, gemäß den Bestimmungen des Schengener Grenzkodex und des österreichischen Grenzkontrollgesetzes. Die Verarbeitung der Daten in der Grenzkontrollsoftware und im EES verfolgt, insbesondere im Hinblick auf Art. 6 EES-VO, folgende Ziele: • Prüfung der Voraussetzungen für die Einreise- und Ausreise gemäß Art. 6 sowie Art. 8 Schengener Grenzkodex für alle Reisenden, die sich der Grenzkontrolle stellen • Die in §15 Abs. 1 GrekoG genannten Zwecke (z.B. Durchführung von Fahndungsabfragen im Rahmen der Sicherheitsverwaltung und im Dienste der Strafrechtspflege) • Erhöhung der Effizienz der Grenzübertrittskontrollen durch Berechnung und Überwachung der Dauer des zulässigen Aufenthalts bei der Ein- und der Ausreise von Drittstaatsangehörigen, die für einen Kurzaufenthalt zugelassen sind; • Beitrag zur Identifizierung von Drittstaatsangehörigen, die die Voraussetzungen für die Einreise in das oder den Kurzaufenthalt im Hoheitsgebiet der Mitgliedstaaten nicht oder nicht mehr erfüllen; • Ermöglichung der Identifizierung und des Auffindens von Aufenthaltsüberziehern sowie der Ergreifung der erforderlichen Maßnahmen durch die zuständigen Behörden der Mitgliedstaaten; • Ermöglichung der elektronischen Überprüfung von Einreiseverweigerungen im EES; • Ermöglichung der Automatisierung der Grenzübertrittskontrollen von Drittstaatsangehörigen; • Ermöglichung des Zugangs der Visumbehörden zu Informationen über die vorschriftsmäßige Verwendung früher erteilter Visa; • Unterrichtung von Drittstaatsangehörigen über die Dauer ihres zulässigen Aufenthalts;

	• Erstellung von Statistiken zur Ein- und Ausreise von Drittstaatsangehörigen, zu Einreiseverweigerungen für Drittstaatsangehörige und zu Aufenthaltsüberziehungen durch Drittstaatsangehörige, um eine bessere Abschätzung des Risikos von Aufenthaltsüberziehungen zu ermöglichen und eine faktenbasierte Gestaltung der Migrationspolitik der Union zu unterstützen; • Bekämpfung von Identitätsbetrug und von Missbrauch von Reisedokumenten; • Sicherstellung der korrekten Identifizierung von Personen. • Beitrag zur Verhütung, Aufdeckung und Untersuchung terroristischer oder sonstiger schwerer Straftaten; • Ermöglichung der Erstellung von Informationen für Ermittlungen im Zusammenhang mit terroristischen oder sonstigen schweren Straftaten, einschließlich der Identifizierung von Tätern, Verdächtigen und Opfern derartiger Straftaten, die die Außengrenzen überschritten haben.
3. Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten gem. Art. 30 Abs 1 lit c DSGVO	Alle Reisenden, die sich an den österreichischen Außengrenzen der Grenzkontrolle stellen, werden mittels der Grenzkontrollsoftware kontrolliert. Dies umfasst Unionsbürger i.S.d. Art. 8 Abs. 2 SGK sowie Drittstaatsangehörige i.S.d. Art. 8 Abs. 3 SGK. Alternativ kann auch die sog. BMI-Webanwendung Adminkonsole für diese Zwecke herangezogen werden. **Die Verarbeitung von Daten im EES betrifft jedoch ausschließlich Drittstaatsangehörige i.S.d. Art. 2 EES-VO i.V.m. Art. 6a SGK**: **a)** Drittstaatsangehörige, die für einen Kurzaufenthalt im Hoheitsgebiet der Mitgliedstaaten zugelassen sind und sich an den Grenzen, an denen das EES eingesetzt wird, den in der Verordnung (EU) 2016/399 vorgesehenen Grenzübertrittskontrollen unterziehen müssen, und

	b) Drittstaatsangehörige bei der Einreise in das und der Ausreise aus dem Hoheitsgebiet der Mitgliedstaaten, die i) Familienangehörige eines unter die Richtlinie 2004/38/EG fallenden Unionsbürgers oder Familienangehörige eines Drittstaatsangehörigen sind, der auf der Grundlage eines Abkommens zwischen der Union und ihren Mitgliedstaaten einerseits und einem Drittstaat andererseits ein dem Recht von Unionsbürgern gleichwertiges Recht auf Freizügigkeit genießt, und ii) nicht im Besitz einer Aufenthaltskarte gemäß der Richtlinie 2004/38/EG oder eines Aufenthaltstitels gemäß der Verordnung (EG) Nr. 1030/2002 des Rates sind. **c)** außerdem Drittstaatsangehörige, denen die Einreise für einen Kurzaufenthalt im Hoheitsgebiet der Mitgliedstaaten gemäß Art. 14 der Verordnung (EU) 2016/399 verweigert wird. **Kategorien personenbezogenen Daten, die gem. Art. 16 ff. EES-VO verarbeitet werden:** • Nachname (Familienname), Vorname(n) (Vornamen), Geburtsdatum, Staatsangehörigkeit(en), Geschlecht; • Art und Nummer der Reisedokumente mit Angabe des Datums des Ablaufs der Gültigkeit; • Informationen betreffend ETIAS-Reisegenehmigung • Datum und Uhrzeit der Einreise, Ausreise oder Einreiseverweigerung, d.h. Reisehistorie; • Die Grenzübergangsstelle der Einreise, Ausreise oder Einreiseverweigerung und die zuständige Behörde; • Gründe für eine allfällige Einreiseverweigerung gem. Anhang V SGK • Die Nummer der Visummarke für den kurzfristigen Aufenthalt; • Informationen über den Status der biometrischen Überprüfung; • Informationen über die Überschreitung der Aufenthaltsdauer.

	• Besondere Kategorien sind:
	• Biometrische Daten;
	  ○ das Gesichtsbild der betroffenen Person gem. Art. 15 EES-VO;
	  ○ die Fingerabdruckdaten der betroffenen Person (vier Finger der rechten Hand, alternativ der linken Hand) gem. Art. 17 Abs. 1 EES-VO

4. Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen gem. Art. 30 Abs 1 lit d DSGVO	Neben der in §15 GrekoG ausdrücklich genannten Übermittlungsbefugnisse und Empfängern, sind auch spezifisch im Hinblick auf EES folgende Behörden relevant: • **Grenzkontrollbehörden** gem. Art. 3 Abs. 1 Z 3 VO 2017/2226 zwecks Eingabe, Änderung, Löschung und Abfrage von Daten gem. Art. 9 Abs. 2 VO (EU) 2017/2226 • **Einwanderungsbehörden** gem. Art. 3 Abs. 1 Z 4 VO 2017/2226 zwecks Eingabe, Änderung, Löschung und Abfrage von Daten gem. Art. 9 Abs. 2 VO (EU) 2017/2226 • **Visumbehörden** gem. Art. 3 Ab. 1 Z 5 VO 2017/2226 zwecks Eingabe, Änderung, Löschung und Abfrage von Daten gem. Art. 9 Abs. 2 VO (EU) 2017/2226 • **Zentrale Zugangsstelle** gem. Art. 29 Abs. 3 VO 2017/2226 i.V.m. § 43a EU-Polizeikooperationsgesetz, die für die Überprüfung der Zugangsbedingungen gem. Art. 32 EES-VO zuständig ist (Zugang der benannten Behörden auf EES-Daten zu Zwecken der Strafverfolgung) • **Benannte Behörden** gem. Art. 3 Abs. 1 Z 26 VO i.V.m. Art. 29 2017/2226 gem. Art. 29 Abs. 1 VO (EU) 2017/2226 auf Antrag und unter eingeschränkten Voraussetzungen gem. Art. 32 VO (EU) 2017/2226 (i.V.m. Art. 22 Abs. 1, Abs. 3 VO(EU) 2019/817) • **Benannte Europol-Stelle** gem. Art. 30 Abs. 1 VO (EU) 2017/2226 auf Antrag und unter eingeschränkten Voraussetzungen gem. Art 33 Abs. 1 VO (EU) 2017/2226 (i.V.m. Art. 22 Abs. 1, Abs. 3 VO(EU) 2019/817)

	• **ETIAS-Zentralstelle** und die nationalen ETIAS-Stellen zwecks Aufdeckung etwaiger Mehrfachidentitäten gem. Art. 21 i.V.m. Art. 29 Abs. 1 lit c VO (EU) 2019/817 • **SIRENE-Büro** zwecks Aufdeckung etwaiger Mehrfachidentitäten gem. Art. 21 i.V.m. Art. 29 Abs. 1 lit d VO (EU) 2019/817 Die hier aufgelisteten Kategorien von Behörden umfassen nicht nur die Behörden in Österreich, sondern sämtliche andere Behörden der verantwortlichen Mitgliedstaaten gem. Art. 4 EES-VO, die sich am EES beteiligen und in die genannten Kategorien fallen.
5. Übermittlung von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation gem. Art. 30 Abs 1 lit e DSGVO	Neben der Übermittlungsbefugnisse gem. §15 GrekoG, die für Drittstaatsangehörige etwa die Übermittlung an das BFA umfassen kann (Z3) oder für alle Reisenden die Übermittlung von Daten an eine andere Sicherheitsbehörde zwecks Strafverfolgung (Z4), gilt im Hinblick auf das EES Folgendes: Grundsätzlich werden die im EES personenbezogenen Daten gespeicherte Daten Drittstaaten, internationalen Organisationen oder privaten Stellen gem. Art. 41 Abs. 1 EES-VO nicht übermittelt oder zur Verfügung gestellt. Allerdings besteht die Möglichkeit der Übermittlung an ein Drittland oder an eine internationale Organisation durch die Grenz- oder Einwanderungsbehörden unter bestimmten Voraussetzungen gemäß Artikel 41 Abs. 2, 3, 5 und 6 EES-VO. Dabei sind die Bestimmungen des Kapitels V der Verordnung (EU) 2016/679 zu beachten.
6. Die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien gem. Art. 30 Abs 1 lit f DSGVO	Für EES-pflichtige Passagiere (oben genannte Kategorien von Drittstaatsangehörigen) gilt die verpflichtende Erfassung von im Punkt 6 aufgelisteten personenbezogenen Daten im **EES-Zentralsystem**, welches von der eu-LISA betrieben wird. Ein entsprechendes nationales EES existiert nicht. Gem. Art. 34 EES-VO wird jeder mit einem persönlichen Dossier verknüpfte Ein-/Ausreisedatensatz oder Einreiseverweigerungsdatensatz im Gemeinsamen Speicher für Identitätsdaten nach Art. 17 As. 1 VO 2019/817 (engl. Common Identity Repository, in weiterer Folge CIR) und im Zentralsystem des EES während drei Jahren nach dem Datum des Ausreisedatensatzes oder des Einreiseverweigerungsdatensatzes gespeichert.

	Jedes persönliche Dossier und die damit verknüpften Ein-/Ausreisedatensätze oder Einreiseverweigerungsdatensätze werden im CIR und im Zentralsystem des EES während drei Jahren und einem Tag nach dem Datum des letzten Ausreisedatensatzes oder Einreiseverweigerungsdatensatzes gespeichert, sofern innerhalb von drei Jahren nach dem Datum des letzten Ausreisedatensatzes oder Einreiseverweigerungsdatensatzes kein Einreisedatensatz eingegeben wurde. Wenn nach Ablauf der Dauer des zulässigen Aufenthalts kein Ausreisedatensatz eingegeben wurde, werden die Daten während fünf Jahren nach dem Datum des Endes des zulässigen Aufenthalts gespeichert. Bei Drittstaatsangehörigen, die Status eines Familienangehörigen eines unter die Richtlinie 2004/38/EG fallenden Unionsbürgers oder die Familienangehörige eines Drittstaatsangehörigen sind, der auf der Grundlage eines Abkommens zwischen der Union und ihren Mitgliedstaaten einerseits und einem Drittstaat andererseits ein dem Recht von Unionsbürgern gleichwertiges Recht auf Freizügigkeit genießt, und die nicht im Besitz einer Aufenthaltskarte gemäß der Richtlinie 2004/38/EG oder eines Aufenthaltstitels gemäß der Verordnung (EG) Nr. 1030/2002 des Rates sind wird jeder Ein- /Ausreisedatensatz im EES nach der Ausreise dieser Drittstaatsangehörigen höchstens ein Jahr gespeichert. Falls kein Ausreisedatensatz vorhanden ist, werden die Daten während fünf Jahren ab dem Datum des letzten Einreisedatensatzes gespeichert. Nach Ablauf der Speicherfrist werden die entsprechenden Daten automatisch aus dem Zentralsystem des EES und aus dem CIR gelöscht.

	Bei Reisenden, die **nicht EES-pflichtig** sind, findet **keine Speicherung** von personenbezogenen Daten in einem nationalen System statt.
7. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 DSGVO gem. Art. 30 Abs 1 lit g DSGVO	• Pseudonymisierung und Verschlüsselung personenbezogener Daten: geeignete Verschlüsselungstechniken, die unbefugte Dateneingabe sowie die unbefugte Kenntnisnahme, Änderung oder Löschung gespeicherter personenbezogener Daten zu verhindern • Zugang zum EES ausschließlich durch berechtigte Personen nur mittels einer persönlichen und eindeutigen Benutzerkennung und vertraulicher Zugriffsverfahren • Zugriff ausschließlich auf die der Zugriffsberechtigung unterliegenden Daten • Aufstellung von Notfallplänen für den Schutz kritischer Infrastrukturen • Redundante Speicherung von Daten • Schutzmechanismen zur Sicherstellung, dass eingesetzte Systeme im Störungsfall für den Normalbetrieb wiederhergestellt werden können: BMI-interne Pläne zur Bewältigung der Sicherheitsvorfälle sowie zum Krisen- und Notfallmanagement • Regelmäßige Überwachung, Überprüfung, und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung i.S.d Art. 43 Abs. lit n, regelmäßige interne Evaluierung der Informationssicherheit im Bundesministerium für Inneres und bei den Landespolizeidirektionen, regelmäßige Überprüfungen der Datenverarbeitungsvorgänge in der nationalen Grenzinfrastruktur nach einschlägigen internationalen Prüfungsstandards durch die Datenschutzbehörde als Aufsichtsbehörde gem. Art. 55 Abs. 2 EES-VO

5. Zu verarbeitende personenbezogene Daten

Um die Überprüfung der Einreisevoraussetzungen gemäß Art. 6 nach Maßgabe des Art. 8 SGK sicherzustellen, werden folgende Kategorien von personenbezogenen Daten verarbeitet:

1. Nachname (Familienname), Vorname oder Vornamen (Art. 16 Abs. 1 lit a, Art. 17 Abs. 1 lit a, Art. 18 Abs. 1 lit a, Art. 18 Abs. 2 EES-VO)

2. Geburtsdatum (Art. 16 Abs. 1 lit a, Art. 17 Abs. 1 lit a, Art. 18 Abs. 1 lit a, Art. 18 Abs. 2 EES-VO)

3. Staatsangehörigkeit oder Staatsangehörigkeiten (Art. 16 Abs. 1 lit a, Art. 17 Abs. 1 lit a, Art. 18 Abs. 1 lit a, Art. 18 Abs. 2 EES-VO)

4. Geschlecht (Art. 16 Abs. 1 lit a, Art. 17 Abs. 1 lit a, Art. 18 Abs. 1 lit a, Art. 18 Abs. 2 EES-VO)

5. Art und Nummer des Reisedokuments oder der Reisedokumente sowie dem aus drei Buchstaben bestehenden Code des ausstellenden Staates (Art. 16 Abs. 1 lit b, Art. 17 Abs. 1 lit a, Art. 18 Abs. 1 lit a, Art. 18 Abs. 2 EES-VO)

6. Datum des Ablaufs der Gültigkeitsdauer des Reisedokuments oder der Reisedokumente (Art. 16 Abs. 1 lit c, Art. 17 Abs. 1 lit a, Art. 18 Abs. 1 lit a, Art. 18 Abs. 2 EES-VO)

7. Das Gesichtsbild (Art. 15, Art. 16 Abs. 1 lit d, Art. 17 Abs. 1 lit b, Art. 18 Abs. 1 bis 5 EES-VO)

8. Bei visumbefreiten Drittstaatsangehörigen Fingerabdruckdaten der rechten Hand, falls vorhanden, ansonsten entsprechende Fingerabdruckdaten der linken Hand (Art. 17 Abs. 1 c EES-VO, Art. 18 Abs. 1 bis 5 EES-VO)

9. Gegebenenfalls gem. Art 16 Abs. 2 lit c EES-VO der Status dieses Drittstaatsangehörigen mit der Angabe, dass es sich um einen Drittstaatsangehörigen handelt, der

   - ein Familienangehöriger eines unter die Richtlinie 2004/38/EG fallenden Unionsbürgers oder ein Familienangehöriger eines Drittstaatsangehörigen ist, der auf der Grundlage eines Abkommens zwischen der Union und ihren Mitgliedstaaten einerseits und einem Drittstaat andererseits ein dem Recht von Unionsbürgern gleichwertiges Recht auf Freizügigkeit genießt und

- nicht im Besitz einer Aufenthaltskarte gemäß der Richtlinie 2004/38/EG oder eines Aufenthaltstitels gemäß der Verordnung (EG) Nr. 1030/2002 ist

10. Bei visumpflichtigen Drittstaatsangehörigen gegebenenfalls die Nummer der Visummarke des Visums für einen kurzfristigen Aufenthalt mit dem aus drei Buchstaben bestehenden Code des ausstellenden Mitgliedstaats, die Art des Visums für einen kurzfristigen Aufenthalt, das Enddatum der Höchstdauer des aufgrund des Visums für einen kurzfristigen Aufenthalt zulässigen Aufenthalts, das bei jeder Einreise aktualisiert wird, sowie gegebenenfalls das Datum des Ablaufs der Gültigkeitsdauer des Visums für einen kurzfristigen Aufenthalt (Art. 16 Abs. 2 lit d EES-VO)

11. Bei visumpflichtigen Drittstaatsangehörigen bei der ersten Einreise mit einem Visum für einen kurzfristigen Aufenthalt die auf der Visummarke des Visums für einen kurzfristigen Aufenthalt angegebene Anzahl der zulässigen Einreisen und Dauer des zulässigen Aufenthalts auf der Grundlage des Visums für einen kurzfristigen Aufenthalt (Art. 16 Abs. 2 lit e EES-VO)

12. Bei visumpflichtigen Drittstaatsangehörigen gegebenenfalls die Angabe, dass das Visum für einen kurzfristigen Aufenthalt mit räumlich beschränkter Gültigkeit gemäß Art. 25 Absatz 1 Buchstabe b der Verordnung (EG) Nr. 810/2009 ausgestellt wurde (Art. 16 Abs. 2 lit f EES-VO)

13. Im Falle einer Entscheidung über Aufhebung, Annullierung oder Verlängerung einer Genehmigung für einen kurzfristigen Aufenthalt, werden im letzten einschlägigen Ein-/Ausreisedatensatz auch folgende Informationen hinzugefügt:

    - Statusinformation, der zu entnehmen ist, dass die Genehmigung für einen kurzfristigen Aufenthalt oder das Visum aufgehoben oder annulliert oder die Dauer des zulässigen Aufenthalts oder das Visum verlängert wurde (Art. 19 Abs. 1 lit a EES-VO)

    - gegebenenfalls Nummer der neuen Visummarke mit dem aus drei Buchstaben bestehenden Code des ausstellenden Staates (Art. 19 Abs. 1 lit d EES-VO)

    - gegebenenfalls Zeitraum der Verlängerung der Dauer des zulässigen Aufenthalts (Art. 19 Abs. 1 lit e EES-VO)

    - gegebenenfalls neues Ablaufdatum des zulässigen Aufenthalts oder des Visums (Art. 19 Abs. 1 lit f EES-VO)

14. Bei Verlängerung des zulässigen Aufenthalts gemäß Art. 20 Abs. 2 des Übereinkommens zur Durchführung des Schengener Übereinkommens die Daten bezüglich des Zeitraums der Verlängerung des zulässigen Aufenthalts sowie gegebenenfalls die Angabe, dass der zulässige Aufenthalt verlängert wurde (Art. 19 Abs. 2 EES-VO). Bei Entscheidung, ein Visum zu annullieren, aufzuheben oder zu verlängern, werden die unter Punkt 13 genannten Daten unverzüglich im VIS abgerufen und gemäß den Art. 13 und 14 der Verordnung (EG) Nr. 767/2008 direkt in das EES importiert (Art. 19 Abs. 3 EES-VO).

15. Bei visumbefreiten Drittstaatsangehörigen die ETIAS-Daten gem. Art. 17 Abs. 2 EES-VO: die ETIAS-Antragsnummer; das Ablaufdatum der ETIAS-Reisegenehmigung; Angaben über räumliche Beschränkung der ETIAS-Reisegenehmigung (dies gilt ab der Inbetriebnahme des ETIAS).

16. Im Falle einer Einreiseverweigerung zusätzlich zu den o.g. alphanummerischen und biometrischen Daten gem. Art. 18 EES-VO den bzw. die Kennbuchstabe(n) für den Grund bzw. die Gründe der Einreiseverweigerung, gemäß Anhang V Teil B der Verordnung (EU) 2016/399.

Die in Punkt 1 bis 8 aufgelisteten Datenkategorien betreffen auch die Datenverarbeitung bei **nicht EES-pflichtigen Personen** im Rahmen der Grenzkontrolle nach Maßgabe des SGK sowie des GrekoG.

6. Datenverarbeitung durch zugangsberechtigtes Personal und Protokollierung

[redacted]

Diese Umsetzung erfüllt die Anforderungen [redacted] des Art. 46 EES-VO sowie des Durchführungsbeschlusses der Europäischen Kommission EU) 2019/328 und gewährleistet eine **vollständige Protokollierung der Verarbeitungsvorgänge**, um deren **Nachvollziehbarkeit und Integrität** sicherzustellen.

Im Hinblick auf das **EES**, sind darüber hinaus folgende Aspekte zu berücksichtigen:

Gem. Art. 46 Abs. 3 EES-VO ist jeder Mitgliedstaat verpflichtet, Protokolle über die zur Verarbeitung der EES-Daten befugten Bediensteten zu führen. Dabei wird die Nutzerkennung des zugriffsberechtigten Bediensteten, der den Datenverarbeitungsvorgang eingeleitet hat, protokolliert. Diese Protokolle dürfen nur zur datenschutzrechtlichen Kontrolle, einschließlich zur Prüfung der Zulässigkeit eines Antrags und der Rechtmäßigkeit der Datenverarbeitung sowie zum Zweck der Sicherstellung und der Datensicherheit gemäß Art. 43 EES-VO verwendet werden. Diese Protokolle werden durch geeignete Maßnahmen vor unbefugtem Zugriff geschützt und ein Jahr nach Ablauf der Speicherfrist gemäß Art- 34 EES-VO gelöscht, es sei denn, sie werden für bereits eingeleitete Kontrollverfahren benötigt.

Die Mitgliedstaaten und Europol gewährleisten, dass alle Datenverarbeitungsvorgänge, die aus Anträgen auf Zugang zu EES-Daten zwecks Strafverfolgung resultieren, zum Zwecke der Prüfung der Zulässigkeit des Antrags, der Überwachung der Rechtmäßigkeit der Datenverarbeitung sowie der Datenintegrität und -sicherheit und zur Eigenkontrolle protokolliert oder dokumentiert werden. Dies umfasst gem. Art. 59 Abs. 2 lit h EES-VO die einzigartige Benutzeridentität des Beamten, der die Abfrage vorgenommen hat, und des Beamten, der die Abfrage angeordnet hat. Genauere Regelungen zu der Protokollierung enthält der Durchführungsbeschluss (EU) 2019/328 der Europäischen Kommission zur Festlegung von Maßnahmen für die Führung von und den Zugang zu Protokollen im Einreise-/Ausreisesystem (EES). Die in Österreich EES-zugriffsberechtigten Zentralen Zugangsstellen der Strafverfolgungsbehörden (DSN und BK/SPOC) sorgen im eigenen Zuständigkeitsbereich für die Einhaltung dieser Vorgaben.

7. Beschreibung der Verarbeitungsvorgänge und Zwecke der Datenverarbeitung

a. Zuständigkeit zur Verarbeitung von personenbezogenen Daten

Die Landespolizeidirektionen sind zur Arbeit mit der Grenzkontrollsoftware befugt. Sie verwenden die Anwendung für die Zwecke der Grenzkontrolle an den Außengrenzen gemäß den Bestimmungen des Schengener Grenzkodex (SGK) und des Grenzkontrollgesetzes (GrekoG) sowie zur Erfüllung ihrer Verpflichtungen zur Eingabe, Aktualisierung und Löschung von EES-Daten im Inland.

Der Zugriff auf das EES ist für die Zwecke der Eingabe, Änderung, Löschung und Abfrage von Daten gemäß Art. 14 sowie Art. 16 bis 20 EES-VO dem ordnungsgemäß befugten Personal der nationalen

Behörden der Mitgliedstaaten, welche für die in Art. 23 bis 35 EES-VO genannten Aufgaben zuständig sind, vorbehalten. Der Zugang ist auf das zur Wahrnehmung der Aufgaben erforderliche Ausmaß beschränkt und muss im angemessenen Verhältnis zu den verfolgten Zielen stehen.

Gem. Art. 39 EES-VO betreffend die Zuständigkeit zur Verarbeitung von personenbezogenen Daten benennt jeder Mitgliedstaat die Behörde, die als Verantwortlicher nach Art. 4 Nummer 7 Verordnung (EU) 2016/679 (DSGVO) zu betrachten ist und der die zentrale Zuständigkeit für die Verarbeitung zukommt. Jeder Mitgliedstaat teilt der Europäischen Kommission diese Behörde mit. Wie bereits oben angeführt sind das in Österreich das Bundesministerium für Inneres und die Landespolizeidirektionen. Jeder Mitgliedstaat stellt sicher, dass die erhobenen Daten rechtmäßig verarbeitet werden und, dass der Zugriff auf diese Daten auf das ordnungsgemäß befugte Personal, zwecks Wahrnehmung seiner Aufgaben, beschränkt ist. Die zum Zugang zum EES berechtigten Personen können nur mittels einer persönlichen und eindeutigen Benutzerkennung und vertraulicher Zugriffsverfahren ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen. Alle zum Zugang zum EES berechtigten Behörden erstellen gem. Art. 43 Abs. 2 lit h EES-VO Profile mit einer Beschreibung der Aufgaben und Befugnisse der Personen, die berechtigt sind Daten zu verarbeiten. Diese Profile sind der Aufsichtsbehörde zur Verfügung zu stellen.

Die in Österreich eingerichtete Aufsichtsbehörde für Datenschutz ist die Datenschutzbehörde sowohl nach der Datenschutz-Grundverordnung (DSGVO) als auch nach dem Datenschutzgesetz (DSG) für den Strafverfolgungsbereich. Jeder Mitgliedstaat muss sicherstellen, dass die Daten rechtmäßig und unter uneingeschränkter Achtung der Menschenwürde des betreffenden Drittstaatsangehörigen erhoben werden, rechtmäßig in das EES eingegeben werden und richtig und aktuell sind, wenn sie an das EES übermittelt werden. Des Weiteren muss eu-LISA sicherstellen, dass der Betrieb des EES im Einklang mit der EES-VO erfolgt. eu-LISA ergreift, unbeschadet der Zuständigkeiten der Mitgliedstaaten, die erforderlichen Maßnahmen, um die Sicherheit des Zentralsystems des EES und der Kommunikationsinfrastruktur zwischen dem Zentralsystem des EES und der einheitlichen nationalen Schnittstelle zu gewährleisten. Diese Maßnahmen teilt eu-LISA dem Europäischen Parlament, dem Rat und der Kommission sowie dem Europäischen Datenschutzbeauftragten mit. Weiters muss eu-LISA sicherstellen, dass nur ordnungsgemäß befugtes Personal Zugriff auf die im EES verarbeiteten Daten hat.

b. Zugriffsberechtigte Behörden

Gem. Art. 9 Abs. 2 EES-VO übermitteln die Mitgliedstaaten eine Liste mit den für die Zwecke der EES-VO zuständigen nationalen Behörden, bei denen es sich um Grenzbehörden, Visumbehörden bzw. Einwanderungsbehörden handeln muss, aufzustellen und an eu-LISA zu übermitteln. In dieser Liste wird angegeben zu welchem Zweck die jeweilige Behörde Zugang zu den Daten im EES hat.

Bundesministerium
Inneres

Folgende Übersicht soll einen Überblick der Stellen und Behörden verschaffen, die Zugang zu EES-Daten auf Grundlage der EES-VO haben:

Tabelle 2 zugangsberechtigte Stellen und Behörden

Akteur	Grundlage für den Zugang zu EES-Daten laut EES-VO	Akteur auf nationaler Ebene	Nationale Rechtgrundlage
eu-LISA	Art. 39 Abs. 2 EES-VO	-	-
Mitgliedstaaten	Art. 39 Abs. 1 EES-VO	-	-
Europäische Kommission	Art. 63 EES-VO	-	-
Grenzbehörden Art. 3 Z 3 EES-VO	Art. 14 bis 23, 27 EES-VO	Landespolizeidirektionen	Gem. §2 Abs. 2 SPG i.V.m. § 12 Abs. 1 i.V.m. § 8 Abs. 1 GrekoG wird die Grenzkontrolle von der Landespolizeidirektion durchgeführt. Daher sind die Landespolizeidirektionen Grenzbehörden iSd Art. 3 Z 3 EES-VO.
Einwanderungsbehörde gem. Art. 3 Z4 lit a EES-VO	Art. 26, 27 EES-VO	• Landespolizeidirektionen als Fremdenpolizei	In § 2 Abs. 2 Z 2 FPG wird u.a. als Aufgabe der Fremdenpolizei die Überwachung des Aufenthalts Fremder im Bundesgebiet definiert. Gem. § 5 Abs. 1 Z 1 FPG obliegt der Landespolizeidirektion die Besorgung der Fremdenpolizei. Damit können die Landespolizeidirektionen in ihrer Funktion als Fremdenpolizei als Einwanderungsbehörde iSd Z 4 lit a EES-VO gesehen werden.

		• Bundesamt für Fremdenwesen und Asyl	Gem. § 3 Abs. 2 Z 3 und 4 BFA-VG obliegt dem Bundesamt für Fremden- und Asylwesen die Anordnung der Abschiebung, die Feststellung der Duldung und die Vollstreckung von Rückführungsentscheidungen von EWR-Staaten gemäß dem 7. Hauptstück des FPG, sowie die Erlassung von aufenthaltsbeendenden Maßnahmen gemäß dem 8. Hauptstück des FPG. Damit kann das Bundesamt für Fremdenwesen und Asyl in seiner Funktion als Fremdenbehörde (nicht in seiner Funktion als Asylbehörde) als Einwanderungsbehörde iSd Art. 3 Z 4 lit b EES-VO gesehen werden.
		• Landeshauptmann, bzw. die Bezirksverwaltungs-behörde	Gem. § 21 Abs. 2 NAG ist die Antragsstellung für die Ausstellung eines Aufenthaltstitels im Inland für Fremde dann möglich, wenn sie rechtmäßig eingereist sind und sich rechtmäßig im Bundesgebiet aufhalten. Daher gibt es eine Befugnis diese Voraussetzungen zu überprüfen. Sachlich zuständig ist gem. § 3 Abs. 1 NAG der Landeshauptmann, bzw. die Bezirksverwaltungsbehörde, wenn er/sie diese zur Ausübung dieser Aufgabe mit Verordnung ermächtigt hat. Daher können auch diese Behörden als Einwanderungsbehörden i.S.d. Art. 3 Z 4 lit a EES-VO gesehen werden.
		• Konsulate als Vertretungsbehörden und BMEIA	Vertretungsbehörden: Aufgrund der Kompetenz für die Erteilung, die Versagung und die Annullierung von Visa D (§ 7 FPG).

Visumbehörden gem. Art. 3 Abs. 1 Z 5 EES-VO	Art. 24 EES-VO	• Konsulate als Vertretungsbehörden und BMEIA • Bundesministerium für Inneres • Landespolizeidirektionen	Gem. Art. 4 Abs. 1 Visa-Kodex werden die Anträge für die Visumerteilung von den Konsulaten geprüft und beschieden. Ihre sachliche Zuständigkeit ist im §7 FPG geregelt. Gem. Art. 6 Abs. 1 Visa-Kodex ist der Antrag von dem Konsulat des Mitgliedstaats zu prüfen, in dessen Konsularbezirk der Antragsteller seinen rechtmäßigen Wohnsitz hat. Zuständig ist gem. Art. 5 Visa-Kodex der Mitgliedstaat, in dessen Hoheitsgebiet das (Haupt-)Reiseziel liegt. Den Landespolizeidirektionen und dem Bundesministerium für Inneres obliegt die Besorgung der Visaangelegenheiten im Inland gem. § 5 Abs. 1 Z 2 FPG.
Benannte Behörden gem. Art. 3 Z 26 EES-VO, die den Zugang zum Zwecke der Verhütung, Aufdeckung und Untersuchung einer terroristischen oder sonstigen schweren Tat benötigen	Art. 29 EES-VO	• Bundeskriminalamt und • Direktion für Staatsschutz und Nachrichtendienst (diese Stellen agieren auch als zentrale Zugangsstelle gem. Art. 29 Abs. 3 EES-VO und prüfen die Bedingungen für den Zugang zu EES-Daten gem. Art. 32 EES-VO durch die benannten Behörden)	Eine nach Art. 29 EES-VO benannte Behörde muss für die Verhütung, Aufdeckung oder Untersuchung von terroristischen Straftaten oder sonstigen schweren Straftaten zuständig sein. Dies umfasst nach Maßgabe der Aufgaben gemäß § 4 Abs. 3 BKA-G und § 6 Abs. 1 i.V.m. §10 SNG das Bundeskriminalamt und die Landeskriminalämter in den Bundesländern sowie die Direktion für den Staatsschutz und Nachrichtendienst und entsprechende Landesämter in den Bundesländern.

		• Landespolizeidirektionen	
Zentrale Zugangsstelle		• Bundeskriminalamt und • Direktion für Staatsschutz und Nachrichtendienst	Die zentrale Zugangsstelle gem. Art. 29 Abs. 3 EES-VO ist verantwortlich für die Überprüfung der Anträge der benannten Behörden auf Zugang zu EES-Daten. Die zentrale Zugangsstelle ist nationalrechtlich im § 43a EU-Polizeikooperationsgesetz definiert. Demnach übt der Bundesminister für Inneres die Funktion der zentralen Zugangsstelle aus. Innerhalb des Bundesministeriums für Inneres ist vorgesehen, dass diese Kompetenz durch das Bundeskriminalamt (BK) und die Direktion für den Staatsschutz und Nachrichtendienst (DSN) wahrgenommen wird.
Europol gem. Art. 1 Abs. 2 i.V.m. Art. 30 EES-VO (Europol-Stelle, zentrale Europol-Zugangsstelle)	Art. 30 Abs. 1 EES-VO	-	Gem. Art. 30 Abs. 1 EES-VO kann die benannte Europol-Stelle den Zugang zum EES bei der zentralen Europol-Zugangsstelle beantragen. Die zentrale Europol-Zugangsstelle prüft, ob die Bedingungen für die Beantragung des Zugangs zum EES gemäß Artikel 33 EES-VO erfüllt sind. Dabei nimmt die zentrale Europol-Zugangsstelle ihre Aufgaben unabhängig wahr und nimmt in Bezug auf den Ausgang ihrer Prüftätigkeiten keine Anweisungen von der genannten benannten Europol-Stelle entgegen.
FRONTEX (Europäischen Agentur für die Grenz- und Küstenwache)	Art. 63 EES-VO	-	Das ordnungsgemäß ermächtigte Personal der gemäß der Verordnung (EU) 2019/1896 des Europäischen Parlaments und des eingerichteten Europäischen Agentur für die Grenz- und Küstenwache hat zur Durchführung von Risikoanalysen und Schwachstellenbeurteilungen Zugriff zu der Statusinformation gem. Art. 63 Abs. 1 lit a EES-VO für Zwecke der Berichterstattung und Statistikerstellung.

Beförderungsunternehmen	Art. 13 Abs. 3 EES-VO		Zur Erfüllung ihrer Verpflichtungen gemäß Art. 26 Absatz 1 Buchstabe b des Übereinkommens zur Durchführung des Übereinkommens von Schengen (national im §111 FPG verankert) verwenden Beförderungsunternehmer den Web- Dienst, um zu überprüfen, ob Drittstaatsangehörige, die im Besitz eines für eine oder zwei Einreisen ausgestellten Visums für einen kurzfristigen Aufenthalt sind, die Zahl der mit ihrem Visum zulässigen Einreisen bereits in Anspruch genommen haben.

Des Weiteren werden in der EES-Verordnung Aufgaben und Zuständigkeiten angeführt, die jedoch keinen der o.a. Behörden eindeutig zugeordnet sind, sondern nur allgemein den „zuständigen Behörden“ obliegen, ohne diese genauer zu definieren:

Tabelle 3 Nicht eindeutig zugeordnete Aufgaben gemäß EES-VO und zuständige Stellen in Österreich

Rechtsgrundlage	Beschreibung	Zuständige Stelle
Art. 9 Abs. 2 EES-VO	Benennung der zuständigen Behörden	BMI, Abteilung V/B/6
Art. 14 Abs. 3 SGK	Berichtigung einer zu Unrecht ausgesprochenen Einreiseverweigerung nach Entscheidung im Rechtsmittelverfahren	Landespolizeidirektionen
Art. 14 Abs. 8 EES-VO	Antrag eines Drittstaatsangehörigen auf Erstellung eins pers. Dossiers im Inland nach Ablauf eines Aufenthalts auf Grundlage eines Aufenthaltstitels oder Visums für den längerfristigen Aufenthalt (Beginn der EES-Pflicht)	Landespolizeidirektionen (in beiden Fällen)
Art. 19 Abs. 2 i.V.m. 60 EES-VO	Verlängerung der Aufenthaltsdauer gem. Altabkommen im Inland (nach erfolgter Einreise)	Landespolizeidirektionen

Art. 20 Unterabsatz 2 lit a, b und c EES-VO i.V.m. Art. 12 Abs. 3 SGK	Hinzufügen von Daten bei Widerlegung der Annahme, dass ein Drittstaatsangehöriger die Voraussetzungen hinsichtlich der Dauer des zulässigen Aufenthalts nicht erfüllt	Landespolizeidirektionen
Art. 21 Abs. 2 EES-VO	Information an die Europäische Kommission bei Stempelung in Ausnahmefällen	Nationales Koordinationszentraum (NCC)
Art. 35 Abs. 2 EES-VO	Änderung und vorzeitige Löschung von Daten → im Falle von Asylantragsstellung	Landespolizeidirektion, Bundesamt für Asyl und Fremdenwesen
Art. 35 Abs. 6 EES-VO	Vorzeitige Löschung von Daten → Verleihung Staatsbürgerschaft, Langzeitvisum	Landesregierung, Landespolizeidirektionen, bzw. Vertretungsbehörden
Art. 35 Abs. 6 EES-VO	Vorzeitige Löschung von Daten → Verleihung Aufenthaltstitel	Landeshauptmann, bzw. die Bezirksverwaltungsbehörde
Art. 35 Abs. 3 EES-VO	Konsultation mit anderen MS bei Annahme, dass Daten sachlich unrichtig, unvollständig oder unter Verstoß gegen die EES-Verordnung verarbeitet wurden	BMI, Abteilung V/B/6
Art. 35 Abs. 4 EES-VO	Konsultation mit anderen MS bei Annahme, dass visumsbezogene Daten sachlich unrichtig, unvollständig oder unter Verstoß gegen die EES-Verordnung verarbeitet wurden	BMI, Abteilung V/B/7
Art. 35 Abs. 5 EES-VO	Löschung des Eintrags von der Liste der Aufenthaltsüberzieher gem. Art. 12 EES-VO, wenn der Drittstaatsangehörige aufgrund von unvorhersehbaren und ernsten Ereignissen gezwungen war, den Aufenthalt zu überziehen	Landespolizeidirektionen
Art. 38 Abs. 2 EES-VO	Benennung einer nationalen Behörde, die den zuständigen Behörden gem. Art. 9 Abs. 2 EES-VO den Zugang zum EES gewährleistet	BMI, Abteilung V/B/6
Art. 52 EES-VO	Bearbeitung von Anträgen von Drittstaatsangehörigen im Zusammenhang mit den Art. 15 bis 18 DSGVO	BMI, Abteilung V/B/6 sowie Landespolizeidirektionen
Art. 63 Abs. 1 EES-VO	Abfrage von Daten zur Erstellung von Statistiken und Berichten	BMI, Abteilung V/B/6, NCC sowie Landespolizeidirektionen

c. Speicherung von personenbezogenen Daten

Die nach Art. 16 bis Art. 18 EES-VO erhobenen personenbezogenen Daten werden im Zentralsystem des EES und im gemeinsamen Speicher für Identitätsdaten (CIR) gem. Art. 7 Abs. 1a EES-VO gespeichert. Eine nationale Speicherung von personenbezogenen Daten ist gem. Art. 28 EES-VO in Einzelfällen möglich, in denen dies erforderlich ist und nur im Einklang mit dem Zweck, für den sie abgerufen wurden, sowie mit den einschlägigen Rechtsvorschriften der Union — insbesondere den Datenschutzbestimmungen. Die Daten dürfen nur so lange in nationalen Dateien gespeichert werden, wie in dem jeweiligen Einzelfall unbedingt erforderlich. Die Speicherung der Daten in nationale Dateien ist gem. Art. 40 EES-VO auf alphanumerische Daten beschränkt und die Speicherung muss im Einklang mit den Zwecken des EES und unter uneingeschränkter Achtung des Unionsrechts erfolgen. Dabei darf die Speicherfrist nicht länger als bei der Speicherung im zentralen EES sein. Zusätzlich macht Art. 40 Abs. 3 EES-VO deutlich, dass jede Verwendung von Daten, die nicht Art. 40 Abs. 1 EES-VO 1 entspricht, als missbräuchliche Verwendung gemäß dem nationalen Recht des jeweiligen Mitgliedstaats sowie dem Unionsrecht anzusehen ist. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

9. Verarbeitung von Daten

10. Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in den Anwendungen für die Durchführung der Grenzkontrollsoftware sowie im EES

a. Verarbeitungsprozesse nach der EES-VO

1. Verarbeitung gem. Art. 12 EES-VO i.V.m. dem Durchführungsbeschluss der Kommission (EU) 2018/1548 – *Informationsmechanismus*

Art. 12 EES-VO regelt den Mechanismus mit dem unmittelbar nach Ablauf des zulässigen Aufenthalts automatisch angezeigt wird, wenn im Ein-/Ausreisedatensatz ein Ausreisedatum fehlt und wenn die Höchstdauer des zulässigen Aufenthalts überschritten wurde. Gem. Art. 12 Abs. 3 EES-VO wird eine Liste generiert, welche die in den Art. 16 und 17 EES-VO und im Durchführungsbeschluss (EU) 2018/1548 genannten Daten aller Personen, die als Aufenthaltsüberzieher identifiziert wurden, enthält. Diese Liste wird den gemäß Art. 9 Abs. 2 EES-VO benannten, zuständigen Einwanderungsbehörden zur Verfügung gestellt, damit sie geeignete Maßnahmen treffen können.

2. Verarbeitung gem. Art. 13 EES-VO i.V.m. dem Durchführungsbeschluss der Kommission (EU) 2021/1224 – *Verarbeitung durch Beförderungsunternehmen*

Gem. Art. 13 EES-VO i.V.m. Art. 26 Abs. 1 lit b des Übereinkommens zur Durchführung des Übereinkommens von Schengen sind die Beförderungsunternehmen verpflichtet, mithilfe eines von eu-LISA entwickelten Web-Dienstes zu überprüfen, ob Drittstaatsangehörige, die im Besitz eines für eine oder zwei Einreisen ausgestellten Visums für einen kurzfristigen Aufenthalt sind, die Zahl der mit ihrem Visum zulässigen Einreisen bereits in Anspruch genommen haben. Beförderungsunternehmen erhalten eine vereinfachte Antwort „OK“ bzw. „NOT OK“. Beförderungsunternehmer dürfen die übermittelten Angaben und die erhaltene Antwort im Einklang mit den geltenden Rechtsvorschriften speichern. eu-LISA protokolliert alle Datenverarbeitungsvorgänge, die von Beförderungsunternehmern unter Verwendung des Web-Dienstes vorgenommen werden. Diese Protokolle enthalten das Datum und die Uhrzeit jedes Vorgangs, die zur Abfrage verwendeten Daten, die vom Web-Dienst übermittelten Daten und den Namen des jeweiligen Beförderungsunternehmens. Die Verarbeitung von Daten der Beförderungsunternehmen erfolgt daher nicht durch die Mitgliedstaaten.

3. Verarbeitung gem. Art. 14 EES-VO i.V.m. dem Durchführungsbeschluss der Kommission (EU)2019/326 – *Verfahren für die Eingabe von Daten in das EES*

Zwecks Verarbeitung von Daten nach dieser Vorschrift haben die Grenzbehörden Zugang zum EES. Die Verarbeitung umfasst das Anlegen eines persönlichen Dossiers im EES, soweit ein Drittstaatsangehöriger noch nicht im EES erfasst wurde. Das Anlegen des Dossiers erfolgt durch Eingabe der personenbezogenen Daten gem. Art. 16, Art. 17 bzw. Art. 18 EES-VO. Gegebenenfalls, soweit ein persönliches Dossier des Drittstaatsangehörigen im EES bereits existiert, aktualisiert die Grenzbehörde das vorhandene persönliche Dossier bzw. die Angaben gemäß den Art. 16 bis 18 EES-VO, soweit einschlägig und gibt für jede Einreise einen Einreisedatensatz, für jede Ausreise einen

Ausreisedatensatz gem. Art. 16 und 17 ESS-VO oder einen Einreiseverweigerungsdatensatz gemäß Art. 18 EES-VO ein.

Eine Ausnahme stellt die Verarbeitung gem. Art. 14 Abs. 8 EES-VO dar. Bei Personen, die sich schon im Hoheitsgebiet eines Mitgliedsstaates auf Basis eines Aufenthaltstitels oder eines Visums für den längerfristigen Aufenthalt befinden und deren Kurzaufenthalt unmittelbar danach beginnt, kann der Drittstaatsangehörige im Inland die zuständige Behörde (Einwanderungsbehörde, in Österreich die Landespolizeidirektion) ersuchen, sein persönliches Dossier anzulegen und einen entsprechenden Einreisedatensatz zu erfassen. Die Behörde führt diese Erfassung durch Eingabe der personenbezogenen Daten gem. Art. 16 Abs. 1, 2 und 6 und Art. 17 Abs. 1 EES-VO durch, wobei anstatt des Einreisedatums das Datum des Beginns des Kurzaufenthaltes im Inland angegeben wird, da sich die Person bereits im Inland befindet und für das EES nur der Beginn des Kurzaufenthalts relevant ist. Analog wird statt der Grenzübergangsstelle die Bezeichnung der eingebenden Behörde im Inland im Einreisedatensatz vermerkt.

Diese Verarbeitung passiert daher auf Ersuchen des Drittstaatsangehörigen. Durch die Erstellung des Dossiers bei Beginn des Kurzaufenthalts im Inland und nicht erst im Rahmen der Ausreise, haben die Betroffenen den Vorteil, dass sie im Rahmen einer Inlandskontrolle gem. Art. 26 EES-VO bereits ein Dossier haben und i.d.R. somit die Annahme eines rechtmäßigen Aufenthalts/einer rechtmäßigen Einreise gilt (20 EES-VO i.V.m. Art. 12 SGK).

4. Verarbeitung gem. Art. 16 EES-VO – *Personenbezogene Daten von visumpflichtigen Drittstaatsangehörigen*

Zugangsberechtigt sind die Grenzbehörden an den Grenzen, an denen das EES eingesetzt wird. Die Verarbeitung umfasst das Anlegen eines persönlichen Dossiers durch Eingabe von personenbezogenen Daten gem. Art. 16 Abs. 1 bis Abs. 3 sowie Abs. 6 EES-VO. Zum Zwecke der Eingabe oder der Aktualisierung des Ein-/Ausreisedatensatzes können die in Art. 16 Abs. 2 lit c bis f EES-VO genannten Daten von der Grenzbehörde gemäß Art. 18a der Verordnung (EG) Nr. 767/2008 (in weiterer Folge „VIS-Verordnung“) auch aus dem Visainformationssystem (in weiterer Folge „VIS“) abgerufen und in das EES importiert werden.

5. Verarbeitung gem. Art. 17 EES-VO – *Personenbezogene Daten von visumbefreiten Drittstaatsangehörigen*

Zugangsberechtigt sind die Grenzbehörden an den Grenzen, an denen das EES eingesetzt wird. Die Verarbeitung umfasst das Anlegen eines persönlichen Dossiers durch Eingabe von personenbezogenen Daten gem. Art. 17 Abs. 1 i.V.m. Art. 16 Abs. 1 lit a, b und c i.V.m. Art. 15 i.V.m. Art. 16 Abs. 6 EES-VO sowie Art. 17 Abs. 2 i.V.m. Art. 16 Abs. 2 lit a, b, c i.V.m. Art. 16 Abs. 2 lit a, b, c i.V.m. Art. 16 Abs. 4

EES-VO. Im Wesentlichen unterscheidet sich das Dossier eines visumbefreiten Drittstaatsangehörigen dadurch, dass dieses auch Fingerabdruckdaten der rechten Hand (vier Finger) enthält, die bei visumpflichtigen Drittstaatsangehörigen bereits durch die VIS-VO vorgesehen sind und daher i.d.R. bereits im VIS enthalten sind.

6. Verarbeitung gem. Art. 18 EES-VO – *Personenbezogene Daten von Drittstaatsangehörigen, denen die Einreise verweigert wurde*

Zugangsberechtigt sind die Grenzbehörden. Die Verarbeitung umfasst, soweit noch kein persönliches Dossier im EES existiert, das Anlegen eines persönlichen Dossiers durch die Eingabe von alphanummerischen Daten gem. Art. 16 Abs. 1 EES-VO und ggf. Daten nach Art. 16 Abs. 6 EES-VO bei visumpflichtigen Drittstaatsangehörigen und Daten nach Art. 17 Abs. 1 EES-VO bei visumbefreiten Drittstaatsangehörigen. Im Falle einer Einreiseverweigerung wegen eines Grundes nach Anhang V Teil B Kennbuchstabe B, D oder H der VO 2016/399 werden zusätzlich bei visumpflichtigen Drittstaatsangehörigen Gesichtsbilder gem. Art. 18 Abs. 2 lit a i.V.m. Art. 16 Abs.1 lit d EES-VO, bei visumbefreiten Drittstaatsangehörigen das Gesichtsbild und die Fingerabdrücke gem. Art. 18 Abs. 2 lit b iVm Art. 17 Abs. 1 lit b und c EES-VO und bei nicht im VIS registrierten visumpflichtigen Drittstaatsangehörigen das Gesichtsbild gem. Art. 18 Abs. 2 lit c iVm Art. 16 Abs. 1 lit d EES-VO und Fingerabdrücke gem. Art. 18 Abs. 2 lit c iVm Art. 17 Abs. 1 lit c EES-VO erfasst. Biometrische Daten werden jedoch nicht erfasst, wenn nach Art. 18 Abs. 3 EES-VO diese Daten schon in einer SIS-Ausschreibung, die zur Einreiseverweigerung führt, enthalten sind. Im Falle einer Einreiseverweigerung nach Art. 18 Abs. 5 EES-VO wegen eines Grundes nach Anhang V Teil B Kennbuchstabe J SGK wird ein persönliches Dossier ebenfalls ohne biometrische Daten angelegt, es kann jedoch das Gesichtsbild aus einem eMRTD (electronic Machine Readable Travel Document – elektronisch maschinenlesbares Reisedokument) extrahiert werden. Weiters werden in einem gesonderten Einreiseverweigerungsdatensatz die Informationen betreffend Einreiseverweigerung nach Art. 18 Abs. 6 lit a bis d EES-VO eingegeben und für visumpflichtige Drittstaatsangehörige zusätzlich auch noch die Daten gem. Art. 16 Abs. 2 lit d bis g EES-VO.

7. Verarbeitung gem. Art. 19 EES-VO i.V.m. Durchführungsbeschluss der Kommission (EU) 2019/1270 – *Hinzufügung von Daten bei Aufhebung, Annullierung oder Verlängerung einer Genehmigung für einen kurzfristigen Aufenthalt*

In Artikel 8 der EES-VO sind die Vorgänge, die Teil der Interoperabilität zwischen dem EES und VIS darstellen, sowie deren Zwecke beschrieben. Ferner wird mit der EES-VO die VIS-VO geändert und ein neuer Artikel 17a über die Herstellung der Interoperabilität zwischen den beiden Systemen eingeführt. Art. 19 EES-VO ist einer der Anwendungsfälle, die auf Basis der Interoperabilität erfolgen.

Zugangs- und verarbeitungsberechtigt ist die Behörde, die eine Entscheidung über die Aufhebung, Annullierung oder Verlängerung einer Genehmigung für einen kurzfristigen Aufenthalt getroffen hat.
Die Verarbeitung der personenbezogenen Daten umfasst die Eingabe von Informationen gem. Art. 19 Abs. 1 lit a bis f EES-VO in den letzten einschlägigen Ein-/Ausreisedatensatz. Für den Fall, dass die Dauer des zulässigen Aufenthalts verlängert wurde, fügt die Behörde, die den Aufenthalt verlängert hat, die Daten betreffend die Verlängerung dem letzten Ein-/Ausreisedatensatz hinzu. Im Falle einer Entscheidung über die Annullierung, Aufhebung oder Verlängerung des Visums, ruft die entscheidungsbefugte Visumbehörde die Daten nach Art. 19 Abs. 1 lit a bis f EES-VO im VIS ab und importiert diese Daten aus dem VIS in das EES gem. Art. 13 und 14 VO Nr. 767/2008.
Des Weiteren werden gem. Art. 19 Abs. 4 EES-VO Entscheidungen als Gründe für die Aufhebung oder Annullierung des kurzfristigen Aufenthalts angegeben. Auch die Gründe für die Verlängerung der Dauer des zulässigen Aufenthalts werden gem. Art. 19 Abs. 5 EES-VO in das EES eingegeben.
Für den Fall einer Verlängerung der Aufenthaltsdauer auf Grundlage eines bilateralen Abkommens gem. Art. 19 Abs. 2 EES-VO i.V.m. Art. 20 Schengener Durchführungsübereinkommen (SDÜ) fügt die zuständige Behörde die Daten bezüglich des Zeitraums der Verlängerung des zulässigen Aufenthalts sowie gegebenenfalls die Angabe, dass der zulässige Aufenthalt gemäß Artikel 20 Absatz 2 Buchstabe b (SDÜ) verlängert wurde, dem letzten einschlägigen Ein-/Ausreisedatensatz hinzu.

8. Verarbeitung gem. Art. 20 EES-VO i.V.m. Art. 12 Abs. 3 SGK - *Hinzufügung von Daten bei Widerlegung der Annahme, dass ein Drittstaatsangehöriger die Voraussetzungen hinsichtlich der Dauer des zulässigen Aufenthalts nicht erfüllt*

Zugangs- und verarbeitungsberechtigt sind die zuständigen Behörden, die nach einer erfolgten Abfrage im EES mangels eines persönlichen Dossiers oder mangels eines einschlägigen Ein/Ausreisedatensatzes von einem Drittstaatsangehörigen davon ausgehen dürfen, dass der Drittstaatsangehörige die Voraussetzungen hinsichtlich der Dauer des zulässigen Aufenthalts im Hoheitsgebiet nicht oder nicht mehr erfüllt.
Die Verarbeitung der personenbezogenen Daten umfasst in diesem Fall bei Widerlegung der betreffenden Annahme das Anlegen eines persönlichen Dossiers zu dem Drittstaatsangehörigen gem. Art. 20 lit a EES-VO, beziehungsweise Aktualisierung des letzten Ein-/Ausreisedatensatzes gem. Art. 20 lit b i.V.m. Art. 16 und 17 EES-VO oder die Löschung eines vorhandenen Dossiers soweit Art. 35 EES-VO dies vorsieht (z.B. etwa bei Erwerb der Berechtigung für einen Aufenthalt).
Wird die betreffende Annahme nicht widerlegt und stellt sich heraus, dass der Aufenthalt des Drittstaatsangehörigen rechtswidrig ist, so umfasst die Verarbeitung der personenbezogenen Daten die Übermittlung der Daten an die zuständigen Behörden zur Einleitung der Rückführung gem. Richtlinie 2008/115/EG oder Richtlinie 2004/38/EG.

9. Verarbeitung gem. Art. 23 EES-VO i.V.m. Art. 8 Abs. 1 lit b, Abs. 3 lit a SGK - *Verwendung der Daten zum Zwecke der Verifizierung an den Grenzen, an denen das EES eingesetzt wird*

Zugangs- und verarbeitungsberechtigt sind die Grenzbehörden zum Zwecke der Verifizierung der Identität und der vorherigen Erfassung im EES des Drittstaatsangehörigen, zur Aktualisierung der EES-Daten soweit erforderlich, zur Durchführung von Abfragen in dem für die Durchführung der Grenzkontrollen notwendigen Umfang. Zu diesem Zweck haben die Grenzbehörden Zugang auf die in Art. 16 Abs. 1 lit a, b und c und Art. 17 Abs. 1 lit a EES-VO genannten Daten.

Weiters erfolgt anhand der in das EES eingegebenen alphanumerischen personenbezogenen Daten bei visumpflichtigen Drittstaatsangehörigen eine Suchabfrage im VIS direkt aus dem EES gem. Art. 18 VIS-VO. Alternativ kann anhand der Nummer der Visummarke gem. Art. 18 Abs. 3 VIS-VO direkt im VIS durchgeführt werden, wenn besondere Umstände dies erfordern, insbesondere wenn eine Abfrage anhand der alphanummerischen Daten aufgrund der spezifischen Situation eines Drittstaatsangehörigen angemessener ist, oder bei einer technischen Unmöglichkeit der Abfrage im EES/beim Ausfall des EES. Sind die Daten des Drittstaatsangehörigen im EES vorhanden, erfolgt die Verifizierung anhand der Gesichtsbilder – das vor Ort aufgenommene Gesichtsbild wird mit dem Gesichtsbild aus dem vorhandenen Dossier gemäß Art. 16 Absatz 1 lit d und Artikel 17 Abs. 1 lit b EES-VO. Ist die Verifizierung anhand des Gesichtsbilds nicht erfolgreich, kann eine Verifizierung anhand der Fingerabdruckdaten durchgeführt werden, und zwar bei visumbefreiten Drittstaatsangehörigen anhand der im EES vorhandenen Fingerabdrücke und bei visumpflichtigen Drittstaatsangehörigen anhand der im VIS gespeicherten Fingerabdrücke gem. Art. 18 Abs. 6 VIS-VO.

Sollte die Suchabfrage anhand der alphanummerischen bzw. biometrischen Daten im VIS nach Art. 23 Abs. 2 EES-VO, wie im letzten Absatz beschrieben, zeigen, dass Daten des Drittstaatsangehörigen im EES gespeichert sind, so kann die Grenzbehörde die vorhandenen Daten im EES abfragen. Wenn jedoch keine Daten über den Drittstaatsangehörigen im EES gespeichert sind, wenn die Verifizierung nach Art. 23 Abs. 2 EES-VO nicht erfolgreich ist oder bei Zweifeln an der Identität des Drittstaatsangehörigen bestehen, erhalten die Grenzbehörden Zugang zu Daten zwecks Identifizierung gem. Art. 27 EES-VO (zu dieser Verarbeitung siehe Pkt. 14).

Zu der o.g. Verifizierung anhand von VIS-Daten bzw. Identifizierung anhand der biometrischen Suche im VIS stellt Art. 23 Abs. 4 EES-VO klar: Wenn die alphanummerische Suchabfrage ergibt, dass Daten des Drittstaatsangehörigen im VIS vorhanden sind, wird eine Verifizierung anhand der Fingerabdrücke im VIS vorgenommen (Art. 18 Abs. 6 VIS-VO). War diese Verifizierung nicht erfolgreich, kann u.U. ein Verdacht einer Dokumentenfälschung/Identitätsdiebstahl vorliegen, daher kann eine Identifizierung gem. Art. 20 VIS-VO durchgeführt werden – es wird also mit Fingerabdrücken gem. Art. 20 Abs. 1 VIS-VO im VIS gesucht (alternativ mit alphanummerischen Daten gem. Art. 9 Nummer 4 Buchstaben a

und/oder c VIS-VO oder in Kombination mit den in Art. 9 Nummer 4 Buchstabe b VIS-VO aufgeführten Daten). Auch bei visumbefreiten Drittstaatsangehörigen ist zwecks Verifizierung eine Abfrage im VIS mit alphanummerischen Daten gem. Artikel 19a VIS-VO bzw. zwecks Identifizierung mit Fingerabdruckdaten gem. Art. 20 VIS-VO möglich, wenn bei einer Identifizierungsabfrage im EES gemäß Artikel 27 EES-VO keine Daten gefunden werden (siehe Pkt. 14).

10. Verarbeitung gem. Art. 24 EES-VO i.V.m. Durchführungsbeschluss der Kommission (EU) 2019/1270 – *Nutzung des EES zur Prüfung und Bescheidung von Visumanträgen*

Auch bei diesem Verarbeitungsvorgang handelt es sich um einen Anwendungsfall der Interoperabilität zwischen EES und VIS gem. Art. 8 EES-VO. Zugangsberechtigt sind die Visumbehörden, die direkt aus dem VIS heraus im EES-Suchabfragen durchführen können. Zugang wird zum Zwecke der Prüfung und Bescheidung von Visumanträgen einschließlich der Entscheidung über die Annullierung oder Aufhebung eines Visums oder über die Verlängerung seiner Gültigkeitsdauer gewährt. Die Visumbehörden der Mitgliedstaaten, die den Schengen-Besitzstand noch nicht vollständig anwenden, sich aber am EES-Betrieb beteiligen, bekommen Zugang zum Zwecke Abfrage der im Durchführungsbeschluss der Kommission (EU) 2019/327 Art. 2 Abs 2 genannten Daten für die Prüfung und Bescheidung von Anträgen auf ein nationales Visum für einen kurzfristigen Aufenthalt, einschließlich Entscheidung über die Annullierung oder Aufhebung eines nationalen Visums für einen kurzfristigen Aufenthalt oder über die Verlängerung seiner Gültigkeitsdauer.
Die Abfragen im EES durch die Visumbehörden erfolgen anhand alphanummerischer Daten gem. Art. 16 Abs. 1 lit a, b, und c EES-VO, anhand der Marke des Visums für den kurzfristigen Aufenthalt gem. Art. 16 Abs. 2 lit d EES-VO und anhand der Fingerabdruckdaten oder Fingerabdruckdaten in Verbindung mit dem Gesichtsbild.
Die Visumbehörden können bei Vorhandensein der Daten über den Drittstaatsangehörigen im EES-Suchabfragen tätigen und zu diesem Zweck das persönliche Dossier und alle damit verbundene Ein-/Ausreisedatensätze sowie Einreiseverweigerungsdatensätze abrufen. Des Weiteren haben die Visumbehörden Zugriff auf das automatische Berechnungssystem, um die Höchstdauer des zulässigen Aufenthalts automatisch bestimmen können.

11. Verarbeitung gem. Art. 25a EES-VO – Zugang der ETIAS-Zentralstelle (anwendbar ab ETIAS-Inbetriebnahme)

Zur Wahrnehmung der ihr durch die Verordnung (EU) 2018/1240 (ETIAS-VO) übertragenen Aufgaben ist die ETIAS-Zentralstelle gemäß Art. 11 Absatz 8 der genannten Verordnung befugt, auf EES-Daten zuzugreifen und diese abzufragen.

12. Verarbeitung gem. Art. 25b – Nutzung des EES zur manuellen Bearbeitung von Anträgen durch die nationalen ETIAS-Stellen

Die nationalen ETIAS-Stellen führen anhand der alphanumerischen Daten Abfragen durch, um die automatisierten Überprüfungen gemäß Art. 20, Art. 24 Abs. 6 lit. c Ziffer ii, Art. 41 und Art. 54 Abs. 1 lit. b ETIAS-VO durchzuführen. Die nationalen ETIAS-Stellen haben zum Zwecke der Prüfung von Anträgen auf Erteilung einer ETIAS-Reisegenehmigung lesenden Zugang zum EES. Die nationalen ETIAS-Stellen können die in den Art. 16 bis 18 EES-VO genannten Daten abfragen. Nach der Abfrage des EES durch die nationalen ETIAS-Stellen speichern die dazu ermächtigten Bediensteten der nationalen ETIAS-Stellen das Ergebnis der Abfrage ausschließlich in den ETIAS-Antragsdatensätzen.

13. Verarbeitung gem. Art. 26 EES-VO i.V.m. Durchführungsbeschluss (EU) 2019/327 – *Zugang zu Daten zwecks Verifizierung im Hoheitsgebiet der Mitgliedstaaten*

Zugangsberechtigt sind die Einwanderungsbehörden der Mitgliedstaaten, die zum Zwecke der Verifizierung der Identität des Drittstaatsangehörigen oder zur Prüfung oder Verifizierung, ob die Voraussetzungen für eine Einreise in das Hoheitsgebiet der Mitgliedstaaten oder den dortigen Aufenthalt erfüllt sind, Suchabfragen im EES anhand der in Artikel 16 Absatz 1 Buchstaben a, b und c sowie Artikel 17 Absatz 1 Buchstabe a EES-VO und in Übereinstimmung mit dem im Durchführungsbeschluss (EU) 2019/327 Art. 2 Abs. 4 genannten alphanummerischen Daten durchführen können.

Wenn Daten über den Drittstaatsangehörigen im EES enthalten sind, können die Einwanderungsbehörden das vor Ort aufgenommene Gesichtsbild des Drittstaatsangehörigen mit dem Gesichtsbild gemäß Art. 16 Abs. 1 lit d und Art. 17 Abs. 1 lit b EES-VO vergleichen oder

die Fingerabdrücke von Drittstaatsangehörigen, die von der Visumpflicht befreit sind, im EES und die Fingerabdrücke von visumpflichtigen Drittstaatsangehörigen im VIS gemäß Art. 19 der VO (EG) Nr. 767/2008 verifizieren.

Die Einwanderungsbehörden erhalten Zugang zur Abfrage des automatischen Berechnungssystems gem. Art. 11 EES-VO, der Daten im persönlichen Dossier des betreffenden Drittstaatsangehörigen, des Ein-/Ausreisedatensatzes bzw. der Ein-/Ausreisedatensätze sowie aller Einreiseverweigerungsdatensätze.

Soweit aber keine Daten über den Drittstaatsangehörigen im EES enthalten sind, erhalten die Einwanderungsbehörden Zugang zu Daten Zwecks Verifizierung gem. Art. 27 EES-VO.

14. Verarbeitung gem. Art. 27 EES-VO, Art. 8 Abs. 3 lit i SGK - *Zugang zu Daten zwecks Identifizierung*

Zugangsberechtigt sind die Grenzbehörden oder Einwanderungsbehörden ausschließlich zum Zwecke der Identifizierung von Drittstaatsangehörigen, die möglicherweise bereits unter einer anderen Identität im EES erfasst wurden oder die Voraussetzungen für eine Einreise in das Hoheitsgebiet der Mitgliedstaaten oder den dortigen Aufenthalt nicht oder nicht mehr erfüllen.

Die genannten Behörden können Suchabfragen anhand der Fingerabdruckdaten oder der Fingerabdruckdaten in Verbindung mit dem Gesichtsbild durchführen. Soweit die Suchabfrage ergibt, dass keine Daten im EES vorhanden sind, so erfolgt der Zugang zu Daten zwecks Identifizierung im VIS gemäß Artikel 20 der Verordnung (EG) Nr. 767/2008.

Die Grenzbehörden an den Grenzen, an denen das EES eingesetzt wird, greifen vor einer Identifizierung durch Abgleich mit dem VIS zunächst gemäß den Artikeln 18 oder 19a der Verordnung (EG) Nr. 767/2008 auf das VIS zu. Soweit die Suchabfrage im EES anhand der Fingerabdrücke ev. in Verbindung mit dem Gesichtsbild nicht erfolgreich ist, wird die Abfrage anhand der Daten in Art. 16 Abs. 1 lit a, b und c sowie Art. 17 Abs. 1 lit a EES-VO genannten Daten durchgeführt. Sind jedoch Daten über den Drittstaatsangehörigen im EES enthalten, so haben die genannten Behörden Zugang zur Abfrage der Daten im persönlichen Dossier und in den Ein-/Ausreisedatensätzen sowie in Einreiseverweigerungsdatensätzen, die mit diesem persönlichen Dossier verknüpft sind.

15. Verarbeitung gem. Art. 29 EES-VO i.V.m. dem Durchführungsbeschluss 2018/1547 – *Verfahren und Bedingungen für den Zugang zum EES zu Gefahrenabwehr- und Strafverfolgungszwecken*

Die Mitgliedstaaten benennen gemäß Artikel 29 Absatz 1 EES-VO die Behörden, die berechtigt sind, die EES-Daten zum Zwecke der Verhütung, Aufdeckung und Untersuchung terroristischer oder sonstiger schwerer Straftaten abzufragen.

Als eine terroristische Straftat gilt gemäß Artikel 3 Absatz 1 Ziffer 24 eine Straftat nach nationalem Recht, die den in der Richtlinie (EU) 2017/541 aufgeführten Straftaten entspricht oder diesen gleichwertig ist. Im Wesentlichen handelt es sich hierbei um sämtliche Tatbestände gemäß §278b bis §278g StGB. Als schwere Straftaten gelten Straftaten, die den in Artikel 2 Absatz 2 des Rahmenbeschlusses 2002/584/JI aufgeführten Straftaten entspricht oder diesen gleichwertig sind, wenn die Straftat nach dem nationalen Recht mit einer freiheitsentziehenden Strafe oder Sicherungsmaßnahme für eine Höchstdauer von mindestens drei Jahren geahndet werden kann. Diese Straftaten finden sich Anhang 1 Teil A des EU-JZG wieder.

Jeder Mitgliedstaat führt eine Liste der benannten Behörden, die eu-LISA und der Europäischen Kommission mitzuteilen ist. Die Mitteilung kann jederzeit geändert oder ersetzt werden. Die benannten Behörden in Österreich sind entsprechend ihren Aufgaben nach § 4 Absatz 3 BKA-G sowie § 6 Absatz 1 SNG das Bundeskriminalamt und die Direktion für Staatsschutz und Nachrichtendienst.

Des Weiteren kommt ebenfalls den Staatsanwaltschaften und Landesgerichten die Rolle der benannten Behörden zu.

Jeder Mitgliedstaat benennt eine oder mehrere zentrale Zugangsstellen, die Zugang zum EES haben. Ihr Zweck ist die Überprüfung, ob die Bedingungen gemäß Artikel 32 EES-VO für den Zugang der benannten Behörden zu EES-Daten erfüllt sind. Daher können die benannten Behörden den Zugang für die Abfragen erst dann enthalten, wenn bestimmte Bedingungen wie Erforderlichkeit, Verhältnismäßigkeit der Abfrage erfüllt sind und hinreichende Beweise oder Gründe für die Abfrage der EES-Daten vorhanden sind. Durch das neue Bundesgesetz, mit dem das EU-Polizeikooperationsgesetz, das Sicherheitspolizeigesetz, das BFA-Verfahrensgesetz, das Niederlassungs- und Aufenthaltsgesetz, das Fremdenpolizeigesetz 2005, das Grenzkontrollgesetz und das Staatsbürgerschaftsgesetz 1985 (kurz: Erstes EU-Informationssysteme–Anpassungsgesetz) geändert werden, wird die zentrale Zugangsstelle für das EES im neuen § 43a EU-Polizeikooperationsgesetz definiert. Demnach übt der Bundesminister für Inneres die Funktion der zentralen Zugangsstelle im Sinne des Artikel 29 Absatz 3 EES-VO aus. Innerhalb des Bundesministeriums für Inneres ist vorgesehen, dass diese Kompetenz durch das Bundeskriminalamt (BK) und die Direktion für den Staatsschutz und Nachrichtendienst (DSN) wahrgenommen wird. Die Details zur Anbindung der zentralen Zugangsstellen an die einheitliche nationale Schnittstelle werden im Durchführungsbeschluss (EU) 2018/1547 geregelt. Die zentrale Zugangsstelle ist organisatorisch von den benannten Behörden getrennt und führt ihre Prüftätigkeit unabhängig durch; sie unterliegt dabei keinerlei Weisungen hinsichtlich des Ergebnisses ihrer Prüfungen. Gemäß Artikel 29 Absatz 6 EES-VO sind nur ordnungsgemäß

ermächtigte Mitarbeiter der zentralen Zugangsstelle zum Zugriff auf das EES berechtigt.

Innerhalb der benannten Behörden sind operative Stellen festzulegen, welche berechtigt sind, über die zentralen Zugangsstellen Zugang zu EES-Daten zu beantragen. In Österreich wird gemäß Artikel 29 Absatz 5 EES-VO eine Liste der operativen Stellen geführt.

Die benannten Behörden können gemäß Artikel 32 Absatz 1 EES-VO den Zugang zum EES erhalten, wenn alle folgende Bedingungen erfüllt sind:

a) Der Zugang zum Zwecke von Abfragen ist für die Verhütung, Aufdeckung oder Untersuchung einer terroristischen oder sonstigen schweren Straftat erforderlich;
b) der Zugang zum Zwecke von Abfragen ist im Einzelfall erforderlich und verhältnismäßig;
c) es liegen Beweise oder hinreichende Gründe für die Annahme vor, dass die Abfrage der EES-Daten zur Verhütung, Aufdeckung oder Untersuchung der betreffenden Straftaten beiträgt, insbesondere, wenn der begründete Verdacht besteht, dass der Verdächtige, der Täter oder

das Opfer einer terroristischen oder sonstigen schweren Straftat einer Personengruppe angehört, die unter Art. 2 EES-VO fällt.

Außerdem ist neben den Mitgliedstaaten auch EUROPOL im Rahmen der Strafverfolgung gem. Artikel 30 EES-VO zugangsberechtigt. Europol benennt eine seiner operativen Stellen als „benannte Europol-Stelle“ und ermächtigt diese, über die zentrale Europol-Zugangsstelle Zugang zum EES zu beantragen, um die Maßnahmen der Mitgliedstaaten zur Verhütung, Aufdeckung und Untersuchung terroristischer oder sonstiger schwerer Straftaten zu unterstützen und zu stärken. Die zentrale Europol-Zugangsstelle prüft, ob die Bedingungen für die Beantragung des Zugangs zum EES gemäß Art. 33 EES-VO erfüllt sind. Für die Verarbeitung der EES-Daten durch die Strafverfolgungsbehörden gilt Art. 58 EES-VO zum Schutz der personenbezogenen Daten. Jeder Mitgliedstaat trägt dafür Sorge, dass nationales Recht und nationale Verwaltungsvorschriften, die gemäß der Richtlinie (EU) 2016/680 (JI-Datenschutzrichtlinie) erlassen wurden, auch für den Zugang zum EES gelten, auch hinsichtlich der Rechte der Personen, auf deren Daten zugegriffen wird. Die Datenschutzbehörde überwacht die Rechtmäßigkeit des Zugriffs auf personenbezogene Daten durch die Mitgliedstaaten gemäß Kapitel IV der vorliegenden Verordnung, einschließlich der Übermittlung dieser Daten an das und vom EES. Die Verarbeitung personenbezogener Daten durch Europol nach Maßgabe der vorliegenden Verordnung erfolgt im Einklang mit der Verordnung (EU) 2016/794 und wird vom Europäischen Datenschutzbeauftragten überwacht.

Das Zentralsystem des EES, die benannten Behörden, die zentralen Zugangsstellen und Europol führen Aufzeichnungen über Abfragen, damit die gemäß Artikel 41 Absatz 1 der Richtlinie (EU) 2016/680 errichtete Aufsichtsbehörde und der Europäische Datenschutzbeauftragte die Einhaltung der Datenschutzvorschriften der Union und der nationalen Datenschutzvorschriften bei der Datenverarbeitung überwachen können. Außer zu diesem Zweck werden die personenbezogenen Daten sowie die Abfrageaufzeichnungen nach Ablauf von 30 Tagen aus allen Dateien des Mitgliedstaats und Europols gelöscht, es sei denn, diese Daten und Aufzeichnungen sind für eine bestimmte laufende strafrechtliche Ermittlung, für die sie von einem Mitgliedstaat oder von Europol angefordert wurden, erforderlich.

Des Weiteren gelten besondere Bestimmungen für die Dokumentierung des Zugriffs der Strafverfolgungsbehörden auf EES-Daten. Gem. Art. 59 EES-VO müssen die Mitgliedstaaten und Europol gewährleisten, dass alle Datenverarbeitungsvorgänge, die aus Anträgen auf Zugang zu EES-Daten im Einklang mit Kapitel IV resultieren, zum Zwecke der Prüfung der Zulässigkeit des Antrags, der Überwachung der Rechtmäßigkeit der Datenverarbeitung sowie der Datenintegrität und -sicherheit und zur Eigenkontrolle protokolliert oder dokumentiert werden. Die Dokumentation enthält stets folgende Angaben:

a) den genauen Zweck des Antrags auf Zugang zu EES-Daten, einschließlich Angaben zur betreffenden terroristischen und sonstigen schweren Straftat, und im Falle Europols den genauen Zweck des Antrags auf Zugang;

b) die angegebenen hinreichenden Gründe, aus denen kein Abgleich mit anderen Mitgliedstaaten nach dem Beschluss 2008/615/JI durchgeführt wurde, wie dies in Artikel 32 Absatz 2 Buchstabe b EES-VO vorgesehen ist;

c) das nationale Aktenzeichen;

d) das Datum und den genauen Zeitpunkt des Antrags der zentralen Zugangsstelle auf Zugang zum Zentralsystem des EES;

e) die Bezeichnung der Behörde, die den Zugriff zwecks Datenabfrage beantragt hat;

f) gegebenenfalls die Anwendung des Dringlichkeitsverfahrens gemäß Artikel 31 Absatz 2 der EES-VO und das Ergebnis der nachträglichen Überprüfung;

g) die für die Abfrage verwendeten Daten;

h) nach Maßgabe der nationalen Rechtsvorschriften oder der Verordnung (EU) 2016/794 die einzigartige Benutzeridentität des Beamten, der die Abfrage vorgenommen hat, und des Beamten, der die Abfrage angeordnet hat.

Die Dokumentationen dürfen nur zur Überwachung der Rechtmäßigkeit der Datenverarbeitung sowie zur Gewährleistung der Datenintegrität und -sicherheit verwendet werden. Die Datenschutzbehörde, kann zur Erfüllung ihrer Aufgaben Zugang zu diesen Protokollen erhalten.

- <u>Abfrage durch Strafverfolgungsbehörden zwecks Identifizierung unbekannter Personen</u>

Für den Fall, dass Verdächtige, Straftäter oder mutmaßliche Opfer unbekannt sind, ist der Zugang zum EES gemäß Artikel 32 Absatz 2 EES-VO zwecks Identifizierung nur zulässig, wenn zusätzlich zu den in Artikel 32 Absatz 1 genannten Bedingungen, folgende Bedingungen erfüllt sind:

a) Die nationalen Datenbanken wurden zuvor abgefragt, und

b) im Falle einer Suche anhand von Fingerabdrücken wurde zuvor das automatisierte Fingerabdruck-Identifizierungssystem der anderen Mitgliedstaaten gemäß dem Beschluss 2008/615/JI (Prümer Beschluss) abgefragt, wenn Abgleiche von Fingerabdrücken technisch möglich sind, und diese Abfrage wurde entweder vollständig durchgeführt oder diese Abfrage war nicht innerhalb von zwei Tagen, nachdem sie gestartet wurde, vollständig abgeschlossen

Diese zusätzlichen Bedingungen finden jedoch keine Anwendung, wenn hinreichende Gründe für die Annahme vorliegen, dass ein Abgleich mit den Systemen der anderen Mitgliedstaaten nicht zur Verifizierung der Identität der betroffenen Person führen würde, oder im Dringlichkeitsfall, wenn eine unmittelbar bevorstehende Lebensgefahr, die im Zusammenhang mit einer terroristischen Straftat oder einer anderen schweren Straftat steht, abgewendet werden muss. Diese hinreichenden Gründe sind in dem elektronischen oder schriftlichen Antrag anzugeben, den die operative Stelle der benannten Behörde der zentralen Zugangsstelle übermittelt. Ein Antrag auf eine Abfrage im VIS zu derselben betroffenen Person kann parallel zu einem Antrag auf eine Abfrage im EES gemäß den festgelegten Bedingungen im Beschluss 2008/633/JI (Beschluss über den Zugang der benannten Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem (VIS) für Datenabfragen zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten) gestellt werden. Die Abfrage des EES zu Identifizierungszwecken ist auf die Suche anhand folgender EES-Daten beschränkt:

a) Fingerabdrücke von Drittstaatsangehörigen, die von der Visumpflicht befreit sind, oder von Inhabern eines FTD. Zur Einleitung dieser Abfrage des EES können Fingerabdruckspuren verwendet werden, die somit mit den im EES gespeicherten Fingerabdrücken abgeglichen werden können;

b) Gesichtsbilder

Im Falle eines Treffers ermöglicht ist ein Zugriff auf alle sonstigen alphanummerischen Daten aus dem persönlichen Dossier gemäß Artikel 16 Absätze 1 und 6, Artikel 17 Absatz 1 und Artikel 18 Absatz 1 EES-VO möglich.

- <u>Abfrage zwecks Ermittlung der Reisehistorie</u>

Die EES-VO erlaubt in Artikel 32 Absatz 3 auch den Zugang zum EES zwecks <u>Abfrage von Daten zu den bisherigen Reisen oder Aufenthalten</u> im Hoheitsgebiet der Mitgliedstaaten von bekannten Verdächtigen, Straftätern oder mutmaßlichen Opfern terroristischer oder sonstiger schwerer Straftaten, wenn die oben genannten Bedingungen gemäß Artikel 32 Absatz 1 EES-VO erfüllt sind.

16. <u>Verarbeitung gem. Art 35 EES-VO - *Änderung und vorzeitige Löschung von Daten*</u>

Art. 35 EES-VO regelt, dass der gem. Art. 3 Abs. 1 Z 12 EES-VO verantwortliche Mitgliedstaat das Recht hat, die Daten, die er in das EES eingegeben hat, zu berichtigen, zu vervollständigen oder zu löschen. Zugangsberechtigt sind die Behörden des Mitgliedstaates, die jeweils im Einklang mit der EES-VO wie

oben genannten Fällen Zugang zum Zwecke der Eingabe, Berichtigung, Vervollständigung und Löschung haben.

Hat der verantwortliche Mitgliedstaat Grund zu der Annahme, dass im EES gespeicherte Daten sachlich unrichtig oder unvollständig sind oder dass Daten im EES unter Verstoß gegen die EES-VO verarbeitet wurden, so überprüft er die Daten und berichtigt oder vervollständigt sie in bzw. löscht diese Daten aus dem EES sowie gegebenenfalls aus der in Art. 12 Abs. 3 EES-VO genannten Liste der ermittelten Personen.

Auch andere Mitgliedstaaten können aus dem gleichen Grund die genannten Verarbeitungsprozesse durchführen, sofern dies ohne Konsultation mit dem verantwortlichen

Mitgliedstaat möglich ist. Ist jedoch die Überprüfung der Daten ohne Konsultation nicht möglich, so wird der verantwortliche Mitgliedstaat kontaktiert und dieser überprüft sodann die Richtigkeit der Daten. Die Daten können auch auf Antrag des betreffenden Drittstaatsangehörigen gemäß Art. 52 EES-VO überprüft und berichtigt, vervollständigt oder gelöscht werden.

Hat ein Mitgliedstaat Grund zu der Annahme, dass im EES erfasste visumbezogene Daten

sachlich unrichtig oder unvollständig sind oder dass diese Daten im EES unter Verstoß gegen

die EES-Verordnung verarbeitet wurden, so wird ein Abgleich mit dem VIS vorgenommen und die Daten berichtigt, vervollständigt oder aus dem EES gelöscht.

Die Daten gem. Art. 12 EES-VO betreffend Ablauf des zulässigen Aufenthalts bzw. über fehlende Ausreisedaten können auf Antrag des betroffenen Drittstaatsangehörigen berichtigt,

vervollständigt oder aus dem EES bzw. aus der in Artikel 12 Absatz 3 EES-VO genannten Liste der ermittelten Personen gelöscht werden, wenn entsprechende Nachweise entsprechend den Bestimmungen in Art. 35 Abs. 5 EES-VO den nationalen Behörden vorlegt werden.

Bei Erwerb der Staatsangehörigkeit eines Mitgliedstaates oder für den Fall, dass Art. 2 Abs. 3 EES-VO anwendbar wird und die Person nicht mehr EES-pflichtig ist, werden die personenbezogenen Daten spätestens fünf Tage ab dem Tag des Staatsangehörigkeitserwerbs oder ab dem Tag, an dem Art. 2 Abs. 3 EES-VO anwendbar wurde aus dem EES gelöscht. Die Löschung erfolgt durch den Mitgliedstaat, dessen Staatsangehörigkeit erworben wurde oder durch den Mitgliedstaat, der die Aufenthaltskarte, den Aufenthaltstitel bzw. das Visum für den längerfristigen Aufenthalt ausgestellt hat.

Dem Drittstaatsangehörigen muss unbeschadet eines verfügbaren verwaltungsrechtlichen

oder außergerichtlichen Rechtsbehelfs ein wirksamer gerichtlicher Rechtsbehelf zur Verfügung stehen, um eine Berichtigung, Vervollständigung oder Löschung der Daten erwirken zu können. Das Zentralsystem des EES und der CIR informieren alle Mitgliedstaaten unverzüglich über die Löschung von EES- oder CIR-Daten und entfernen sie gegebenenfalls aus der in Art. 12 Abs. 3 EES-VO genannten Liste der ermittelten Personen.

Alle vorgenommenen Berichtigungen, Vervollständigungen und Löschungen von Daten werden im EES gespeichert.

17. Verarbeitung gem. Art. 52 EES-VO - *Recht auf Zugang zu und Berichtigung, Vervollständigung und Löschung von personenbezogenen Daten sowie auf Beschränkung ihrer Verarbeitung*

Anträge im Zusammenhang mit Art. 15 bis Art. 18 DSGVO können an die zuständige Behörde jedes Mitgliedstaats gerichtet werden, die dann binnen 45 Tagen zu beantworten sind. Bei Einreichung von Anträgen auf Berichtigung, Vervollständigung oder Löschung personenbezogener Daten oder auf Beschränkung ihrer Verarbeitung bei einem anderen Mitgliedstaat als dem verantwortlichen Mitgliedstaat, überprüft dieser Mitgliedstaat die Richtigkeit der Daten und die Rechtmäßigkeit der Datenverarbeitung im EES binnen 30 Tagen nach Antragseingang, soweit die Überprüfung ohne Konsultation des verantwortlichen Mitgliedstaats erfolgen kann. Andernfalls sind die Behörden des verantwortlichen Mitgliedstaats binnen 7 Tagen zu kontaktieren, woraufhin der verantwortliche Mitgliedstaat die Richtigkeit der Daten und die Rechtmäßigkeit der Datenverarbeitung binnen 30 Tagen nach der Kontaktaufnahme überprüft.

Bei Anträgen von Drittstaatsangehörigen nach Art. 35 EES-VO bestätigt der verantwortliche Mitgliedstaat der betroffenen Person unverzüglich schriftlich, dass er Maßnahmen zur Berichtigung, Vervollständigung oder Löschung der personenbezogenen Daten dieser Person oder zur Beschränkung der Verarbeitung dieser personenbezogenen Daten ergriffen hat.

Ist der verantwortliche Mitgliedstaat oder gegebenenfalls der Mitgliedstaat, an den der Antrag gerichtet wurde, nicht der Ansicht, dass die im EES gespeicherten Daten sachlich unrichtig oder unvollständig sind oder unrechtmäßig erfasst wurden, so erlässt er eine Verwaltungsentscheidung, in der er dem betroffenen Drittstaatsangehörigen unverzüglich schriftlich erläutert, warum er nicht zu einer Berichtigung, Vervollständigung oder Löschung der sie betreffenden personenbezogenen Daten oder zu einer Beschränkung der Verarbeitung dieser Daten bereit ist. Zudem belehrt der Mitgliedstaat über die möglichen Rechtsmittel. Hierzu gehören Angaben darüber, auf welche Weise bei den zuständigen Behörden und Gerichten dieses Mitgliedstaats Klage erhoben oder Beschwerde eingelegt werden kann und darüber, ob gemäß den Rechts-, Verwaltungs- und Verfahrensvorschriften dieses Mitgliedstaats eine Unterstützung, unter anderem seitens der gemäß Art. 51 Abs. 1 der Verordnung (EU) 2016/679 errichteten Aufsichtsbehörde, vorgesehen ist.

Die Anträge im Zusammenhang mit Art. 15 bis 18 DSGVO und Anträge auf Berichtigung, Vervollständigung oder Löschung personenbezogener Daten oder auf Beschränkung der Verarbeitung enthalten die zur Identifizierung des betroffenen Drittstaatsangehörigen notwendigen Mindestangaben. Fingerabdrücke können für diesen Zweck nur in hinreichend begründeten Fällen und

bei erheblichen Zweifeln an der Identität des Antragstellers verlangt werden. Diese Angaben werden ausschließlich dafür verwendet, dass der Drittstaatsangehörige die in Art. 52 Abs. 1 EES-VO genannten Rechte wahrnehmen kann und werden anschließend unverzüglich gelöscht.

Bei Antragsstellung im Zusammenhang mit Art. 15 bis 18 DSGVO gem. Art 52 Abs. 1 EES-VO wird von der zuständigen Behörde des verantwortlichen Mitgliedstaats oder des Mitgliedstaats, an den der Antrag gerichtet wurde, eine schriftliche Aufzeichnung mit Informationen darüber, auf welche Weise und von welcher Behörde der Antrag bearbeitet wurde gefertigt. Die zuständige Behörde stellt dieses Dokument der gemäß Artikel 51 Absatz 1 DSGVO errichteten Aufsichtsbehörde (die unabhängige Aufsichtsbehörde gem. Art. 51 Abs. 1 DSGVO bzw. Art. 41 Abs. 1 RL 2016/680 ist in Österreich die Datenschutzbehörde) innerhalb von sieben Tagen zur Verfügung.

18. Verarbeitung gem. Art. 63 EES-VO - *Datenabfrage zwecks Erstellung von Berichten und Statistiken*

Das ordnungsgemäß ermächtigte Personal der zuständigen Behörden der Mitgliedstaaten, der Europäischen Kommission, von eu-LISA und der Europäischen Agentur für die Grenz- und Küstenwache (gem. Art. 10 Abs. 1 lit a und c Verordnung (EU) 2019/1896 (FRONTEX-VO)) kann ausschließlich zur Erstellung von Berichten und Statistiken folgende Daten abfragen — ohne dass die Identifizierung einzelner Personen möglich ist und im Einklang mit den in Art. 10 Abs. 2 EES-VO verankerten Schutzklauseln in Bezug auf die Nichtdiskriminierung:

a) Statusinformationen;

b) Staatsangehörigkeit, Geschlecht und Geburtsjahr des Drittstaatsangehörigen;

c) Datum und Grenzübergangsstelle der Einreise in einen Mitgliedstaat sowie Datum und Grenzübergangsstelle der Ausreise aus einem Mitgliedstaat;

d) die Art des Reisedokuments und der aus drei Buchstaben bestehende Code des ausstellenden Staates;

e) die Zahl der als Aufenthaltsüberzieher ermittelten Personen nach Art. 12 EES-VO, die Staatsangehörigkeiten der als Aufenthaltsüberzieher ermittelten Personen und die Grenzübergangsstelle der Einreise;

f) die Daten, die in Bezug auf aufgehobene oder verlängerte Aufenthaltsberechtigungen eingegeben wurden;

g) der aus drei Buchstaben bestehende Code des Mitgliedstaats, der das Visum ausgestellt hat, falls zutreffend;

h) die Zahl der Personen, die gemäß Art. 17 Abs. 3 und 4 EES-VO von der Pflicht zur Abgabe von Fingerabdrücken befreit sind;

i) die Zahl der Drittstaatsangehörigen, denen die Einreise verweigert wurde, die Staatsangehörigkeiten dieser Drittstaatsangehörigen, die Art der Grenze (Land-, Luft- oder Seegrenze) der Grenzübergangsstelle, an der die Einreise verweigert wurde, und die Gründe für die Verweigerung der Einreise nach Art. 18 Abs. 6 lit d EES-VO.

Diese Daten werden von eu-LISA im zentralen Speicher für Berichte und Statistiken nach Art. 39 der Verordnung (EU) 2019/817 gespeichert. eu-LISA kann gem. Art. 72 Abs. 1 EES-VO regelmäßige Statistiken zur Überwachung der Entwicklung und der Funktionsweise des EES erstellen. Die Statistiken, welche die oben genannte personenbezogenen Daten aus dem EES enthalten, werden von eu-LISA vierteljährlich veröffentlicht. Die täglichen Statistiken werden im zentralen Speicher für Berichte und Statistiken gespeichert. Es wird auch ein Jahresbericht mit statistischen Daten zusammengestellt und dieser wird dem Europäischen Parlament, dem Rat, der Europäischen Kommission, der Europäischen Agentur für die Grenz- und Küstenwache, dem Europäischen Datenschutzbeauftragten und den nationalen Aufsichtsbehörden übermittelt. Auf Ersuchen der Kommission stellt eu-LISA der Kommission Statistiken zu spezifischen Aspekten der Umsetzung dieser Verordnung sowie die Statistiken zwecks Gewährleistung der Überwachung der Entwicklung und Funktionsweise von EES zu zur Verfügung.

b. Sonstige Verarbeitungsprozesse (nicht EES-pflichtige Personen)

Die Grenzkontrollsoftware dient auch der Überprüfung der Voraussetzungen für die Ein- und Ausreise von Reisenden, die sich der Grenzkontrolle stellen, jedoch nicht EES-pflichtig sind – etwa EU-Bürger, Drittstaatsangehörige mit Aufenthaltstiteln oder Visa D sowie andere nicht EES-pflichtige Personen.
Dies umfasst die Prüfung des Reisedokuments sowie gegebenenfalls eines entsprechenden Aufenthaltstitels oder Visums für einen längerfristigen Aufenthalt.
Die Dokumentenprüfung beinhaltet insbesondere:

- die Chip-Authentifizierung,
- die Überprüfung der Gültigkeit der Ausstellerzertifikate,
- die Prüfung der Dokumentengültigkeit,
- sowie den Vergleich der maschinenlesbaren Zone (MRZ) sowohl optisch als auch mit den Daten des Chips.

Darüber hinaus werden – wie auch bei EES-pflichtigen Personen – bei jeder Ein- und Ausreise die relevanten nationalen und internationalen Datenbanken im Sinne des Schengener Grenzkodex (Art. 8 Abs. 2 lit. a Z 3 und Art. 8 Abs. 3 lit. a Z 3) abgefragt. Bei relevanten Treffern, die in der zweiten Kontrolllinie einer näheren Überprüfung bedürfen, ermöglicht die Grenzkontrollsoftware eine

Übergabe der Daten in diese Kontrolllinie. Dabei werden die erforderlichen Daten [XXX für XXX] vorübergehend zwischengespeichert.
Die biometrische Prüfung ist bei EES-pflichtigen Personen gemäß den oben genannten Rahmenbedingungen der EES-Verordnung möglich. Für nicht EES-pflichtige Personen ist eine biometrische Prüfung ebenfalls möglich, beschränkt sich jedoch auf die Verifizierung der Identität in Zweifelsfällen gemäß § 12a Abs. 3 GrekoG.
Alle hier beschriebenen Funktionen der Grenzkontrollsoftware stehen auch in der Adminkonsole zur Verfügung.

c. Automatisierung der Grenzkontrolle: Verwendung von Self-Service-Systemen zur Voreingabe von Daten in das EES

I. Voraussetzungen für die Verwendung der Self-Service-Systeme und Abläufe gem. Art. 8a SGK

Artikel 8a des SGK schafft die rechtliche Grundlage für die Verwendung von Self-Service-Systemen („SSS“ oder auch umgangssprachlich „Kioske“ genannt) durch EES-pflichtige Personen zur Vorabeingabe von Daten in das EES. Durch die Verwendung der Kioske soll der Mehraufwand der Grenzkontrollbediensteten im Zusammenhang mit dem EES reduziert werden, da einige Schritte des Grenzkontrollprozesses bereits am Kiosk erledigt werden können.
Den Passagieren wird am Beginn des Prozesses am Kiosk zunächst die Information über die Verarbeitung der personenbezogenen Daten im EES gem. Art. 50 bereitgestellt.
Personenbezogene Daten können mittels SSS unter folgenden Voraussetzungen in das EES vorab eingegeben werden:

a) Das Reisedokument verfügt über ein elektronisches Speichermedium (Chip) und die Echtheit und Integrität der Daten auf dem Chip sind anhand der vollständigen gültigen Zertifikatkette bestätigt;

b) das Reisedokument enthält ein Gesichtsbild auf dem Chip, das für das Self- Service-System technisch zugänglich ist, damit die Identität des Inhabers des Reisedokuments überprüft werden kann (durch einen Abgleich mit dem am Kiosk vor Ort aufgenommenen Gesichtsbild).

Visumpflichtige Drittstaatsangehörige können ihre alphanummerischen Daten und das Gesichtsbild gemäß Artikel 16 EES-VO mit Hilfe des Kiosks vorab in das EES eingeben. Visumbefreite Drittstaatsangehörige können ihre alphanummerischen Daten sowie beide biometrische Indikatoren, Gesichtsbild und Fingerabdrücke, gemäß Artikel 17 EES-VO mit Hilfe des Kiosks vorab in das EES

eingeben. Alle Kiosknutzer müssen auch die Einreisebefragung (4 Fragen, die bei der Einreise nach Maßgabe des Art. 6 SGK gestellt werden können).

Danach wird die Person an einen Grenzkontrollbediensteten verwiesen, der

i) vorab die betreffenden Daten eingibt, soweit die Erhebung aller erforderlichen Daten mit Hilfe des SSS nicht möglich war

ii) überprüft, dass das am Kiosk verwendete Reisedokument dem Dokument entspricht, das die Person dem Grenzkontrollbediensteten nun vorlegt, sowie dass die vor Ort (bei der Grenzkontrollkoje) abgenommenen biometrischen Daten den biometrischen Daten entsprechen, die bei der Verwendung des Kiosks eingegeben wurden.

iii) nach der Entscheidung über die Genehmigung oder Verweigerung der Einreise die oben genannten Daten bestätigt und andere für den jeweiligen Datensatz benötigten Daten eingibt (z.B. Datum, Uhrzeit der Einreise, Grenzübergangsstelle, Behörde, Kennbuchstabe(n) für den Grund der Einreiseverweigerung gemäß Anhang V Teil B SGK etc.)

Sehr wichtig ist, dass die Kioske gemäß Artikel 8a Absatz 7 SGK nur **unter der Aufsicht eines Grenzkontrollbediensteten** betrieben werden, der die Aufgabe hat, **jedwede unsachgemäße, betrügerische oder abweichende Nutzung des Self-Service-Systems festzustellen**. Laut der Stellungnahme der Europäischen Kommission zu der Auslegung dieses Artikels, darf diese Aufsicht auch mittels Verwendung technischer Einrichtungen, z.B. durch Videoüberwachung erfolgen. Wichtig ist allerdings, dass der Grenzkontrollbedienstete jederzeit **Zugriff auf die Ergebnisse der Überwachung** hat, um rasch reagieren zu können.

II. Standards für automatisierte Grenzkontrollsysteme gemäß dem neuen Artikel 8c SGK und Datenschutz

Automatisierte Grenzkontrollsysteme müssen gemäß Artikel 8c SGK, soweit möglich, so gestaltet sein, dass sie von allen Personen, mit **Ausnahme von Kindern unter 12 Jahren**, genutzt werden können. Mitgliedstaaten, die sich für die Verwendung von automatisierten Grenzkontrollsystemen entscheiden, haben dafür Sorge zu tragen, dass vor Ort ausreichend Personal zur Verfügung steht das bei der Nutzung solcher Systeme Hilfestellung leistet. In Österreich wird dies durch den Einsatz sogenannter „Advisor“ (Mitarbeiter eines Privatunternehmens, die keine hoheitlichen Befugnisse haben) sichergestellt.

Der Touchscreen-Monitor der Selbstregistrierkioske ist so angeordnet, dass der Winkel und die Anbringung innerhalb des Kiosksystems verhindert, dass Reisende, die in der Warteschlange hinter der

Person stehen, die den Kiosk benutzt, nicht sehen können, welche Daten während des Kioskvorgangs eingegeben wurden. Darüber hinaus ist ein Sichtschutzfilter auf dem Touchscreen-Monitor angebracht, der auch die seitliche Einsicht durch Personen am benachbarten Kiosk verhindert. Durch die Anwendung beider Maßnahmen wird ein vollständiger Schutz der Privatsphäre und der Daten des Reisenden gewährleistet.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

a. Eingriff in die Grundrechte

Was den **Wesensgehalt des Grundrechts auf Privatsphäre** (Art. 7 GRC) und des **Rechts auf Achtung des Privatlebens** (Art. 8 EMRK) betrifft, ist festzuhalten, dass die in der **EES-Verordnung** vorgesehene Datenspeicherung zwar einen Eingriff in diese Rechte darstellt, jedoch **nicht geeignet ist, ihren Wesensgehalt zu beeinträchtigen**. Die Verordnung erlaubt die Nutzung der EES-Daten ausschließlich

zugriffsberechtigten Bediensteten der für Grenz- und Migrationskontrolle zuständigen Behörden und nur im **gesetzlich geregelten Mindestausmaß**.
Auch das in **§ 1 DSG** und **Art. 8 GRC** verankerte **Grundrecht auf Datenschutz** bleibt gewahrt, da die EES-VO die **Einhaltung strenger Datenschutz- und Sicherheitsgrundsätze** durch die Mitgliedstaaten ausdrücklich vorschreibt. Sie verpflichtet die Staaten, **wirksame Rechtsbehelfsmechanismen** vorzusehen (Art. 35 Abs. 5 f., Art. 52 Abs. 5, Art. 54 EES-VO). Betroffene können eine **Berichtigung, Vervollständigung oder Löschung** ihrer Daten verlangen und – im Fall einer Ablehnung – gerichtliche Schritte einleiten. Damit steht die EES-VO im Einklang mit dem **Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht** nach Art. 47 GRC.

Nach **Art. 43 EES-VO** müssen die Mitgliedstaaten zudem umfassende **Datensicherheitsmaßnahmen** treffen, darunter Sicherheits- und Notfallpläne, physische und logische Zugangsbeschränkungen, Schutz vor unbefugtem Zugriff oder Veränderung sowie eine vollständige **Protokollierung aller Datenverarbeitungen**.

Insgesamt liegt **kein Eingriff in den Kern des Rechts auf Privatsphäre** vor: Das EES zeichnet keine Datenmengen auf, die eine lückenlose Verfolgung von Bewegungen ermöglichen würden. Die Erfassung erfolgt ausschließlich bei **Überschreitung der Außengrenzen** und betrifft **keine Bewegungen innerhalb des Schengen-Raums**.

b. Verhältnismäßigkeit der Verarbeitung

Die Verarbeitung personenbezogener Daten im Rahmen der österreichischen Grenzkontrollsoftware (einschließlich der Adminkonsole) erfolgt zur Erfüllung gesetzlicher Aufgaben der Grenzkontrollbehörden gemäß:

- Art. 6 Abs. 1 lit. c und e DSGVO (rechtliche Verpflichtung / Wahrnehmung einer Aufgabe im öffentlichen Interesse),
- Grenzkontrollgesetz (GrekoG),
- Schengener Grenzkodex (SGK),
- Verordnung (EU) 2017/2226 (EES-Verordnung),
- sowie einschlägiger Bestimmungen des Fremdenpolizeigesetzes (FPG) und der SIS-Verordnung Grenze.

Die Verarbeitung erfolgt ausschließlich zur gesetzlich vorgesehenen Durchführung von Grenzkontrollen und zur Erfüllung der Aufgaben gemäß der EES-Verordnung.
Im Folgenden wird zwischen zwei Verarbeitungsbereichen unterschieden:

1. Verarbeitung im Rahmen des EES (EES-pflichtige Drittstaatsangehörige)
2. Verarbeitung außerhalb des EES (nicht EES-pflichtige Personen)

a. Verarbeitung im Rahmen des Entry/Exit-Systems (EES)

Ziele und Notwendigkeit

Die Datenverarbeitung im EES dient den in Art. 6 EES-VO genannten Zielen:

- der Verbesserung der Grenzverwaltung,
- der Bekämpfung irregulärer Migration,
- der Reduktion von Aufenthaltsüberziehungen,
- sowie der Erhöhung der inneren Sicherheit.

Das System wurde geschaffen, um auf die steigende Zahl von Grenzübertritten durch Drittstaatsangehörige zu reagieren (ca. 200 Mio. im Jahr 2014, Prognose: 300 Mio. bis 2025), ohne dass die Zahl der Grenzbeamtinnen und -beamten im gleichen Maß wächst.
Die Automatisierung der Grenzkontrollen ermöglicht eine zielgerichtete Konzentration auf jene Personen, die ein Migrations- oder Sicherheitsrisiko darstellen. Die **Verarbeitung der personenbezogenen Daten** im EES ist notwendig, um:

- die **Identität von Drittstaatsangehörigen eindeutig festzustellen**,
- die **Ein- und Ausreisedaten systematisch zu erfassen**,
- die **zulässige Aufenthaltsdauer** präzise zu berechnen,
- **Mehrfachidentitäten, Identitätsbetrug und Dokumentenfälschungen** zu verhindern,
- und den **Sicherheitsbehörden Zugriff** auf relevante Daten zur Bekämpfung schwerer Straftaten und terroristischer Bedrohungen zu ermöglichen.

Die Verifizierung biometrischer Daten (Gesichtsbild und vier Fingerabdrücke) stellt ein erforderliches und wirksames Mittel zur Betrugsprävention dar.
Dadurch werden sowohl Mehrfachidentitäten als auch Identitätsdiebstähle verhindert.

Rechtmäßigkeit und Grundrechtsschutz

Die EES-VO beschränkt die Verarbeitung streng auf den zur Aufgabenerfüllung erforderlichen Umfang. Die Verordnung verpflichtet die Mitgliedstaaten zur Umsetzung umfassender technischer und organisatorischer Schutzmaßnahmen (Art. 43 EES-VO), insbesondere:

- Sicherheits- und Notfallpläne zur Aufrechterhaltung des Betriebs,
- physische und logische Zugriffskontrollen,
- Protokollierung sämtlicher Datenzugriffe,
- Sicherstellung der Integrität und Vertraulichkeit der Daten,
- sowie Mechanismen zur Missbrauchsverhinderung und Nachvollziehbarkeit.

Darüber hinaus garantiert die EES-VO **Rechte der betroffenen Personen**, u. a.:

- Recht auf **Auskunft, Berichtigung, Löschung und Ergänzung,**
- sowie den Anspruch auf eine **detaillierte Rechtsbelehrung** im Falle ablehnender Entscheidungen.

Die Verarbeitung erfolgt somit im Einklang mit Art. 7 und 8 der Grundrechtecharta (GRC) sowie Art. 8 EMRK. Der Eingriff in das Grundrecht auf Datenschutz ist gesetzlich vorgesehen, notwendig und verhältnismäßig, der Wesensgehalt der Rechte bleibt unberührt.

Verhältnismäßigkeit

Die im EES verarbeiteten Daten sind auf das **erforderliche Minimum** beschränkt:

- **Alphanumerische Daten** stammen aus dem Reisedokument,
- **Biometrische Daten** (Gesichtsbild und vier Fingerabdrücke) sind erforderlich, um eine verlässliche Identitätsprüfung bei hoher Personenzahl sicherzustellen,
- **Ein- und Ausreisedaten** werden ausschließlich zum Zeitpunkt des Grenzübertritts erhoben

Eine Beschränkung des Datenumfangs oder eine Einschränkung der Behördenzugriffe wäre **nicht gleich geeignet**, die Ziele der EES-VO zu erreichen, und würde die **Effektivität des Systems** erheblich beeinträchtigen. Die EES-Verarbeitung trägt somit **nachweislich zur Aufrechterhaltung der öffentlichen Sicherheit** bei und steht in einem **angemessenen Verhältnis** zu den Grundrechtseingriffen.

b. Verarbeitung außerhalb des EES (nicht EES-pflichtige Personen)

Ziele und Notwendigkeit

Die Grenzkontrollsoftware wird darüber hinaus für die Durchführung der Grenzkontrolle bei **nicht EES-pflichtigen Reisenden** eingesetzt, insbesondere bei:

- EU-, EWR- und CH-Bürgerinnen und -Bürgern,
- Drittstaatsangehörigen mit **Aufenthaltstitel oder Visum D**,
- sowie sonstigen **nicht EES-pflichtigen Personengruppen**.

Die Verarbeitung dient der Erfüllung der **gesetzlichen Kontrollpflichten gemäß Art. 8 SGK** und **§§ 12a ff. GrekoG** und verfolgt folgende Zwecke:

- **Überprüfung der Authentizität und Gültigkeit** von Reisedokumenten (inkl. Chip-Authentifizierung, Zertifikatsprüfung, MRZ-Abgleich),
- **Feststellung der Identität** des Reisenden,
- **Sicherheitsüberprüfung** gegen nationale und europäische Datenbanken (SIS, VIS, Interpol, nationale Register),
- **Datenweitergabe** in die zweite Kontrolllinie bei sicherheitsrelevanten Treffern.

Eine **biometrische Identitätsverifizierung** ist auch bei nicht EES-pflichtigen Personen zulässig, erfolgt jedoch nur **in begründeten Zweifelsfällen** gemäß **§§ 12 ff. GrekoG**.
Eine Einschränkung des Datenumfangs oder die Verwendung alternativer, weniger invasiver Verfahren wäre **nicht geeignet**, die gesetzlichen Anforderungen an Sicherheit, Geschwindigkeit und Zuverlässigkeit der Grenzkontrolle zu erfüllen.

Verhältnismäßigkeit

Die Verarbeitung erfolgt **zweckgebunden und datensparsam** im Einklang mit **Art. 5 DSGVO**:

- Erhebung nur jener personenbezogenen Daten, die für die Grenzkontrolle **unmittelbar erforderlich** sind,
- **Rollenbasierte Zugriffsbeschränkungen** und technische Zugriffskontrolle,
- **Protokollierung** sämtlicher Datenzugriffe,
- **Keine automatisierte Entscheidungsfindung** ohne menschliche Prüfung,
- **Speicherfristen** entsprechend den gesetzlichen Vorgaben.

Die Verarbeitung ist **geeignet, erforderlich und angemessen**, um eine **rechtmäßige, sichere und effiziente Grenzkontrolle** zu gewährleisten.

c. Abschließende Verhältnismäßigkeitsprüfung

Die Verarbeitungsvorgänge in beiden Bereichen – **EES-Verarbeitung** und **nicht EES-Verarbeitung** – sind notwendig, um die gesetzlichen Aufgaben der Grenzkontrollbehörden wirksam zu erfüllen.
Die Maßnahmen:

- **sind gesetzlich vorgesehen**,
- **verfolgen legitime Ziele** im öffentlichen Interesse (Art. 6 Abs. 1 lit. e DSGVO),
- und sind **erforderlich und verhältnismäßig** im engeren Sinne, da keine milderen, gleich geeigneten Mittel zur Verfügung stehen.

Im Hinblick auf die obigen Ausführungen lässt sich schlussfolgern, dass die Datenverarbeitung gemäß der EES-VO notwendig, angemessen, und sachdienlich ist. Darüber hinaus steht sie in einem angemessenen Verhältnis zu den aktuellen Herausforderungen im Bereich der Migration.

Die Verarbeitung personenbezogener Daten in der Grenzkontrollsoftware trägt wesentlich zur **Effizienz der Grenzverwaltung**, zur **Bekämpfung irregulärer Migration** und zur **Sicherung der öffentlichen Ordnung** bei. Sie erfolgt im **Einklang mit den Datenschutzgrundsätzen der DSGVO** und den **Grundrechten der Europäischen Union**.

12. Identifizierte Risiken und Maßnahmen zur Risikominderung

Risiko 1	
Identifiziertes Risiko (Beschreibung)	**Durch die Verarbeitung personenbezogener Daten könnten die Rechte von betroffenen Personen grundsätzlich eingeschränkt werden.** Dabei könnten personenbezogene Daten auch über die gesetzlich zulässige Zweckbindung und deren Einschränkungen hinaus verarbeitet, mit anderen als den definierten Datenbanken abgeglichen und auf unzulässige Weise an unbefugte Behörden, Organe oder sonstige Adressaten weitergeleitet werden. Das Recht der betroffenen Personen auf eine umfassende Information, hinsichtlich der Kategorien personenbezogenen Daten, der Art ihrer Verarbeitung und Löschung dieser personenbezogenen Daten, sowie die Auskunft, ob tatsächlich deren personenbezogenen Daten im EES verarbeitet wurden oder werden, könnte von diesem Risiko betroffen sein. Darüber hinaus könnte es zu irrtümlichen und ungewollten Verwechslungen im Zuge von Trefferfällen kommen, die ernstzunehmende Konsequenzen und Nachteile für die allenfalls betroffenen Personen zur Folge hätten.
Auswirkungen (Schwere)	**Hoch**
Eintrittswahrscheinlichkeit	**Mittel**
Risikograd	**Mittel**
Maßnahmen (TOM)[1]	Die Verarbeitung von Daten besonderer Kategorien gem. § 39 DSG i.V.m. Art. 9 DSGVO, nämlich von biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person ist gem. §38 DSG rechtmäßig, da sie auf einem unmittelbar anwendbaren

[1] TOM: Technische und organisatorische Maßnahme zur Erfüllung der Sicherheits- und Schutzanforderung

	Rechtsakt basiert und sich auf Daten bezieht, welche die betroffene Person vor Ort im Rahmen der Grenzkontrolle bekanntgegeben hat. Zudem wurden durch die EES-VO wirksame Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen getroffen. Art. 50 Abs. 1 EES-VO (i.V.m. Art. 13 DSGVO) regelt das Recht auf Information. Abs. 1 dieses Artikels enthält eine detaillierte Übersicht an Informationen, über welche der verantwortliche Mitgliedstaat die Drittstaatsangehörigen zum Zeitpunkt der Erstellung des persönlichen Dossiers im Einklang mit den Art. 16, 17 oder 18 EES-VO unterrichten muss. So sind, unter anderem, die EES-pflichtigen Personen über den Umstand zu informieren, dass die Erhebung der Daten nach der EES-VO für die Prüfung der Einreisevoraussetzungen notwendig ist. Weiters ist über die Tatsache zu informieren, dass die Einreise verweigert wird, wenn sich die betroffenen Reisenden weigern, die geforderten biometrischen Daten zur Registrierung, Verifizierung oder Identifizierung im EES bereitzustellen. Darüber hinaus sind im Rahmen dieser Information die Betroffenen über die Speicherfristen, das Recht auf Auskunft betreffend maximale Dauer ihres zulässigen Aufenthalts sowie über die Möglichkeit der Übermittlung der Daten an Dritte zu belehren. Art. 50 EES-VO sieht außerdem vor, dass die EES-pflichtigen Personen das Recht auf Auskunft über die Datenverarbeitung sowie Berichtigung oder Vervollständigung der unrichtigen/unvollständigen Daten, Löschung unrechtmäßig verarbeiteter personenbezogenen Daten oder Beschränkung der Verarbeitung haben. Weiters besteht das Recht auf Informationen über die Verfahren zur Ausübung der Rechte gem. Art. 15 bis 18 DSGVO i.V.m. Art. 52 Abs. 1 EES-VO, einschließlich der Kontaktdaten des für die Datenverarbeitung Verantwortlichen sowie der Aufsichtsbehörden oder gegebenenfalls des Europäischen Datenschutzbeauftragten, die Beschwerden hinsichtlich des Schutzes personenbezogener Daten entgegennehmen, zu erhalten. Ebenso sieht Art. 50 EES-VO das Recht auf eine Beschwerde bei der Aufsichtsbehörde vor. Um sicherzustellen, dass betroffene Drittstaatangehörige über ihre Rechte informiert werden, sind die Informationen nach Art. 50 Abs. 1 EES-VO schriftlich, mit geeigneten Mitteln, in prägnanter, transparenter, verständlicher und leicht zugänglicher Form, und in einer in klarer und einfacher Sprache verfassten Sprachfassung, die die betreffende Person versteht oder von der vernünftigerweise angenommen werden darf, dass sie sie versteht bereitzustellen. Ferner richtet die Kommission eine Website ein, die sämtliche in Art. 50 Abs. 1 EES-VO genannten Informationen enthält. Das Recht auf Änderung sowie vorzeitige Löschung von personenbezogenen Daten ergibt sich aus Art. 35 Abs. 5 und Abs. 6 EES-VO. Art. 52 EES-VO regelt zudem das Recht auf Zugang zu und Berichtigung, Vervollständigung und Löschung von

	personenbezogenen Daten sowie auf Beschränkung ihrer Verarbeitung. Mehr über diese Möglichkeiten ist den oberen Punkten „Verarbeitung gem. Art. 35 EES-VO – Änderung und vorzeitige Löschung“ und „Verarbeitung gem. Art. 52 EES-VO - Recht auf Zugang zu und Berichtigung, Vervollständigung und Löschung von personenbezogenen Daten sowie auf Beschränkung ihrer Verarbeitung“ zu entnehmen. Die Weitergabe von personenbezogenen Daten ist durch die EES-VO auf einige wenige Ausnahmen beschränkt. Art. 41 EES-VO regelt die Übermittlung von Daten an Drittstaaten, internationale Organisationen und private Stellen – die Weitergabe ist beschränkt auf bestimmte personenbezogene Daten und ist an eine Reihe von Bedingungen geknüpft. Die Bestimmungen des Kapitels V der Verordnung (EU) 2016/679 sind stets zu beachten. Gleiches gilt für die Übermittlung von Daten an einen Mitgliedstaat, der sich noch nicht am EES-Betrieb beteiligt und an einen Mitgliedstaat, für den diese Verordnung gem. Art. 42 EES-VO nicht gilt. In Bezug auf die Gefahren der Verarbeitung über die gesetzliche Zweckbindung hinaus, sowie der Weiterleitung von personenbezogenen Daten an unbefugte Behörden und des Abgleichs mit anderen, gesetzlich nicht vorgesehenen Datenbanken, hält Art. 43 EES-VO zur Datensicherheit fest, dass jeder Mitgliedstaat in Bezug auf seine nationale Grenzinfrastruktur die erforderlichen Maßnahmen, die einen Sicherheitsplan sowie einen Notfallplan zur Aufrechterhaltung und Wiederherstellung des Betriebs einschließen, treffen muss, um (unter anderem): a) die Daten physisch zu schützen, unter anderem durch Aufstellung von Notfallplänen für den Schutz kritischer Infrastrukturen; b) Unbefugten den Zugang zu Datenverarbeitungsanlagen und nationalen Einrichtungen, in denen der Mitgliedstaat Tätigkeiten im Einklang mit den Zwecken des EES durchführt, zu verwehren; c) zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können; d) die unbefugte Dateneingabe sowie die unbefugte Kenntnisnahme, Änderung oder Löschung gespeicherter personenbezogener Daten zu verhindern; e) zu verhindern, dass automatisierte Datenverarbeitungssysteme mithilfe von Datenübertragungseinrichtungen von Unbefugten genutzt werden;

	f) die unbefugte Verarbeitung von Daten im EES und jegliche unbefugte Änderung oder Löschung von Daten, die im EES verarbeitet werden, zu verhindern; g) sicherzustellen, dass die zum Zugang zum EES berechtigten Personen nur mittels einer persönlichen und eindeutigen Benutzerkennung und vertraulicher Zugriffsverfahren ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können; h) sicherzustellen, dass alle zum Zugang zum EES berechtigten Behörden Profile mit einer Beschreibung der Aufgaben und Befugnisse der Personen erstellen, die berechtigt sind, die Daten einzugeben, zu ändern, zu löschen und abzufragen und in den Daten zu suchen, und diese Profile den Aufsichtsbehörden zur Verfügung zu stellen; i) sicherzustellen, dass überprüft und festgestellt werden kann, welchen Stellen personenbezogene Daten durch Datenübertragungseinrichtungen übermittelt werden können; j) sicherzustellen, dass überprüft und festgestellt werden kann, welche Daten im EES verarbeitet wurden, sowie wann, von wem und zu welchem Zweck diese Verarbeitung vorgenommen wurde; k) das unbefugte Lesen, Kopieren, Ändern oder Löschen von personenbezogenen Daten während der Übermittlung personenbezogener Daten an das oder aus dem EES oder während des Transports von Datenträgern zu verhindern, insbesondere durch geeignete Verschlüsselungstechniken; […]. Durch diese Maßnahmen wird das Risiko des unbefugten Zugriffs auf die EES-Daten minimiert. Des Weiteren wird sowohl von eu-LISA gem. Art. 46 als auch auf nationaler Ebene gem. Art. 43 Abs. 2 lit j EES-VO jede Verarbeitung der Daten protokolliert. Die Protokollierung gem. Art. 46 EES-VO ist auch für die Zugriffe auf das EES von den anderen Informationssystemen der EU wie z.B. VIS oder ETIAS aus (siehe Art. 46 Abs. 2 EES-VO) einschlägig.
Finaler Risikograd	**Mittel**

Risiko 2	
Identifiziertes Risiko (Beschreibung)	**Datenmissbrauch durch Mitarbeiter**. Mitarbeiter wären in der Lage in personenbezogene Daten Einsicht zu nehmen, die sie nicht für die unmittelbare Erfüllung ihrer Aufgaben benötigen. Darüber hinaus könnten sie personenbezogene Daten durch Unkenntnis der datenschutzrelevanten Normen oder aufgrund persönlicher Interessen unbefugt verarbeiten oder weiterleiten. Wenn die Mitarbeiter nicht ordnungsgemäß für die Verwendung personenbezogener Daten geschult sind und die Passagiere nicht ordnungsgemäß über den Zweck und die Beschränkung der Datenverarbeitung informiert werden, besteht die Gefahr, dass die Datenverarbeitung nicht rechtmäßig ist.
Auswirkungen (Schwere)	**Sehr hoch**
Eintrittswahrscheinlichkeit	**Mittel**
Risikograd	**Mittel**
Maßnahmen (TOM)	Eine gesetzeskonforme Verarbeitung von EES-Daten und die Verhinderung unbefugter Kenntnisnahme werden dadurch sichergestellt, dass gemäß Art. 43 EES-VO nur berechtigte Personen mittels einer persönlichen und eindeutigen Benutzerkennung sowie vertraulicher Zugriffsverfahren Zugang zum EES haben – und zwar ausschließlich zu den Daten, die ihrer jeweiligen Zugriffsberechtigung entsprechen. [redacted] Art. 46 Abs. 3 EES-VO legt die Verpflichtung der Mitgliedstaaten fest, Protokolle über die zur Verarbeitung der EES-Daten befugten Bediensteten zu führen. Durch geeignete Verschlüsselungstechniken wird in Übereinstimmung mit Art. 43 Abs. 2 lit. k EES-VO das unbefugte Lesen, Kopieren, Ändern oder Löschen personenbezogener Daten während der Übermittlung an oder aus dem EES sowie während des Transports von Datenträgern verhindert.

	Gemäß Art. 59 EES-VO gewährleisten die Mitgliedstaaten und Europol, dass alle Datenverarbeitungsvorgänge, die aus Anträgen auf Zugang zu EES-Daten im Einklang mit Kapitel IV EES-VO (Zugang zu EES-Daten durch Strafverfolgungsbehörden) resultieren, zum Zwecke der Prüfung der Zulässigkeit des Antrags, der Überwachung der Rechtmäßigkeit der Datenverarbeitung sowie der Datenintegrität und -sicherheit und zur Eigenkontrolle protokolliert oder dokumentiert werden. Die Protokolle oder Dokumentationen dürfen ausschließlich zur Überwachung der Rechtmäßigkeit der Datenverarbeitung sowie zur Gewährleistung der Datenintegrität und -sicherheit verwendet werden. Für die Überwachung und Bewertung gemäß Art. 72 EES-VO dürfen nur Protokolle verwendet werden, die keine personenbezogenen Daten enthalten. Die Wirksamkeit dieser Maßnahmen wird überwacht, und die erforderlichen organisatorischen Maßnahmen im Hinblick auf die interne Kontrolle werden getroffen, um die Einhaltung der EES-VO sicherzustellen. Zusätzlich zur internen Überwachung müssen gemäß Art. 55 EES-VO durch die Österreichische Datenschutzbehörde mindestens alle drei Jahre nach Inbetriebnahme des EES die Datenverarbeitungsvorgänge in der nationalen Grenzinfrastruktur nach einschlägigen internationalen Prüfungsstandards überprüft werden. Dabei besteht die Verpflichtung zur Bereitstellung sämtlicher von der Datenschutzbehörde angeforderten Informationen, insbesondere der Protokolle nach Art. 46 EES-VO, sowie die Verpflichtung, den Zutritt zu allen mit dem EES in Verbindung stehenden Gebäuden zu ermöglichen. Erwähnenswert ist in diesem Zusammenhang auch die Bestimmung des Art. 31 Abs. 3 EES-VO: Wird bei einer nachträglichen Überprüfung festgestellt, dass der Zugang zu EES-Daten nicht berechtigt war, so löschen alle Behörden, die auf solche Daten zugegriffen haben, die aus dem Zugriff auf das EES gewonnenen Informationen und melden die Löschung der betreffenden zentralen Zugangsstelle des Mitgliedstaats, in dem der Antrag gestellt wurde. Außerdem wird der Zugang zum EES abhängig vom Aufgabenbereich der zugangsberechtigten Behörde unterschiedlich geregelt, sodass die jeweilige Behörde nur in dem für ihre Aufgaben erforderlichen Ausmaß auf EES-Daten zugreifen und diese verarbeiten kann. [redacted]

	[redacted] [redacted] Jeder Mitarbeiter wird nachweislich über seine nach dem DSG, der DSGVO und den innerorganisatorischen Datenschutzvorschriften – einschließlich der Datensicherheitsvorschriften – bestehenden Pflichten belehrt. Diese relevanten datenschutzrechtlichen Normen sind für die Mitarbeiter jederzeit einsehbar und liegen in der jeweiligen Dienststelle auf. Zudem werden die Passagiere auf unterschiedlichsten Wegen über die Bedingungen der Datenverarbeitung im EES informiert. Insbesondere im Rahmen der Grenzkontrolle erhalten die Passagiere die Information über die Datenverarbeitung gemäß Art. 50 EES-VO zum Zeitpunkt der Erstellung des persönlichen Dossiers. Durch diese Transparenzmaßnahme wird sichergestellt, dass die Passagiere ausreichend darüber informiert sind, welche personenbezogenen Daten im Rahmen der Grenzkontrolle nach der EES-VO tatsächlich verpflichtend verarbeitet werden. Die Information gemäß Art. 50 EES-VO ist durch den Durchführungsbeschluss (EU) 2022/1337 definiert und wird den Passagieren in vollem Umfang zur Verfügung gestellt. Die Wahrscheinlichkeit mangelnder Transparenz ist somit als gering einzustufen.
Finaler Risikograd	**Mittel**

Risiko 3	
Identifiziertes Risiko (Beschreibung)	**Physische, materielle oder immaterielle Schäden, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, Verlust der Vertraulichkeit bei Berufsgeheimnissen oder erhebliche wirtschaftliche oder gesellschaftliche Nachteile.** Das Risiko besteht sowohl durch den Eintritt der angeführten Schäden, das Fehlen von oder den Mangel an vorhandenen, technischen Sicherheitsvorkehrungen, durch das Umgehen von vorhandenen Sicherheitseinrichtungen und den daraus resultierenden Nachteilen, als auch durch unbefugte Aktivitäten von Mitarbeitern. Eine allfällige Rufschädigung könnte durch einen irrtümlich herbeigeführten Trefferfall und den damit im Zusammenhang stehenden Folgemaßnahmen hervorgerufen werden.
Auswirkungen (Schwere)	**Sehr hoch**
Eintrittswahrscheinlichkeit	**Gering**
Risikograd	**Gering**
Maßnahmen (TOM)	Das Risiko materieller oder immaterieller Schäden sowie Rufschädigung im Zusammenhang mit dem EES ergibt sich zum einen aus der Gefahr, dass unrichtige Daten in das System eingegeben werden und dadurch Verifizierungsprobleme eintreten. Dieses Risiko ist allerdings nicht als hoch zu bewerten, da in der Regel die alphanummerischen Daten direkt vom dem elektronischen Speichermedium (Chip) des Reisedokumenten übernommen werden. Die visumbezogenen Informationen gem. Art. 16 Abs. 2 lit d bis g EES-VO werden gem. Art. 16 Abs. 5 EES-VO aus dem VIS importiert. Soweit die Informationen im VIS nicht unrichtig sind, stellt das EES diesbezüglich kein höheres Risiko dar. Die Grenzkontrollbediensteten werden entsprechend geschult und haben bei der Durchführung der Kontrollen zu berücksichtigen, dass Ergebnisse biometrischer Verifizierungen und Identifizierungen im Einzelfall fehlerhaft sein können. Daher sind alle Reisenden unabhängig von etwaigen Treffern diskriminierungsfrei zu kontrollieren. In Zweifelsfällen sind die vom System vorgeschlagenen Ergebnisse zu überprüfen und weitere relevante Umstände einzubeziehen.

[redacted]

Das Risiko des Verlusts der Vertraulichkeit bei Berufsgeheimnissen oder der erheblichen wirtschaftlichen oder gesellschaftlichen Nachteile kann als gering eingestuft werden, da das EES keine Informationen im Zusammenhang mit dem Berufsleben der Drittstaatsangehörigen erfasst und auch sonst keine sensiblen Informationen erfasst, die sich auf das soziale Leben auswirken könnten.

In Bezug auf materielle/immaterielle Schäden regelt Art. 45 EES-VO, dass jede Person oder jeder Mitgliedstaat, der/dem durch eine rechtswidrige Verarbeitung oder durch andere gegen diese Verordnung verstoßende Handlungen ein materieller oder immaterieller Schaden entsteht, das Recht hat, von dem für den Schaden verantwortlichen Mitgliedstaat Schadenersatz zu

	verlangen. Dieser Mitgliedstaat wird teilweise oder vollständig von der Haftung befreit, wenn er nachweist, dass er für den Umstand, durch den der Schaden eingetreten ist, in keinerlei Hinsicht verantwortlich ist. Verursacht eine Verletzung der in dieser Verordnung festgelegten Pflichten durch einen Mitgliedstaat einen Schaden, haftet dieser Mitgliedstaat für den entstandenen Schaden, sofern es eu-LISA oder ein anderer am EES beteiligter Mitgliedstaat nicht versäumt haben, angemessene Maßnahmen zur Verhütung des Schadens oder zur Verringerung seiner Auswirkungen zu ergreifen.
Finaler Risikograd	**Gering**

Risiko 4	
Identifiziertes Risiko (Beschreibung)	**Verlust der Kontrolle über personenbezogene Daten.** Es besteht die Gefahr, dass personenbezogene Daten durch einen technischen Defekt, durch Sabotage, durch unsachgemäße Bedienung durch Mitarbeiter oder durch Manipulationen von betriebsfremden, unbefugten Personen, verloren gehen könnten. Darüber hinaus könnten personenbezogene Daten durch IT-Angriffe von externer Seite abgezogen, zerstört, verändert oder gelöscht werden. Der Verlust der Kontrolle von personenbezogenen Daten würde schwerwiegende Folgen für betroffene Personen nach sich ziehen.
Auswirkungen (Schwere)	**Sehr hoch**
Eintrittswahrscheinlichkeit	**Gering**
Risikograd	**Mittel**
Maßnahmen (TOM)	Gem. Art. 38 EES-VO ist jeder Mitgliedstaat für die Verwaltung und die Regelung des Zugangs des dazu ordnungsgemäß befugten Personals und der ordnungsgemäß ermächtigten Mitarbeiter der zuständigen nationalen Behörden zum EES im Einklang mit der EES-VO und für die Erstellung und regelmäßige Aktualisierung eines Verzeichnisses jener Bediensteten und ihrer Profile zuständig. Die Mitgliedstaaten sorgen dafür, dass die technische Leistungsfähigkeit der Grenzkontrollinfrastruktur, deren Verfügbarkeit, die Dauer der Grenzkontrollen und die Qualität der Daten genau überwacht werden, damit sichergestellt ist, dass sie die allgemeinen Anforderungen für das ordnungsgemäße Funktionieren des EES und für ein effizientes Verfahren der Grenzübertrittskontrolle erfüllen. Die Bediensteten der Behörden mit Zugangsberechtigung für das EES erhalten eine angemessene Schulung insbesondere über die Vorschriften betreffend Datensicherheit und -schutz sowie über die einschlägigen Grundrechte, bevor sie ermächtigt werden EES-Daten zu verarbeiten. Sie verarbeiten die Daten im EES oder aus dem EES nur zu den in der EES-VO festgelegten Zwecken. Durch die umfassenden Schulungen wird somit sichergestellt, dass das Risiko einer unsachgemäßen Bedienung durch die Mitarbeiterinnen niedrig ist. Die Mitgliedstaaten stellen insbesondere sicher, dass die Daten rechtmäßig und unter uneingeschränkter Achtung der Menschenwürde des betreffenden Drittstaatsangehörigen erhoben, rechtmäßig in das EES eingegeben werden und dass sie richtig und aktuell sind, wenn sie an das EES übermittelt werden.

	Betreffend die Gefahr der Manipulation der personenbezogenen Daten und der Gefahr der Verlust von Daten durch externe IT-Angriffe lässt sich ausführen, dass seitens des Bundesministeriums für Inneres im Rahmen der nationalen Umsetzung des EES zahlreiche Schutzmechanismen bestehen, welche die Verhinderung solcher Vorfälle gewährleisten [redacted] Gem. Art. 37 Abs. 3 EES-VO ist eu-LISA zuständig für das Betriebsmanagement des Zentralsystems des EES und des CIR, der einheitlichen nationalen Schnittstellen und des sicheren Kommunikationskanals zwischen dem Zentralsystem des EES und dem Zentralsystem des VIS. In Zusammenarbeit mit den Mitgliedstaaten gewährleistet die Agentur, dass vorbehaltlich einer Kosten-Nutzen-Analyse jederzeit die beste verfügbare Technologie für das Zentralsystem des EES und des CIR, die einheitlichen nationalen Schnittstellen, die Kommunikationsinfrastruktur, den sicheren Kommunikationskanal zwischen dem Zentralsystem des EES und dem Zentralsystem des VIS, den Web-Dienst gemäß Art. 13 EES-VO und das Datenregister gemäß Art. 63 Abs. 2 EES-

	VO eingesetzt wird. eu-LISA muss unbeschadet der Zuständigkeiten der Mitgliedstaaten die nötigen Maßnahmen ergreifen, um die Sicherheit des Zentralsystems des EES und der Kommunikationsinfrastruktur zwischen dem Zentralsystem des EES und der einheitlichen nationalen Schnittstelle zu gewährleisten. Außerdem muss sie sicherstellen, dass nur das dazu ordnungsgemäß befugte Personal Zugriff auf die im EES verarbeiteten Daten hat. Aufgrund dieser Datensicherheitsmaßnahmen ist die Eintrittswahrscheinlichkeit des Verlusts der Kontrolle über personenbezogene Daten als mittel einzustufen.
Finaler Risikograd	**Mittel**

Risiko 5	
Identifiziertes Risiko (Beschreibung)	**Diskriminierung.** Es besteht die Gefahr, dass betroffene Personen durch die Verarbeitung ihrer personenbezogenen Daten und deren Weiterleitung einer Diskriminierung ausgesetzt werden. Insbesondere wäre diese Gefahr durch die Verarbeitung und Weiterleitung von besonderen Kategorien personenbezogener Daten (sensible Daten) wesentlich erhöht.
Auswirkungen (Schwere)	**Hoch**
Eintrittswahrscheinlichkeit	**Gering**
Risikograd	**Gering**
Maßnahmen (TOM)	Art. 10 EES-VO enthält den Grundsatz, dass jede zuständige Behörde sicherzustellen hat, dass die Nutzung des EES, einschließlich der Erfassung biometrischer Daten, im Einklang mit den in der Konvention zum Schutze der Menschenrechte und Grundfreiheiten, in der Charta der Grundrechte der Europäischen Union und im VN- Übereinkommen über die Rechte des Kindes verankerten Garantien steht. Damit sind entsprechende Schutzklauseln in Bezug auf die Nichtdiskriminierung in der EES-VO verankert. Zudem erhalten gem. Art. 38 Abs. 5 EES-VO die Bediensteten der Behörden mit Zugangsberechtigung für das EES eine angemessene Schulung insbesondere über die Vorschriften betreffend Datensicherheit und Datenschutz sowie über die einschlägigen Grundrechte. Auch bei der Erstellung von Berichten und Statistiken gem. Art 63 EES-VO wird betont, dass die Erstellung nur im Einklang mit dem Grundsatz der Nichtdiskriminierung erfolgen soll. Die Einhaltung der Grundrechte wird auch regelmäßig überwacht. Gem. Art 72 EES-VO wird eine Gesamtbewertung (drei Jahre nach EES-Inbetriebnahme und danach alle vier Jahre) durch die Kommission erstellt. Unter anderem umfasst diese Bewertung die Auswirkungen des EES auf die Grundrechte. Die Bewertungsberichte, die dabei entstehen, werden auch an die durch die Verordnung (EG) Nr. 168/2007 des Rates errichtete Agentur der Europäischen Union für Grundrechte übermittelt. Diskriminierung aufgrund rassischer oder ethnischer Zugehörigkeit wird insofern auch dadurch verhindert, dass die Überprüfung von Personen in der zweiten Kontrolllinie nicht auf Grundlage einer subjektiven Einschätzung durch die

	Grenzkontrollbediensteten erfolgt, sondern allein aufgrund der Indizien auf Basis der Rückmeldungen des Systems und einschlägiger Treffer im System ausgelöst werden kann. Die Überprüfung der Trefferfälle durch die Grenzkontrollbediensteten hat jedoch auch im Einklang mit dem Grundsatz der Nichtdiskriminierung zu erfolgen - die betroffenen Drittstaatsangehörigen sind auch während der Grenzkontrolle in Bezug auf ihre Grundrechte schonend zu behandeln. Dafür wird im Rahmen der Schulungen des zuständigen Personals gesorgt. Das Verbot der Diskriminierung aus Gründen der Rasse, der ethnischen Herkunft, der genetischen Merkmale, der Religion oder der Weltanschauung, der politischen oder sonstigen Anschauung, einer Behinderung oder der sexuellen Ausrichtung wird folglich durch die Einführung von EES nicht berührt. Zudem regelt Art. 42 EES-VO die Fälle, in welchen die personenbezogenen Daten an die im Anhang I genannten internationalen Behörden und private Stellen sowie an Drittstaaten weitergeleitet werden können und sieht zahlreiche Auflagen und Einschränkungen vor, sodass die Gefahr der Weiterleitung der personenbezogenen Daten somit reduziert ist.
Finaler Risikograd	**Gering**

Risiko 6	
Identifiziertes Risiko (Beschreibung)	**Einschränkung der Rechte der betroffenen Personen.** Es besteht die Gefahr, dass betroffene Personen nicht- oder nicht ausreichend über die Erhebung, Verarbeitung und Weiterleitung personenbezogener Daten informiert werden. Davon betroffen sind sowohl die vorab wahrzunehmenden Informationspflichten durch den Betreiber der Datenanwendung, als auch die Auskunft über eventuell im EES gespeicherte Personendatensätze.
Auswirkungen (Schwere)	**Gering**
Eintrittswahrscheinlichkeit	**Gering**
Risikograd	**Gering**
Maßnahmen (TOM)	Mit der Bestimmung in Art. 50 EES-VO wird das Recht auf Information geregelt. Unbeschadet des Rechts auf Erhalt von Informationen gem. Art. 13 DSGVO werden Drittstaatsangehörige, deren Daten im EES aufzuzeichnen sind, von dem verantwortlichen Mitgliedstaat über Folgendes unterrichtet: a) die Tatsache, dass die Mitgliedstaaten und Europol zu Gefahrenabwehr- und Strafverfolgungszwecken auf das EES zugreifen dürfen; b) die Pflicht für Drittstaatsangehörige, die von der Visumpflicht befreit sind, ihre Fingerabdrücke abnehmen zu lassen; c) die Pflicht für alle Drittstaatsangehörigen, die im EES erfasst werden, ihr Gesichtsbild aufnehmen zu lassen; d) den Umstand, dass die Erhebung der Daten für die Prüfung der Einreisevoraussetzungen vorgeschrieben ist; e) die Tatsache, dass die Einreise verweigert wird, wenn ein Drittstaatsangehöriger sich weigert, die geforderten biometrischen Daten zur Registrierung, Verifizierung oder Identifizierung im EES bereitzustellen; f) das Recht, Informationen über die maximal verbleibende Dauer ihres zulässigen Aufenthalts gemäß Art. 11 Abs. 3 EES-VO zu erhalten; g) die Tatsache, dass im EES gespeicherte personenbezogene Daten an einen Drittstaat oder eine internationale Organisation, der bzw. die in Anhang I aufgeführt ist, für die Zwecke der Rückkehr übermittelt werden können, oder gemäß Art. 41 Abs. 6 EES-VO an Drittstaaten bzw. gem. Art. 42 EES-VO an Mitgliedstaaten;

	h) das Bestehen des Rechts, beim für die Datenverarbeitung Verantwortlichen um Zugang zu den sie betreffenden Daten zu ersuchen, des Rechts, zu beantragen, dass sie betreffende unrichtige Daten berichtigt, sie betreffende unvollständige personenbezogene Daten vervollständigt, sie betreffende unrechtmäßig verarbeitete personenbezogene Daten gelöscht werden oder ihre Verarbeitung beschränkt wird, sowie des Rechts, Informationen über die Verfahren zur Ausübung dieser Rechte, einschließlich der Kontaktdaten des für die Datenverarbeitung Verantwortlichen sowie der Aufsichtsbehörden oder gegebenenfalls des Europäischen Datenschutzbeauftragten, die bzw. der Beschwerden hinsichtlich des Schutzes personenbezogener Daten entgegennehmen, zu erhalten; i) die Tatsache, dass für Zwecke des Grenzmanagements und der Erleichterung auf EES-Daten zugegriffen wird und dass Aufenthaltsüberziehungen automatisch die Aufnahme ihrer Daten in die Liste der ermittelten Personen nach Art. 12 Abs. 3 EES-VO nach sich ziehen, sowie eine Erläuterung der etwaigen Konsequenzen einer Aufenthaltsüberziehung; j) die für Ein- und Ausreisedatensätze, Einreiseverweigerungsdatensätze und persönliche Dossiers nach Art. 34 EES-VO festgelegte Speicherfrist; k) das Recht von Aufenthaltsüberziehern auf Löschung ihrer personenbezogenen Daten von der Liste der ermittelten Person gemäß Art. 12 Abs. 3 EES-VO und auf Berichtigung im EES, wenn sie nachweisen, dass sie die zulässige Aufenthaltsdauer aufgrund unvorhersehbarer, ernster Ereignisse überschritten haben; l) das Recht, bei den Aufsichtsbehörden Beschwerde einzulegen. Diese Informationen werden schriftlich, mit geeigneten Mitteln, in prägnanter, transparenter, verständlicher und leicht zugänglicher Form, und in einer in klarer und einfacher Sprache verfassten Sprachfassung, von der vernünftigerweise angenommen werden darf, dass die betroffene Person diese versteht, zu dem Zeitpunkt bereitgestellt, zu dem das persönliche Dossier dieser Person im EES angelegt wird. Ferner richtet die Kommission eine Website ein, die oben genannten Informationen enthält. Des Weiteren begleitet gem. Art. 51 EES-VO die Kommission in Zusammenarbeit mit den Aufsichtsbehörden und dem Europäischen Datenschutzbeauftragten den Beginn des Betriebs des EES mit einer Informationskampagne, mit der die

	Öffentlichkeit und insbesondere Drittstaatsangehörige über die Zielsetzungen des EES, die im EES gespeicherten Daten, die Behörden, die Zugriff haben, und die Rechte der betroffenen Person aufgeklärt werden. Durch sämtliche oben beschriebene Maßnahmen sind die Anforderungen des §43 DSG i.V.m. Art. 13 DSGVO erfüllt. Des Weiteren besteht für die Drittstaatsangehörigen gem. Art. 52 Abs. 1 EES-VO i.V.m. Art. 15 DSGVO i.V.m. §44 DSG das Recht auf Auskunft über die Datenverarbeitung. Der Antrag auf Auskunft ist innerhalb von 45 Tagen nach Antragseingang zu beantworten.. Drittstaatsangehörige können allerdings gem. Art. 26 Abs. 3 DSGVO dieses Recht bei jedem der einzelnen Verantwortlichen geltend machen, daher ist es möglich, sich zwecks Antragstellung sowohl an das Bundesministerium für Inneres als auch an die Landespolizeidirektionen als gemeinsam Verantwortliche gem. Art. 4 Z 7 i.V.m. Art. 26 DSGVO zu wenden.
Finaler Risikograd	**Gering**

Risiko 7	
Identifiziertes Risiko (Beschreibung)	**Komplikationen in Verbindung mit der Erfassung von biometrischen Daten minderjährigen Personen.** Das EES enthält Gesichtsbilder gem. Art. 15 EES-VO von minderjährigen Personen (ohne Altersbegrenzung). Durch die altersbedingten Veränderungen im Aussehen werden Kinder häufigeren Trefferfällen und den damit im Zusammenhang stehenden Folgemaßnahmen ausgesetzt. Weiters besteht die Gefahr, dass die Gesichtsbilderfassung bei Kindern aufgrund mangelnder Mitwirkung schwieriger gelingen kann und somit sowohl Kinder als ihre Eltern besonders langen Abfertigungszeiten und Unannehmlichkeiten bei der Grenzkontrolle ausgesetzt sind.
Auswirkungen (Schwere)	**mittel**
Eintrittswahrscheinlichkeit	**mittel**
Risikograd	**mittel**
Maßnahmen (TOM)	Nachdem Artikel 15 EES-VO tatsächlich keine Altersgrenzen für die Erfassung von Gesichtsbildern vorsieht, besteht die Gefahr, dass aufgrund von altersbedingten Veränderungen der Gesichtszüge bei Kindern im Rahmen der Verifizierungsvorgänge tatsächlich vermehrt Fehler auftreten und „false negative“ Fälle auftreten. Zu diesem Zweck werden die Grenzkontrollbediensteten im Rahmen der Systemschulungen sensibilisiert, sodass sie in solchen Fällen einen besonders rücksichtsvollen Umgang pflegen und mehr Freiheit beim „Overrulling“ des Systems erhalten und die Gesichtsbilder nach einer individuellen Bewertung und manuellen Verifizierung zwecks leichterer Abfertigung austauschen können. Bei einem erhöhten Passagierverkehr kann gem. Art. 15 EES-VO in Fällen, in denen die die Qualität und die Auflösung betreffenden Spezifikationen für die Eingabe der vor Ort aufgenommenen Gesichtsbilder in das EES nicht eingehalten werden können, das Gesichtsbild elektronisch aus dem Chip des elektronischen maschinenlesbaren Reisedokuments (electronic Machine Readable Travel Document, eMRTD) extrahiert werden. In diesen Fällen darf das Gesichtsbild erst in das persönliche Dossier

	eingefügt werden, nachdem elektronisch verifiziert wurde, dass das auf dem Chip des eMRTD gespeicherte Gesichtsbild dem vor Ort aufgenommenen Gesichtsbild des betreffenden Drittstaatsangehörigen entspricht. Jeder Mitgliedstaat übermittelt der Kommission einmal jährlich einen Bericht über die Anwendung dieser Möglichkeit. Dieser Bericht muss die Zahl der betroffenen Drittstaatsangehörigen sowie eine Erläuterung der aufgetretenen Ausnahmefälle enthalten. Dieser Ausweichmechanismus verschafft eine Abhilfe bei kleinen Kindern, bei welchen die Gesichtsbildaufnahme mit besonderen Schwierigkeiten verbunden ist und die technische Qualität des Gesichtsbildes schwer zu erreichen ist.
Finaler Risikograd	**Mittel**

13. Ergebnis

Grundsätzlich sind durch die Einführung des EES gewisse Risiken nicht auszuschließen, da dieses System eine **besonders große Menge an Daten besonderer Kategorie erfasst, schutzbedürftige Personen betrifft und im Rahmen der Verifizierungen oder Identifizierungen anhand biometrischer Daten keine hundertprozentige Richtigkeit der Ergebnisse gewährleistet werden kann.**

Allerdings ist der Eintritt der Risiken, die in diesem Dokument genannt sind, insgesamt als nicht sehr wahrscheinlich einzustufen. Die EES-VO und die Maßnahmen im Rahmen der nationalen Umsetzung sehen zahlreiche, wirksame und auf den jeweiligen Einzelfall bezogene Maßnahmen und Überwachungsmechanismen vor.

Die Behörden, die aus spezifischen Zwecken Zugang zum EES benötigen, die sich aus ihren Aufgabenbereichen ergeben, müssen von den Mitgliedstaaten benannt werden. Der Zugang zur Abfrage der EES-Daten ist ausschließlich den ordnungsgemäß ermächtigten Bediensteten der Behörden der einzelnen Mitgliedstaaten vorbehalten und auf den Umfang beschränkt, in dem die Daten für die Erfüllung der Aufgaben gemäß diesen Zwecken erforderlich sind. Die Bediensteten der zugangsberechtigten Behörden haben weiterhin die Möglichkeit, allfällige Systemfehler zu korrigieren und im Rahmen ihrer Kompetenzen selbständig Entscheidungen zu treffen (etwa im Fall von „false positives“ oder falschen Ergebnissen der Berechnung der Aufenthaltsdauer etc.).

Erforderliche Garantien und Mechanismen werden sowohl auf nationaler Ebene als auch auf der Unionsebene (insbesondere durch die eu-LISA) gewährleistet, um die Grundrechte der Reisenden, insbesondere das Privatleben und die personenbezogenen Daten, wirksam zu schützen. Datenschutzrechtliche Bestimmungen der EES-VO sorgen dafür, dass die Drittstaatsangehörigen sämtliche Rechte, die in der DSGVO festgelegt sind, ausüben können und entsprechende Anträge an jeden Mitgliedstaat stellen können sowie dass der Rechtsschutz und Kontrolle durch eine Aufsichtsbehörde im adäquaten Umfang (angemessenen Zeitabständen) gewährleistet ist.

Das EES wahrt somit den Kern des Rechts auf Privatsphäre, entspricht klar definierten Zielen von allgemeinem Interesse und ist verhältnismäßig, da die im EES gespeicherten Daten genau den mit der Verordnung verfolgten legitimen Zielen entsprechen und der Kreis der betroffenen Drittstaatsangehörigen demjenigen Personenkreis entspricht, der von der geltenden Vorschrift über die Dauer des Kurzaufenthalts betroffen ist.

Die Softwareanwendungen **Adminkonsole und Grenzkontrollsoftware** wurden entsprechend den Sicherheitsvorgaben der EES-Verordnung entwickelt und umgesetzt. Die Systeme sind so ausgestaltet, dass eine unbefugte Verarbeitung von Daten innerhalb des EES ausgeschlossen ist. Der Zugriff auf die Anwendungen ist ausschließlich befugten Mitarbeiterinnen und Mitarbeitern vorbehalten, die über eine entsprechende Berechtigung verfügen. Die Zugriffskontrolle erfolgt über ein dreistufiges Authentifizierungsverfahren sowie ein rollenbasiertes Berechtigungskonzept, das sicherstellt, dass nur Personen mit entsprechender Funktion und Autorisierung Daten einsehen oder verarbeiten können.

Darüber hinaus wird jede Datenverarbeitung vollständig protokolliert, sodass jederzeit nachvollzogen werden kann, welche Daten, von wem, wann und zu welchem Zweck verarbeitet wurden. Diese Protokollierung erfolgt sowohl auf nationaler als auch auf EU-Ebene, wodurch eine durchgängige Nachvollziehbarkeit und Kontrolle der Datenverarbeitung gewährleistet ist.

Die Nutzung mobiler Datenträger ist ausgeschlossen, wodurch das Risiko einer unbefugten Datenübertragung oder eines Datenabflusses zusätzlich minimiert wird. Sämtliche vom Bundesministerium für Inneres etablierten Sicherheitsstandards werden eingehalten.

Aufgrund der beschriebenen technischen und organisatorischen Maßnahmen kann festgestellt werden, dass die Verarbeitungstätigkeiten im Zusammenhang mit der Adminkonsole und der Grenzkontrollsoftware ein insgesamt geringes Restrisiko aufweisen und somit kein hohes Risiko im Sinne von Art. 35 DSGVO besteht.

Schließlich kann festgehalten werden, dass der Einsatz von modernen IT-Systemen bei den Grenzkontrollen zu einem ausschließlich faktenbasierten System führen, das unter Umständen weniger Diskriminierungspotenzial als die von Menschen durchgeführten Kontrollen mit sich bringt, und somit einen zusätzlichen Schutz im Hinblick auf Art. 21 GRC darstellt. Durch umfassende und konkrete Angabe über die jeweilige Ein- oder Ausreise sowie Einreiseverweigerung und entsprechende Protokollierung, können Gründe für die Entscheidungen der zuständigen Behörde besser nachvollzogen und im Rahmen allfälliger Verfahren berücksichtig werden.

Die hier vorgenommenen Abschätzungen der Risiken zeigen, dass der durchschnittliche Risikograd der Anwendungen Grenzkontrollsoftware und Adminkonsole inkl. die Datenverarbeitung für die Zwecke des Entry/Exit Systems als **„mittel“** eingestuft werden kann und im Ergebnis **kein hohes Risiko** i.S.d. § 52 DSG/Art. 35 DSGVO besteht.